

EdgeMarc VoIP System (VOS) User Guide

Software Release 14 | August 2016

U.S. Headquarters:

Edgewater Networks, Inc.
5225 Hellyer Ave. #100
San Jose, California 95138

Phone: 408.351.7200
Fax: 408.727.6430

edgewaternetworks.com

© 2016, Edgewater Networks, Inc.

Edgewater Networks, All Rights Reserved.

Trademarks

EDGEWATER NETWORKS and Design, EDGEMARC, EDGEPROTECT, and EDGECONNECT are registered trademarks of Edgewater Networks, Inc. EDGEWATER NETWORKS and EDGEVIEW are trademarks of Edgewater Networks, Inc. Any other trademarks appearing in this manual are owned by their respective companies.

Copyright

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Edgewater Networks, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement of the implied warranties of merchantability or fitness for a particular purpose.

Export Notice

You (Purchaser) acknowledge that these products are subject to the U.S. Export Administration Regulations (the “EAR”) and that you will comply with the EAR. You are not located in Cuba, Iran, North Korea, Sudan, or Syria. You will not export or re-export this product, directly or indirectly, to: (1) any countries that are subject to US export restrictions (currently including, but not necessarily limited to, Cuba, Iran, North Korea, Sudan, or Syria); (2) any end user who you know or have reason to know will utilize them in the design, development or production of nuclear, chemical or biological weapons, or rocket systems, space launch vehicles, and sounding rockets, or unmanned air vehicle systems; or (3) any end user who has been prohibited from participating in US export transactions by any federal agency of the US government. In addition, you are responsible for complying with any local laws in your jurisdiction which may impact your right to import, export or use these products.

Licensing

Use of this product is subject to Edgewater Networks Software License Agreement.

Portions of this product include software sponsored by the Free Software Foundation and are covered by the GNU GENERAL PUBLIC LICENSE.

Refer to www.edgewaternetworks.com/licensing for more information regarding licenses and the warranty.

Warranty

Product warranty does not apply to damage caused by lightning, power surges, or wrong voltage usage.

Typographical Errors

This publication could include technical inaccuracies or typographical errors, for which Edgewater Networks never can or shall be held liable. Changes are made periodically to the information herein; these changes will be incorporated in new releases of this publication. Edgewater Networks may make improvements or changes in the product or products described in this publication at any time, without prior notice.

Document Release Date

8/4/16

Contents

About This Guide

Typographic Conventions i
Online Help ii
Document Organization iii
Contact and Support Information iv

1 Getting Started

Understanding the EdgeMarc VoIP Operating System 1
Deploying the EdgeMarc 2
Deploying the EdgeMarc in IP Centrex Networks 2
Deploying the EdgeMarc in Station Side IP PBX Networks 4
Accessing the Web-Based GUI Interface 5
Logging Into the EdgeMarc 5
Where to Go Next 6

2 System Administration

Using the Administration Page 8
Managing the License Key 10
Where Do I Find My License Key? 10
What If I Lose My License Key? 10
How Do I Purchase an Upgrade License Key? 10
Viewing and Editing Your License Key 10
Managing Encryption Key Settings 11
Changing Your Password 12
Changing the Administrative Password 12
Changing the Read-Only Password 14
Password Restrictions 16
Configuring Backup and Restore 16
Creating a New Backup Configuration File 18
Restoring a Previous Backup File 20
Uploading a Backup Configuration File to Your Local Drive . . . 21
Downloading the Saved Configuration to a Local Drive 22
Upgrading Firmware 23
Preparing for Firmware Upgrade 23
Where Do I Download New VOS Firmware? 24
What is the Latest Firmware File Name? 24
Upgrading Your Firmware 24

© 2016 Edgewater Networks. All Rights Reserved.

Upgrading SOC2 Firmware 28
Upgrading SOC2 Firmware Settings 28
Configuring RADIUS Settings. 29
About RADIUS Settings. 29
Using the RADIUS Settings Page 30
Configuring TACACS+. 31
About TACACS+ Management 31
Using the TACACS+ Configuration Page 34
Configuring TACACS+ Settings 35
Disabling TACACS+ Services 37
Configuring Services 37
About SNMP Management 37
About Mean Opinion Scoring (MOS) 39
Using the Services Configuration Page 40
Configuring SNMPv1 47
Deleting a Trap Destination 49
Configuring SNMPv3 49
Configuring SNMP Common Settings 50
Disabling SNMP. 50
Deleting an SNMP Trap 50
Configuring Remote System Logging 51
Managing Source Address Settings. 51
Managing Hostname Settings. 52
Configuring Mean Opinion Score (MOS) Settings 53
Configuring Analytics 53
Configuring an EdgeView Group Name 54
Configuring PacketSmart Services 54
Viewing System Information 55
Configuring Time and Date Settings 57
Configuring Settings With User Commands 59
Using the User Commands Page. 59
Managing File Download 60
Downloading Files 61
Deleting a File 62
Managing the File Server 63
Configuring File Server Settings 63
Managing Server Maintenance 67
Managing FTP Users 67
Deleting an FTP User 69
Configuring the SD Card 69
Enabling the SD Card 70
Managing the SD Card 70

© 2016 Edgewater Networks. All Rights Reserved.

Configuring Technical Report-069 Parameters 72
Configuring V.90 Modem Settings 74
Rebooting the System 75

3 Network Deployment

Using the Network Page 78
Configuring LAN Interface Settings 82
Configuring Multi LAN Ports 84
Configuring WAN Interface Settings 89
Configuring WAN Interface IPv6 Settings 89
IPv6 Static IP 90
IPv6 in IPv4 Tunnel 90
Configuring WAN Interface IPv4 Settings 91
IPv4 ADSL 91
IPv4 PPPoE 92
IPv4 DHCP 93
IPv4 Static IP 93
IPv4 VLAN 94
IPv4 T1/E1 95
Configuring Network Default Gateway Settings 95
Configuring DNS Servers 96
Configuring ADSL Services 97
Overview 97
Configuring ADSL 97
Configuring ADSL for Static IP 102
Viewing ADSL Line Status 103
Configuring NAT Settings 108
Overview 108
Configuring Dynamic NAT 109
Configuring Private Networks 111
Configuring a Private Network 111
Deleting a Private Network 112
Configuring Port Forwarding 112
Adding a Port Forwarding Rule 113
Deleting Port Forwarding Rules 115
Configuring VLAN Support 116
Overview 116
Configuring VLAN Settings 117
Using the VLAN Configuration Page 117
Creating a New VLAN 119
Editing a VLAN 121
Deleting a VLAN 121
Configuring VLAN Port Membership 122

© 2016 Edgewater Networks. All Rights Reserved.

Configuring VLAN Ports 123
Configuring WAN VLAN Settings. 124
Deleting a VLAN 126
Configuring Customer Networks. 126
Deleting a Customer Network 128
Configuring the 802.1X Supplicant 128
Configuring T1/E1 Settings 130
Configuring the T1/E1 Physical Layer 137
Configuring Fractional T1 Links 138
Enabling Fractional Support 139
Configuring the T1/E1 Link Layer 140
Configuring T1 Ports 141
Configuring MLPP Settings 142
Configuring PPP LCP Settings 143
Configuring Frame Relay Settings 143
Configuring Frame Relay Secondary Settings 144
Managing the EdgeMarc Daughter Card 145
Managing T1/E1 Diagnostics 147
Using the T1/E1 Diagnostics Page 147
T1/E1 Loopback Tests, Alarms, and Counters 148
Diagnostic Commands - Loopback Tests 149
T1/E1 Status - Alarm Types 150
T1/E1 Statistics - Diagnostic Counters 150
T1/E1 Interval Data. 151
Viewing Advanced T1 Diagnostics. 152
Configuring PRI 153
Overview. 153
PRI Configuration Requirements 155
Configuring Network Side ISDN PRI (PRI/UA) 156
Configuring Network Side CAS/UA 161
Configuring Client Side ISDN PRI (PRI/GW) 166
Configuring Client Side CAS/GW. 170
Configuring High Availability 174
Overview. 174
Configuring High Availability Settings 175
Administratively Disabling High Availability 180
Configuring DHCP Relay 180
Configuring DHCP Relay IPv4. 180
Configuring DHCP Relay IPv6. 181
Configuring the DHCP Server. 182
Overview. 182
DHCP Server Options. 183

© 2016 Edgewater Networks. All Rights Reserved.

Configuring the DHCP Server IPv4 184
Managing DHCP IPv4 Address Ranges 188
Configuring DHCP Server IPv4 Settings 188
Managing DHCP IPv4 Leases 190
Managing DHCP IPv4 Vendor Specific Configuration . . . 190
Managing DHCP Vendor Options 192
Configuring Vendor Specific Option Tags 192
Configuring DHCP Server IPv6 194
Configuring DHCPv6 Leases 196
Configuring Traffic Shaping 197
Overview. 197
Using the Traffic Shaping Page. 204
Configuring Basic Traffic Shaping 208
Configuring Advanced Traffic Shaping. 210
Configuring Classes of Service 211
Deleting a Class of Service 213
Creating a New Class of Service 213
Configuring Classification Rules. 214
Deleting a Classification Rule 215
Creating a New Classification Rule. 215
Setting GRED/LLQ Configuration Rules 216
Monitoring GRED/LLQ Traffic Shaping Debug Output . . . 219
Configuring Pass-Through Rules 219
Overview. 219
Adding a Pass-Through Rule 220
Deleting a Pass-Through Rule 223
Configuring Subinterfaces 223
Overview. 224
Adding a Network Subinterface 225
Deleting a Subinterface. 226
Configuring Proxy ARP 226
Overview. 226
Using the Proxy ARP Page 227
Deleting a Proxy ARP Entry 229
Managing Switch Ports Settings. 229
Configuring Static Routes 232
Deleting a Static Route 233
Configuring Dynamic DNS. 234
Viewing Network Information 236
Initiating Network Restart 239
Using Network Test Tools 240
Performing a Ping Test 241
Performing a Traceroute Test. 242

© 2016 Edgewater Networks. All Rights Reserved.

Configuring Firewall Traversal 242
Updating a Certificate 242
Current Status 243
Operating Mode 243
Using the Firewall Traversal Page 244
Configuring Internal Client Mode Settings 245
Configuring External Server Mode Settings 248
Configuring the Static Key 252
Configuring Diffie-Hellman Parameters 253
Configuring Remote Client Mode Settings 254
Configuring WAN Failover 257
Overview 257
Configuring WAN Failover Settings 259
Configuring WAN Failover Advanced Settings 262
Configuring Secondary WAN Settings 265
Configuring Secondary WAN Interface IPv6 Settings . . . 268
Configuring Secondary WAN Interface IPv4 Settings . . . 269
Configuring Secondary WAN Network Settings 269
Configuring Dual WAN Ports 270
Managing the Secondary WAN Link Rate 272
Manage Secondary WAN Link Rate Settings 272
Configuring SOC2 IP Settings 275
Configuring Router Advertisement (IPv6) 276

4 Managing System Users

Configuring Session/User Management 281
Session/User Management - Enabling Session Management . . 282
Default Password Change and Strong Password Enforcement 286
Session/User Management - Enabling User Management 289
Using the User Management Page 291
Viewing a User 292
Changing a User Password 292
Management User Password Field Information 294
Adding a User 294
Managing Active User Sessions 296
Disabling User Management 297
Configuring System Audit Settings 297
Enabling System Audit 298
Viewing Audit Logs 299
Disabling System Audit 299
Configuring the Message of the Day (MOTD) 300
Message Types 301

© 2016 Edgewater Networks. All Rights Reserved.

Login Methods 301

5 Configuring System Security

Overview 303
Configuring Basic WAN Firewall Settings 304
Forwarding WAN Firewall Settings 306
Managing Certificates 307
Understanding the Certificate List 308
Understanding HTTPS Usage 308
Understanding VoIP Traversal Usage 308
Creating a New Certificate 310
Downloading a Certificate or Key File 312
Adding a Local Certificate 313
Configuring HTTPS 314
Configure HTTPS 315
Configuring Outbound Settings 316
Configuring Trusted Hosts 316
Adding a Host or Network 317
Deleting a Trusted Host 318
Limiting the Number of SSH Attempts 319

6 Configuring VoIP Settings

Overview 321
Alias Manipulation and Prefix Routing 322
Regular Expressions and Expression Examples 322
SIP Trunking 324
Configuring VoIP ALG Settings 327
Configuring Bandwidth Settings for H.323 334
Configuring H.323 Settings 336
Configuring WAN/Provider-Side Gatekeeper Mode Settings . 336
Configuring LAN/Subscriber-Side Gatekeeper Mode Settings 340
Configuring Peering-Proxy Mode Settings 343
Configuring Embedded Gatekeeper Mode Settings 348
Managing H.323 Settings 356
Managing H.323 Activity 356
H.323 Call Activity Messages 358
Configuring H.323 Alias Manipulation 361
Managing H.323 Call Status 364
Configuring H.323 Neighboring 365
Configuring H.323 Bandwidth Scheduling 369
Configuring Registration Rules 373
Configuring H.323 B2B Rules 375

© 2016 Edgewater Networks. All Rights Reserved.

Configuring the H.323 Clients List 378
Configuring MGCP Settings 380
Configuring MGCP Protocol Settings 382
Re-Registering Clients. 382
Configuring the Audit Endpoint 383
Configuring SIP Settings 384
Using the SIP Settings Page 385
Configuring SIP Protocol Settings 391
Configuring Allowed SIP Proxies 392
Managing the List of SIP Servers 392
Configuring the SIP Stale Timer 393
Configuring UDP Settings 394
Configuring TCP Settings. 394
Configuring TLS Settings 395
Configuring SDP Modifications Settings 395
Configuring SIP ALG Trunking 397
Configuring SIP Trunking Devices 399
Configuring Header Transformation 400
Configuring Dial Rules 402
SIP Trunking Patterns 406
Configuring VoIP SIP B2BUA Trunking 407
SIP B2BUA Request Methods 407
Creating a New Trunking Device 408
Managing B2BUA Credentials and Registration 411
Managing B2BUA Actions 415
Managing B2BUA Pattern and Digit Matching 418
Managing Header Manipulation Language. 421
Configuring SIP UA. 423
Overview 424
Configuring Basic SIP UA FXS Settings. 425
Configuring Basic FXS/Phone Port Level Settings 430
Configuring Advanced SIP UA FXS Settings 431
Configuring Advanced FXS/Phone Global Settings 433
Configuring Advanced FXS/Phone Port Level Settings . . 437
Managing Extended Hunt Group Members 440
Configuring Fax 441
Configuring Distinctive Ring 444
Adding a Distinctive Ring Pattern Rule 446
Editing or Deleting a Distinctive Ring 447
Configuring Network Side ISDN PRI (PRI/UA) 448
Configuring Network Side (CAS/UA) 448
Configuring the SIP Gateway 448
Overview 448
Using the SIP GW Page 450
Configuring Global SIP Gateway FXO/Line Port Settings. 451

© 2016 Edgewater Networks. All Rights Reserved.

Registering with the SIP Server 453
Configuring SIP Gateway FXO Ports. 455
Configuring Network Side ISDN PRI (PRI/UA) 456
Configuring Network Side (CAS/UA) 456
Configuring SIP Routing 456
Creating and Managing Routing Groups and Keepalives . 457
Configuring the SIP Media Server 460
Configuring Survivability 460
Overview. 461
Viewing Current Survivability Status. 465
Configuring Survivability Common Settings 466
Configuring SIP Server Reachability 468
Configuring SIP Server Redundancy 473
Configuring Local Call Control 474
Configuring SIP Registration Control. 476
Configuring the Clients List 478
SIP Clients List. 479
MGCP Clients List 480
H.323 Clients List 482
Managing Test UA 483
Using the Test UA Settings Page 484
Verifying Connectivity with Test UA 487
Configuring IP Phones, IADs, or Softphones 487

7 Configuring VPN Settings

Configuring VPNs 489
Using the VPN Configuration Page 490
Adding a VPN Tunnel 490
Modifying a VPN Tunnel 495
Disabling a VPN Connection 495
Deleting a VPN Tunnel 496
Managing VPN Subnets. 496
Adding or Editing a VPN Subnet 497
Deleting a VPN Subnet 498
Configuring the PPTP Server 498
Overview. 498
Enabling PPTP 499
Configuring PPTP Usernames 500
Adding a User to the PPTP Server 501
Deleting PPTP Users 501
Displaying PPTP Active Users 502
Displaying PPTP Log Messages 502

© 2016 Edgewater Networks. All Rights Reserved.

8 Configuring Switch Settings

Configuring the Management LAN IP 504
Managing Mirror Monitoring 505
Configuring PoE (Power over Ethernet) 506
Managing Port Statistics 508
Configuring RSTP 509
Overview 509
Configuring RSTP Settings 510
Managing RSTP System Configuration 512
Configuring Switch Ports 513
Configuring Storm Control 516

9 Troubleshooting Tips

Contacting Edgewater Networks Support 519
How to Contact Edgewater Support 519
Locating Information About Your EdgeMarc 520
EdgeMarc System Call Messages 521

License and Warranty Information

EdgeMarc Warranty 523
Hardware Warranty 523
Software Warranty 523

What's New

New GUI Features in the VOS 14.7 Releases 525
New GUI Features in the VOS 14.6 Releases 526

Glossary

© 2016 Edgewater Networks. All Rights Reserved.

About This Guide

Thank you for choosing the EdgeMarc™ Session Border Controller. This guide describes the EdgeMarc VoIP Operation System (VOS), and is intended for network installers and system administrators.

This guide assumes that you have already installed and cabled your device according to the instructions in the hardware installation guide that came with your EdgeMarc.

The chapters in this guide represent configuration tasks in the EdgeMarc GUI Configuration Menu. Your Configuration Menu may vary, depending on your EdgeMarc model and features included with your software version.

Before You Begin

Before you use the information in this guide, make sure that you are connected to the device through a supported web browser.

Additional information about the features provided by VOS can be found in our extensive knowledge base:

http://www.edgewaternetworks.com/kb

See the following sections for more information about this guide:

- Typographic Conventions
- Online Help
- Document Organization
- Contact and Support Information

Typographic Conventions

User input is displayed in **boldface** type and can represent keyboard input, mouse selections in a browser window, and buttons on the GUI, depending on the context. For example, the notation **File** > **Open...** means that you first click the **File** menu and then select **Open...** from the sub-menu in the GUI.

Command Line Interface (CLI) text is shown in `courier font`.



Note

Notes highlight information that is important or that has special interest.



Tip

Tips provide additional information that is helpful in performing a particular task but is not mandatory to perform the task.

Caution

Cautions alert you of actions or events that may cause system damage or loss of data.

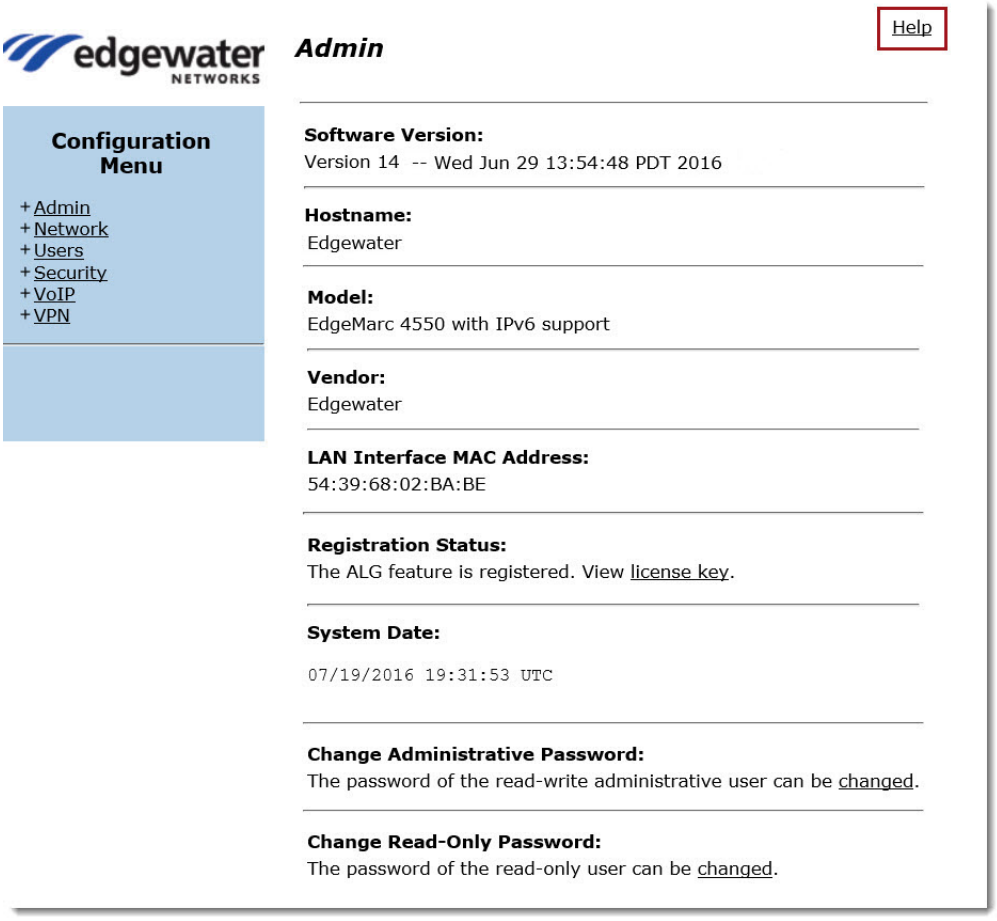
Warning

Warnings alert you of actions or events that may cause bodily harm.

Online Help

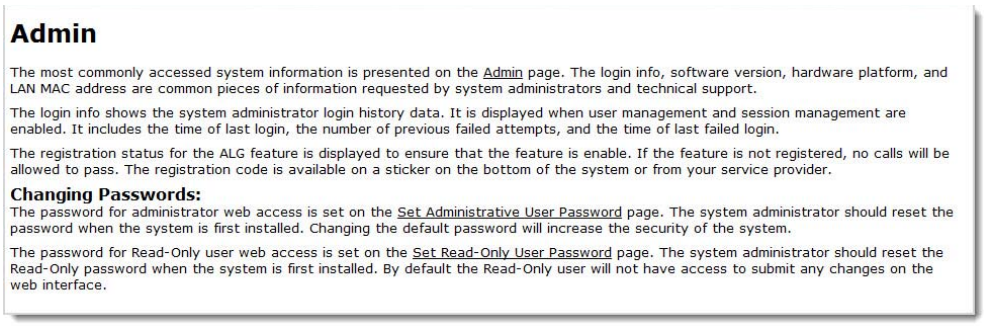
Each EdgeMarc GUI page includes a **Help** link which provides information and tips for configuring settings on the page. The OLH may also include links to other GUI pages for performing related functions. To access the online help, click the **Help** link at the top of the page.

Figure 1-1 EdgeMarc Online Help Link



The online help page opens, as shown.

Figure 1-2 EdgeMarc Online Help - Admin Page



Admin

The most commonly accessed system information is presented on the Admin page. The login info, software version, hardware platform, and LAN MAC address are common pieces of information requested by system administrators and technical support.

The login info shows the system administrator login history data. It is displayed when user management and session management are enabled. It includes the time of last login, the number of previous failed attempts, and the time of last failed login.

The registration status for the ALG feature is displayed to ensure that the feature is enable. If the feature is not registered, no calls will be allowed to pass. The registration code is available on a sticker on the bottom of the system or from your service provider.

Changing Passwords:
The password for administrator web access is set on the Set Administrative User Password page. The system administrator should reset the password when the system is first installed. Changing the default password will increase the security of the system.

The password for Read-Only user web access is set on the Set Read-Only User Password page. The system administrator should reset the Read-Only password when the system is first installed. By default the Read-Only user will not have access to submit any changes on the web interface.

Document Organization

Chapter	Description
Chapter 1, *Getting Started*	Describes how to get started using the EdgeMarc.
Chapter 2, *System Administration*	Provides system information and describes common tasks used by system administrators and technical support.
Chapter 3, *Network Deployment*	Describes how to configure the EdgeMarc to support network services.
Chapter 4, *Managing System Users*	Manages user settings, administrative user accounts, access server user accounts, and user sessions.
Chapter 5, *Configuring System Security*	Configures firewall features on the EdgeMarc.
Chapter 6, *Configuring VoIP Settings*	Configures Voice over IP (VoIP) Application Layer Gateway (ALG) on the EdgeMarc to recognize and register network devices.
Chapter 7, *Configuring VPN Settings*	Configures IPsec virtual private networks (VPNs) on the EdgeMarc to protect data communication.
Chapter 8, *Configuring Switch Settings*	Describes how to configure management IP LAN switch settings.
Chapter 9, *Troubleshooting Tips*	Describes common troubleshooting tips and system maintenance utilities.
What's New	Describes new features in version software.
License and Warranty Information	License information related to the operation of EdgeMarc™ hardware and software.

Contact and Support Information

U.S. Headquarters:
Edgewater Networks, Inc.
5225 Hellyer Ave. #100
San Jose, California 95138
Phone: 408.351.7200
Fax: 408.727.6430
edgewaternetworks.com

General: info@edgewaternetworks.com
Sales: sales@edgewaternetworks.com

Edgewater Networks, Inc. - Technical Assistance Center
Phone: 408.351.7200 ext. 2
Support@edgewaternetworks.com

1

Getting Started

The EdgeMarc is a flexible, easy-to-use session border controller that provides many critical networking functions for IP-based voice and data. The following sections describe how to get started:

- Understanding the EdgeMarc VoIP Operating System
- Deploying the EdgeMarc
- Accessing the Web-Based GUI Interface
- Where to Go Next

Understanding the EdgeMarc VoIP Operating System

Edgewater EdgeMarc VoIP Operating System software (VOS) provides award-winning features for converged networking environments. These features enable the EdgeMarc to act as an enterprise session border controller and demarcation point for managed services.

VOS supports all EdgeMarc session border controller models from Edgewater Networks. For a current list of available models, go to the Edgewater Networks web site: www.edgewaternetworks.com

Using the VOS web-based user interface, you can easily configure settings that allow the EdgeMarc to provide the following:

- Network Address Translation (NAT) and firewall traversal using a VoIP Application Layer Gateway (ALG) supporting SIP, MGCP, and H.323.
- Support for 2 to 30 concurrent VoIP calls.
- Enterprise LAN protection using a stateful packet inspection (SPI) firewall for voice and data traffic.
- NAT and Port Address Translation (PAT) for voice and data.
- Static IP routing.
- Traffic management:
  - Prioritization
  - Classification
  - Queuing
  - Type of Service (TOS) bit setting
  - Call admission control for voice

- Voice call quality monitoring and testing.
- Integrated test tools to facilitate problem isolation.
- DHCP server options for enterprise computers and IP phones.
- TFTP relay for IP phone images.
- SNMP for logging to external syslog servers and interfaces to network management systems.

Deploying the EdgeMarc

Your EdgeMarc configuration is based on your deployment scenario, VoIP topology, and presence of other networking equipment such as firewalls or DHCP servers.

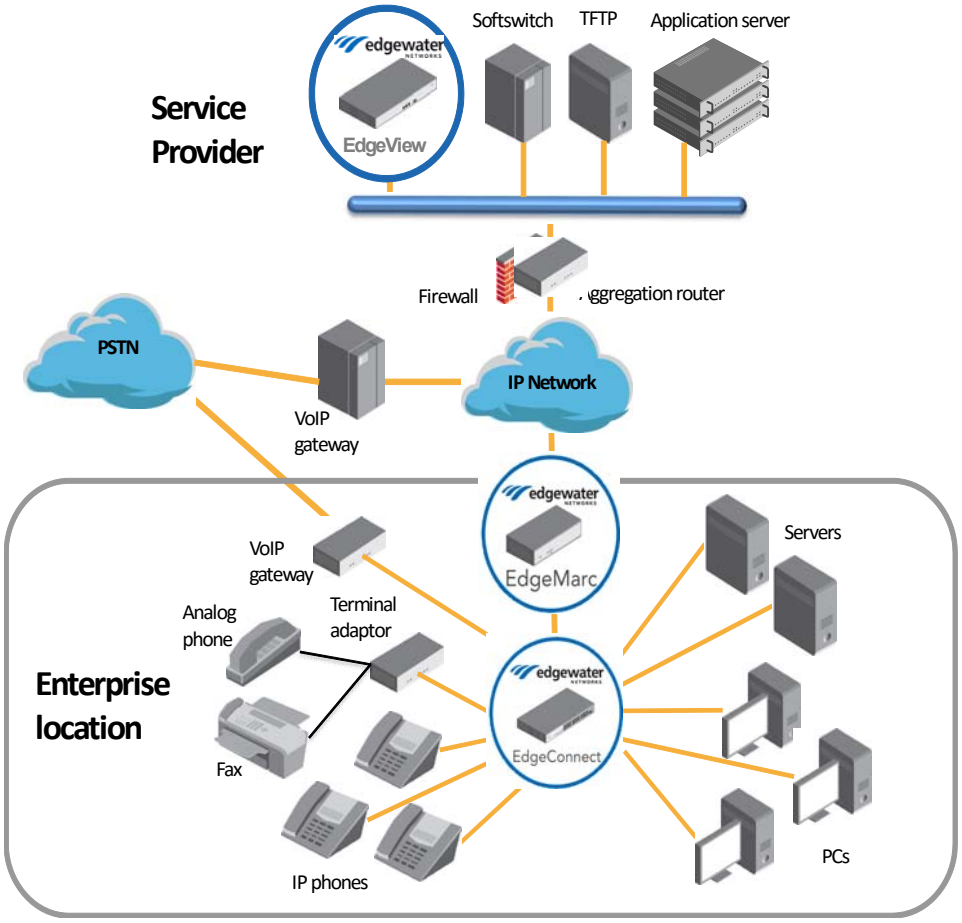
Although the EdgeMarc can be installed in many different VoIP topologies, this document describes how to configure the EdgeMarc to support two basic deployment scenarios:

- Deploying the EdgeMarc in IP Centrex Networks
- Deploying the EdgeMarc in Station Side IP PBX Networks

Deploying the EdgeMarc in IP Centrex Networks

Figure 1-1 shows a typical IP Centrex deployment with the Edgewater EdgeMarc, EdgeView, and EdgeProtect devices.

Figure 1-1 Sample Configuration for IP Centrex Deployments



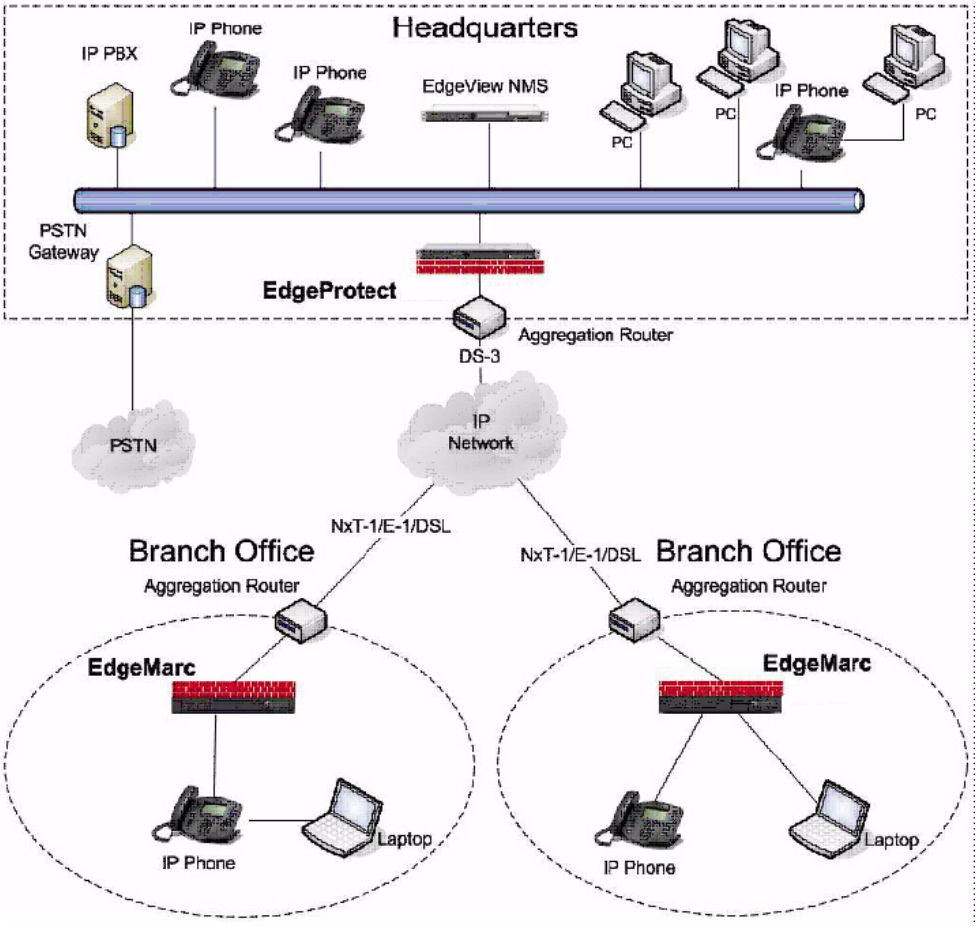
In this sample IP Centrex deployment:

- The WAN link from the service provider is terminated by an external router, xDSL, or cable modem.
- The EdgeMarc is connected directly to the WAN termination device and to the enterprise LAN (typically a layer 2 switch).
- VoIP signaling is performed in the service provider network via a softswitch.
- The EdgeMarc acts as a proxy for the voice devices installed in the enterprise LAN.
- A single public IP address is used as proxy for the IP phones. It is also used to route calls to multiple PCs on the LAN.
- Static NAT routes calls to publicly addressable servers.

Deploying the EdgeMarc in Station Side IP PBX Networks

Most private enterprise VoIP networks use an IP PBX at the corporate headquarters to provide voice switching among headquarters, branch offices, and the PSTN. The EdgeMarc is used in these environments to securely connect branch office employees to the IP PBX installed in the corporate headquarters location. Figure 1-2 shows a sample IP PBX deployment with Edgewater EdgeMarc, EdgeView, and EdgeProtect devices.

Figure 1-2 Deploying the EdgeMarc in a Station-side IP PBX Network



In the sample station-side IP PBX deployment:

- The branch office is connected to the corporate network using VPNs or private T1 links terminated by a WAN router.
- The EdgeMarc is connected directly to the WAN router and to the enterprise Ethernet LAN (typically a layer 2 switch).
- The IP PBX in the corporate headquarters location performs VoIP signaling.
- The EdgeMarc acts as a proxy for the voice devices installed at the branch office.

Accessing the Web-Based GUI Interface

The EdgeMarc VOS user interface is accessible through a web browser. The VOS interface includes intuitive menus and options for:

- System administration
- Network configuration and management
- User management
- Security
- VoIP ALG
- VPN

Before You Begin

You must first configure the system WAN interface with the IP address, default gateway, and valid Primary and Secondary DNS server address or credentials assigned by your Internet Services Provider (ISP). Refer to the *EdgeMarc Hardware Installation Guide* for details on how to install the EdgeMarc and access the GUI for the first time. Support documentation is available from the Edgewater Networks Knowledgebase at www.edgewaternetworks.com.

Once you have configured the EdgeMarc device, you can access EdgeMarc VOS GUI.

Logging Into the EdgeMarc

Log into the EdgeMarc using a web browser such as Microsoft Internet Explorer, Google Chrome, or Mozilla Firefox.

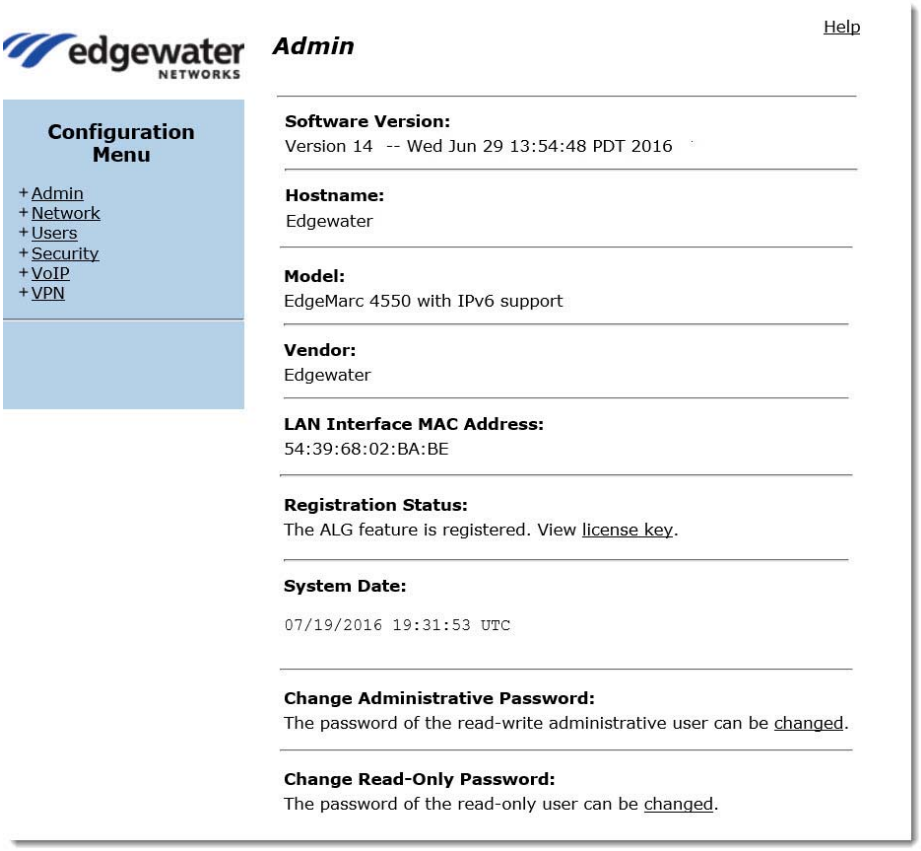
1. Launch a web browser on your computer and enter the URL assigned to your EdgeMarc.

   The EdgeMarc login screen is displayed.



2. Enter your initial username in the field provided: **root**
3. Enter your initial password in the field provided: **default**
4. Click **OK**. The EdgeMarc Admin landing page is displayed (Figure 1-3).

Figure 1-3 EdgeMarc VOS Admin Landing Page



Where to Go Next

It is strongly recommended that you change your password after you complete your initial login to the system. See Changing Your Password in Chapter 2, *System Administration* for complete information about the using the Admin page.

2

System Administration

The following sections describe common administration tasks using the **Admin** tab in the Configuration Menu. The Admin page is the landing page when you log in to the EdgeMarc.

- Using the Administration Page
- Managing the License Key
- Changing Your Password
- Configuring Backup and Restore
- Upgrading Firmware
- Upgrading SOC2 Firmware
- Configuring RADIUS Settings
- Configuring TACACS+
- Configuring Services
- Viewing System Information
- Configuring Time and Date Settings
- Configuring Settings With User Commands
- Managing File Download
- Managing the File Server
- Configuring the SD Card
- Configuring Technical Report-069 Parameters
- Configuring V.90 Modem Settings
- Rebooting the System

Using the Administration Page

1. Choose **Admin** from the Configuration Menu (Figure 2-1).

Figure 2-1 Admin Page

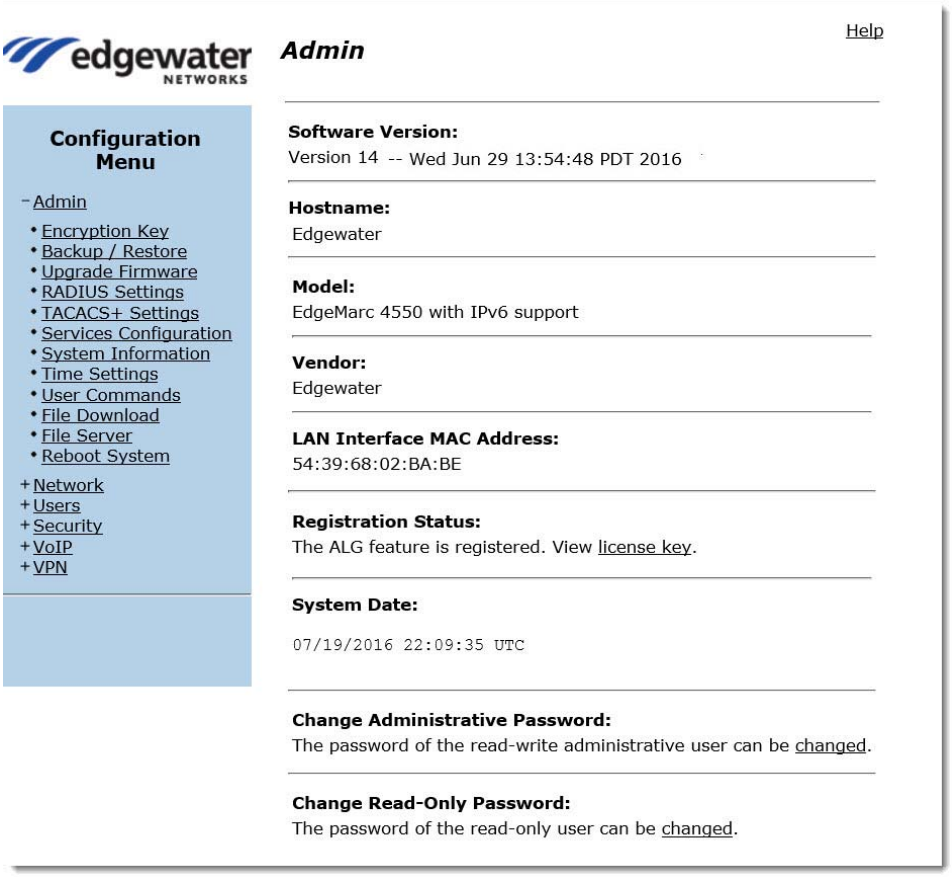


Table 2-1 describes information displayed on the Admin page.

Table 2-1 Administration Page Information

Item	Description
Software Version	EdgeMarc VOS software version. To upgrade firmware, see Upgrading Firmware.
SOC2 Version	EdgeMarc 250 Series software. To upgrade SOC2 firmware, see Upgrading SOC2 Firmware.
Hostname	By default, the hostname is the system type. For example, “4550.” The hostname can also be a unique identifying string of numbers and letters. To change the system hostname, choose **Admin** > **Services Configuration** and enter a new name in the **Set Hostname** field. Refer to Managing Source Address Settings.

Table 2-1 Administration Page Information (continued)

Item	Description
Model	Displays the model and associated support. For example, “EdgeMarc 4550 with IPv6 support.”
Daughter Card	EdgeMarc 4808. Optional Enhanced SD host controller (eSDHC) SD High Capacity Version 2.0 daughter card enables up to 4 T1 ports. Maximum storage capacity is 32 GB per SD card, 4 GB per file. SD card capabilities are configured with the web-based configuration menu and with command-line interface (CLI).
Vendor	Displays basic vendor specific parameters. To manage vendor attributes, choose **Network** > **DHCP Server** > **Vendor Specific Configuration** and refer to Chapter 3, *Network Deployment*.
LAN Interface MAC Address	Displays LAN MAC address information. Use this information when requesting a new or replacement license key. See Managing the License Key.
Registration Status	Shows whether the ALG feature is registered using a valid license key. See Managing the License Key.
System Date	Displays the current date and time in Coordinated Universal Time (UTC). To manage date and time settings, choose **Admin** > **Time Settings** and refer to Configuring Time and Date Settings.
Change Administrative Password	Changes the read-write administrative user password. See Changing the Administrative Password.
Change Read-Only Password	Changes the read-only user password. See Changing the Read-Only Password.
Daily Configuration Update Check - Update Timer	Sets the time of day that the system checks for configuration updates. Only available on some EdgeMarc models. Set the Hour (0-23) and Minute (0-59).

Managing the License Key

Your device feature license key is installed on the EdgeMarc when it arrives from Edgewater Networks. The license key determines the software features that are available on your EdgeMarc.

Where Do I Find My License Key?

A card is included in the EdgeMarc box that contains your license key for reference.

What If I Lose My License Key?

If you lose the card that contains your license key, request a replacement by sending an email to sales@edgewaternetworks.com that includes your system LAN MAC address.

How Do I Purchase an Upgrade License Key?

If you would like to purchase an upgrade license key to add specific features, contact sales@edgewaternetworks.com.

Viewing and Editing Your License Key

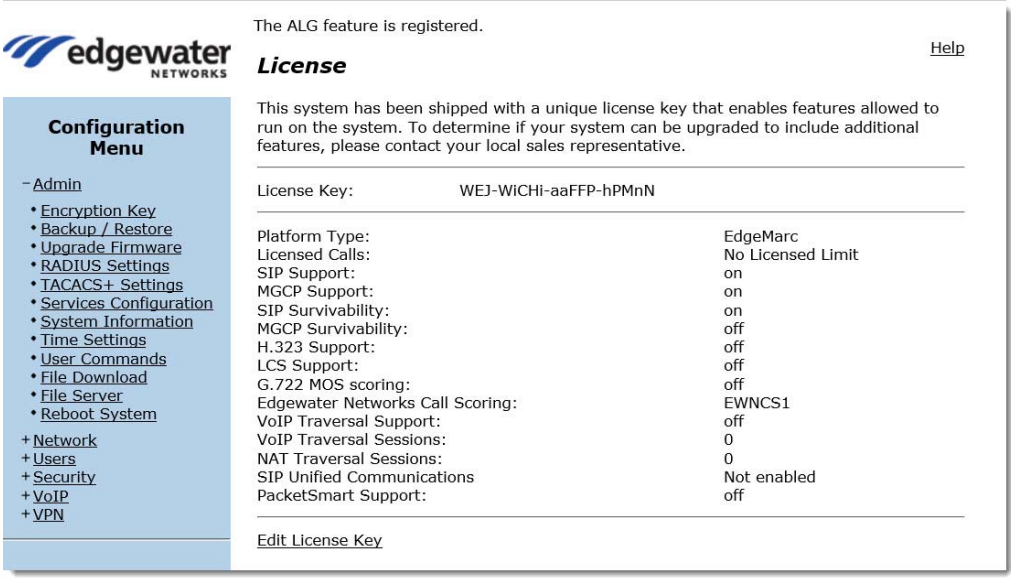


Warning
When you update your software, including your license key, telephone services are unavailable for several minutes. It is therefore advised that upgrades be performed during a maintenance window when telephone traffic can be interrupted.

To view or edit your license key:

1. Choose **Admin** from the Configuration Menu (Figure 2-1).
2. Note your LAN MAC address in the **LAN Interface MAC Address** field.
3. Scroll to **Registration Status** and click **View License Key**. The License page is displayed (Figure 2-2).

Figure 2-2 View License Key



4. To enter a new or replacement license key, click **Edit License Key** at the bottom of the page to activate the **Enter License Key** field.
5. Clear the previous license key from the **Enter License Key** field and enter the new license key that you have obtained from Edgewater Networks.



6. Click **Submit**.

Managing Encryption Key Settings

The Encryption Key Configuration page allows you to change the Encryption Key in the device. This feature is only available on some EdgeMarc devices.

1. Choose **Admin** > **Encryption Key** (Figure 2-3).

Figure 2-3 Encryption Key Configuration Page



The Key in use field displays the current key in use, for example, “Default key.”

2. Choose a key type from the Encryption Key drop-down list:
   - Default Key—Device uses its default encryption key.
   - New Key—Device uses a user defined encryption key. The **New Key** field becomes active.
3. Enter a new key in the **New Key** field. Encryption key size must be 16 characters and must not contain {%,<,>,$,',"} characters.
4. Click **Submit** to save your settings.

Changing Your Password

The first time you access the VOS, change the administrator password:

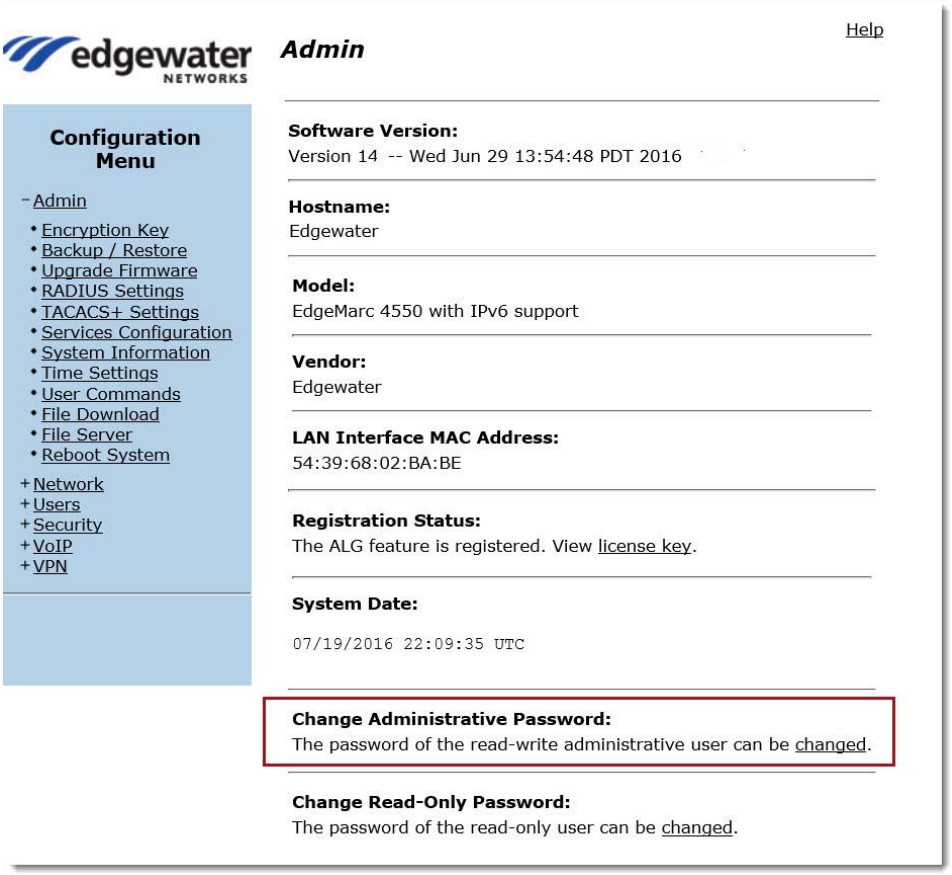
- Changing the Administrative Password
- Changing the Read-Only Password

Note
For more information about system passwords, refer to Default Password Change and Strong Password Enforcement in Chapter 4, *Managing System Users*

Changing the Administrative Password

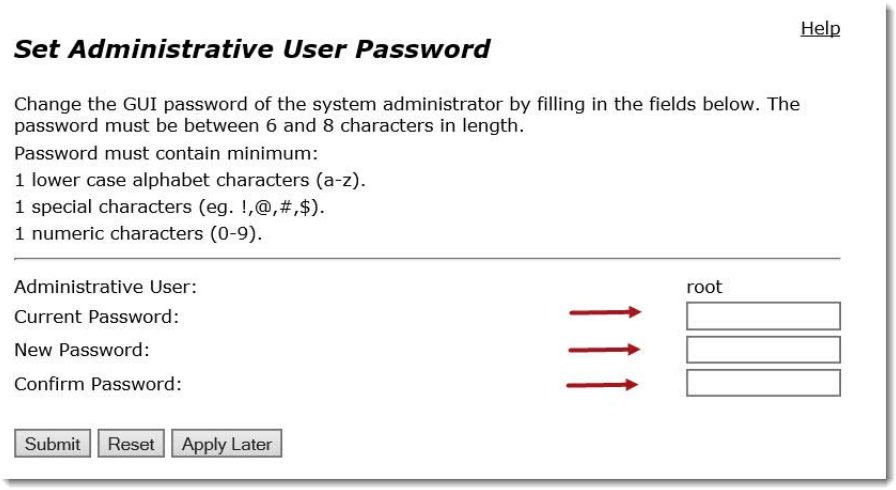
1. Choose **Admin** from the Configuration Menu.
2. Scroll to **Change Administrative Password** and click **Changed** (Figure 2-4).

Figure 2-4 Admin - Changing the Administrative Password



3. On the Set Administrative User Password page (Figure 2-5), enter your current password in the **Current Password** field.

Figure 2-5 Set Administrative User Password Page

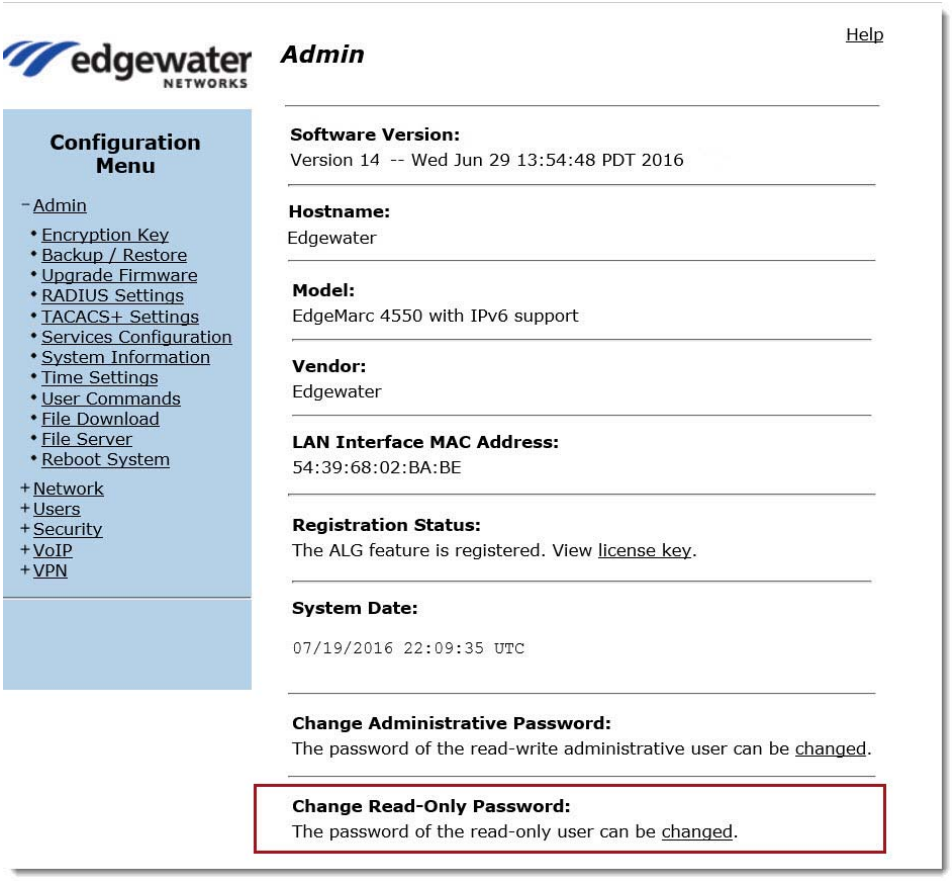


4. In the **New Password** field, enter a password between six and eight characters long that contains at least one non-repeating number.
5. Re-enter the new password in the **Confirm Password** field.
6. Click **Submit**.

Changing the Read-Only Password

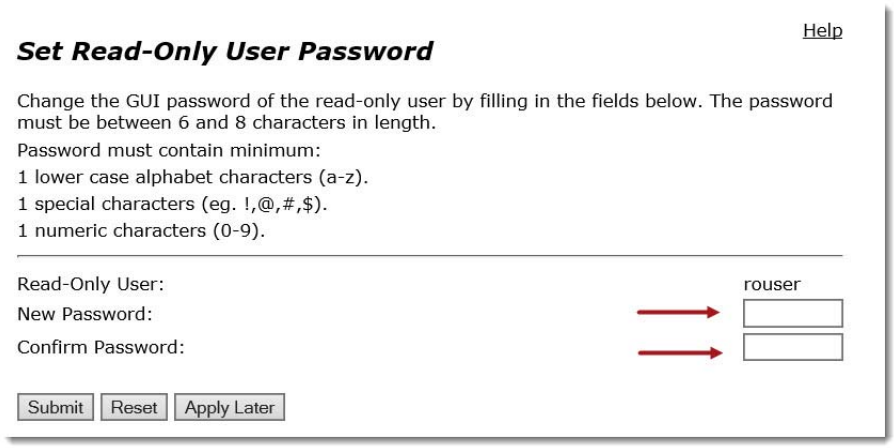
1. Choose **Admin** from the Configuration Menu.
2. Scroll to **Change Read-Only Password** and click **Changed** to open the Set Read-Only User Password page (Figure 2-7).

Figure 2-6 Change Read-Only Password



3. On the Set Read-Only User Password page (Figure 2-7), enter your current password in the **Current Password** field.

Figure 2-7 Set the Read-Only User Password



4. In the **New Password** field, enter a new password between six and eight characters long and that contains at least one non-repeating number.
5. Re-enter the new password in the **Confirm Password** field.
6. Click **Submit**.

Password Restrictions

Passwords must meet the following complexity requirements:

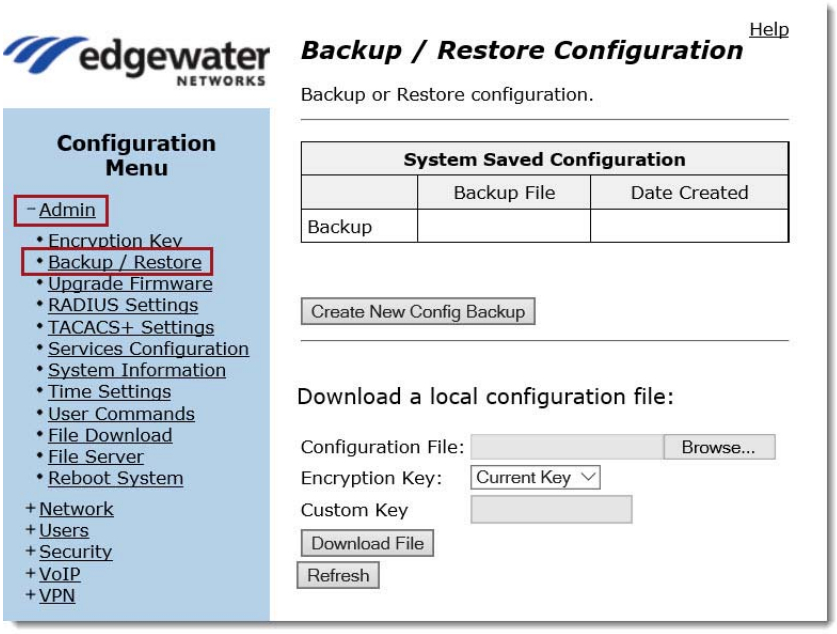
- Must have a minimum length in the range of 8 to 15 characters, depending on the configured value.
- Must contain the minimum configured number of alphabet, numeric and special characters. Configurable range is 1 to 2 characters for each character class.
- Must not exceed the maximum number of consecutive repeating characters that are allowed in the password. Configurable range is 1 to 4 repeating characters.
- Must contain the minimum configured number of changed characters from the previously used password. Configurable range is 1 to 4 characters
- Must not be identical to configured number of previously used password. Configurable range is 8 to 16 previously used passwords.

Configuring Backup and Restore

Use the Backup / Restore Configuration page to save your current configuration or restore a previous one. You can also download the saved configuration to a local PC or upload one from the local PC.

1. Choose **Admin** > **Backup/Restore** (Figure 2-8).

Figure 2-8 Backup/Restore Configuration Page



2. Manage backup configuration files using the information in Table 2-2 as a guide.

Table 2-2 Backup/Restore Configuration Parameters

Item	Description
System Saved Configuration	
Displays saved backup files.	
Create New Config Backup	Click **Create New Config Backup** to create a new backup configuration based on the currently running configuration. The new backup file is given a new name based on the hostname, date, and time. The resulting filename is displayed in the Backup File column in the System Saved Configuration table. See Creating a New Backup Configuration File.
Restore Saved Configuration	Click **Restore Saved Configuration** to use the contents of the backup file shown in the System Saved Configuration table to restore the original EdgeMarc configuration. See Restoring a Previous Backup File.
Upload a Local Configuration	
See Uploading a Backup Configuration File to Your Local Drive.	
Configuration File	Click **Browse** to upload a backup configuration file from the local computer drive to the EdgeMarc.

Table 2-2 Backup/Restore Configuration Parameters (continued)

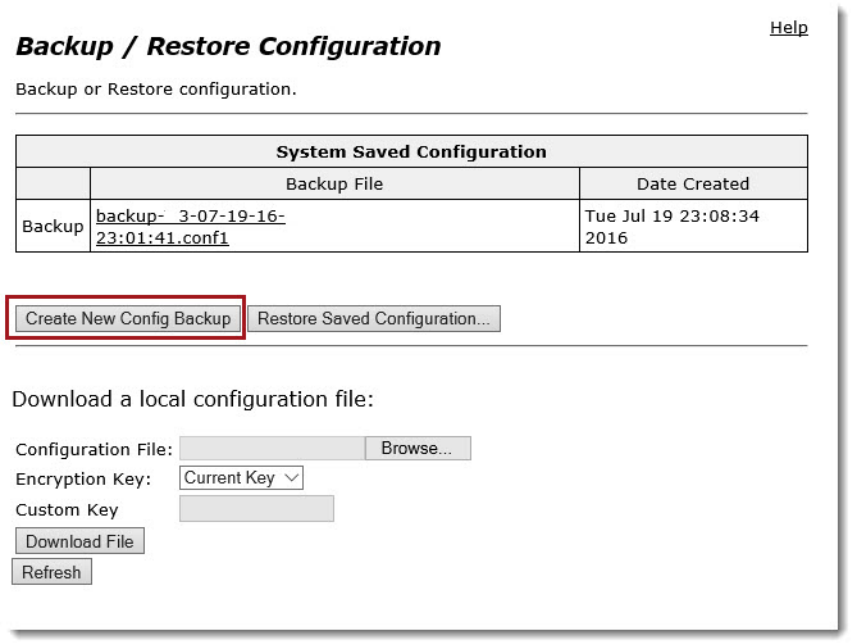
Item	Description
Encryption Key	Select the encryption key to decrypt the configuration file. You can choose: ■ Default Key—Uses the default Encryption Key to decrypt. ■ Current Key—Uses the Current Encryption Key in the device. ■ Custom Key—Enter a 16 character key in the field provided. The key must not contain {%, $, <, >,',"} characters.
Download the Configuration	Click the hyperlinked file in the System Saved Configuration table to download the saved configuration from the EdgeMarc to your local drive. See Downloading the Saved Configuration to a Local Drive.

Creating a New Backup Configuration File

You can create a new backup configuration based on the currently running configuration. The new backup file is given a new name based on the hostname, date, and time. The resulting filename is displayed under the Backup File column in the System Saved Configuration table.

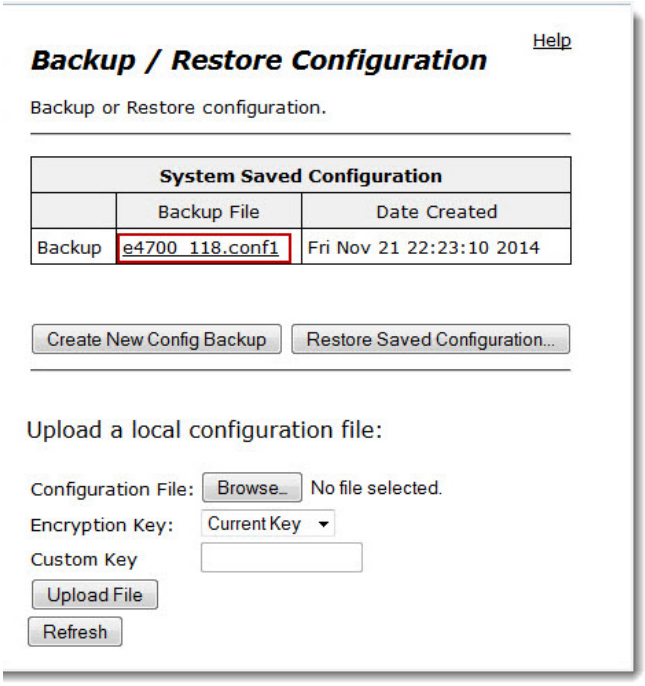
1. On the Backup/Restore Configuration page, click **Create New Config Backup** (Figure 2-9).

Figure 2-9 Create New Config Backup



2. A message alerts you that you are overwriting the existing backup file Click **OK** to continue. The new backup file appears in the System Saved Configuration table.
3. To download the saved configuration from the EdgeMarc to your local drive, click your hyperlinked backup file in the System Saved Configuration table (Figure 2-10).

Figure 2-10 Restore Saved Configuration



4. In the dialog box, choose whether to save or open the file and click **OK**.

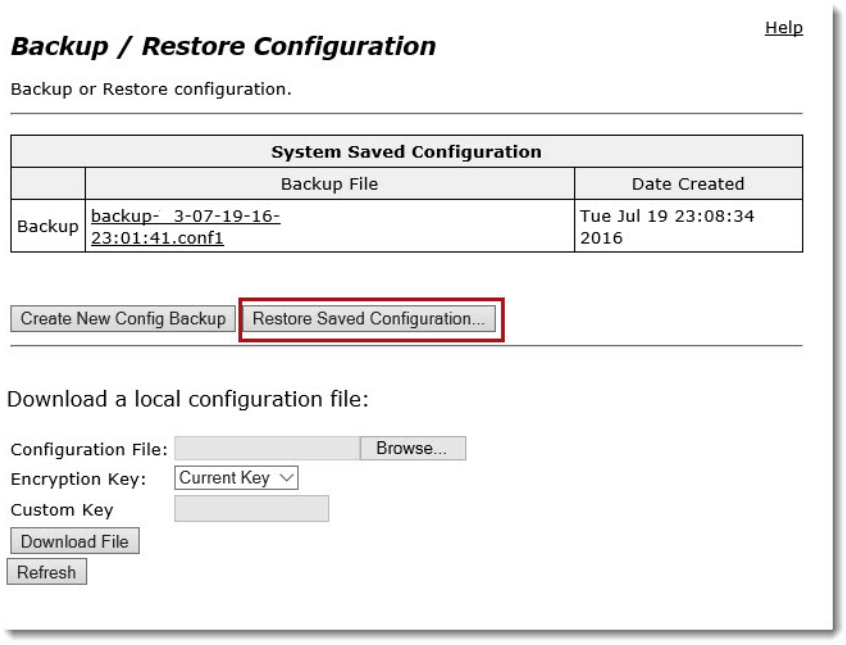
Restoring a Previous Backup File

The system uses the contents of the backup file shown in the System Saved Configuration table to restore the system configuration.

1. Click **Restore Saved Configuration** (Figure 2-11).

Note
The matching encryption key must be used with the restored configuration. You will be restoring the System to the previously saved configuration.

Figure 2-11 Restore Saved Configuration

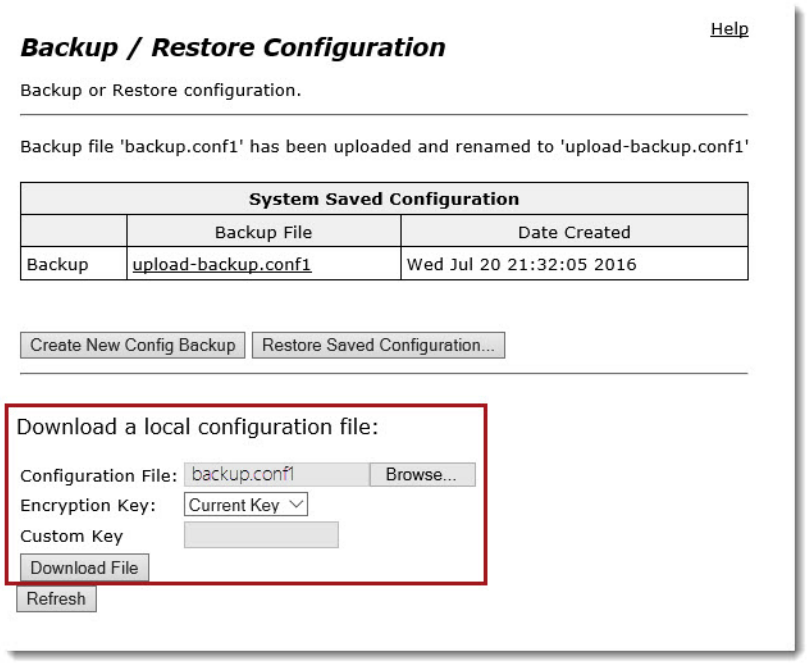


2. A message indicates that service will be temporarily interrupted. Click **OK** to confirm

Uploading a Backup Configuration File to Your Local Drive

1. Click **Browse** to locate the file on your PC. The file must have the .conf1 extension as shown in Figure 2-12.

Figure 2-12 Upload File



2. Click **Upload File**. The uploaded file becomes the new System Saved Configuration file.

Downloading the Saved Configuration to a Local Drive

If desired, you can download the saved configuration from the system to your local drive as follows:

1. On the Backup/Restore Configuration page, click the hyperlinked file in the System Saved Configuration table.
2. In the dialog box, choose whether to save or open the file and click **OK**.

Tip
Backup and restore can be automated with the EdgeView Service Control Center (EdgeView SCC).

Upgrading Firmware

Preparing for Firmware Upgrade

Before performing a firmware update to the system, you must contact Edgewater Networks technical support to obtain the correct filename for the desired hardware platform.

The default download server is ftp.edgewaternetworks.com. CLI commands can also be used to transfer a VOS software upgrade image by SCP.

When performing a local firmware update, your Edgewater Networks technical support representative will provide instructions for creating the correct directory structure on your local FTP server to allow the system to perform a local firmware update.

To upgrade your system, you will need both the firmware image and the associated md5 checksum file available on the local computer. For each file, select **Browse** and navigate to the appropriate directory, choose the file, and then click **Upload** to transfer the file. Once both files have been uploaded, select **Submit** to write the new image onto the device.

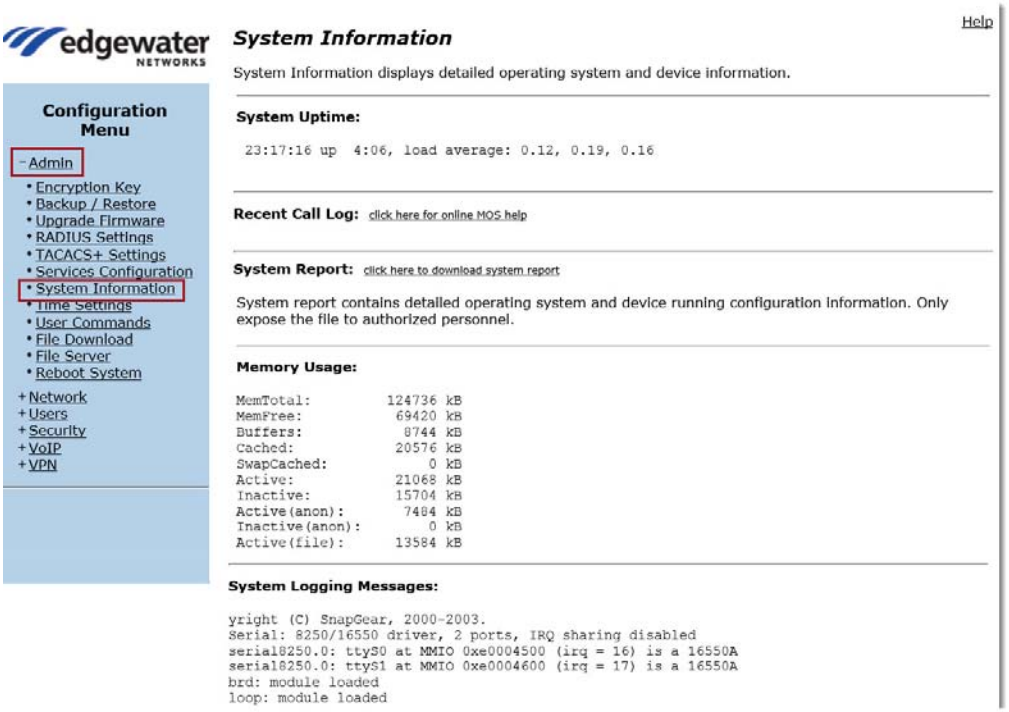


Warning
When you update your software, telephone services are unavailable for several minutes. It is therefore advised that upgrades be performed during a maintenance window when telephone traffic can be interrupted.

Before You Begin

1. It is recommended that you reboot the EdgeMarc before performing an upgrade. The reboot will ensure that enough dynamic memory is available to handle the upgrade process. Refer to Rebooting the System for more information.
2. Check the System Information page to make sure there are no active calls in the **Number of Active Streams** field. Choose **Admin** > **System Information** (Figure 2-13) and refer to Viewing System Information.

Figure 2-13 System Information Page



Where Do I Download New VOS Firmware?

VOS firmware is available on the Edgewater Networks FTP site. Call Edgewater TAC/support to obtain the name of the file to look for when you log into ftp.edgewaternetworks.com.

What is the Latest Firmware File Name?

To obtain the name of the most current upgrade firmware for your system, contact Edgewater Networks technical support:

Support@edgewaternetworks.com

Upgrading Your Firmware

Note
When the Write process begins, 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.

The system automatically restarts after the new image has been loaded. Once the upgrade process has completed, verify that the new firmware version number is displayed on the **Admin** > **Upgrade Firmware** page.

To upgrade system firmware:

1. Choose **Admin** > **Upgrade Firmware** (Figure 2-14).

Figure 2-14 Upgrade Firmware - FTP

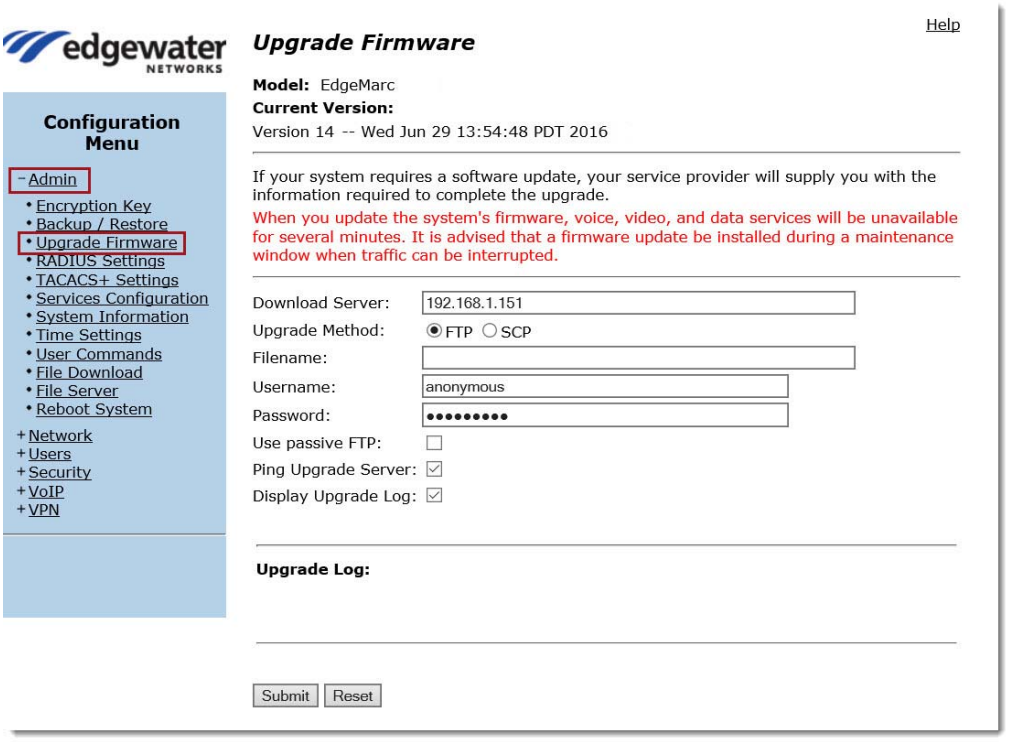
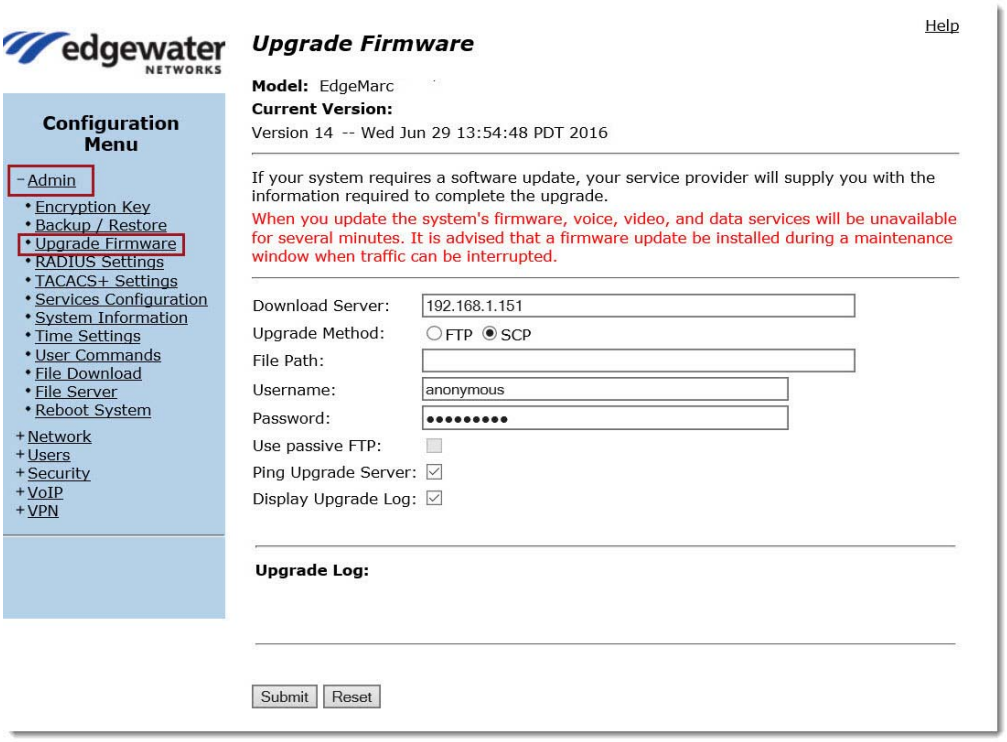


Figure 2-15 Upgrade Firmware - SCP



2. Configure settings using the information in Table 2-3 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 2-3 Upgrade Firmware Page

Item	Description
Model	Displays the system platform type.
Current Version	Displays the system current firmware version.
Download Server	The FTP / SCP server hosting the firmware. This field can be an IP or DNS name of a LAN or WAN side FTP / SCP server. For example, the Edgewater Networks FTP site: ftp.edgewaternetworks.com
Upgrade Method	Select an upgrade method: ■ FTP ■ SCP
Filename / File Path	For FTP—Enter the firmware image filename. For SCP—Enter the full firmware image file path.
Username	Enter the username to log in on the server for the selected upgrade method.

Table 2-3 Upgrade Firmware Page

Item	Description
Password	Enter a password. See Password Restrictions for information about creating passwords for the EdgeMarc.
Use passive FTP	Select the **Use passive FTP** checkbox to allow the FTP server to determine the port over which data is sent. By default, the system uses active FTP.
Ping Upgrade Server	Select the **Ping Upgrade Server** checkbox to send an Internet Control Message Protocol (ICMP) Type 8 echo request to the configured Download Server. If the server does not respond to the echo request, the upgrade is not initiated and fails. This option is enabled by default.
Display Upgrade Log	Select the **Display Upgrade Log** checkbox to display an upgrade status log of the firmware upgrade progress.

Click **Submit** to save all settings on the Upgrade Firmware page.

Upgrading SOC2 Firmware

Note
This upgrade procedure is for the EdgeMarc 250 Series only.

If your system requires a software update, Edgewater Networks support will supply you with the information required to complete the upgrade.

Before You Begin

It is recommended that you reboot the EdgeMarc before performing an upgrade. The reboot will ensure that enough dynamic memory is available to handle the upgrade process. Choose **Admin** > **Reboot** and refer to Rebooting the System.

Caution
When you update your software, telephone services are unavailable for several minutes. It is therefore advised that upgrades be performed during a maintenance window when telephone traffic can be interrupted.

Upgrading SOC2 Firmware Settings

1. Choose **Admin** > **Upgrade SOC2** (Figure 2-16).

Figure 2-16 EdgeMarc 250 Series SOC2 Upgrade Page



2. Check whether you have an upgrade message on the page similar to the following:

   "SOC2 software version mismatch, suggest upgrade."

3. Select the file type radio button. **Local file** is selected by default.
4. Click **Submit**. Wait for the SOC2 upgrade to complete.



Caution
When the Write process begins, 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.

Where to Go Next

See Configuring SOC2 IP Settings in Chapter 3, *Network Deployment*.

Configuring RADIUS Settings

Use the Radius Settings page to configure the EdgeMarc to communicate with a network-deployed RADIUS server to authenticate serial console, SSH, TELNET, HTTP, and HTTPS management sessions.

- About RADIUS Settings
- Using the RADIUS Settings Page

About RADIUS Settings

Remote Authentication Dial In User Service (RADIUS) is an authentication, authorization and accounting protocol that is used for management sessions with the EdgeMarc. If RADIUS authentication is configured, the EdgeMarc communicates with a network deployed RADIUS server to authenticate serial console, SSH, TELNET, HTTP, and HTTPS management sessions.

If the EdgeMarc cannot contact the network-based RADIUS server in the specified number of retries, or the configured shared secret does not match the secret on the RADIUS server, the EdgeMarc uses the credentials supplied by the user to perform local authentication.

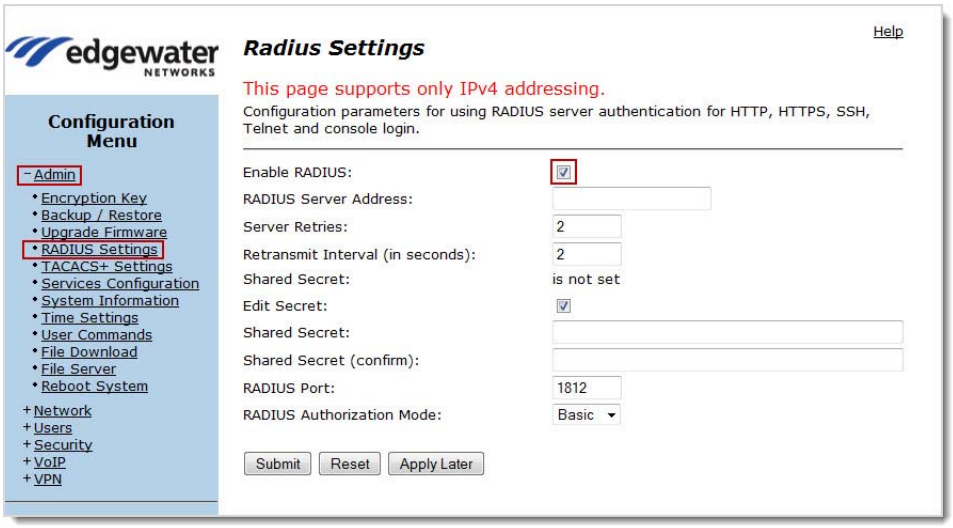
The RADIUS Settings page contains parameters for RADIUS server authentication for HTTP, HTTPS, SSH, Telnet, and console login. For all protocols except SSH, feedback is given to the operator indicating whether the login is being sent to the RADIUS server or verified locally. Sessions involving the RADIUS server are identified with the string “Radius” in the login prompt. Sessions authenticated locally on the EdgeMarc are identified with the string “System” in the login prompt.

Using the RADIUS Settings Page

Configure a single RADIUS entry for the system:

1. Choose **Admin** > **RADIUS Settings** (Figure 2-17).

Figure 2-17 RADIUS Settings Page



2. Configure settings using the information in Table 2-4 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 2-4 RADIUS Settings

Item	Description
Enable RADIUS	Select the E**nable RADIUS** checkbox.
RADIUS Server Address	Enter the primary RADIUS server IP address.
Server Retries	Specify the number of times to try to reach the RADIUS server if an attempt fails. Default is two times.
Retransmit Interval (in seconds)	Sets the delay in seconds between server retries. Default is two seconds.
Shared Secret	Displays whether a password for RADIUS authentication requests has been set.
Edit Secret	Select the **Edit Secret** checkbox to allow you to set the shared secret password.

Table 2-4 RADIUS Settings (continued)

Item	Description
Shared Secret	Enter a password for RADIUS authentication requests. The client and the server must have the same password.
Shared Secret (confirm)	Re-enter the shared secret to confirm.
RADIUS Port	Enter the port for local clients to use for communication with the RADIUS servers. Default is 1812.
RADIUS Authorization Mode	Select the mode for RADIUS authorization from the drop-down list: ■ **Basic**—Confirms the shared secret with the server. Default. ■ **CHAP**—Shares the secret with the server and includes a built-in challenge as part of the CHAP protocol.

Click **Submit**.

A message indicates that service will be temporarily interrupted.

Click **OK** to confirm

Configuring TACACS+

Use the TACACS+ Settings page to manage Terminal Access Controller Access Control System (TACACS+) authentication.

- About TACACS+ Management
- Using the TACACS+ Configuration Page
- Configuring TACACS+ Settings
- Disabling TACACS+ Services

About TACACS+ Management

Terminal Access Controller Access Control System (TACACS)+ is an authentication and accounting protocol designed for use with UNIX platforms. TACACS+ divides authentication, authorization, and accounting into separate functions. A remote TACACS+ server stores the store user and password information. This information is supplied during the authentication process. TCP is used as the communications protocol for TACACS+ messages.

TACACS+ authentication support is provided for the following management interfaces on the EdgeMarc:

- HTTP/HTTPS
- Console Login
- SSH
- Telnet

If TACACS+ is enabled, the system prompts for user name and password whenever a user attempts to log in. Upon receiving the user name and password, the EdgeMarc attempts to establish a connection with the TACACS+ server. When the connection is established, the user authentication request is transmitted to the TACACS+ server. The details of the request depend upon the authentication mode configured in the EdgeMarc.

TACACS+ authentication may result in any of the following scenarios:

- The TACACS server authenticates the user, and login is successful.
- Connection to the TACACS+ server fails (times out). Administrator password authentication is used for the next login attempt.
- Connection is established with the TACACS+ server, but the authentication parameters (user name and password) are not validated and authentication fails. TACACS+ authentication mechanism is used again for the next login attempt.

TACACS+ Authentication

The EdgeMarc supports the following TACACS+ authentication modes:

- ASCII—The user name is sent as part of the TACACS client request and the password is sent as part of the continue message.
- Password Authentication Protocol (PAP)—Both username and password are sent as part of the request message.
- Challenge Handshake Authentication Protocol (CHAP)—The password is used to calculate the response to a random challenge. Both the challenge and response are sent as part of the TACACS+ request message.

For successful authentication, the user name and password entered for TACACS+ authentication at run-time must match the values that are configured on the TACACS+ server. The user name and password settings depend on the authentication mode (PAP/CHAP/ASCII).

TACACS+ Accounting

TACACS+ accounting support is provided for the EdgeMarc to track user interactions with the system and provide a user audit trail that can be used for resource allocation or billing.

GUI Interaction Logging

When TACACS+ logging is enabled, all the configured parameters that have changed from their original stored values are sent as a sequence of attribute-value pairs (AV pairs). The format is

attributename=attributevlaue

Where *attributename* is the name of the configurable parameter (similar to the GUI field name) and *attributevalue* is the new value of that parameter.

All TACACS+ parameters except for TACACS+ Authentication Mode are applicable for both logging and authentication features.

For the GUI interface, the TACACS+ logging message also contains the following protocol-specific fields:

- service=*http*
- page_name=*symbolic name of the web page e.g. pg_vpn*
- operation=*self explanatory action name such as submit, add, delete*

For Telnet, SSH and console the logging messages consists of the following:

Command=*issued command*

If the parameter value or command name exceeds the maximum AV Pair length of 255 characters, then the message is broken into multiple AV pairs, as follows (This is a TACACS+ limitation):

- *attrname=attrvalue*
- *attrname_continued=attrvalue_cont.*

In addition to the field information, the TACACS+ logging message also contains some protocol-specific fields.

TACACS+ and RADIUS

The EdgeMarc supports TACACS+ or Remote Authentication Dial In User Service (RADIUS), but not both at the same time. If you attempt to enable TACACS+ while RADIUS is enabled, or vice versa, an error message is displayed, and the configuration is not applied.

If either TACACS+ or RADIUS are enabled but the system is not able to communicate with the server (TACACS+ or RADIUS respectively), then the system reverts to administrator password authentication.

Using the TACACS+ Configuration Page

Before You Begin

1. Disable RADIUS on your system:
   a. Choose **Admin** > **RADIUS Settings**.
   b. Clear the **Enable RADIUS** checkbox.
   c. Click **Submit**.



Tip
See Configuring RADIUS Settings for more information about managing RADIUS settings.

2. By default, TACACS performs authentication on every page access. To prevent this, enable Session Management on the Session/User Management - Advanced page:
   a. Choose **Users** > **Advanced** or click the **Session Management Configuration** link provided on the TACACS+ Settings page and click **Advanced**.
   b. Select the **Enable Session Management** checkbox.
   c. Click **Submit**.

   See Configuring Session/User Management in Chapter 4, *Managing System Users*.

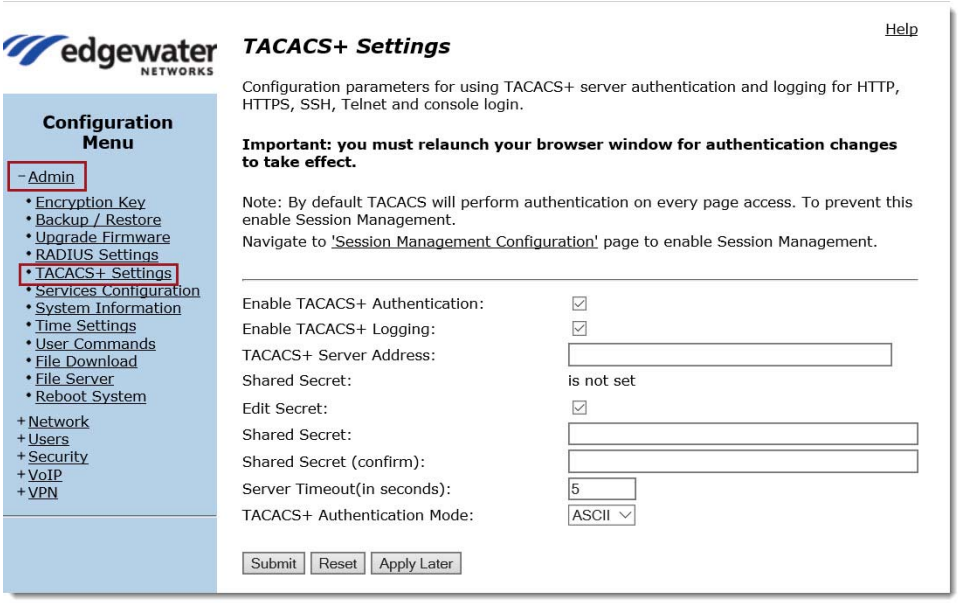
Configuring TACACS+ Settings

Configure a single TACACS+ entry for the system.

Tip
You must relaunch your browser window for authentication changes to take effect.

1. Choose **Admin** > **TACACS Settings** (Figure 2-18).

Figure 2-18 TACACS Settings Page



2. Configure settings using the information in Table 2-5 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 2-5 TACACS Settings

Item	Description
Enable TACACS+ Authentication	Select the **Enable TACACS+ Authentication** checkbox.
Enable TACACS+ Logging	If enabled, all configuration changes over HTTP, HTTPS, SSH, Telnet, and System Console are logged. **Note:** Enable TACACS+ Authentication and Enable TACACS+ Logging can be independently enabled.
TACACS+ Server Address	Enter the TACACS+ server IP address to contact for authentication.
Shared Secret	Displays whether a password for TACACS+ authentication requests has been set.

Table 2-5 TACACS Settings (continued)

Item	Description
Edit Secret	Select the **Edit Secret** checkbox to allow you to set the shared secret password.
Shared Secret	Enter a password for the TACACS+ request. The client and the server must have the same secret.
Shared Secret (confirm)	Reenter the shared secret to confirm.
Server Timeout (in seconds)	Enter the amount of time that a TACACS+ server does not respond to a request and is deemed to be unavailable. Valid range is 1 to 100 seconds, default is 5 seconds.
TACACS+ Authentication Mode	Select a TACACS+ authentication mode from the drop-down list: ■ **ASCII**—The username is sent as part of the TACACS client request and the password is sent as part of the continue message. ■ **Password Authentication Protocol (PAP)**—Both username and password are sent as part of the request message. ■ **Challenge Handshake Authentication Protocol (CHAP)**—The password is used to calculate the response to a random challenge. Both the challenge and response are sent as part of the TACACS+ request message.
Enable TACACS+ Logging	Select the **Enable TACACS+ Logging** checkbox to enable logging for all configuration changes over HTTP, HTTPS, SSH, Telnet, and the system console.

Click **Submit**.

A message indicates that service will be temporarily interrupted.

Click **OK** to confirm

Disabling TACACS+ Services

1. To disable TACACS+ authentication, clear the **Enable TACACS+ Authentication** checkbox and click **Submit**.
2. To disable TACACS+ logging, clear the **Enable TACACS+ Logging** checkbox and click **Submit**.

Configuring Services

Use the Services Configuration page to customize the configuration of accessible services on the System.

- About SNMP Management
- About Mean Opinion Scoring (MOS)
- Using the Services Configuration Page

About SNMP Management

The EdgeMarc can be managed remotely by an SNMP network management system.



Tip
If you are using EdgeView Service Control Center (EdgeView SCC), and SNMP polling is enabled, SNMP v1 must be enabled and the community must be identical on both ends.

Figure 2-19 shows an example of the EdgeMarc configured for an SNMP Network.

Figure 2-19 SNMP Configuration Example

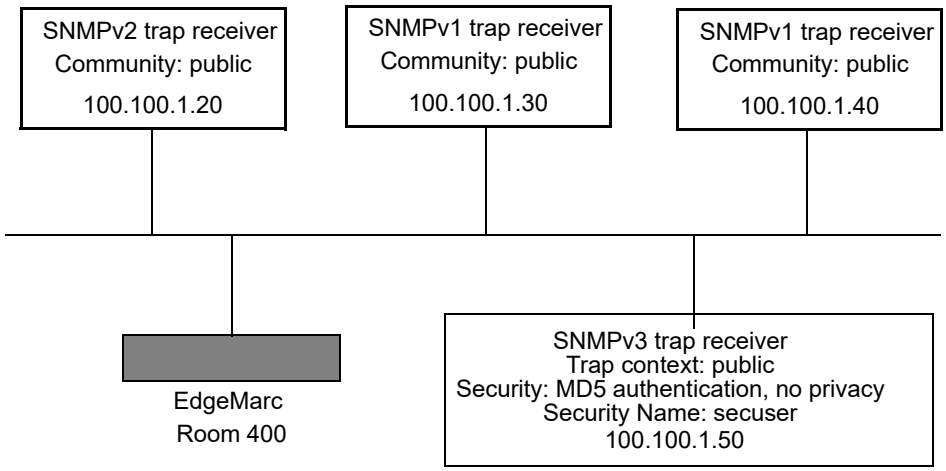


Table 2-6 lists SNMP management support.

Table 2-6 SNMP Support

Item	Description
SNMP	EdgeMarc SNMP version support. ■ SNMPv1— ■ Can be configured by itself or with SNMPv3. ■ Supports multiple SNMPv1 and SNMPv2 trap destination configurations. ■ Traps are sent to each of the configured destination using the appropriate protocol version and community string. See Configuring SNMPv1. ■ SNMPv2— ■ Supported as part of SNMPv1. ■ Choose **Show Trap Destinations** > **Add a Trap Destination** and enter "**2**" in the **Version** field to tell the EdgeMarc to send a message to every remote host in the list when errors are present. See Configuring SNMPv1. ■ SNMPv3— ■ Supports password-protected security. ■ Can be configured by itself or with SNMPv1. ■ Supports only one trap destination. See Configuring SNMPv3.
MIBS	EdgeMarc read-only MIB support.

Table 2-6 SNMP Support (continued)

Item	Description
	■ MIB-II (RFC 1213) ■ IF-MIB (RFC 2863) ■ SNMPv2-MIB (RFC 3418) ■ TCP-MIB (RFC 4022) ■ IP-MIB (RFC 2011) ■ UDP-MIB (RFC 4113) ■ SNMP-VIEW-BASED-ACM-MIB (RFC 3415) ■ SNMP-MPD-MIB (RFC 3412) ■ SNMP-USER-BASED-SM-MIB (RFC 3414) ■ SNMP-FRAMEWORK-MIB (RFC 3411)
Traps	EdgeMarc trap support. ■ coldStart ■ authenticationFailure ■ linkup ■ linkDown

About Mean Opinion Scoring (MOS)

Mean Opinion Score (MOS) is a numeric representation of the audio quality of a call, taking a value between 1.0 (worst) through 5.0 (best). It is a subjective measurement; a good MOS depends on the codec. For example, for G711 and G722 the top score is 4.5. For G729, the top score is 3.9.

The EdgeMarc MOS value is assigned to every call and for each direction of the call. This value is calculated by a mathematical formula that approximates real MOS scores. It is calculated using 10-second snippets of audio. The worst case 10-second period is logged at the end of the call.

Every time a call is started and terminated (and sometimes mid-call) a logging record is added to the VOS log file. The log file can viewed from the **Admin** > **System Information** page. Refer to Viewing System Information.

MOS scores are measured at the point that the audio (RTP) stream reaches the EdgeMarc. The scores calculated by the EdgeMarc make certain approximations:

- The same call (RTP stream) can sound different on different VoIP phones. Some phones do a better job than others at hiding errors in a stream. The MOS score, however, will be the same regardless of endpoint. So a given score can sound better or worse depending on the endpoint in use.

- A momentary packet loss in a stream may not be noticed by the user, but such a loss might result in low MOS score. A single low MOS score should not be assumed to mean poor quality for the user. A pattern of low scores across multiple calls is more significant.

What to look for in a low score:

- For outbound scores (VOIP phone to Network), this is a measurement of the handset and intervening local area network. A low score in this direction can mean a handset or network issue.
- For inbound scores (Network endpoint to VoIP phone), this is a measurement of the originating endpoint and full WAN path.

Using the Services Configuration Page

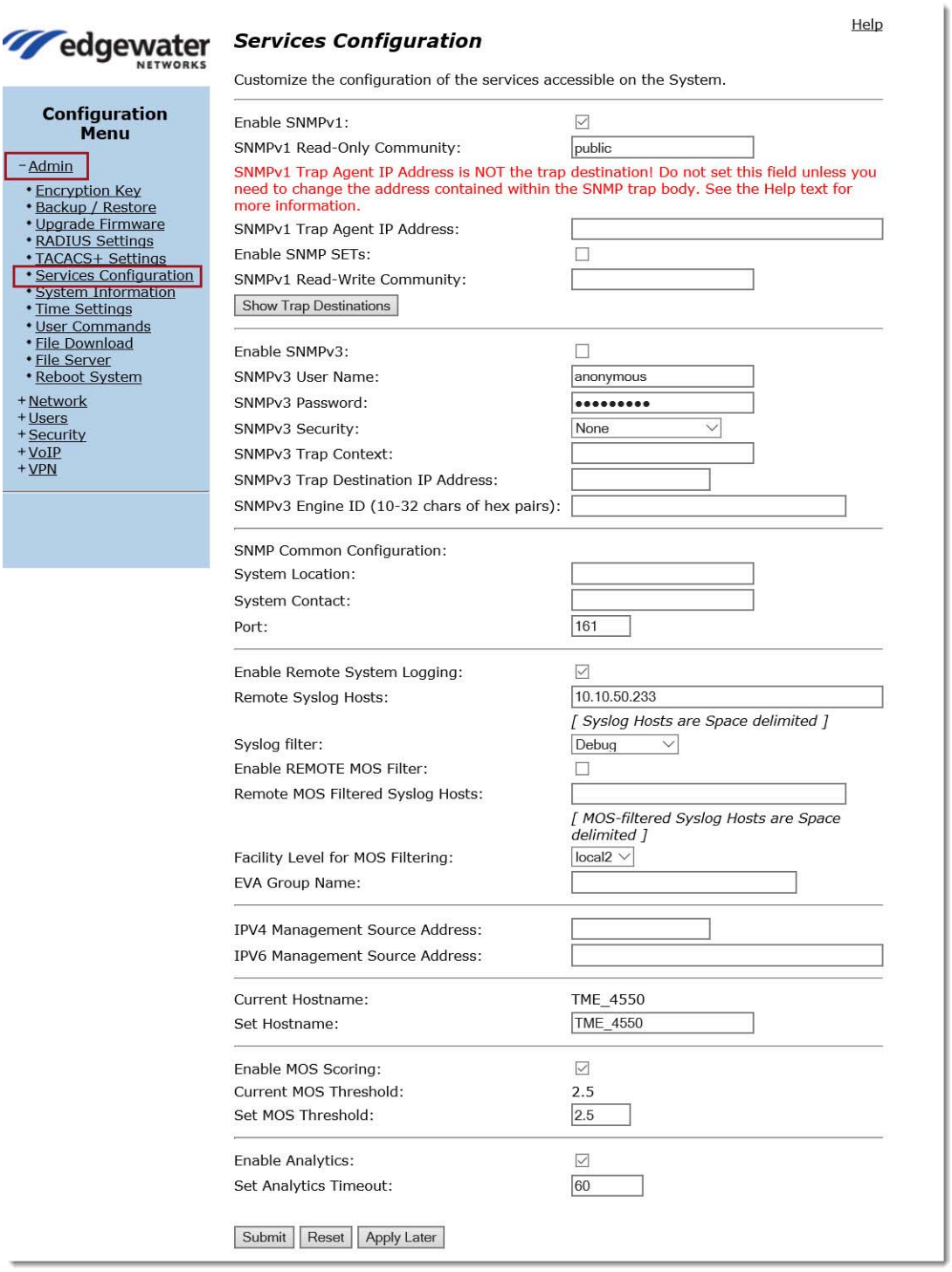
The following services are available on the Services Configuration page:

- Configuring SNMPv1
- Configuring SNMPv3
- Configuring SNMP Common Settings
- Configuring Remote System Logging
- Managing Source Address Settings
- Managing Hostname Settings
- Configuring Mean Opinion Score (MOS) Settings

To configure service settings:

1. Choose **Admin** > **Services Configuration** (Figure 3).

Figure 3 Services Configuration Page



2. Configure settings using the information in Table 2-7 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 2-7 Services Configuration

Item	Description
SNMPv1	
Configures settings for SNMPv1. See Configuring SNMPv1.	
Enable SNMPv1	Enables SNMPv1 services.
SNMPv1 Read-Only Community	Specifies the community string that the management station uses to access read-only objects from the system. SNMPv1 requires a read-only community string name in this field. For example: “Public”
SNMPv1 Trap Agent IP Address	Sends an SNMPv1 trap agent to this address. It is recommended that the IP address be one of the public addresses configured on the system. If this value has not been set, the agent uses the system WAN/Provider address. **Note:** SNMPv1 Trap Agent IP Address is *not* the trap destination. Do not set this field unless you need to change the address contained within the body of the SNMP trap.
Enable SNMP SETs	Enables SNMP SET messages that notify when the alarm threshold is exceeded. An SNMP set is a set of MIB objects used to monitor the performance of SNMP-enabled network devices. You can assign alarm thresholds to any performance object in an SNMP set.
SNMPv1 Read-Write Community	Specifies the community string that the management station uses to access read-write objects from the system.
Show Trap Destinations	
Manages SNMPv1 trap destinations.	
Add a Trap Destination	
IP Address	Specifies the IPv4 address. Specifying this address enables cold start, authentication and linkUp/linkDown SNMP traps.
Version	Specifies the SNMP version (1 or 2).
Community	Specifies the community string for one or more destinations that receive SNMP traps.

Table 2-7 Services Configuration (continued)

Item	Description
SNMPv3	
Configures settings for SNMPv3. See Configuring SNMPv3.	
Enable SNMPv3	Enables SNMPv3 services.
SNMPv3 User Name	Defines the SNMPv3 username for SNMPv3 User-based Security Model (USM) and View-based Access Control Model (VACM) control.
SNMPv3 Password	Authenticates the SNMPv3 user and encrypts the payload based on your SNMPv3 settings. Minimum password length is eight characters.
SNMPv3 Security	Sets the SNMPv3 security level for user authentication and encryption for synchronous requests and asynchronous traps. ■ None—Neither SNMPv3 authentication nor encryption are used. Default. ■ Auth(MD5)—Authenticates using the MD5 hash algorithm. ■ AuthPriv(MD5/DES)—Authenticates using the DES encryption algorithm.
SNMPv3 Trap Context	Sets the SNMPv3 trap context to any string.
SNMPv3 Trap Destination IP Address	Specifies the IPv4 address to send traps to. This address enables cold start, authentication, and linkUp/linkDown traps.
SNMPv3 Engine ID (10-32 chars of hex pairs)	Specifies a preferred engine ID. Every SNMP v3 agent has an engine ID which serves as a unique identifier for the agent. The engine ID is used with a hashing function to generate keys for authentication and encryption of SNMPv3 messages. If you do not specify an engine ID, one is generated when you enable the standalone SNMP agent. The SNMPv3 engine ID must contain between 10 and 32 characters of hexadecimal pairs.
SNMP Common Configuration	
Optional SNMP settings. See Configuring SNMP Common Settings.	
System Location	Specifies a comment string that can be used to indicate the location of the system. By default, no value is set.
System Contact	Specifies the administrative contact information for the system. By default, no value is set.

Table 2-7 Services Configuration (continued)

Item	Description
SNMP Port	Designates the port that the system monitors to read and send SNMP data. Default is 161.
Remote System Logging Settings	
See Configuring Remote System Logging.	
Note: You must configure remote system logging to use MOS scoring. See Configuring Mean Opinion Score (MOS) Settings	
Enable Remote System Logging	Allows syslog messages to be sent to a remote system.
Remote Syslog Hosts	Specifies the remote syslog host IP address of the system running a log server. The system sends to the default syslog port 514. The port cannot be changed. You can enter multiple syslog hosts by separating the IP addresses with a space. Entering multiple host names or IP addresses causes syslog messages to be sent to each of the specified systems. You must configure at least one remote syslog host to use MOS scoring.
Syslog Filter	Specifies the logging level for syslog service on the system. The priorities are: ■ Debug—Lowest priority, logs all levels. Default. ■ Informational ■ Notice ■ Warning ■ Error ■ Critical ■ Alert ■ Emergency—Highest priority, logs only Emergency level Choosing a higher priority excludes lower level syslog messages.
Remote MOS Filter Settings	
Remote MOS filter settings to allow the EdgeMarc to send mean opinion score (MOS) filtered syslog records to an individually defined syslog server that is separate from the server where regular system syslog messages are sent.	
See Configuring Remote System Logging.	
Enable REMOTE MOS Filter	Enables remote syslog MOS filtering.

Table 2-7 Services Configuration (continued)

Item	Description
Remote MOS Filtered Syslog Hosts	Specifies the IP address of the system running a system log server. Multiple IPs can be entered by separating them with spaces. The system sends to the default syslog port 514. The port cannot be changed.
MOS filter facility	Specifies the Syslog facility used to filter MOS records from the syslogs that are sent to the remote MOS filtered syslog hosts. Default is local2.
IPv4 Management Source Address IPv6 Management Source Address	Changes the source IP address for management data that originates from the system. The default is the system public WAN IP. This setting is generally left unchanged. In configurations where the system is acting as a router, the public IP addresses may be assigned to the LAN interface, not the WAN interface. If this field is left blank, syslog, FTP, TFTP, ICMP, and other data that originates from the system uses the non-routable WAN interface address by default. This setting can be used to change the WAN address for the Public LAN IP, or another interface created by the system as the public IP interface. This setting accepts the LAN_IP token, which automatically uses the configured LAN address from the Network page.
Current Hostname	Displays the current hostname for this system.
Set Hostname	Sets the hostname for this system. By default, the hostname is the system type. Once set, this information appears on the Administration home page. A valid host must take the following form: “ABC_company_4500” or “ABC-company-4500” You may enter multiple words to describe your system uniquely. However, you must separate them as shown in the example. Trailing characters must be alphanumeric. The system hostname is limited to 50 characters. See Managing Source Address Settings.
Mean Opinion Score (MOS) Settings	
Configures voice quality settings. See Configuring Mean Opinion Score (MOS) Settings.	

Table 2-7 Services Configuration (continued)

Item	Description
Enable MOS Scoring	Enables MOS scoring for media that is passing through the system. Disabling MOS scoring will improve system performance. By default, MOS scoring is Enabled.
Current MOS Threshold	Displays the current MOS threshold setting.
MOS Threshold	Sets the minimum allowable MOS for the system. MOS values below this value will cause system messages to be sent to the system log. By default, the value is 2.5.
Analytics Settings	
Enable Analytics	Select the checkbox to enable the feature. Prepares the system to gather SIP, Memory, and CPU utilization statistics. By default, analytics is Enabled. Statistics gathering is initiated after the first SNMP GET request is received by the system.
Set Analytics Timeout	Sets the timeout, in minutes, from the last SNMP GET request to disable statistics collection. Timeout values range from 2 to 1666666. By default, the value is 60 minutes.
PacketSmart Settings	
Refer to Figure 2-1.	
PacketSmart Entity ID	Uniquely identifies the PacketSmart agent. This is the ID that will be used in the PacketSmart GUI to locate this device and view its monitoring data. By default the Entity value is COMPANY_DEVMODEL_LANMAC.
PacketSmart Server	Allows communication with a PacketSmart server address, this field can be an IP or Domain Name. By default, the value is not set.
PacketSmart Port	Configures the specified port number to communicate with the PacketSmart server. Default is 80.
Capture Interface	Sets the interface name (used to monitor network traffic). By default, the value is eth0.
Network Interface	Sets the network interface name (used to communicate with PacketSmart Server). By default, the value is eth1.
Enable PacketSmart agent	Select the checkbox to enable the feature. This value is defined as packetsmart agent enable/disable functional control. By default, PacketSmart agent is Disabled.

Table 2-7 Services Configuration (continued)

Item	Description
EV Group Name	Enter the EdgeView group name within which EdgeMarc devices will reside. This overrides any entry of the EdgeMarc MAC address in the EdgeView database.

Click **Submit**.

A message indicates that service will be temporarily interrupted.

Click **OK** to confirm

Figure 2-1 Configuring PacketSmart Features

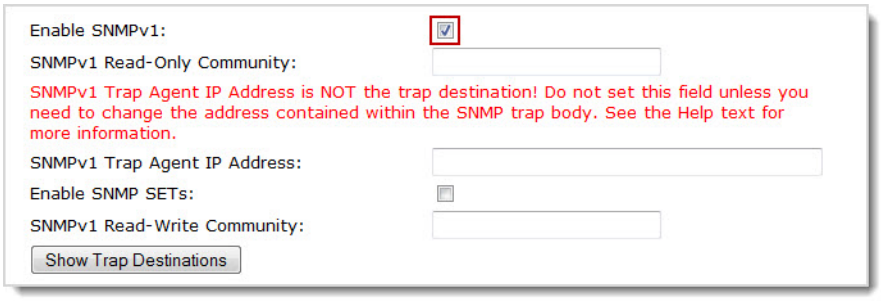


Configuring SNMPv1

Tip
Configure SNMPv1 by itself or with SNMPv3. See Configuring SNMPv3.

1. Choose **Admin** > **Services Configuration** (Figure 3).
2. Select the **Enable SNMPv1** checkbox (Figure 2-2).

Figure 2-2 SNMPv1 Configuration Settings



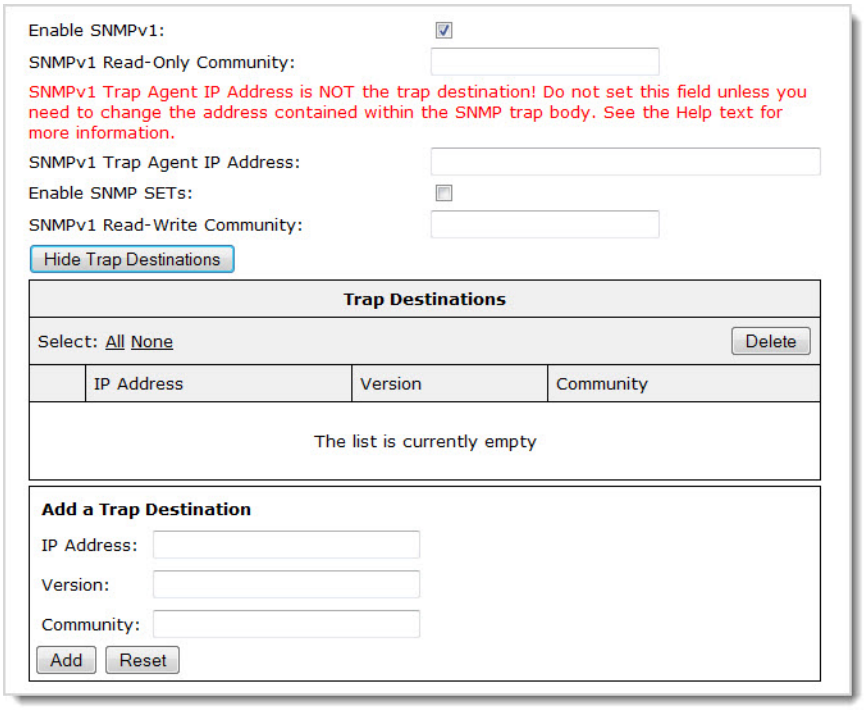
3. In the **SNMPv1 Read-Only Community** field, enter the community string that the management station uses when accessing read-only objects from the system.

4. In the **SNMPv1 Trap Agent IP Address** field, enter a public IP address for the trap agent field that receives an SNMPv1 trap. If this value is not set, the agent uses the system WAN/Provider address.

Note
SNMPv1 Trap Agent IP Address is *not* the trap destination. Do not set this field unless you need to change the address contained within the body of the SNMP trap. See Step 7 to configure the trap destination IP address.

5. Select the **Enable SNMP SETs** checkbox to turn on SET messages that notify when the alarm threshold is exceeded.
6. In the **SNMPv1 Read-Write Community** field, enter a community string that the management station uses to access read-write objects from the system.
7. Click **Show Trap Destinations** to define the IPv4 address, SNMP version (1 or 2), and community string for one or more destinations that will receive SNMP traps (Figure 2-3).

Figure 2-3 Show Trap Destinations



a. In **Add a Trap Destination**, enter information in the fields provided:
   - **IP Address**—IPv4 address. Specifying this address enables cold start, authentication and linkUp/linkDown SNMP traps.
   - **Version**—SNMP version (1 or 2)

- **Community**—Community string for one or more destinations that receive SNMP traps.

b. Click **Add**. Your entry appears in the Trap Destinations table.

Deleting a Trap Destination

1. To delete a Trap Destination, select checkboxes for the entries that you want to delete; click **All** to choose all entries or click **None** to clear your selections.
2. Click **Delete**.

   A message indicates that service will be temporarily interrupted.
3. Click **OK** to confirm.
4. Click **Hide Trap Destinations** to remove the Trap Destinations window.

Proceed to the following:

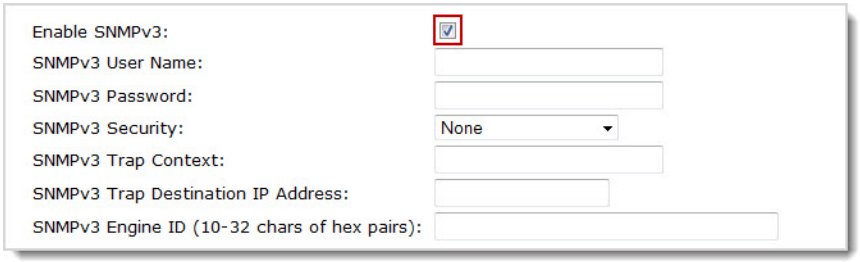
- If you are configuring SNMPv3, proceed to Configuring SNMPv3.
- If you are not configuring SNMPv3, proceed to Configuring SNMP Common Settings.

Configuring SNMPv3

Tip
Configure SNMPv3 by itself or with SNMPv1. See Configuring SNMPv1.

1. Choose **Admin** > **Services Configuration** (Figure 3).
2. Select the **Enable SNMPv3** checkbox (Figure 2-4).

Figure 2-4 SNMPv3 Configuration Settings



3. In the **SNMPv3 User Name** field, enter the SNMPv3 username for SNMPv3 User-based Security Model (USM) and View-based Access Control Model (VACM) control.
4. In the **SNMPv3 Password** field, enter a password to authenticate the user encrypt the payload based on the SNMPv3 Security setting below. Minimum password length is 8 characters.
5. Choose an SNMPv3 security level from the **SNMPv3 Security** drop-down list. This is used for user authentication and for encrypting

synchronous requests and synchronous and asynchronous traps. Default is None.

6. In the **SNMPv3 Trap Context** field, enter any string.
7. In **SNMPv3 Trap Destination IP Address** field, enter the IPv4 address to send SNMPv3 traps to. Specifying this address enables cold start, authentication, and linkUp/linkDown SNMPv3 traps.
8. In the **SNMPv3 Engine ID (10-32 chars of hex pairs)** field, enter a string that contains between 10 and 32 characters of hexadecimal pairs. If an Engine ID is not entered, the system generates one automatically. The ID may be needed by some trap clients that enforce a strict version of SNMPv3 authentication.
9. Proceed to Configuring SNMP Common Settings.

Configuring SNMP Common Settings

1. Choose **Admin** > **Services Configuration** (Figure 3).
2. Scroll to **SNMP Common Configuration** (Figure 2-5).

Figure 2-5 SNMP Common Configuration



3. In the **System Location** field, enter a comment string that can be used to indicate the location of the system. This field is blank by default, no value is set.
4. In the **System Contact** field, enter administrative contact information for the system. This field is blank by default, no value is set.
5. Leave the default SNMP port 161 in the **Port** field. The system monitors Port 161 to read and send SNMP data.
6. Proceed to Configuring Remote System Logging.

Disabling SNMP

1. Choose **Admin** > **Services Configuration** (Figure 3).
2. Clear the **Enable SNMPv1** and **Enable SNMPv3** checkboxes.
3. Click **Submit**.

   A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

Deleting an SNMP Trap

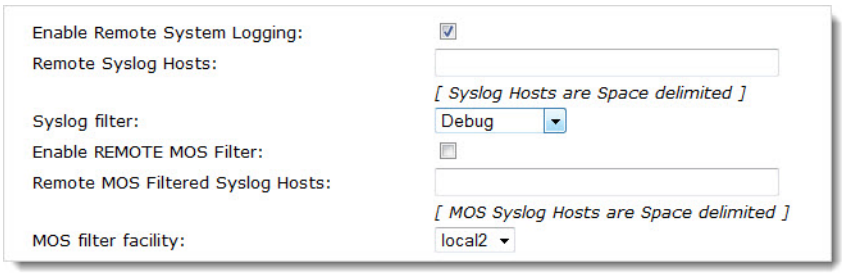
1. Choose **Admin** > **Services Configuration** (Figure 3).
2. Click the wastebasket icon for the trap.
3. Click **Delete**.

Configuring Remote System Logging

You must configure remote system logging to use MOS scoring. See Configuring Mean Opinion Score (MOS) Settings.

1. Choose **Admin** > **Services Configuration** (Figure 3).
2. Select **Remote System Logging** checkbox (Figure 2-6).

Figure 2-6 Remote System Logging Settings



3. In the **Remote Syslog Host** field, enter the IP address of the system running the system log server. Multiple IPs can be entered by separating IPs with a space. You can also enter a fully qualified domain name (FQDN). The system sends to syslog port 514 by default.
4. Choose a logging level for the syslog service from the **Syslog Filter** drop-down list. The default priority is Debug.
5. Select the **Enable REMOTE MOS Filter** checkbox to enable remote syslog MOS filtering. This allows the EdgeMarc to send mean opinion score (MOS) filtered syslog records to an individually defined syslog server.
6. In the **Remote MOS Filtered Syslog Hosts** field, enter the IP address of the system running the system log server. Enter multiple IPs by separating them with a space. The system sends to the default syslog port 514. The port cannot be changed.
7. Choose a MOS filter facility type from the **MOS filter facility** drop-down list. This filters MOS records from the syslogs that are sent to the remote MOS filtered syslog hosts. Default is local2.

Managing Source Address Settings

1. Choose **Admin** > **Services Configuration** (Figure 3).
2. Scroll to **Management Source Address** (Figure 2-7).
3. In the **Management Source Address** field, enter the system public WAN IPv4 or IPv6 source address to manage data that originates from the system. This field is generally not changed. Default is the system public WAN IP.

Figure 2-7 Management Source Address



Managing Hostname Settings

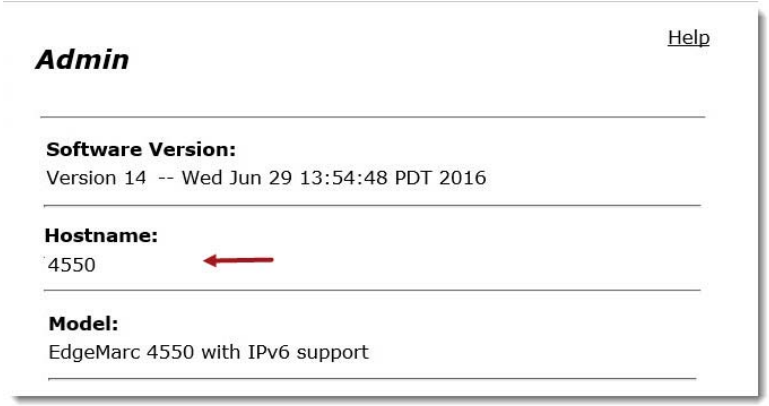
1. Choose **Admin** > **Services Configuration** (Figure 3).
2. Scroll to hostname settings. The current hostname is displayed in the Current Hostname field.
3. Enter a new hostname for the system in the **Set Hostname** field (Figure 2-8). The system hostname is limited to 50 characters and must observe the following format: “ABC_company_4500” or “ABC-company-4500.”

Figure 2-8 Hostname Settings



Once set, this name becomes the Hostname on the Administration home page, as shown in Figure 2-9.

Figure 2-9 Administration Page - Hostname



Configuring Mean Opinion Score (MOS) Settings

Tip
You must configure remote system logging to use MOS scoring. See Configuring Remote System Logging.

1. Choose **Admin** > **Services Configuration** (Figure 3).
2. Scroll to **Enable MOS Scoring** (Figure 2-10).

Figure 2-10 MOS Scoring Settings



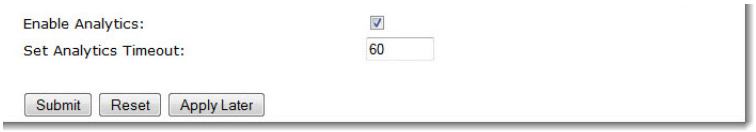
3. Select the **Enable MOS Scoring** checkbox. MOS scoring is enabled by default. Disabling MOS scoring improves system performance.
4. In the **Set MOS Threshold** field, enter the minimum MOS threshold allowed for the system. By default, the value is 2.5. MOS values set below this cause system messages to be sent to the system log.

   The **Current MOS Threshold** field shows the current MOS threshold for this system.
5. Click **Submit**. The new value appears in Current MOS Threshold.
6. To save all settings on the page, click **Submit All**.

Configuring Analytics

1. Choose **Admin** > **Services Configuration** (Figure 3).
2. Scroll to **Enable Analytics** (Figure 2-11).

Figure 2-11 Analytics Settings



3. Select the **Enable Analytics** checkbox to prepare the system to gather SIP, Memory, and CPU utilization statistics. Statistics gathering is initiated after the first SNMP GET request is received by the system.Analytics are enabled by default. Analytics is enabled by default.
4. Enter a value in the **Set Analytics Timeout** field to set the timeout, in minutes, from the last SNMP GET request to disable statistics collection. Timeout values range from 2 to 1666666. By default, the value is 60 minutes.

Configuring an EdgeView Group Name

The **EdgeView Group Name** field allows you to input the EdgeView Service Control Center (EdgeView SCC) group name within which the EdgeMarc will reside. This overrides any entry of the EdgeMarc MAC address in the EdgeView database. To configure the feature:

1. Choose **Admin** > **Services**.
2. Scroll to the **EdgeView Group Name** field.
3. Enter an EdgeView group name and click **Submit**.

Configuring PacketSmart Services

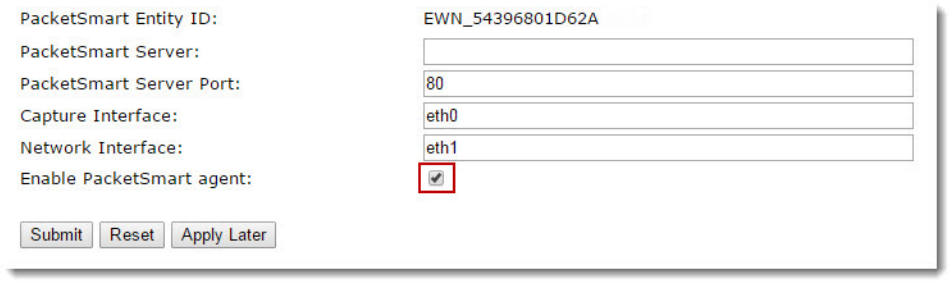
Note
PacketSmart services are supported on the EdgeMarc 4700 Series and the EdgeMarc 7301.

To configure the feature:

1. Choose **Admin** > **Services Configuration** (Figure 3).
2. Scroll to **PacketSmart Entity ID** (Figure 2-12).

   The PacketSmart Entity ID uniquely identifies the PacketSmart agent. This is the ID that will be used in the PacketSmart GUI to locate this device and view its monitoring data. By default the Entity value is COMPANY_DEVMODEL_LANMAC.

Figure 2-12 PacketSmart Services



3. Enter an IP address or a domain name in the **PacketSmart Server** field to set up communication with the PacketSmart server. By default, the value is not set.
4. Enter a port in the **PacketSmart Port** field. This allows the specified port number to communicate with the PacketSmart server. The default is 80.
5. Enter a name in the Capture Interface field to monitor network traffic. By default, the value is eth0.
6. Enter a name in the **Network Interface** field to set the name of the network that communicates with the PacketSmart Server. By default, the value is eth1.

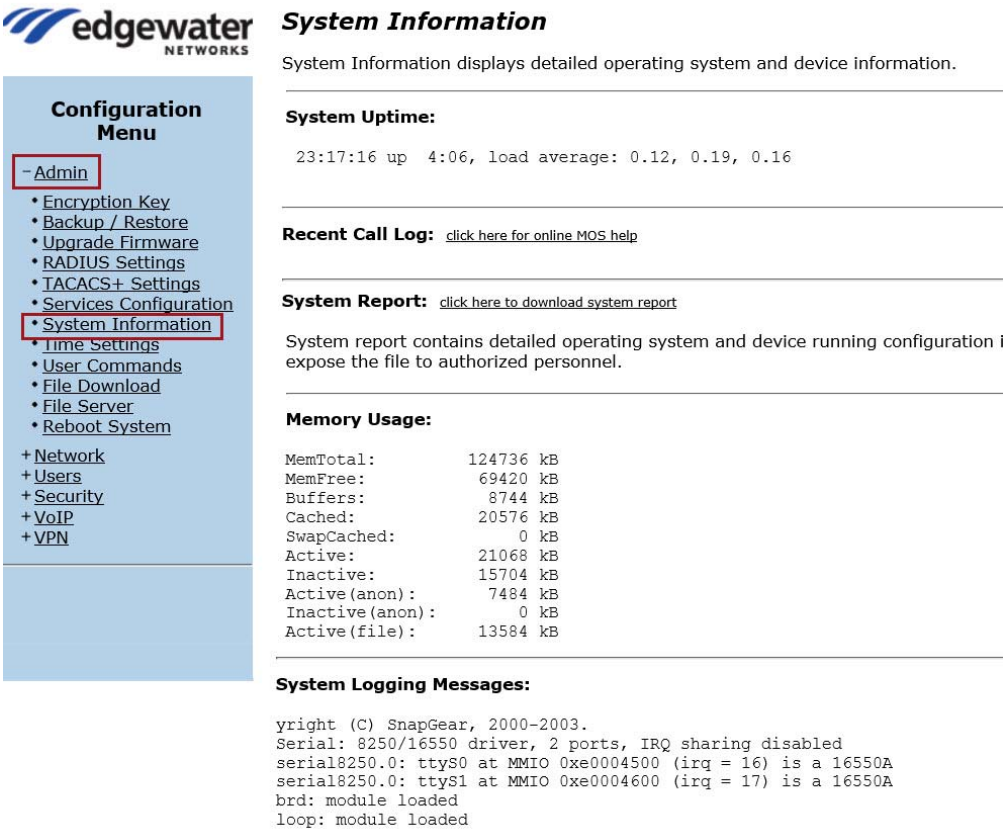
7. Select the Enable PacketSmart agent checkbox to enable the feature. By default, the PacketSmart agent is disabled.
8. Click **Submit** to save your settings.

Viewing System Information

Use the System Information page to view detailed operating system and device information.

1. Choose **Admin** > **System Information** (Figure 2-13).

Figure 2-13 System Information Page



2. View system performance using the information in Table 2-8 as a guide.

Table 2-8 System Information

Item	Description
System Uptime	Shows the current time, the amount of time elapsed since the last system reboot, and the system load averages for the past 1, 5, and 15 minutes. Uptime can help trace when a power outage may have interrupted service. Load averages that remain greater than 2 indicate excessive system loading. Partitioning voice traffic using a second system may be required. **Note:** If you see the system in this state, note the following information and contact your customer support representative: ■ Load average ■ Process Information ■ Memory usage ■ Firmware version (from the Admin page) ■ Platform type (from Admin page)
Number of Active Streams	Indicates how many calls are using the WAN link. Calls that are in progress and between two devices on the system LAN are not counted in this number.
Recent Call Log	Displays quality information for calls that are in progress or have recently completed. If a call falls below the configured MOS threshold, a system log message is created. The MOS score for a call is always displayed when the call is completed. Detailed statistics for the call are reported in the Advanced MOS syslog message. For a description of the fields in the Advanced MOS syslog message, click the **click here for online MOS help** link to access MOS troubleshooting information in the Edgewater Networks Knowledgebase.
System Report	Click the link provided to download a text file named “sysreport.txt” that you can view or save to your system. The system report contains detailed operating system and device running configuration information. **Note:** Only expose this file to authorized personnel.
Process Information	Describes active processes in the EdgeMarc.

Table 2-8 System Information (continued)

Item	Description
Memory Usage	Describes detailed memory allocation information.
System Logging Messages	Displays information logged during system boot and normal operation. Logging messages may include information about unauthorized attempts to access the EdgeMarc, process restart messages, and excessive resource utilization messages.

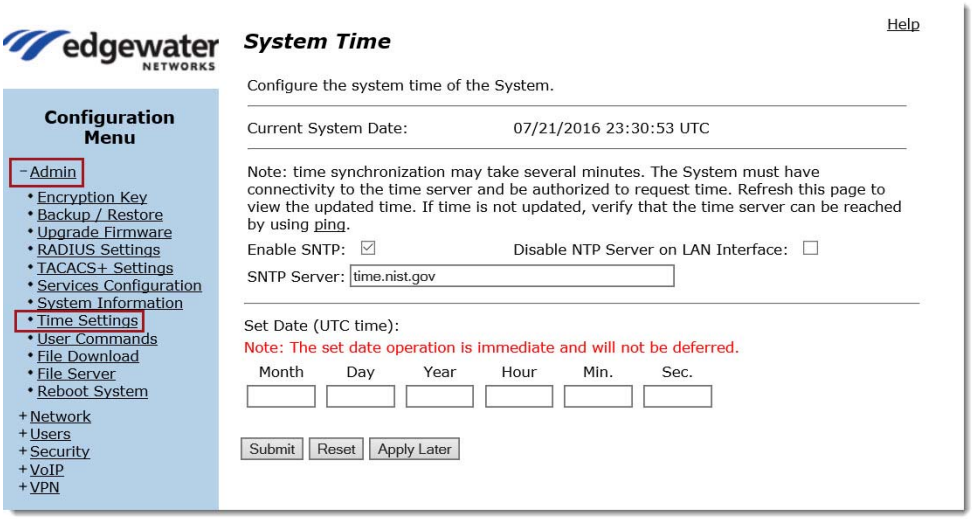
Configuring Time and Date Settings

Note
Time synchronization may take several minutes. The System must have connectivity to the time server and be authorized to request time. Refresh this page to view the updated time. If time is not updated, verify that the time server can be reached by clicking the **Ping** link provided or choose **Network** > **Network Test Tools** and refer to Using Network Test Tools in Chapter 3, *Network Deployment*.

To configure time settings:

1. Choose **Admin** > **Time Settings** (Figure 2-14).

Figure 2-14 System Time Page



2. Configure settings using the information in Table 2-9 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 2-9 System Time Parameters

Item	Description
Enable SNTP	Select the **Enable SNTP** checkbox to enable the Simple Network Time Protocol (SNTP) to synchronize your EdgeMarc clock on the network.
SNTP Server	Enter the SNTP server address, either an IP address or the SNTP server DNS name. For example, “time.nist.gov.” Refer to NIST Internet Time Servers (ITS) for more information.
Disable NTP Server on LAN Interface	Select the checkbox to disable the NTP server service on the system. This field is available only when Enable SNTP is selected. **Note:** Check **Enable SNTP** and un-check the **Disable NTP Server on LAN Interface** checkbox if your system is required to provide local NTP services.
Set Date (UTC time)	Enter specific day and time numeric values in the fields provided: ■ Month range—1 to 12 ■ Day range—1 to 31 ■ Year range—1970 to 2034 ■ Hour range—0 to 23 ■ Minute range—0 to 59 ■ Second range—0 to 59

Click **Submit**.

A message indicates that service will be temporarily interrupted.

Click **OK** to confirm

Your date changes take effect immediately upon **Submit**.

Configuring Settings With User Commands

Use the User Commands page to enter specialized commands or enable features that are not available through other Configuration Menu pages.

Before You Begin

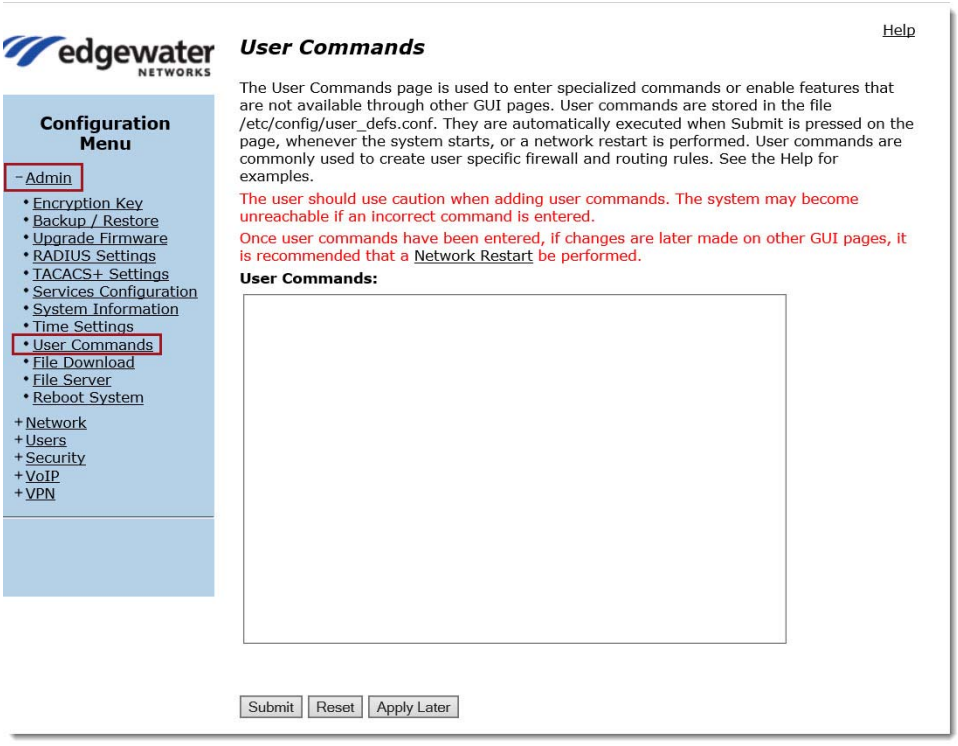
User commands should only be entered when following instructions in an Edgewater Networks Knowledgebase article or by request of Edgewater support.

Caution
The system may become unreachable if an incorrect command is entered.

Using the User Commands Page

1. Choose **Admin** > **User Commands** (Figure 2-15).

Figure 2-15 User Commands Page



2. Enter commands in the User Commands area, as shown in Figure 2-15. Enter each command on a new line.

   User commands are stored in the file /etc/config/user_defs.conf. They are automatically executed whenever the device starts or a Network

Restart is performed. User commands are commonly used to create user specific firewall and routing rules.

User command examples:

```
ifconfig eth0:20 192.100.20.10 netmask 255.255.255.0

iptables -I POSTROUTING -t nat -s 192.168.20.10 -j ACCEPT
```

3. Click **Submit**.

   A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.
5. When you have finished entering commands, perform a Network Restart. See **Network** > **Network Restart** and refer to Initiating Network Restart in Chapter 3, *Network Deployment*.

Managing File Download

File Download allows the EdgeMarc to download files from a central FTP server and store them locally. These files can then be served out by the local TFTP or HTTP servers.

The File Download feature works in conjunction with the File Server feature. The files requested for download cannot be stored locally until a RAMDISK is created by the File Server feature. See Configuring File Server Settings.

When using FTP, File Download logs into the FTP server as the “anonymous” user. File Download assumes the files reside in the /pub directory of the FTP server.

When serving files using HTTP, only the files that are listed on the File Download page can be served out by the HTTP server. Files that are pushed to the local system RAMDISK by an external management system are not available for HTTP download.

VOS software is available on the Edgewater Networks FTP site ftp.edgewaternetworks.com. It is recommended that you reboot your EdgeMarc prior to doing the upgrade. This is to make sure there is enough dynamic memory available to handle the upgrade process. Refer to the following sections for more information:

- Upgrading Firmware
- Rebooting the System

When you update your software, telephone services are unavailable for several minutes. It is therefore advised that upgrades be performed during a maintenance window when telephone traffic can be interrupted.

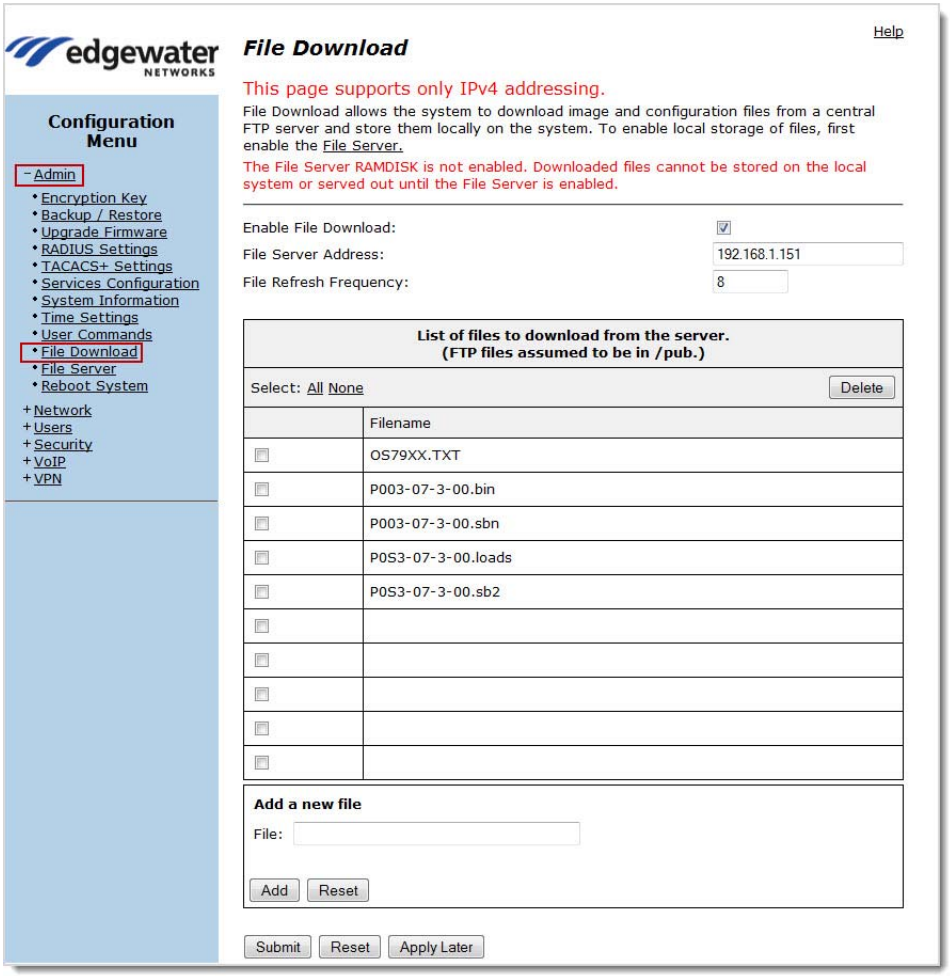
Before You Begin

To use file download, the file server RAMDISK must be enabled. Downloaded files cannot be stored on the local system or served out until the file server is enabled. See Managing the File Server before you download files.

Downloading Files

1. Choose **Admin** > **File Download** (Figure 2-16).

Figure 2-16 File Download Page



2. To enable local file storage, you must enable the File Server. Click **File Server** to open the File Server page and refer to Managing the File Server to configure settings.

3. Return to the File Download page and configure settings using the information in Table 2-10 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 2-10 File Download Parameters

Item	Description
Enable File Download	Select the **Enable File Download** checkbox.
File Server Address	Enter the remote FTP server IP address. For example: ftp.edgewaternetworks.com
File Refresh Frequency	Enter a value in hours that the system contacts the remote FTP server to refresh files.
List the Files to Download from the Server	Displays a list of files that are available to download from the remote server. FTP files are assumed to be in /pub. Enter file names in any of the following formats: ■ <filename> space <filename> or ■ <filename> ■ <filename>
Add a new file	Enter a new file to download in the **File** field. All files must be in the /pub directory on the FTP server. For example: /pub/e_4570/
	Click **Submit**. A message indicates that service will be temporarily interrupted. Click **OK** to confirm

Deleting a File

To delete a file from the table:

1. Select the checkbox of the file entry that you want to delete or click **All** to choose all the entries.
2. Click **Delete**.
3. Click **OK** to confirm.

Managing the File Server

Use the File Server page to enable and configure FTP and/or TFTP file servers on the system. The file servers are used to store phone configuration information.

Note
Files that are stored on the server are stored in RAM. These files are lost when the system is rebooted or when you click **Submit**.

Tip
Enabling the TFTP server disables the default TFTP ALG.

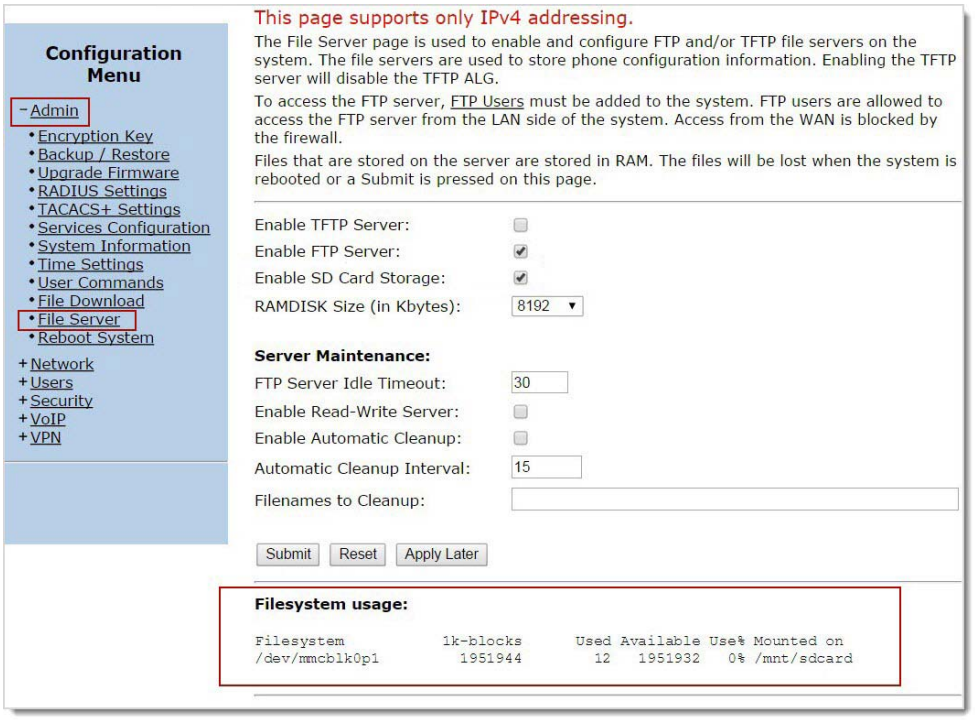
To access the FTP server, FTP Users must be added to the system. FTP users are allowed to access the FTP server from the LAN side of the system. Access from the WAN is blocked by the firewall. To access the FTP Users page, click the **FTP Users** link on the File Server page and refer to Managing FTP Users.

Tip
Configure the settings on this page before downloading files in Managing File Download.

Configuring File Server Settings

1. Choose **Admin** > **File Server** (Figure 2-17).

Figure 2-17 File Server Page



2. Add FTP Users to the system. Click **FTP Users** to open the FTP Users page and refer to Managing FTP Users to configure settings.
3. Return to the File Server page and configure settings using the information in Table 2-11 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 2-11 File Server Parameters

Item	Description
Enable TFTP Server	(Optional) Select the **Enable TFTP Server** checkbox to download files stored in the local RAMDISK using the TFTP protocol. Files that are stored in the local RAMDISK can be downloaded from the system using the TFTP protocol. The system provides an ALG function for the TFTP protocol; TFTP ALG is enabled by default and the TFTP server is disabled. Enable either the TFTP ALG or the TFTP server. You can enable either the FTP or the TFTP server or both servers to download configuration and image files from the system.
Enable FTP Server	Select the **Enable FTP Server** checkbox to download files stored in the local RAMDISK using the FTP protocol. This setting is required for basic file download. Files that are stored in the local RAMDISK can be downloaded from the system using the FTP protocol. Required for basic file download. Default is disabled. **Tip:** The FTP protocol requires an account username and password, which is created from the FTP User page. See the following sections for more information: ■ Managing the File Server ■ Managing File Download
Enable SD Card Storage	Some EdgeMarc devices have an SD card slot to allow the EdgeMarc to save backup and restore configuration information to a 32 GB SD card, 4 GB per file. Click the checkbox to enable and view file system usage in the box at the bottom of the page.
RAMDISK Size	Choose a storage size allowance for your system for downloaded files in the **RAMDISK Size (in Kbytes)** drop-down list. Files that are pushed or downloaded to the system are stored in a temporary RAMDISK. A limited amount of system RAM is available to store these files: ■ 512Kbps ■ 1024Kbps ■ 2048Kbps ■ 4096Kbps ■ 8192Kbps ■ 16384Kbps

Table 2-11 File Server Parameters (continued)

Item	Description
Server Maintenance	
Monitors FTP session activity. See Managing Server Maintenance.	
FTP Idle Timeout	Enter the amount of time before an FTP session times out and is terminated. Once an FTP session is established with the FTP server, the server monitors the session for activity. When there are no requests for information or data transfers in progress, the session is idle. If the session is idle for longer than the configured timeout, the session is terminated. Default is 30 seconds.
Enable Read-Write Server	Select the **Enable Read-Write Server** checkbox to allow server files to be uploaded via FTP. Default is disabled, read-only.
Enable Automatic Cleanup	Select the **Enable Automatic Cleanup** checkbox to ensure that files listed in Filenames to Cleanup field are automatically deleted from the server to conserve space on the server. The files stored on the RAMDISK will be lost. **Note:** If the server file system fills up, phone configuration and image files could be lost.
Automatic Cleanup Interval	Enter the time interval for files listed in the Filenames to Cleanup field to be removed. Default cleanup interval is 15 minutes.
Filenames to Cleanup	Enter files to the list of files to clean up. The filename can include wild cards such as an asterisk (*). For example, to remove all log files, enter ***.log**.
File system usage	
Displays how much of the storage of the RAMDISK is currently in use. If the file system is nearing capacity, consider deleting unneeded files or increasing the size of the RAMDISK.	
Files on server	
Displays the size (in Kbytes) and names of the files currently stored on the server. The files shown include those configured on the File Download page and the files that are pushed to the system by the management system.	

Table 2-11 File Server Parameters (continued)

Item	Description
	Click **Submit**. A message indicates that service will be temporarily interrupted. Click **OK** to confirm Proceed to Managing Server Maintenance.

Managing Server Maintenance

Once an FTP session is established with the FTP server, the server monitors the session for activity.

1. Choose **Admin** > **File Server** (Figure 2-17).
2. In **Server Maintenance** (Figure 2-18), configure settings using the information in Table 2-11 as a guide.

Figure 2-18 Server Maintenance Configuration



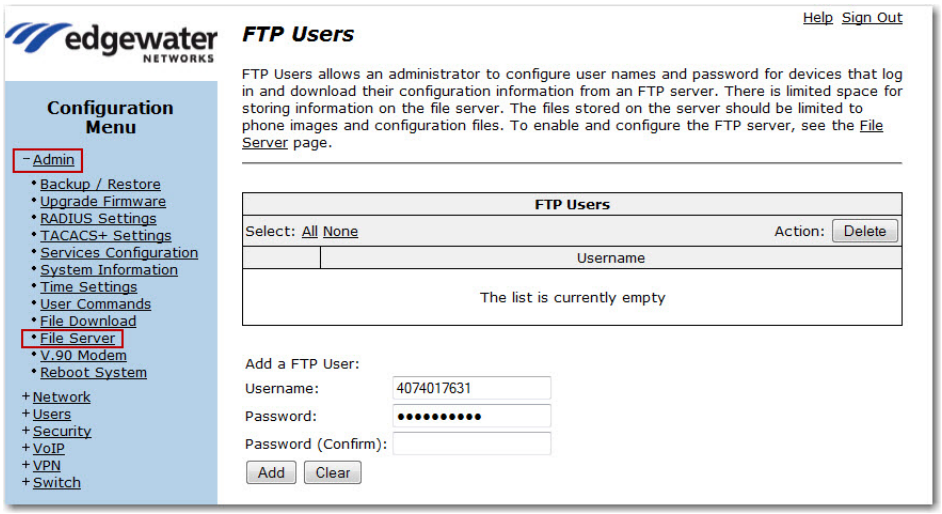
3. Click **Submit** to save your settings.

Managing FTP Users

Use the FTP Users page to configure user names and passwords for devices that log in and download their configuration information from an FTP server. There is limited space for storing information on the file server; files stored on the server should be limited to phone images and configuration files only.

1. Choose **Admin** > **File Server** (Figure 2-17).
2. Click **FTP Users** on the File Server page to open the FTP Users configuration page (Figure 2-19).

Figure 2-19 FTP Users Page



3. Configure settings using the information in Table 2-12 as a guide. When you are done making changes on the page, click **Add** to make your settings take effect.

Table 2-12 FTP Users Page Parameters

Item	Description
FTP Users	
Manages FTP users on the system.	
Add an FTP User	
Adds a username and password for FTP authentication.	
Username	Enter the username for FTP server authentication. The username must be 3 to 20 characters long and can contain the following characters: Uppercase (A) though (Z); lowercase (a) through (z); the numbers (0) through (9); and the characters (-) and (_). **Note:** FTP usernames are for FTP support only. These usernames do not have access to any other management services. The root user has administrator privileges. For this reason, the FTP server does not allow access to the server from the root account. FTP User and RADIUS usernames must be mutually exclusive; using the same username for FTP and RADIUS may prevent logins to both services. The FTP server does not support RADIUS authentication.

Table 2-12 FTP Users Page Parameters (continued)

Item	Description
Password Password (Confirm)	Enter an FTP server authentication password. A password can contain any 7-bit ASCII character. The password must be 5 to 20 characters long.

Click **Add**. The new FTP user appears in the FTP Users table.

To return to the File Server page, click **File Server** on the FTP Users page.

Deleting an FTP User

1. Select the checkbox of the username entry that you want to delete or click **All** to choose all the entries.
2. Click **Delete**. The username entry is deleted from the FTP Users table.

Configuring the SD Card

Some EdgeMarc devices are equipped with an SD card slot to allow the EdgeMarc to save more syslog information and store more files with the File Server feature. SD cards with a maximum storage capacity of 32 GB are supported. The file size limit is 2 GB. SD card capabilities are configured from the EdgeMarc GUI or from the CLI. SD card capability is disabled by default and if your EdgeMarc device does not have an SD card slot, the configuration option will not be visible in the GUI.

Before you Begin

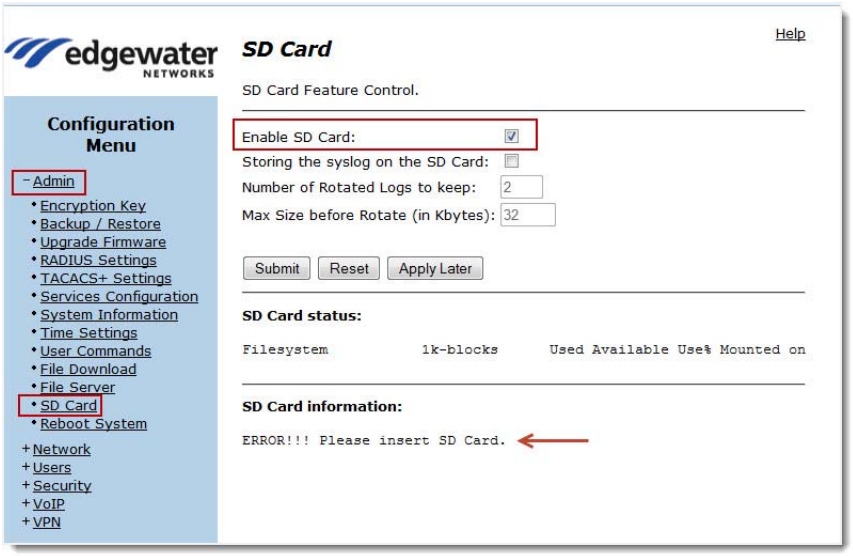
- The SD card should be inserted into the SD card slot and mounted on the system.
- If the SD Card feature is enabled before the card is inserted, the feature needs to be disabled and then re-enabled from the configuration GUI.
- The SD Card feature should be disabled before the card is removed from the SD card slot.

Warning
It is not recommended to remove the SD card while it is mounted and in use. Data may be lost, the system may crash, and the system may require a reboot before a re-inserted card can be remounted.

Enabling the SD Card

1. Insert an SD card into the EdgeMarc 4700 Series SD card slot.
2. Choose **Admin** > **SD Card** (Figure 2-20).

Figure 2-20 Enable the SD Card



3. Select the **Enable SD Card** checkbox and click **Submit**.
4. Proceed to Managing the SD Card

Warning

When the SD Card feature is enabled and the SD card is mounted, the default Admin page displays a warning upon login that the SD card is enabled and that system performance may be degraded. The CPU is needed when logging or writing capture files to disk, which can reduce data throughput and system call capacity.

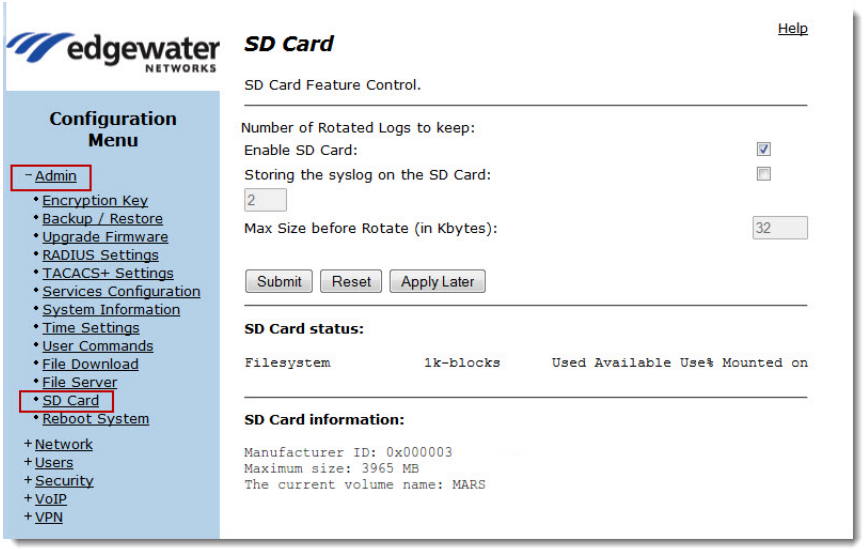
If there is no SD card present on the system, an error message is issued in the SD Card information window.

Managing the SD Card

To manage the SD card:

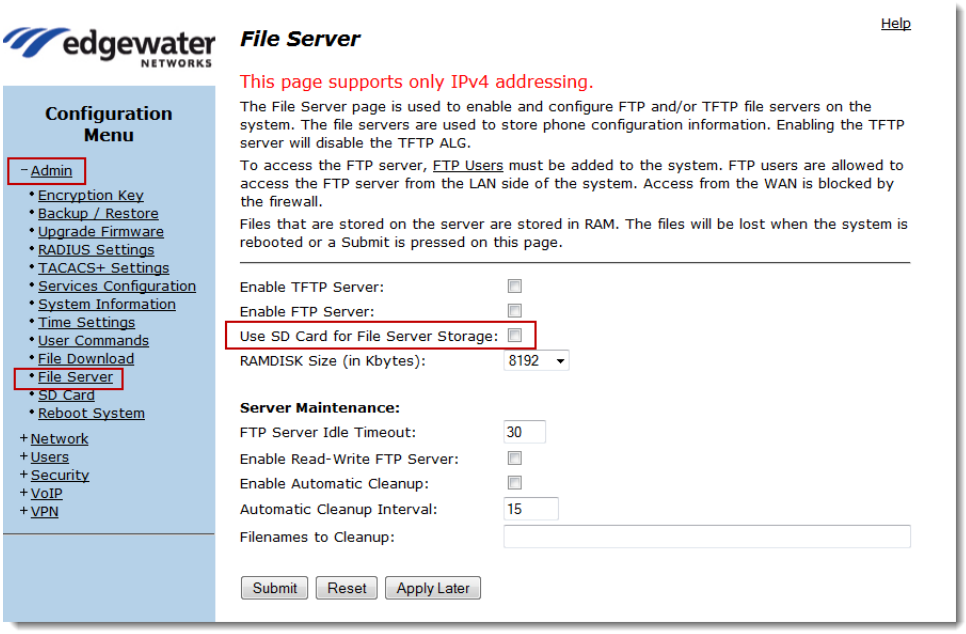
1. Choose **Admin** > **SD Card** (Figure 2-21).
2. If you have not already done so, select the **Enable SD Card** checkbox and click **Submit**.

Figure 2-21 Managing the SD Card



3. Select the **Storing the Syslog on the SD Card** checkbox to store syslog data locally on the system. Larger syslog files can be saved and backed up and older copies of the syslog file can be retained. The following fields become active:
   - **Number of Rotated Logs to keep**—Enter the number of log files to be automatically rotated. This feature is designed to ease administration of systems that generate large numbers of log files.
   - **Max Size before Rotate (in Kbytes)**—Enter the number of log files to be automatically rotated when they grow bigger than the set maximum size.
4. Click **Submit** to save your settings.
5. View the following information on the SD Card page (Figure 2-21):
   - **SD Card Status**—SD card status information like the amount of SD card storage space currently in use, whether the card is mounted or unmounted, and output for the disk free **df** command.
   - **SD Card Information**—Physical SD Card information such as the manufacturer ID, maximum size, and volume name.
6. Choose **Admin** > **File Server** and view active SD Card information on the File Server configuration page (Figure 2-22).

Figure 2-22 File Server Configuration Page



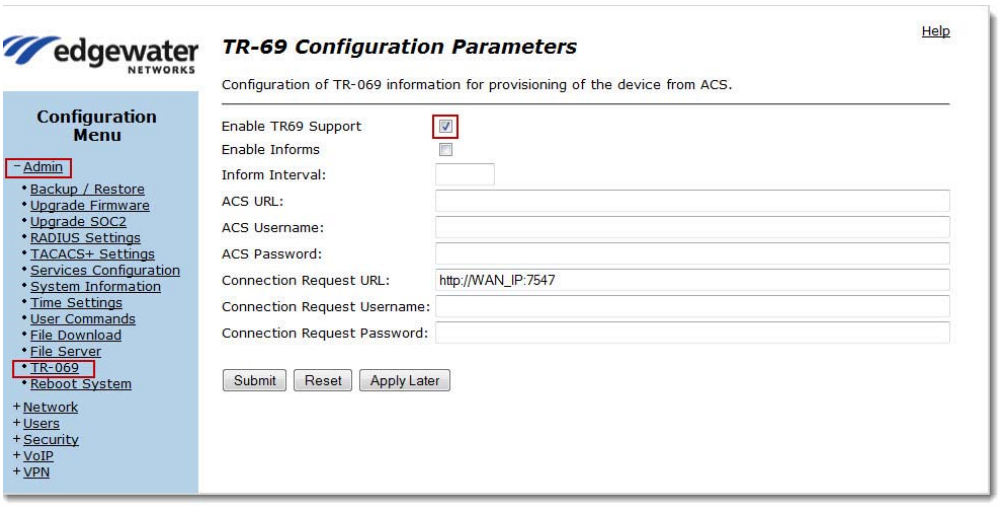
Configuring Technical Report-069 Parameters

Configure the TR-069 application layer protocol for remote management of end-user devices with Auto Configuration Servers (ACS).

Tip
TR-069 is supported on the EdgeMarc 250 Series.

1. Choose **Admin** > **TR-069**.
2. Select the **Enable TR69** checkbox and click **Submit** to activate TR-69 Configuration Parameters configuration fields (Figure 2-23).

Figure 2-23 TR-69 Configuration Parameters Page



3. Configure settings using the information in Table 2-13 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 2-13 TR-69 Configuration Parameters

Item	Description
Enable TR-069 Support	Select the **Enable TR69 Support** checkbox to enable the TR-069 module. **Tip:** When the **Enable TR-069** checkbox is not selected, your configuration is saved but the TR-069 function is disabled on the device.
Enable Informs	Select the **Enable Informs** checkbox to send periodic inform messages to the ACS.
ACS URL	Enter the URL that the EdgeMarc should use to contact the ACS.
ACS Username and Password	Enter a username and password in the **ACS Username** and **ACS Password** fields to authenticate the EdgeMarc to the ACS.
Connection Request URL	Enter the URL the ACS uses to connect to the system. If the WAN IP is configured by a dynamic protocol, use the token **WAN_IP** to substitute for the actual WAN IP.
Connection Request Username and Password	Enter a username and password in the **Connection Request Username** and **Connection Request Password** fields to authenticate the ACS to the EdgeMarc.
Inform Interval	Enter the amount of time in seconds between Inform messages.

Table 2-13 TR-69 Configuration Parameters (continued)

Item	Description
	Click **Submit**. A message indicates that service will be temporarily interrupted. Click **OK** to confirm

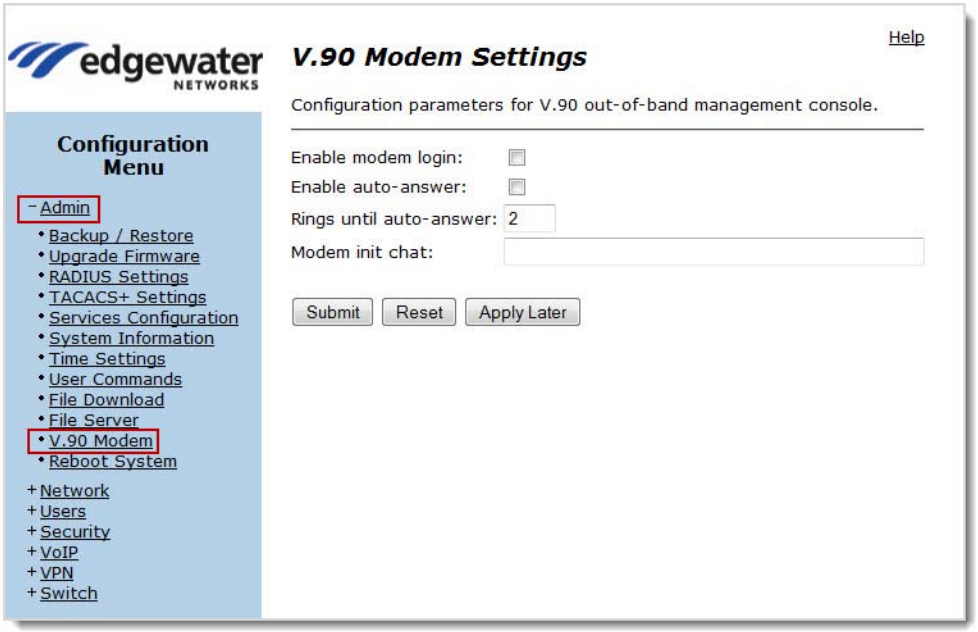
Configuring V.90 Modem Settings

Tip
V.90 modem is only supported on certain EdgeMarc devices.

Use the V.90 Modem Settings page to configure the V.90 out-of-band management console. A remote user can use a modem to dial into the system. Once modem negotiation is complete, the remote user is prompted for a system password. After the remote user has logged in, they have the same access as someone logged into the serial console port on the system.

1. Choose **Admin** > **V.90 Modem** (Figure 2-24).

Figure 2-24 V.90 Modem Settings Page



2. Configure settings using the information in Table 2-14 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 2-14 V.90 Modem Settings Page Parameters

Item	Description
Enable modem login	Select the **Enable modem login** checkbox to enable console login on the V.90 port.
Enable auto-answer	Select the **Enable auto-answer** checkbox to enable automatic answering on the modem port. When the modem and auto-answer are enabled, the modem answers a call after the configured number of "Rings until auto-answer."
Rings until auto answer	Enter the number of rings before the modem automatically answers incoming calls. Both modem and auto-answer must be enabled.
Modem Init Chat	(Optional) Enter a modem init chat string if additional configuration is required. The typical string contains commands followed by the expected response from the modem. The command and response must be separated by spaces.

Click **Submit**.

A message indicates that service will be temporarily interrupted.

Click **OK** to confirm

Rebooting the System



Caution
Rebooting the system interrupts all services for several minutes.

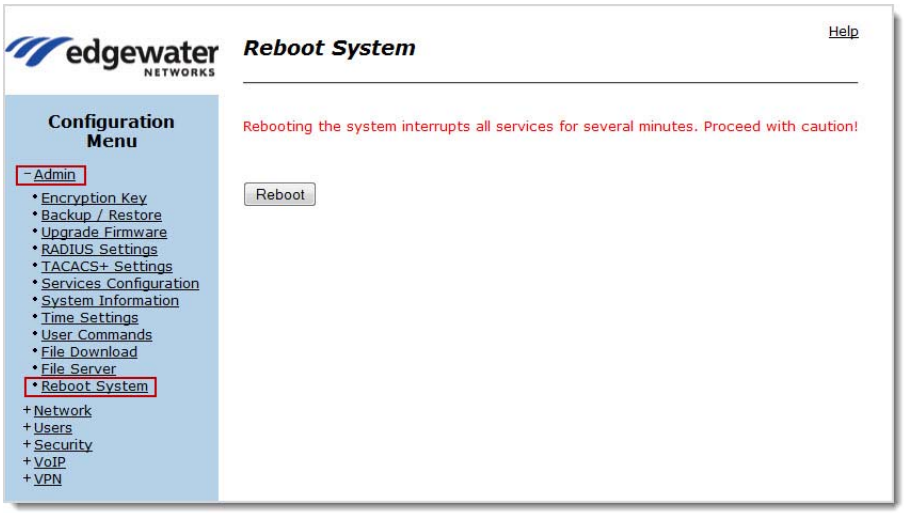
Rebooting the system stops all networking services while the operating system and networking services are loaded from scratch. Reboot is functionally equivalent to power cycling the system. Technical support may request that the system be rebooted during a troubleshooting session.



Tip
As an alternative to rebooting, you can perform a reset locally by temporarily disconnecting the power cable from the EdgeMarc then plugging it back in.

1. Choose **Admin** > **Reboot System** (Figure 2-25).

Figure 2-25 Reboot System Page



2. Click **Reboot**. The following message is displayed:

Caution
All voice, video, and data services will be interrupted. They will be unavailable for several minutes while the system reboots. Do you want to continue?

3. Click **OK** to confirm.

3

Network Deployment

The following sections describe how to configure the EdgeMarc to function in your IP network using the **Network** tab in the Configuration Menu:

- Using the Network Page
- Configuring ADSL Services
- Configuring NAT Settings
- Configuring VLAN Support
- Configuring WAN VLAN Settings
- Configuring Customer Networks
- Configuring the 802.1X Supplicant
- Configuring T1/E1 Settings
- Managing T1/E1 Diagnostics
- Configuring PRI
- Configuring High Availability
- Configuring DHCP Relay
- Configuring the DHCP Server
- Configuring Traffic Shaping
- Configuring Pass-Through Rules
- Configuring Subinterfaces
- Configuring Proxy ARP
- Managing Switch Ports Settings
- Configuring Static Routes
- Configuring Dynamic DNS
- Viewing Network Information
- Initiating Network Restart
- Using Network Test Tools
- Configuring Firewall Traversal
- Configuring WAN Failover
- Configuring SOC2 IP Settings
- Configuring Router Advertisement (IPv6)

Using the Network Page

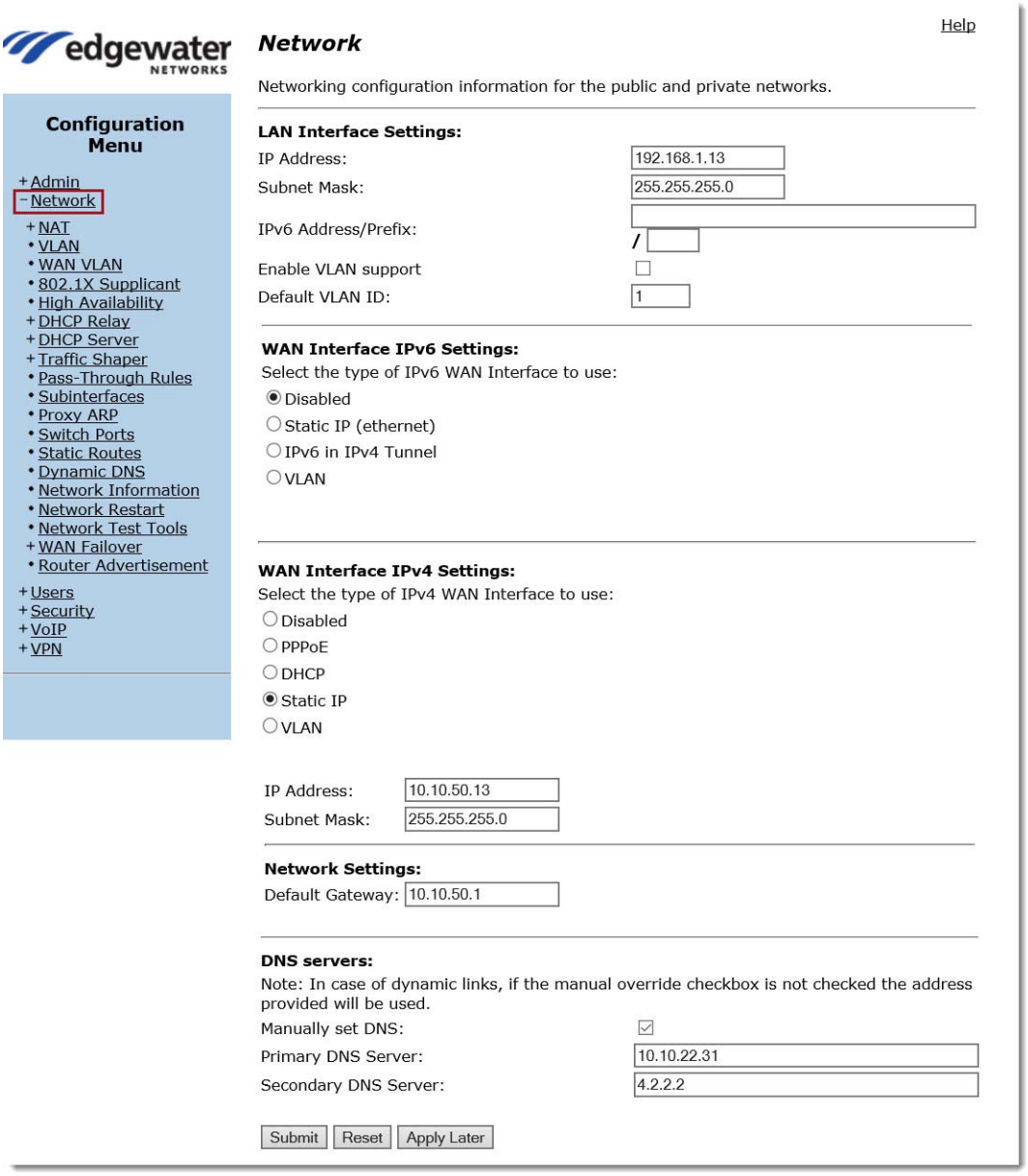
Use the Network page to configure networking configuration parameters for public and private networks.

- Configuring LAN Interface Settings
- Configuring WAN Interface Settings
- Configuring WAN Interface IPv6 Settings
- Configuring WAN Interface IPv4 Settings
- Configuring Network Default Gateway Settings
- Configuring DNS Servers

To configure settings on the Network configuration page:

1. Choose **Network** from the Configuration Menu (Figure 3).

Figure 3 Network Configuration Page



2. Configure settings using the information in Table 3-1 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-1 Network Page Parameters

Item	Description
LAN Interface Settings	
Connects your system to the Local Area Network (LAN) for voice, video, and data service. See Configuring LAN Interface Settings.	
IP Address	Specifies the IP address needed to establish the connection to the LAN. **Note:** The system is shipped with a default LAN IP address of 192.168.1.1 and a default password. Once you configure your system, change the default password using the Administration page. Click **Admin** in the Configuration Menu and refer to Changing Your Password in Chapter 2, *System Administration*.
Subnet Mask	Specifies the network mask associated with the IP address. Default is 255.255.255.0.
IPv6 Address/Prefix	Specifies the local IPv6 address and prefix to configure the LAN interface to be IPv6 enabled.
Enable VLAN Support	Enables VLAN support in the LAN. Click **Network** > **VLAN** in the Configuration Menu and refer to Configuring VLAN Support.
Default VLAN ID	Displays the VLAN ID of the primary LAN interface. If a port has multiple VLANs assigned to it, it will use this VLAN ID as the PVID by default.
Enable Multi LAN Ports	Enables the second and third Ethernet LAN ports on the EdgeMarc 7000 Series. Ports 5 and 6 become active; VLANs are created on Port 1 (eth0) by default. The three LAN ports (1, 5 and 6) are grouped into a bridge (br_lan0). A LAN IP address is assigned to the bridge and services such as VoIP now use the bridge (br_lan0) instead of the physical interface (eth0). You can optionally change settings on the VLAN Membership page to create VLANs on the other ports and change packet types (all, tagged or untagged, along with PVID) on the VLAN Port Configuration page for each port. LANs and VLANs are grouped into bridges accordingly and VoIP and some other services can be configured to work on a specific bridge interface. See Configuring Multi LAN Ports. **Note:** The LAN and WAN networks must be different subnets. The LAN and WAN interfaces must not be attached to the same broadcast domain. For example, the LAN and WAN interfaces cannot be connected to the same hub or switch unless they are segmented with VLANs.

© 2014 Edgewater Networks. All Rights Reserved.

Item	Description
WAN Interface Settings	Selects the method used to obtain a connection to the Internet. See Configuring WAN Interface Settings.
IPv6	Configures IPv6 settings. IPv6 is only available on certain EdgeMarc models. See Configuring WAN Interface IPv6 Settings. ■ **Disabled**—Disables IPv6 functionality depending on your network configuration requirements. ■ **Static IP Address**—Configures the WAN interface with a static IP address (default). ■ **IPv6 in IPv4 Tunnel**—Configures the local and remote tunnel gateway. This allows tunneling of IPv6 packets over an IPv4 network.
IPv4	Configures IPv4 settings. See Configuring WAN Interface IPv4 Settings. ■ **Disabled**—Disables IPv4 functionality depending on your network configuration requirements. ■ **ADSL**—Configures the integrated ADSL modem (available only on certain models). See IPv4 ADSL. ■ **PPPoE**—Initiates a PPP session over your WAN Ethernet port. See IPv4 PPPoE. ■ **DHCP**—Configures the device to obtain the WAN-side IP address using a DHCP server available from the WAN side of the network. To see the WAN IP address for the system, go to **Network** > **Network Information**. See IPv4 DHCP. ■ **Static IP Address**—Configures the WAN interface with a static IP address (default). See IPv4 Static IP. ■ **VLAN**—Selects the VLAN defined in Configuring WAN Interface Settings. ■ **T1/E1**—Configures the WAN interface with a static IP address and tests the T1/E1 interface on the system using the T1/E1 Configuration page. (Available only on certain models). See IPv4 T1/E1 and Configuring T1/E1 Settings.
IP Address	Specifies the WAN Interface IPv4 IP address.
Subnet Mask	Specifies the WAN Interface IPv4 subnet mask.

Item	Description
Network Settings	
Used with Static IP (Ethernet). See Configuring Network Default Gateway Settings.	
Default Gateway	Specifies the IPv4 default gateway.
DNS Servers	
See Configuring DNS Servers.	
Manually Set DNS	Allows you to supply specific DNS configuration information. To configure dynamic DNS, choose **Network** > **Dynamic DNS** and refer to Configuring Dynamic DNS.
Primary DNS	Specifies the primary DNS server supplied by the ISP. The Primary DNS server should be the fastest available DNS server for your system.
Secondary DNS	Specifies the Secondary DNS server supplied by the ISP. Used to reduce the risk of one or more DNS servers not being available.
Primary WAN Redundancy Settings	
See Configuring WAN Failover.	
Enable Ping based status detection	Enables ping-based link detection for the Primary interface if WAN failover (WAN Link Redundancy, or WLR) is enabled. The system periodically sends pings to the specified host to monitor the status of the Primary interface. If no response is received, the link is declared down.
Ping Host	Specifies the ping host. If Ping Based Status Detection is enabled, pings are periodically sent to the ping host specified in this field. If no ping host is specified, pings are sent to the Primary Default Gateway.

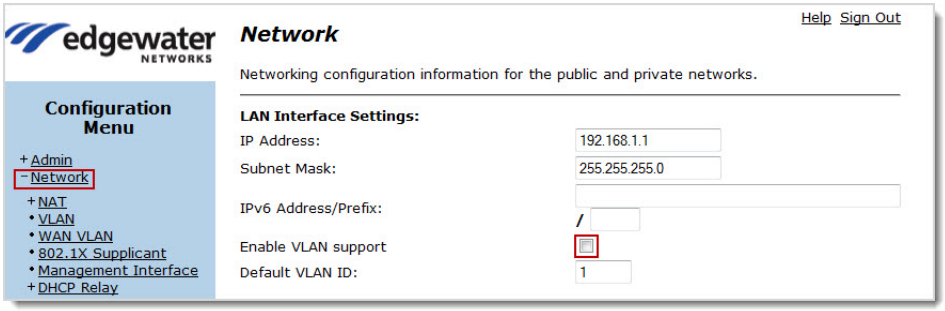
Configuring LAN Interface Settings

This section describes how to set up LAN parameters with and without VLANs. The VLAN configuration feature allows you to connect the appliance to an Ethernet switch that has been configured to use VLANs. Figure 3

shows the Network configuration page. Table 3-1 describes field parameters.

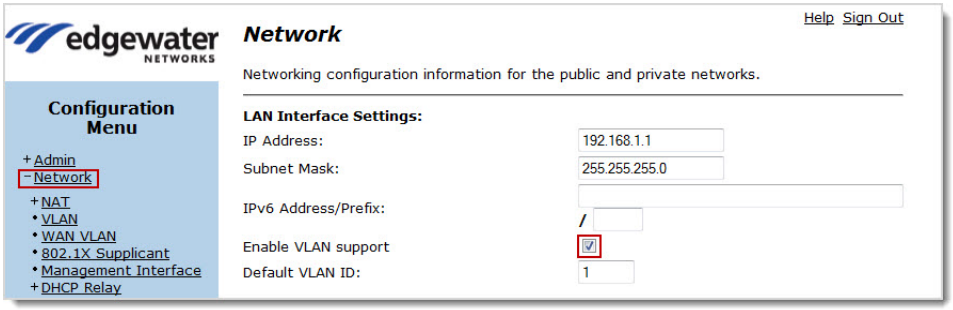
1. Choose **Network** from the Configuration Menu (Figure 3).
2. Your EdgeMarc has been pre-configured with a LAN IP address of 192.168.1.1 for first-time setup. In the **IP Address** field, enter the local area network address of your system LAN port in the IP Address field.
3. Your EdgeMarc has been pre-configured with a Subnet Mask value of 255.255.255.0 for first-time setup. In the **Subnet Mask** field, enter a new subnet mask.
4. To enable IPv6 for expanded IP addressing capability, enter the IPv6 address and a prefix in the **IPv6 Address/Prefix** field.
5. To configure LAN network settings without VLANs, un-check the **Enable VLAN support** checkbox to disable VLANs on your system (Figure 3-1).

Figure 3-1 Disable VLAN Support



6. To configure LAN network settings with VLANs, select the **Enable VLAN support** checkbox to enable VLANs on your system (Figure 3-2).

Figure 3-2 Enable VLAN Support



7. Click **Submit**. A message indicates that service will be interrupted.
8. Click **OK** to confirm. The VLAN Configuration link becomes active on the page.
9. Click the **VLAN Configuration** link to open the VLAN Configuration page and refer to Configuring VLAN Support. You can also choose

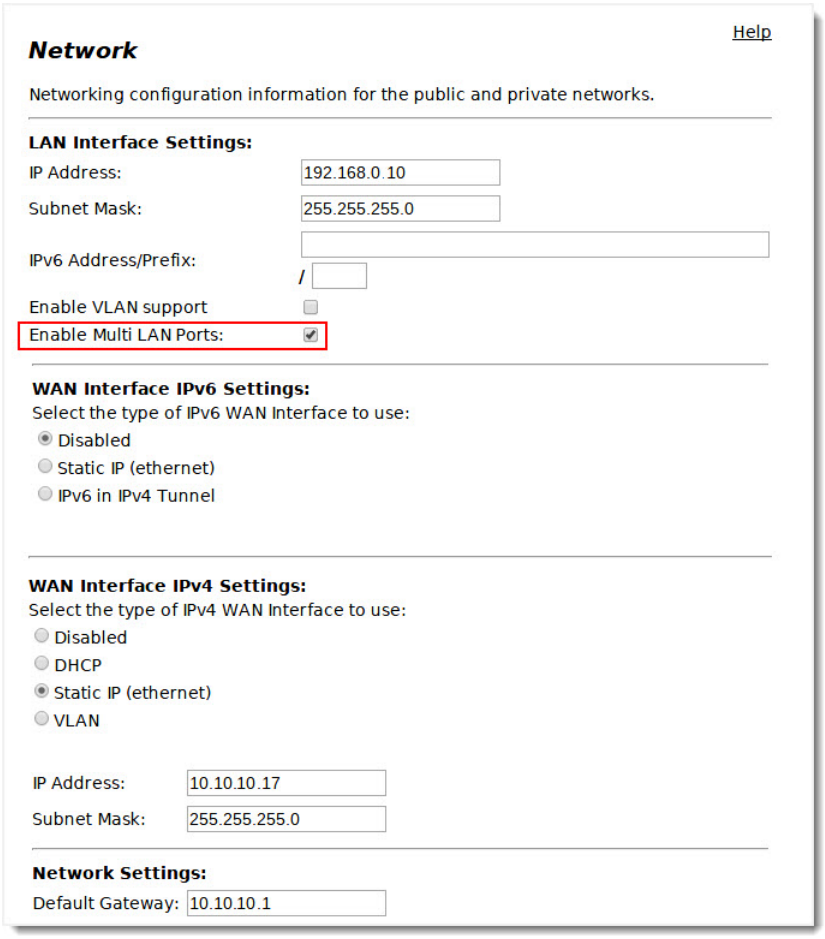
Network > **VLAN** from the Configuration Menu to open the VLAN Configuration page.

Configuring Multi LAN Ports

To configure more than one LAN port:

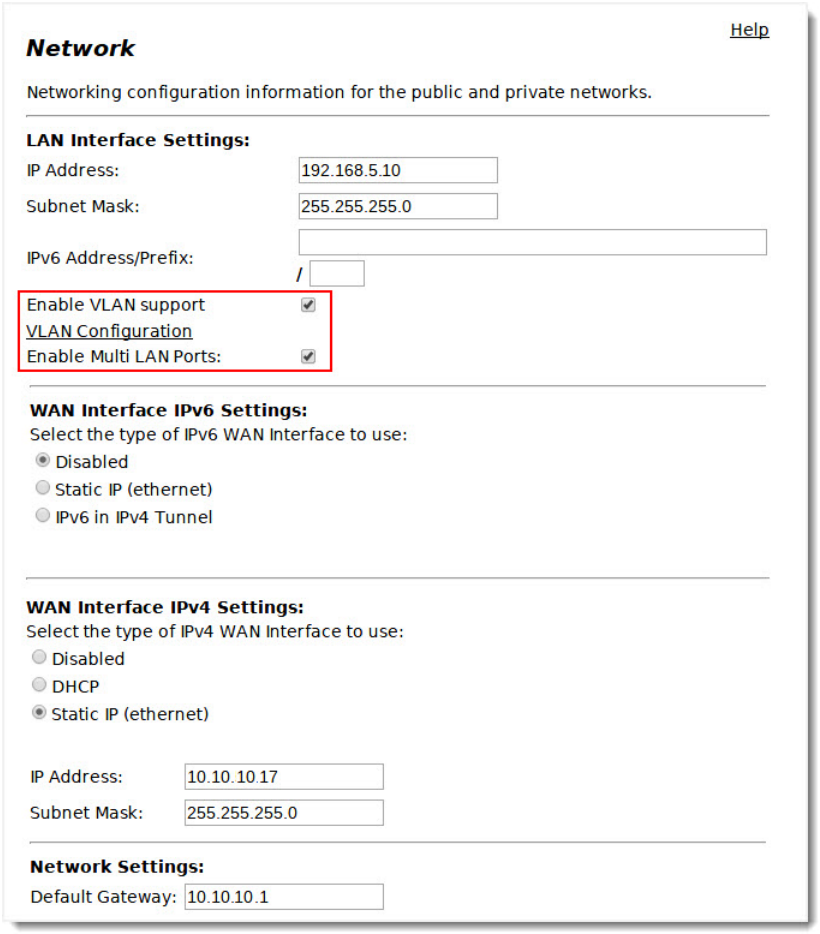
1. Choose **Network** from the Configuration Menu.
2. Select the **Enable Multi LAN Ports** checkbox to enable the second and third LAN ports (Ports 5 and 6) on the system (Figure 3-3).

Figure 3-3 Enable Multi LAN Ports



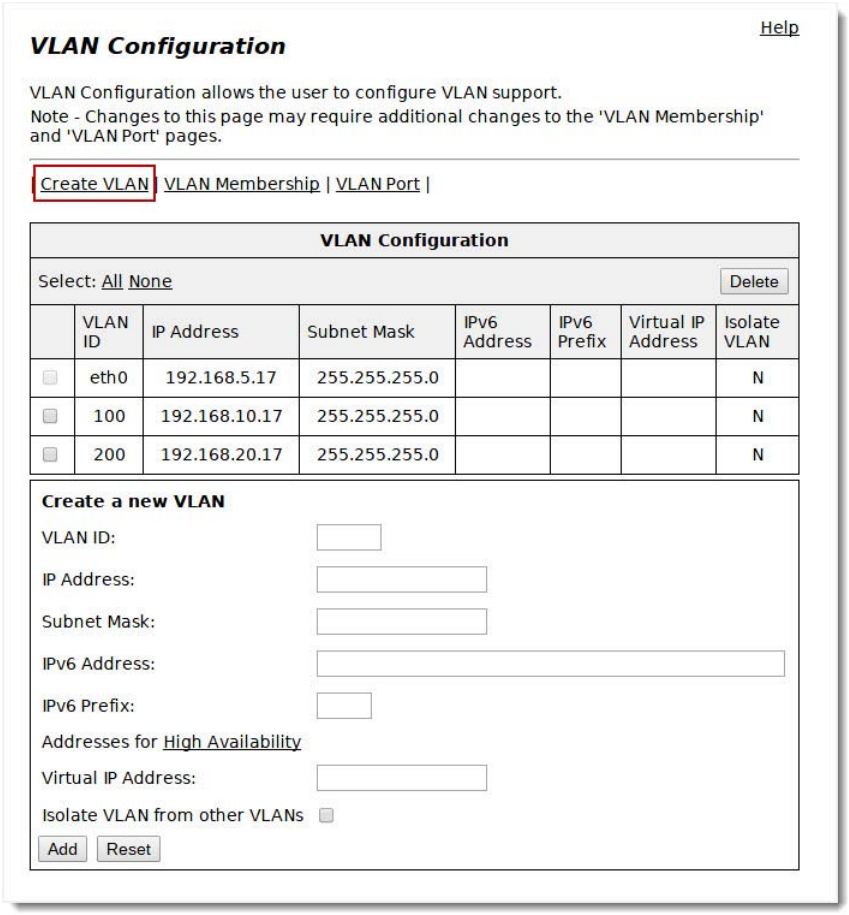
3. Click **Submit**.
4. Select the **Enable VLAN Support** checkbox and click **Submit** (Figure 3-4).

Figure 3-4 Enable VLAN Support



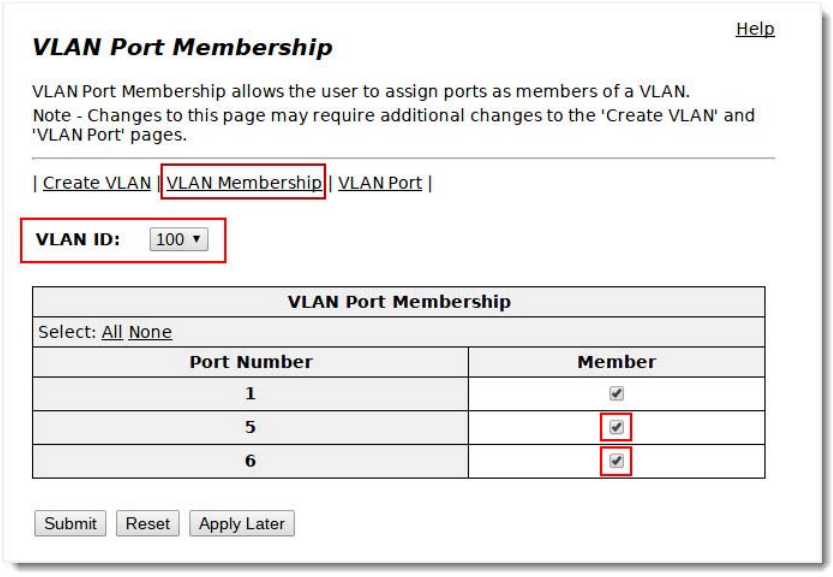
5. On the Network page, click **VLAN Configuration** to open the VLAN Configuration page.
6. Click **Create VLAN** (Figure 3-5).

Figure 3-5 Create a VLAN



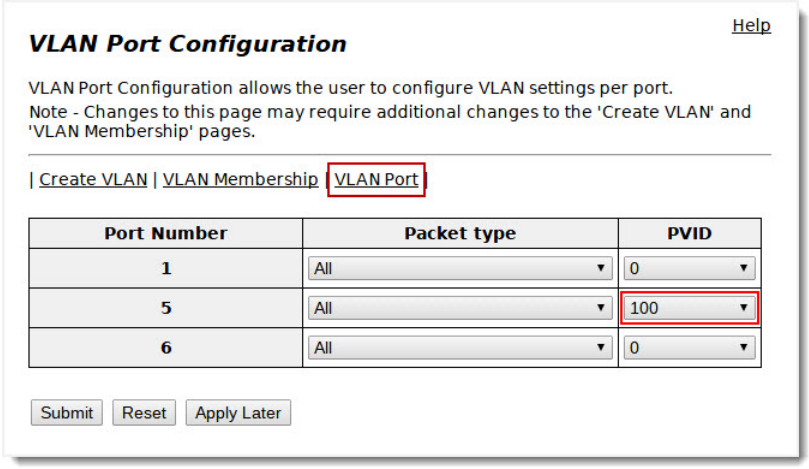
7. Create new VLAN IDs for Ports 5 and 6; Port 1 is configured by default (eth0). Click **Add**.
8. On the VLAN Configuration page, click **VLAN Membership** (Figure 3-6).

Figure 3-6 Create VLAN Membership



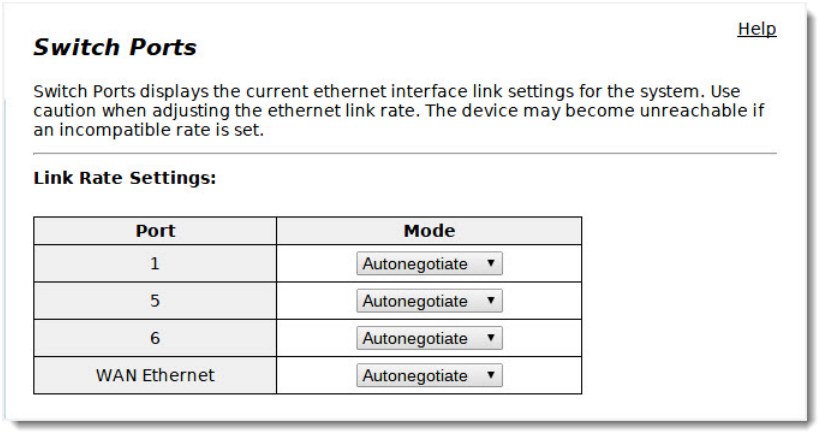
9. Enable VLAN membership for Ports 1, 5, and 6. Click **Submit**.
10. On the VLAN Configuration page, click **VLAN Port** (Figure 3-7).

Figure 3-7 VLAN Port Configuration



11. Configure the Packet Types and PVIDs for each port and click **Submit**.
12. Choose **Switch** > **Switch Ports** (Figure 3-8).

Figure 3-8 Switch Port Settings



13. Choose a link rate from the **Mode** drop-down list for Ports 1, 5, and 6.
14. Click **Submit** to save your settings.
15. To verify that Multi LAN Ports are available and enabled, choose **Network** > **Network Information** and check the link status for Ports 1, 5, and 6.

Configuring WAN Interface Settings

This section describes how to set up WAN network parameters using the Network page:

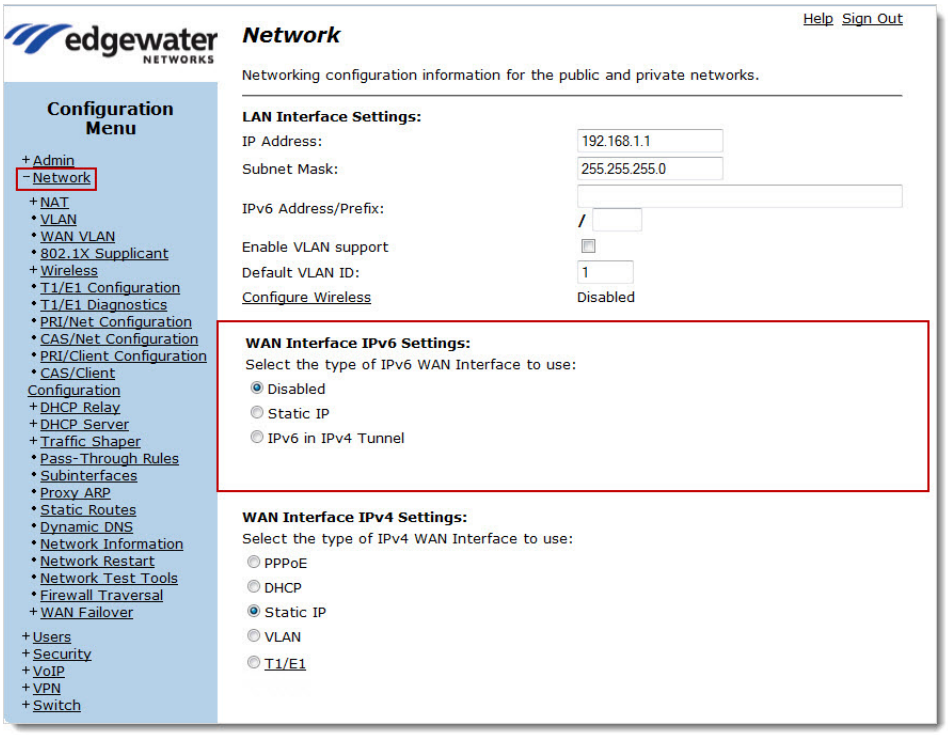
- Configuring WAN Interface IPv6 Settings
- Configuring WAN Interface IPv4 Settings

Tip
WAN interface settings are also required when you are configuring WAN failover (WAN Link Redundancy, or WLR). To configure WLR, choose **Network** > **WAN Failover** and refer to Configuring WAN Failover.

Configuring WAN Interface IPv6 Settings

1. Choose **Network** from the Configuration Menu (Figure 3).
2. Scroll to **WAN Interface IPv6 Settings** (Figure 3-9).

Figure 3-9 WAN Interface IPv6 Settings

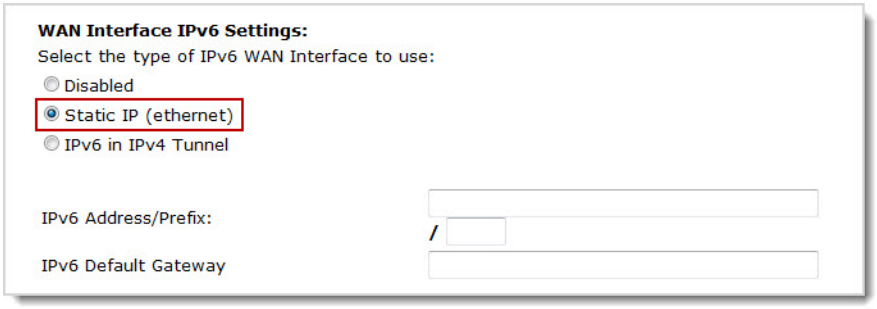


3. Select one of the following methods to establish an Internet connection:
   - Disabled—Default
   - IPv6 Static IP
   - IPv6 in IPv4 Tunnel

IPv6 Static IP

1. Select **Static IP (Ethernet)** to configure a valid IPv6 address, prefix, and optional default gateway (Figure 3-10).

Figure 3-10 WAN Interface IPv6 Settings - Static IP



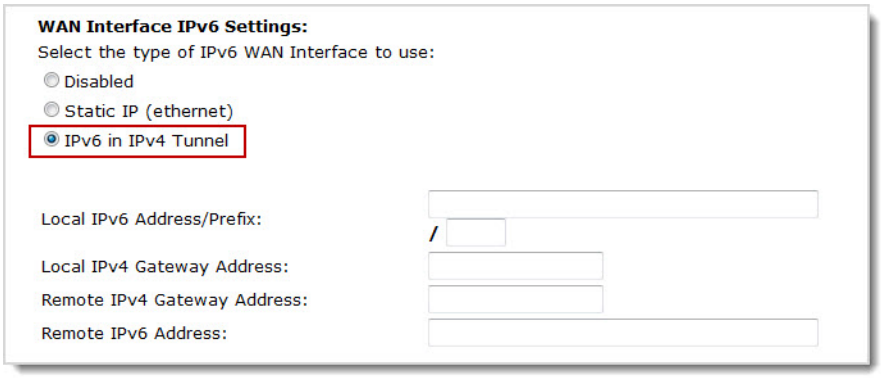
2. In the **IPv6 Address/Prefix** field, enter the IPv6 WAN interface static IP address and prefix.
3. Optional. In the **IPv6 Default Gateway** field, enter the IPv6 default gateway.
4. Click **Submit**.

   A message indicates that service will be temporarily interrupted.
5. Click **OK** to confirm.

IPv6 in IPv4 Tunnel

1. Select **IPv6 in IPv4 Tunnel** to allow IPv6 packet tunneling over an IPv4 network (Figure 3-11).

Figure 3-11 WAN Interface IPv6 Settings - IPv6 in IPv4 Tunnel



2. In the **Local IPv6 Address/Prefix** field, enter the local IPv6 address and prefix.
3. In the **Local IPv4 Gateway Address** field, enter the local IPv4 gateway address (typically the system IPv4 WAN address).
4. In the **Remote IPv4 Gateway Address** field, enter the remote IPv4 gateway address of the remote IPv4 system providing the tunnel.

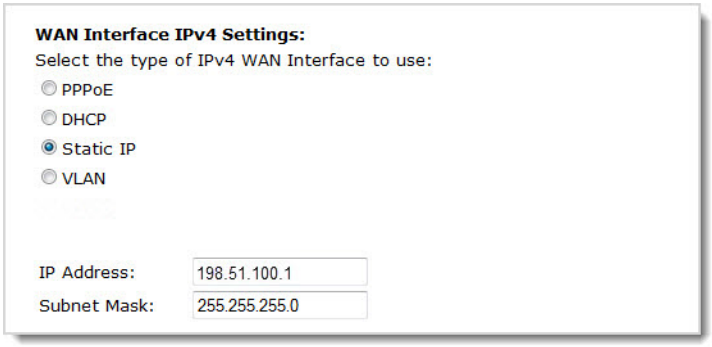
5. In the **Remote IPv6 Address** field, enter the remote IPv6 address.
6. Click **Submit**.

   A message indicates that service will be temporarily interrupted.
7. Click **OK** to confirm.

Configuring WAN Interface IPv4 Settings

1. Choose **Network** from the Configuration Menu (Figure 3).
2. Scroll to **WAN Interface IPv4 Settings** (Figure 3-12). The Static IP radio button is selected by default (see IPv4 Static IP).

Figure 3-12 WAN Interface IPv4 Settings



3. Select one of the following methods to establish an Internet connection:
   - IPv4 ADSL
   - IPv4 PPPoE
   - IPv4 DHCP
   - IPv4 Static IP
   - IPv4 VLAN
   - IPv4 T1/E1

IPv4 ADSL

Use an integrated ADSL modem (available only on certain models, including the EdgeMarc 200AE1, 200AE2, and 250W).

1. Choose **Network** from the Configuration Menu (Figure 3).
2. Scroll to **WAN Interface IPv4 Settings** (Figure 3-12).
3. Select **ADSL** to use the integrated ADSL modem (Figure 3-13). You can also choose **Network** > **ADSL Configuration** (Figure 3-22).

Figure 3-13 WAN Interface IPv4 Settings - ADSL

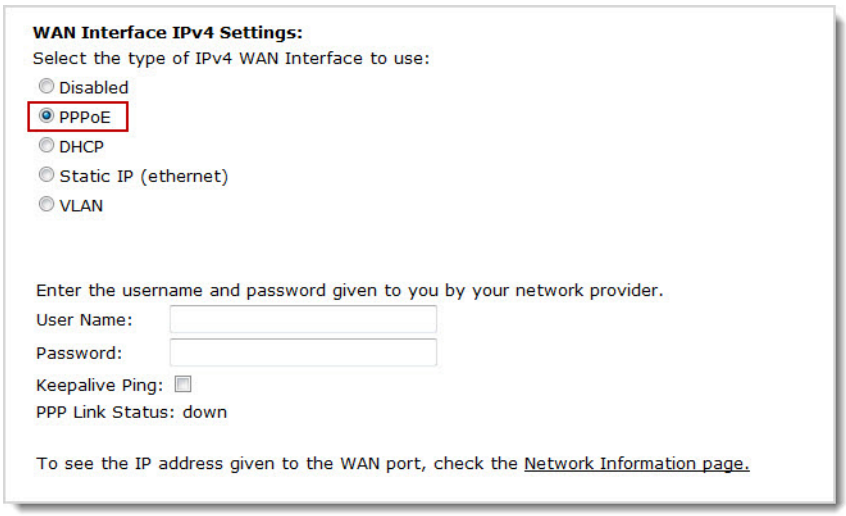


4. Configure settings on the ADSL Configuration page. See Configuring ADSL Services.

IPv4 PPPoE

1. Choose **Network** from the Configuration Menu (Figure 3).
2. Scroll to **WAN Interface IPv4 Settings** (Figure 3-12).
3. Select **PPPoE** to initiate a PPP session over your WAN Ethernet port (Figure 3-14).

Figure 3-14 WAN Interface IPv4 Settings - PPPoE



4. In the **User Name** field, enter the PPPoE username provided by your ISP.
5. Enter a password in the **Password** field.
6. Select the **Keepalive Ping** checkbox to periodically send pings to the specified host to monitor the status of the Primary interface.
7. Click **Submit**.

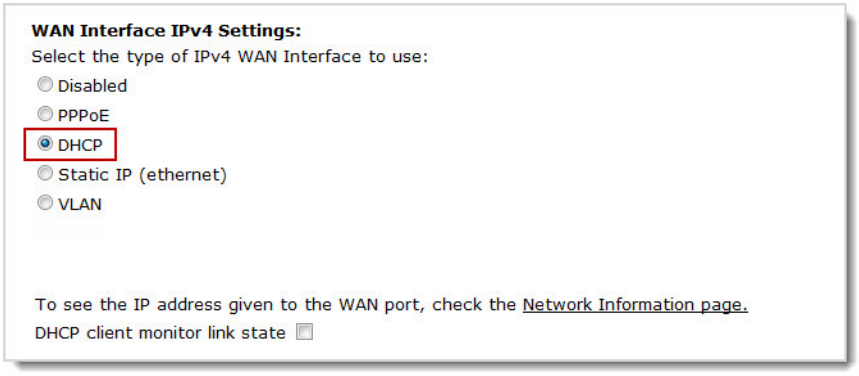
   A message indicates that service will be temporarily interrupted.
8. Click **OK** to confirm.

Tip
To see the IP address given to the WAN port, click the **Network Information** link provided or go to **Network** > **Network Information** and refer to Viewing Network Information.

IPv4 DHCP

1. Choose **Network** from the Configuration Menu (Figure 3).
2. Scroll to **WAN Interface IPv4 Settings** (Figure 3-12).
3. Select **DHCP** to get a WAN side IP address from an available DHCP server on the WAN side of the network (Figure 3-15).

Figure 3-15 WAN Interface IPv4 Settings - DHCP



4. Select the **DHCP client monitor link state** checkbox to display detailed network configuration information for the system.
5. Click **Submit**.

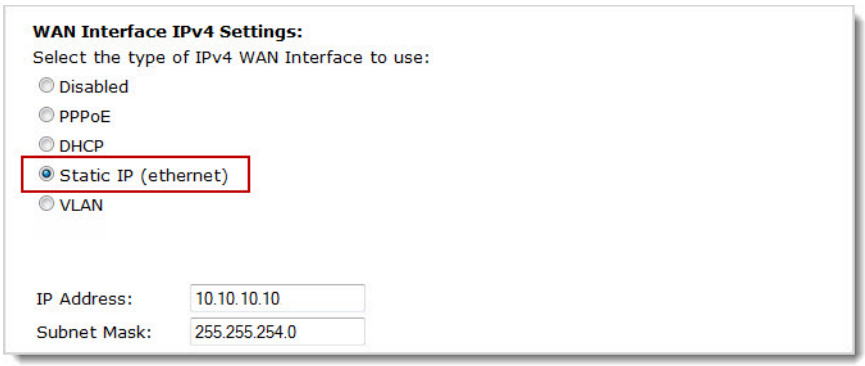
   A message indicates that service will be temporarily interrupted.
6. Click **OK** to confirm.

Tip
To see the IP address given to the WAN port, click the **Network Information** link provided or go to **Network** > **Network Information** and refer to Viewing Network Information.

IPv4 Static IP

1. Choose **Network** from the Configuration Menu (Figure 3).
2. Scroll to **WAN Interface IPv4 Settings** (Figure 3-12).
3. Select **Static IP** to configure the WAN interface manually (Figure 3-16). Static IP is selected by default.

Figure 3-16 WAN Interface IPv4 Settings - Static IP

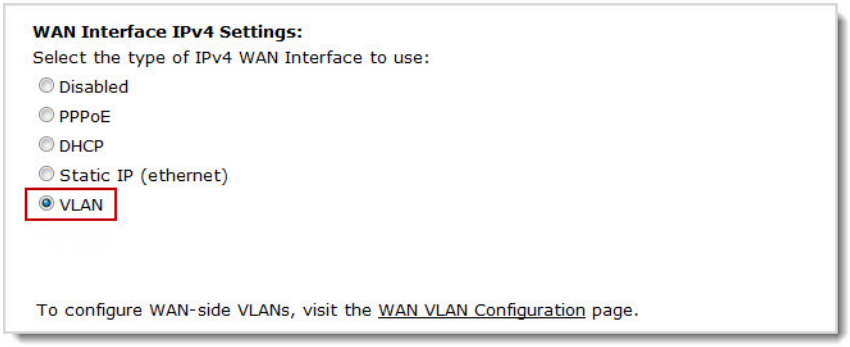


4. In the **IP Address** field, enter an IP address.
5. In the **Subnet Mask** field, enter a subnet mask.
6. Proceed to Configuring Network Default Gateway Settings.

IPv4 VLAN

1. Choose **Network** from the Configuration Menu (Figure 3).
2. Scroll to **WAN Interface IPv4 Settings** (Figure 3-12).
3. Select **VLAN** and click the **WAN VLAN Configuration page** link (Figure 3-17).

Figure 3-17 WAN Interface IPv4 Settings - WAN VLAN



Tip
You can also choose **Network** > **WAN VLAN Configuration**. You must first select the **VLAN** radio button on the Network page to configure settings on the WAN VLAN Configuration page.

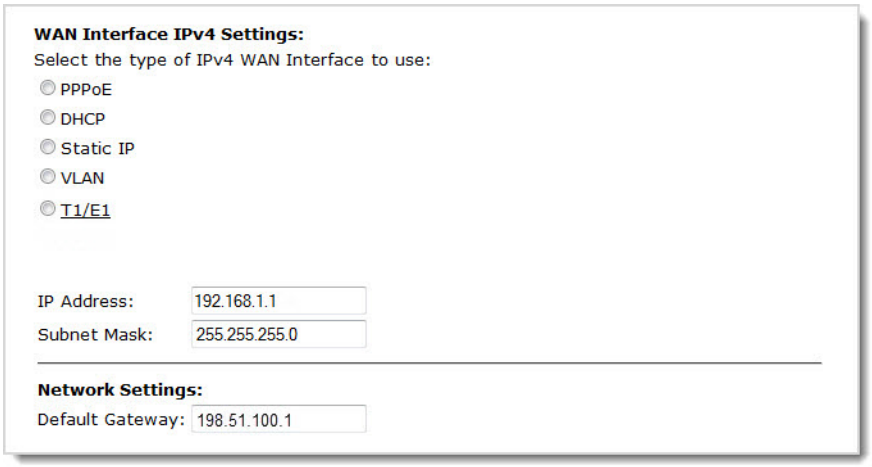
4. Configure settings on the WAN VLAN Configuration page. See Configuring WAN VLAN Settings.

IPv4 T1/E1

Note
E1/T1 configuration is only available on certain EdgeMarc models. See Configuring T1/E1 Settings.

1. Choose **Network** from the Configuration Menu (Figure 3).
2. Scroll to **WAN Interface IPv4 Settings** (Figure 3-12).
3. Select **E1/T1** if your system supports E1/T1 (Figure 3-18).

Figure 3-18 WAN Interface IPv4 Settings - T1/E1



4. In the I**P Address** field, enter the IP address.
5. In the **Subnet Mask** field, enter the subnet mask.
6. In **Network Settings**, enter a default gateway in the **Default Gateway** field.
7. Click **Submit** to apply your changes.

   A message indicates that service will be temporarily interrupted.
8. Click **OK** to confirm.
9. Configure settings on the T1 / E1 Configuration page. See Configuring T1/E1 Settings.

Configuring Network Default Gateway Settings

This setting is available when you select **Static IP (Ethernet)**. Refer to IPv4 Static IP.

1. Choose **Network** from the Configuration Menu (Figure 3).
2. Scroll to **Network Settings** (Figure 3-19).

Figure 3-19 Network Settings - Default Gateway



3. Enter the default gateway address.
4. Click **Submit**.

   A message indicates that service will be interrupted.
5. Click **OK** to confirm.

Configuring DNS Servers

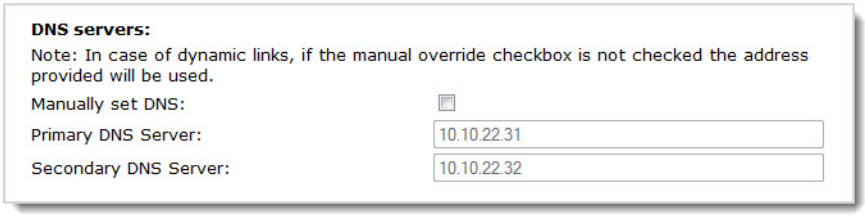
DNS allows one host to refer to another host by its name instead of its IP address (for example, google.com instead of 244.222.333.222). DNS service is hosted on the Internet, so you have to point your EdgeMarc to it. You can configure DNS manually by selecting the **Manually set DNS** checkbox and entering information in the fields, or you can get it automatically.

Note
You can only get a DNS server automatically if you have a dynamic link like ADSL, PPP, or DHCP.

To configure the DNS server:

1. Choose **Network** from the Configuration Menu (Figure 3).
2. Scroll to **DNS Servers** (Figure 3-20).

Figure 3-20 DNS Servers



3. Select the **Manually set DNS** checkbox to enable manual DNS settings. The checkbox is selected by default on most systems.
4. In the **Primary DNS Server** field, enter the Primary server address.
5. In the **Secondary DNS Server** field, enter the Secondary server address.
6. Click **Submit** to apply your changes.

   A message indicates that service will be temporarily interrupted.
7. Click **OK** to confirm.

Configuring ADSL Services

This section describes how to configure the ADSL WAN interface on the EdgeMarc:

- Overview
- Configuring ADSL
- Viewing ADSL Line Status

Note
ADSL is available on the EdgeMarc 250 Series.

Overview

Asymmetric digital subscriber line (ADSL) is a type of digital subscriber line (DSL) technology, a data communications technology that enables faster data transmission over copper telephone lines than a conventional voiceband modem can provide. It does this by utilizing frequencies that are not used by a voice telephone call. A splitter, or DSL filter, allows a single telephone connection to be used for both ADSL service and voice calls at the same time. ADSL can generally only be distributed over short distances from the telephone exchange (the last mile), typically less than 4 kilometers (2 mi), but has been known to exceed 8 kilo meters (5 mi) if the originally laid wire gauge allows for further distribution.

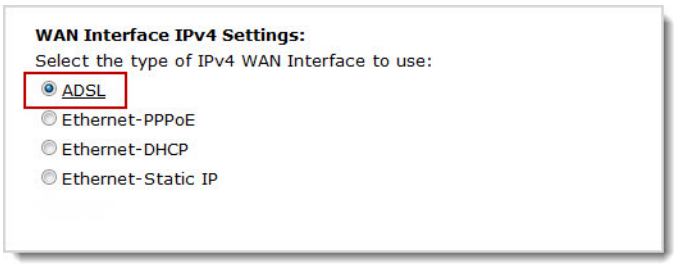
At the telephone exchange the line generally terminates at a digital subscriber line access multiplexer (DSLAM) where another frequency splitter separates the voice band signal for the conventional phone network. Data carried by the ADSL are typically routed over the telephone company's data network and eventually reach a conventional Internet Protocol network.

Most ADSL communication is full-duplex. Full-duplex ADSL communication is usually achieved on a wire pair by either frequency-division duplex (FDD), echo-cancelling duplex (ECD), or time-division duplex (TDD). FDD uses two separate frequency bands, referred to as the upstream and downstream bands. The upstream band is used for communication from the end user to the telephone central office. The downstream band is used for communicating from the central office to the end user.

Configuring ADSL

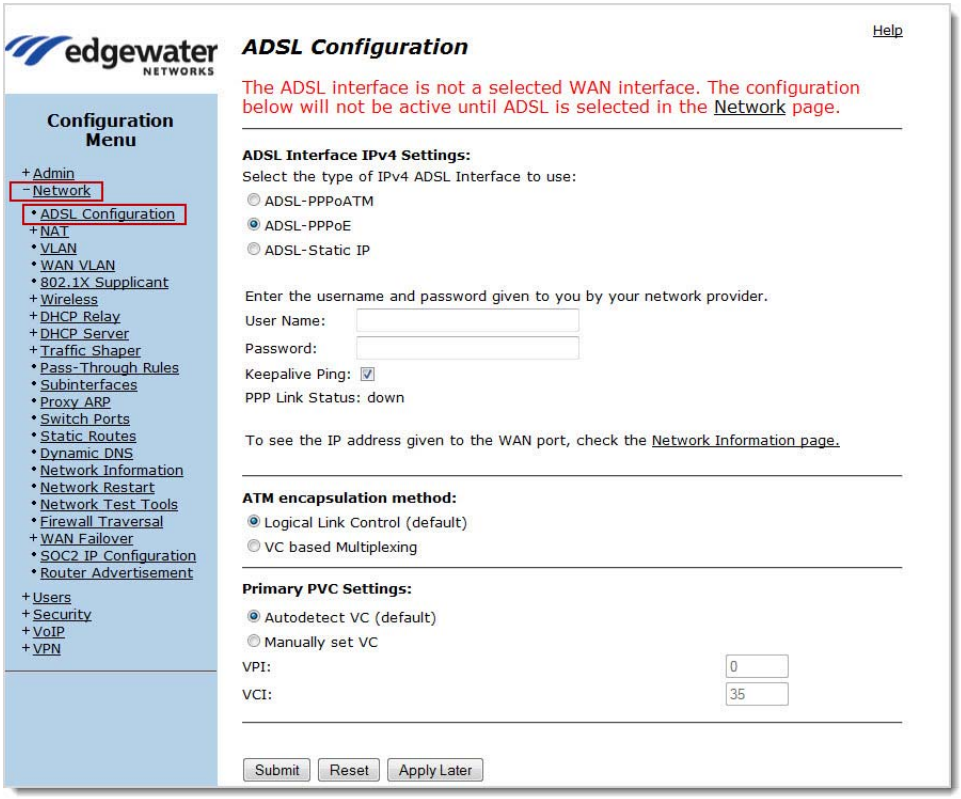
1. Choose **Network** from the Configuration Menu (Figure 3-21).
2. Scroll to WAN Interface IPv4 Settings and select the **ADSL** radio button (Figure 3-21).

Figure 3-21 Enable ADSL from the Network Page



3. Click **Submit**.
4. Choose **Network** > **ADSL Configuration** (Figure 3-22).

Figure 3-22 ADSL Configuration Page



5. Configure settings using the information in Table 3-2 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-2 ADSL Configuration Page Parameters

Item	Description
ADSL Interface IPv4 Settings	
Creates a WAN connection through the ADSL interface.	
Select the type of IP4v ADSL interface to use:	
ADSL-PPPoATM	Establishes a WAN connection using a PPP session over ATM. If you choose ADSL-PPPoATM, enter the username and password given to you by your network provider in the **User Name** and **Password** fields.
ADSL-PPPoE	Establishes a WAN connection using a PPP session over Ethernet over ATM. If you choose ADSL-PPPoE, enter the username and password given to you by your network provider in the **User Name** and **Password** fields.
ADSL-Static IP	Establishes a static IP address over ATM. RFC 2684 is used to bridge IP over ATM. **Note:** This setting requires you to return to the Network Configuration page and manually enter the IP address, Netmask, and Gateway IP given by your service provider. See Configuring ADSL for Static IP.
Keepalive Ping	Select the **Keepalive Ping** checkbox to periodically send pings to the specified host to monitor the status of the Primary interface.
PPP Link Status	Verify the status of your PPP link. The PPP link should be up. See IPv4 PPPoE in Configuring WAN Interface IPv4 Settings to manage PPP settings.
ATM Encapsulation Method	
Provides a way to encapsulate various protocols over ATM. Select the ATM encapsulation method used by your service provider.	
Choose the **ATM encapsulation method** used by your service provider:	
Logical Link Control (default)	Multiplexes multiple protocols over a single ATM VC. The protocol of a carried protocol data unit (PDU) is identified by prefixing the PDU with an Logical Link Control (LLC) header.

Table 3-2 ADSL Configuration Page Parameters (continued)

Item	Description
VC based Multiplexing	Defines one permanent virtual circuit (PVC) per protocol. This uses more VCs than LLC encapsulation, but reduces overhead, because a header is not necessary. For example, to forward IP and IPX over ATM, two dedicated PVCs must be defined. One PVC carries the IP address and another carries Internetwork Packet Exchange (IPX). As the number of protocols increase, PVC also increase.
Primary PVC Settings	
Set the Permanent Virtual Circuit setting to either autodetect or manual:	
Autodetect VC (default)	Identifies encapsulation automatically to dynamically create higher protocol layers.

Table 3-2 ADSL Configuration Page Parameters (continued)

Item	Description
Manually set VC	The following fields become active: ■ VPI—Enter the Virtual Path Identifier (VPI) ■ VCI—Enter the Virtual Channel Identifier (VCI) Specifies the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) values for the Data PVC. If unknown, request this information from your service provider. VCI, used in conjunction with the VPI, indicates where an ATM cell is to travel over a network. ATM, or asynchronous transfer mode, is a method that many Internet Service Providers (ISPs) use to transfer data to client computers. Because ATM sends packets over fixed channels, the data is easier to track than information sent over the standard TCP/IP protocol. The VCI within each ATM cell defines the fixed channel on which the packet of information should be sent. It is a 16-bit field, compared to the VPI, which is only 8 bits. Because this numerical tag specifies the virtual channel that each packet belongs to, it prevents interference with other data being sent across the network.

Secondary PVC Settings

(Optional) If your service provider supports multiple PVCs, you can enable a second PVC to use as a secondary WAN link. This can be used in a WAN failover (WAN Link Redundancy, or WLR) configuration to achieve WAN redundancy or load balancing data and voice traffic between the two virtual links.

Configure Secondary PVC Settings:

- Select the **Enable Secondary PVC** checkbox to enable a second PVC to use as a secondary WAN link.
- Choose **Network** > **WAN Failover** to open the WAN Link Redundancy page and refer to Configuring WAN Failover.
- Select the **Enable WAN Link Redundancy** checkbox and configure settings on the page as needed. Click **Submit** to save your settings.
- Choose **Network** > **WAN Failover** > **Secondary WAN** to open the Secondary WAN Interface Settings page and select the **Virtual Link** for the WAN Interface Setting. Click **Submit** to save your settings.

6. Configure the following settings on the ADSL Configuration page:

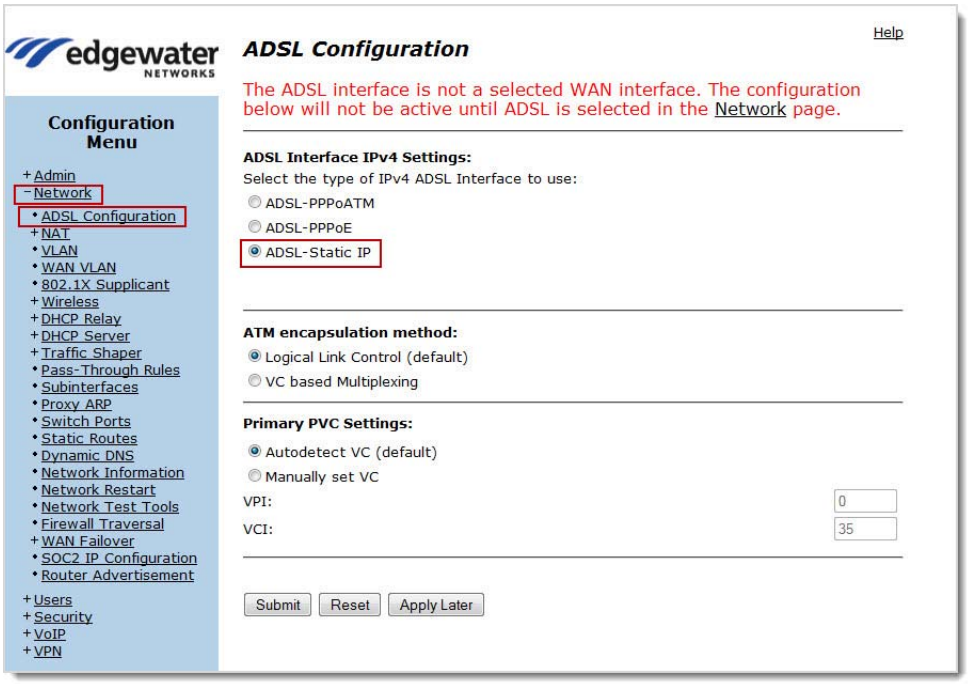
- Configuring ADSL for Static IP

- Viewing ADSL Line Status
- Deleting a Private Network

Configuring ADSL for Static IP

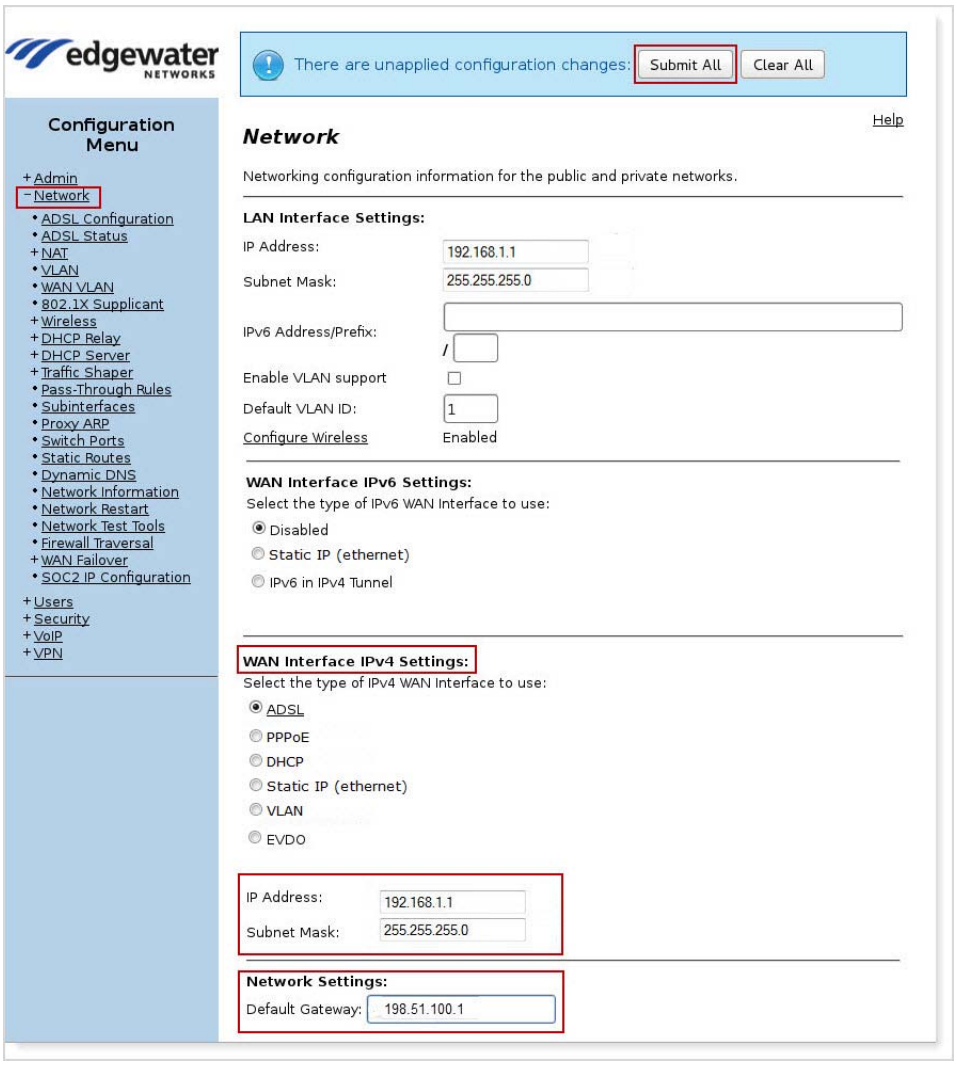
1. Choose **Network** > **ADSL Configuration** (Figure 3-22).
2. Configure settings using the information in Table 3-7 as a guide.
3. In ADSL Interface IPv4 Settings, select **ADSL-Static IP** (Figure 3-23).

Figure 3-23 ADSL Configuration - Static IP



4. Choose the ATM encapsulation method used by your service provider:
   - Logical Link Control (default)
   - VC based Multiplexing
5. Select one of the following **Primary PVC Settings**:
   - Autodetect VC (default)
   - Manually set VC—The following fields become active:
     - VPI—Enter the Virtual Path Identifier (VPI)
     - VCI—Enter the Virtual Channel Identifier (VCI)
6. Select **Apply Later**.
7. Choose **Network** from the Configuration Menu (Figure 3-24).

Figure 3-24 Network Configuration Page - Static ADSL



8. Scroll to WAN Interface IPv4 Settings and enter the **IP Address** and **Subnet Mask** given to you by your service provider.
9. Scroll to **Network Settings** and enter the **Default Gateway** IP address given to you by your service provider.
10. At the top of the Network Configuration page, click **Submit All**.

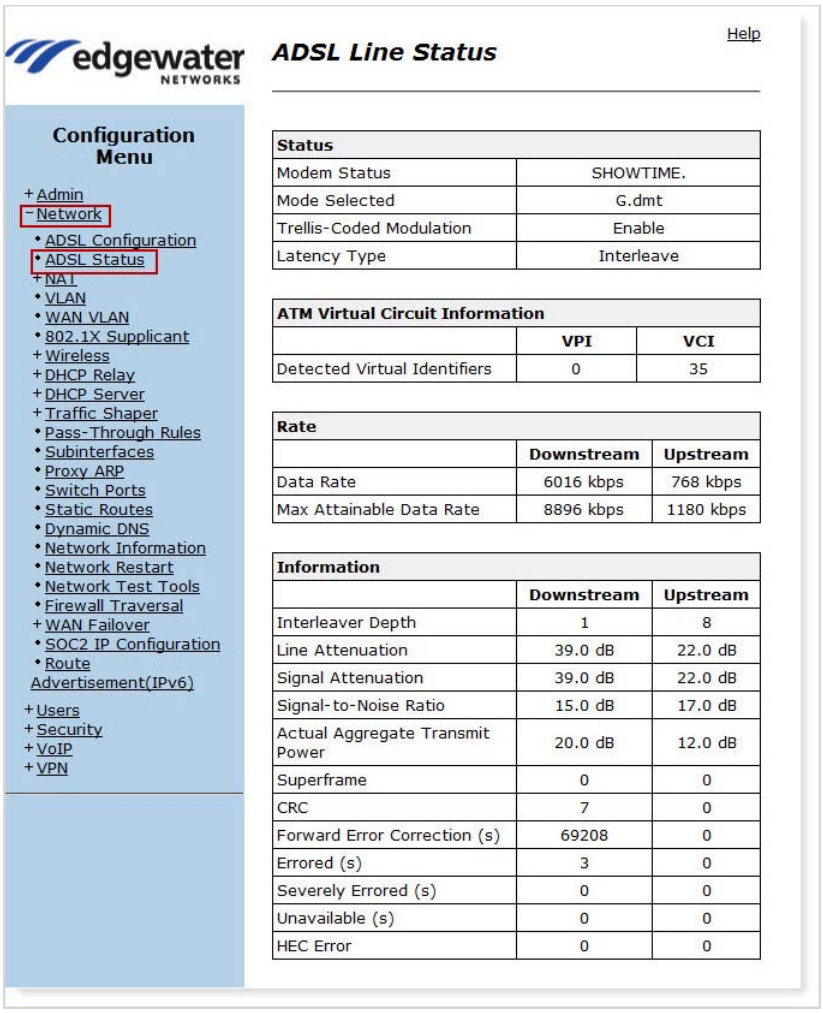
    ADSL for Static IP is now configured on your system.

Viewing ADSL Line Status

The ADSL Line Status page describes ADSL modem status. If the modem is in “Showtime,” rate and statistical information is also provided.

1. Choose **Network** > **ADSL Status** (Figure 3-25).

Figure 3-25 ADSL Line Status Page



2. View ADSL status using the information in Table 3-3 as a guide.

Table 3-3 ADSL Status Description

Item	Description
Status	
Describes ADSL line status.	
Modem Status	The status of the training process with the digital subscriber line access multiplexer (DSLAM). DSLAM connects multiple customer digital subscriber line (DSL) interfaces to a high-speed digital communications channel using multiplexing techniques. “Showtime” indicates that the modem and DSLAM are in sync.

Table 3-3 ADSL Status Description (continued)

Item	Description
Mode Selected	Displays the ITU standard for the operating modem. For example: ■ G.992.1 A is ADSL Annex A— Annex A is ADSL over PSTN. PSTN refers to the standard analogue circuits originally designed for voice with a data rate limit of 56k. Annex A provides a maximum speed of 24Mbps download and 1.4Mbps upload. ■ G.992.5 is ADSL2+ Annex M— ADSL2+ Annex M allows dramatic increases in upstream data speed, with real world upload speeds typically around 1.6 to 2.2Mb/s - sometimes twice as fast as “standard” with a maximum 3.3Mbps. The standard maximum download speed is 24 Mbit/s. ■ (Annex A) upstream speeds.
Trellis-Coded Modulation	Indicates whether trellis coded modulation (TCM) is enabled or disabled. TCM is a modulation scheme which allows highly efficient information transmission over band-limited channels such as telephone lines.
Latency Type	Indicates the modem latency type: ■ Interleave—Increases resistance to noise bursts on a line. Increases latency on the line. If during transit more than a certain amount of data has been lost, the data cannot be correctly decoded by your router. Short bursts of noise on the line can cause these data packets to become corrupt and the modem has to re-request data, which in turn can slow down the overall rate at which data is transmitted. Interleaving is a method of taking data packets, chopping them up into smaller bits and rearranging them so that contiguous data is spaced further apart into a non continuous stream. Data packets are re-assembled by your modem. ■ Fast Path—Improves (lowers) latency and lowers noise margin dB, which can lower line stability. Fast Path is identified on the system by its Depth of Interleaving (D Value) of 1. Fast Path sends one packet at a time.

Table 3-3 ADSL Status Description (continued)

Item	Description
ATM Virtual Circuit Information	
Detected Virtual Identifiers	Displays system virtual channel information: ■ VPI—Virtual Path Identifier ■ VCI—Virtual Channel Identifier
Rate	
Displays ADSL system data rates.	
Data Rate	Displays the data rate in kilobits per second. The EdgeMarc supports several versions of ADSL (ADSL, ADSL2, ADSL2+, and so on) and associated annex versions.
Max Attainable Data Rate	Describes maximum downstream and upstream data rate or speed that the DSLAM negotiates with your ADSL modem. For a given service, the service provider may mandate a given maximum data rate.
Information	
Displays ADSL system details.	
Interleaver Depth	Displays the downstream and upstream Depth of Interleaving (D Value). Interleaving helps maintain tolerance against noise on longer length lines. Various depths of interleaving may be applied by the DSLAM. A depth of 1 indicates the line is on Fast Path with no interleaving applied.
Line Attenuation	Displays downstream and upstream signal loss over the line in decibels. Typical values for line attenuation on an ADSL connection are between 5 dB and 50 dB (lower values are better).
Signal Attenuation	Displays downstream and upstream reduction of signal strength during transmission; when a signal is attenuated so much that the destination cannot interpret the signal or the signal fails en route. Attenuation in both signal frequency and the range between the end points of the medium affect the amount of signal reduction.

Table 3-3 ADSL Status Description (continued)

Item	Description
Signal-to-Noise Ratio	Displays system downstream and upstream signal-to-noise ratio (SNR) information. The higher the noise margin, the stronger the ADSL signal is compared to noise on the line. A ratio between 15 and 18 is good, indicating that your signal is very strong, and/or there is very little noise.
Actual Aggregate Transmit Power	Measures downstream and upstream ADSL transmission power spectrum density (PSD). These calculations can help in designing over voltage protection circuits for ADSL and in debugging ADSL analog circuitry.
Superframe	Displays the number of downstream and upstream superframes received with an error. A superframe consists of 68 ADSL frames plus a synchronization frame. The ADSL modem generates 4000 frames per second. The global duration of an ADSL superframe is 17 ms.
CRC	Displays the number of downstream and upstream Cyclic Redundancy Check (CRC) errors. CRC is an error detection code used to verify packet transmission between the sender and the receiving end. A CRC error indicates that part of the data packet is corrupt and requires retransmission.
Forward Error Corrections	Displays the number of downstream and upstream Forward Error Correction (FEC) errors that have been corrected with error correction applied to the line. Error correction is turned on at the same time as Interleaving. Its normal to see FEC errors on an Interleaved line, indicating that the Interleaving and error correction process is working.
Errored	Displays the number of downstream and upstream Errored Seconds (ES). An ES is a one-second period of time in which one or more coding violations occurred or at least one Loss of Signal events occurred. It is not unusual to see occasional ES.
Severely Errored	Displays the number of downstream and upstream Severely Errored Seconds (SES). An SES is a one-second period that contains 30% or more errored blocks or other events.

Table 3-3 ADSL Status Description (continued)

Item	Description
Unavailable	Displays the number of downstream and upstream Unavailable Seconds (UAS). Ten consecutive Severely Errored Seconds (SES) triggers a UAS event that removes the path from use. The path becomes usable again after 10 consecutive seconds with no SES events.
HEC Error	Displays the number of downstream and upstream Header Error Check/Correction (HEC) errors. HEC is a type of CRC error check which has been performed on the header of an ATM cell. This count is usually where HECs have been uncorrected and have been discarded. If these errors are too high, throughput is slowed and can lead to connection instability.

Configuring NAT Settings

This section describes how to configure Network Address Translation (NAT) on the EdgeMarc to allow two connected networks to use different and incompatible IP addressing schemes:

- Overview
- Configuring Dynamic NAT
- Configuring Private Networks
- Configuring Port Forwarding

Overview

NAT is a method of allowing two connected networks to use different and incompatible IP addressing schemes. Address translation allows hosts on a private internal network to transparently communicate with devices on an external network and vice versa.

NAT is only supported in IPv4. NAT expands the number of hosts that can interact on the Internet by allowing them to share public IP addresses. Because IPv6 has a significantly larger address space, NAT is not required in IPv6.

Static NAT allows you to use a WAN public IP address for data servers (for example web, mail, or FTP) connected behind the EdgeMarc. These servers can then be configured with private IP addresses for additional security.

The NAT process maps a public address on the system and the IP port number associated with a particular session to the private address and port number of the appropriate IP phone device.

NAT allows many private IP addresses to be mapped to a single public address. However, devices behind NAT are hidden and not directly addressable from a public network. Because IP phone devices need to accept calls from the public network, the system implements ALG/B2BUA to map the common public address to unique private addresses.

Refer to Chapter 6, *Configuring VoIP Settings* for more information about ALG/B2BUA.

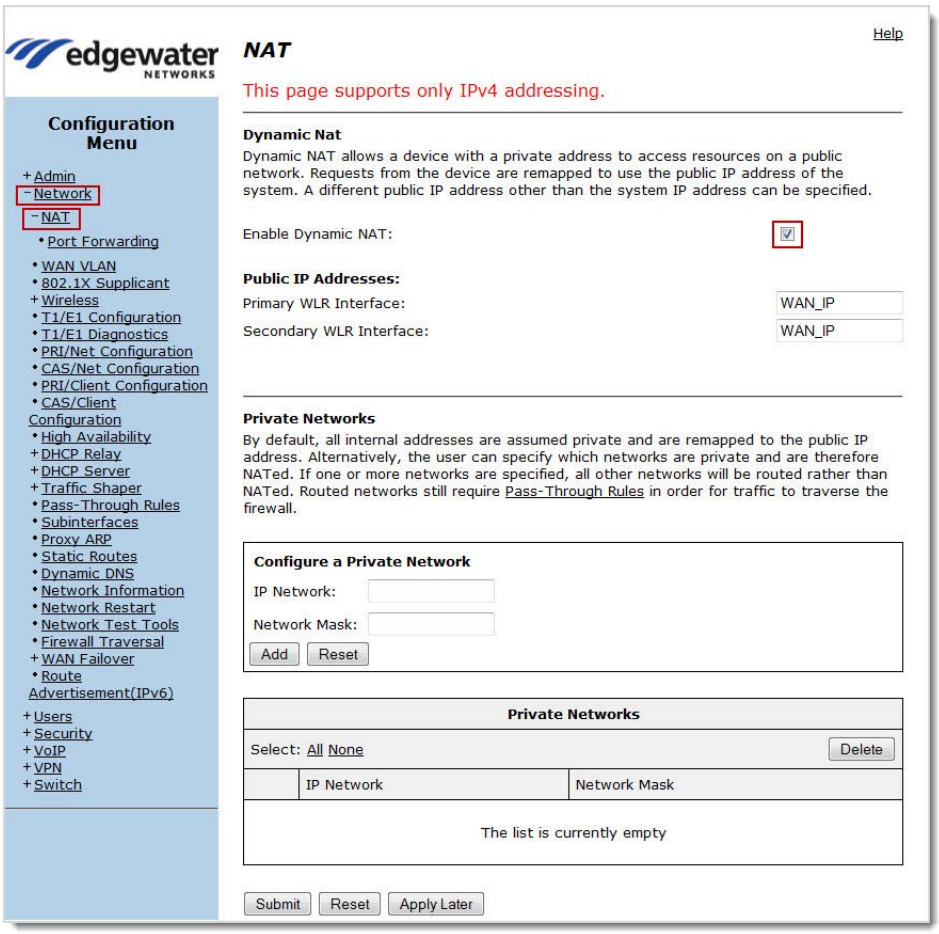
Configuring Dynamic NAT

Dynamic NAT allows a device with a private address to access resources on a public network. Requests from the device are remapped to use the public IP address of the system. A different public IP address other than the system IP address can be specified. NAT can be used to translate LAN IP addresses to the public routable IP address that is assigned to the WAN port.

To configure dynamic NAT:

1. Choose **Network** > **NAT** (Figure 3-26).

Figure 3-26 Nat Page



2. Configure settings using the information in Table 3-4 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-4 Dynamic NAT Parameters

Item	Description
Enable Dynamic NAT	Select the **Enable Dynamic NAT** checkbox.
Public IP Addresses	
These setting apply to services that are running on the system.	
Primary WLR Interface	Enter an IP address in the **Primary WLR Interface** field or leave the default WAN_IP to use the system WAN IP address.
Secondary WLR Interface	(Optional) Enter an IP address in the **Secondary WLR Interface** field, or leave the default WAN_IP to use the system WAN IP address.
Private Networks	
Configures private networks. See Configuring Private Networks.	

Configuring Private Networks

By default, all internal addresses are assumed private and are remapped to the public IP address. You can also specify which networks are private and are therefore NAT-enabled. If one or more networks are specified, all other networks are routed rather than NAT-enabled.

Note
Routed networks still require Pass-Through Rules in order for traffic to traverse the firewall. To configure Pass-Through Rules, choose **Network** > **Pass-Through Rules** and refer to Configuring Pass-Through Rules.

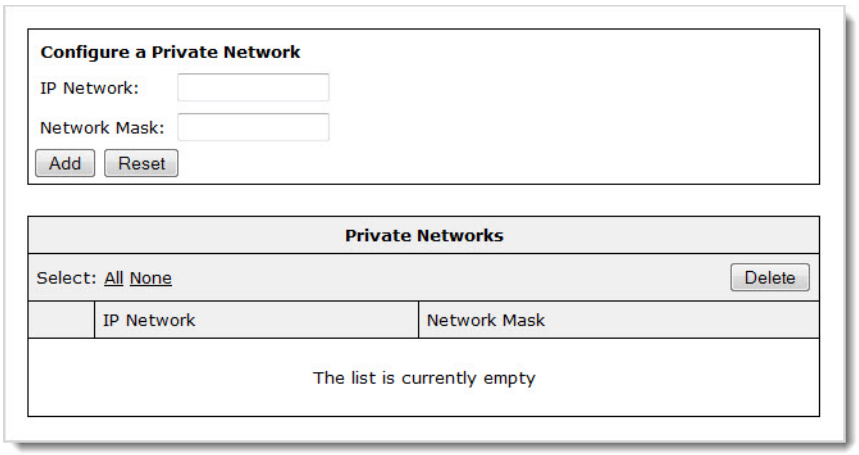
To configure private network settings, see the following sections:

- Configuring a Private Network
- Deleting a Private Network

Configuring a Private Network

1. Choose **Network** > **NAT** (Figure 3-26).
2. Scroll to Private Networks (Figure 3-27).

Figure 3-27 NAT Settings - Private Networks



3. Configure settings using the information in Table 3-5 as a guide. Click **Submit** to save your settings.

Table 3-5 Private Network Parameters

Item	Description
IP Network	Enter an IP address.
Network Mask	Enter a netmask.

Private Networks

Lists configured private networks.

Deleting a Private Network

1. Choose **Network** > **NAT** (Figure 3-26).
2. In the **Private Networks** list, select checkboxes for the entries that you want to delete or click **All** to choose all. Click **None** to clear your selections.
3. Click **Delete**.
4. Click **OK** to confirm.

Configuring Port Forwarding

Port Forwarding allows you to configure Static Network Address Translation on the system. Port Forwarding rewrites the inbound packets destination address and port to an address and port of a host behind the system. When using Port Forwarding, you can access hosts with private addresses from the public network.

To configure port forwarding settings, see the following sections:

- Adding a Port Forwarding Rule

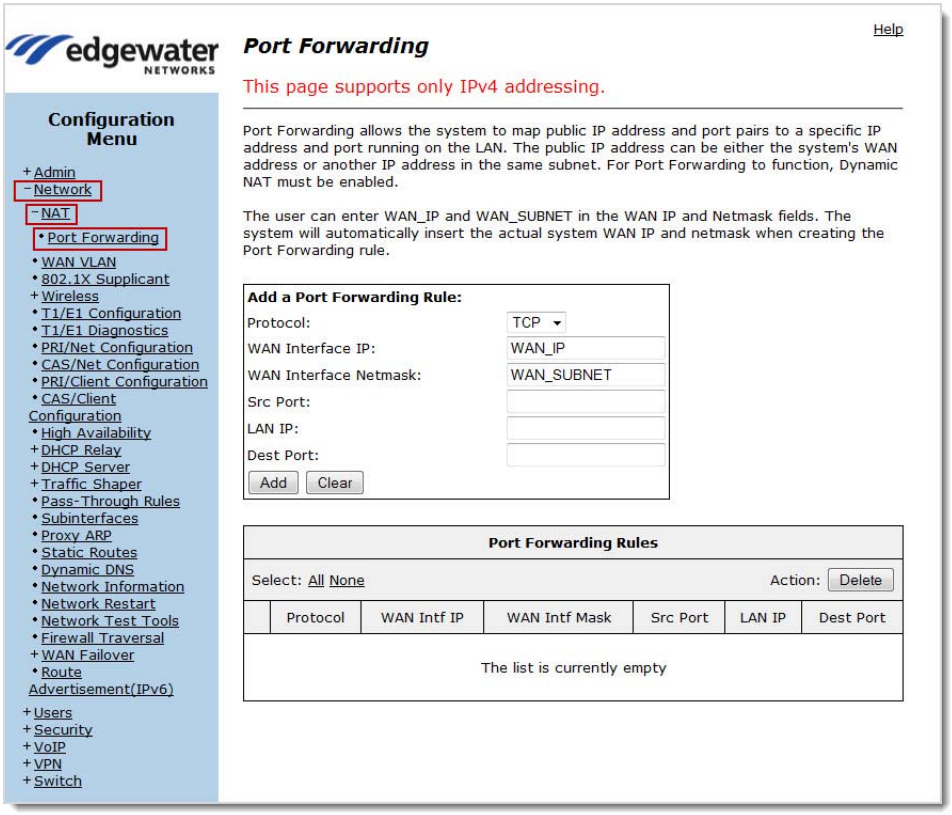
- Deleting Port Forwarding Rules

Note
For Port Forwarding rules to be applied, Dynamic NAT must be enabled. See Configuring Dynamic NAT.

Adding a Port Forwarding Rule

1. Enable Dynamic NAT by choosing **Network** > **NAT** and following the instructions in Configuring Dynamic NAT at the top of the NAT configuration page.
2. Choose **Network** > **NAT** > **Port Forwarding** from the Configuration Menu (Figure 3-28).

Figure 3-28 Port Forwarding



3. Configure settings using the information in Table 3-6 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-6 Port Forwarding Parameters

Item	Description
Protocol	Choose a protocol for the WAN interface from the drop-down list: ■ TCP ■ UDP ■ Any
WAN Interface IP	Enter the device WAN interface IP address or a different public IP address. If you choose different public IP options, the system creates a virtual interface with the WAN address and attaches the virtual interface to the device WAN interface. Packets destined to the WAN address and the WAN port (defined in the **Src Port** field) are translated to the LAN address and port defined in the **Dest Port** field. Specify the “WAN_IP” token to signify a system Primary WAN address. The WAN Address may change dynamically if the WAN interface is using DHCP or PPP. The NAT feature automatically aligns itself to the dynamic WAN IP when using the 'WAN_IP' token. Specify the “HA_VIP” token to signify the High Availability Virtual IP address. Only the MASTER in the High Availability pair sets this rule. See Configuring High Availability.
WAN Interface Netmask	Enter the device WAN subnet or the subnet of the virtual interface. This field sets the “WAN_SUBNET” token to specify the system's Primary WAN Netmask. The WAN Netmask may change dynamically if the WAN interface is using DHCP or PPP. The NAT feature automatically aligns itself to the dynamic WAN Netmask by using the “WAN_SUBNET” token.

Table 3-6 Port Forwarding Parameters (continued)

Item	Description
Src Port	Enter the source WAN port. When the protocol is TCP or UDP, you must define the WAN and LAN ports. Packets destined to the WAN address and port are translated to the **LAN IP** address and LAN **Dest Port**. **Note:** When “any” is specified, all packets destined for the public IP address are translated and sent to the private IP address specified. Port forwarding rules that use a common WAN IP address are treated as an ordered list. Port forwarding rules that appear before the “any” rule for a WAN IP are applied before the “any” rule. Rules for a WAN IP address placed after the “any” rule have no effect. The “any” rule translates and forwards all remaining packets to the selected LAN IP. **WARNING:** When “any” is used, it is recommended that the LAN IP address be protected by a firewall. All packets destined for the specified WAN IP address are translated and forwarded to the LAN IP address. The management services for the system may become unavailable. The management packets could be sent to the specified LAN IP. Make sure an alternative access method is available for management access before adding “any” for the system WAN IP address.
LAN IP	Enter the LAN IP address of the target host behind the voice appliance.
Dest Port	Enter the LAN port on the target host when the protocol is TCP or UDP. Packets destined to the WAN address and port are mapped to a LAN address and port. **Note**: The LAN port is not used if the protocol chosen is “any.”
Private Networks Lists configured private networks.	

Deleting Port Forwarding Rules

1. Choose **Network** > **NAT** > **Port Forwarding** (Figure 3-28).
2. In the **Port Forwarding Rules** list, select checkboxes for the Port Forwarding entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.

3. Click **Delete**.
4. Click **OK** to confirm.

Configuring VLAN Support

Use the VLAN Configuration page to configure VLAN support on the EdgeMarc:

- Overview
- Configuring VLAN Settings
- Configuring WAN VLAN Settings

Overview

The system can be used to connect to an Ethernet switch that has been configured to use VLANs. Typically, VoIP and data devices are separated by different VLANs. This is to ensure priority treatment of the VoIP traffic over data traffic.

The EdgeMarc supports tagged and untagged VLANs. As specified in the IEEE 802.1q standard, tagged VLANs incorporate the VLAN ID and priority in the packet header. Untagged VLAN packets do not include the VLAN ID or priority. Most EdgeMarc models provide support for multiple tagged VLANs. All EdgeMarc models support a maximum of 16 VLANs configured at one time. The following VLAN IDs are used on the EdgeMarc by default:

- VLAN ID 1 (formerly 2730)—Interface management
- VLAN ID 500—Voice
- VLAN ID 600—Data



Note
All voice devices should be placed in the same VLAN.

Configuring VLAN Settings

- Using the VLAN Configuration Page
- Creating a New VLAN
- Configuring VLAN Port Membership
- Configuring VLAN Ports
- Deleting a VLAN

Using the VLAN Configuration Page

If VLAN support is disabled on your system, the following message appears at the top of the VLAN Configuration page:

VLAN support is currently disabled. Configuration shown below will not be active until VLAN support is enabled on the **Network** page.

1. To enable VLAN support, click the **Network** link provided on the VLAN Configuration page.

   Or

2. Choose **Network** from the Configuration Menu (Figure 3).
3. Select the **Enable VLAN Support** checkbox (Figure 3-2) and click **Submit**.

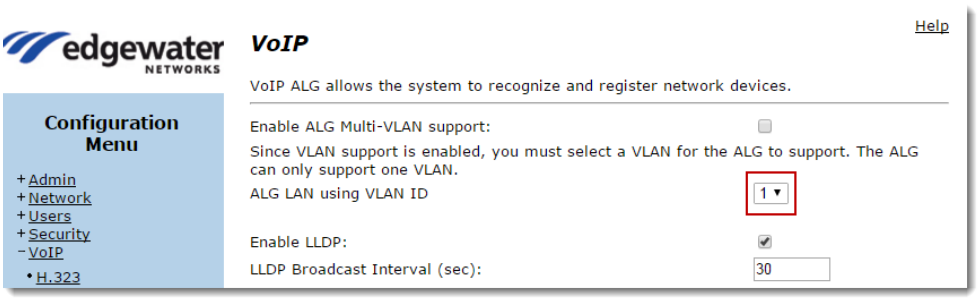
   The system issues the following message:

   WARNING: If changing the IP address, it may be necessary to reach the device by using the new IP address. Please verify the accuracy of the IP address to avoid losing the remote connection. Additionally, all voice and video services will be interrupted. Do you want to continue?
4. Click **OK** to continue.

   The following message is displayed at the top of the Network page:

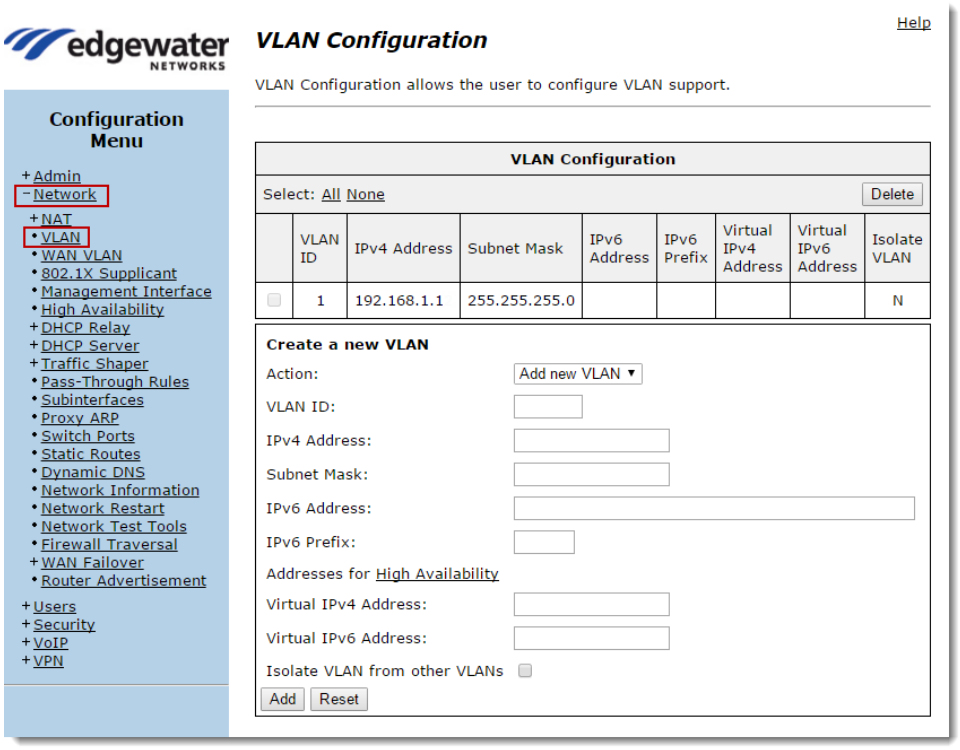
   NOTE: VLAN support enabled. Please ensure that the ALG is set to the correct VLAN ID on the VoIP ALG page.
5. Click the **VoIP ALG** link provided to open the VoIP page or choose **VoIP** from the Configuration Menu.
6. Verify your VLAN ID from the **ALG LAN using VLAN ID** drop-down list (Figure 3-29).

Figure 3-29 ALG LAN Using VLAN IP



7. Choose **Network** > **VLAN** (Figure 3-30).

Figure 3-30 VLAN Configuration Page



8. Configure settings using the information in Table 3-7 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-7 VLAN Configuration Page Parameters

Item	Description
VLAN Configuration	
View and modify existing VLANs configured on the system.	
Create a New VLAN	
Configures VLAN support. See Creating a New VLAN.	
ID	VLAN ID. Valid range is 2 to 4093.
IP Address	IP address of the VLAN.
Network Mask	Network mask of the VLAN.
IPv6 Address	Specifies the VLAN IPv6 address.
IPv6 Prefix	Specifies the VLAN IPv6 prefix.

Table 3-7 VLAN Configuration Page Parameters (continued)

Item	Description
Virtual IP Address	If High Availability is enabled, enter the VLAN virtual IPv4 address.
Virtual IPv6 Address	If High Availability is enabled, enter the VLAN virtual IPv6 address.
Isolate VLAN from other VLANs	Isolates devices on this VLAN from devices on all other VLANs. This allows the isolation at Layer 2 of devices in the same IP subnet to prevent IP address waste. You can restrict some ports on the switch to reach only specific ports that have a default gateway or backup server.

VLAN Port Membership

Assign ports as members of a VLAN. See Configuring VLAN Port Membership.

VLAN Port Configuration

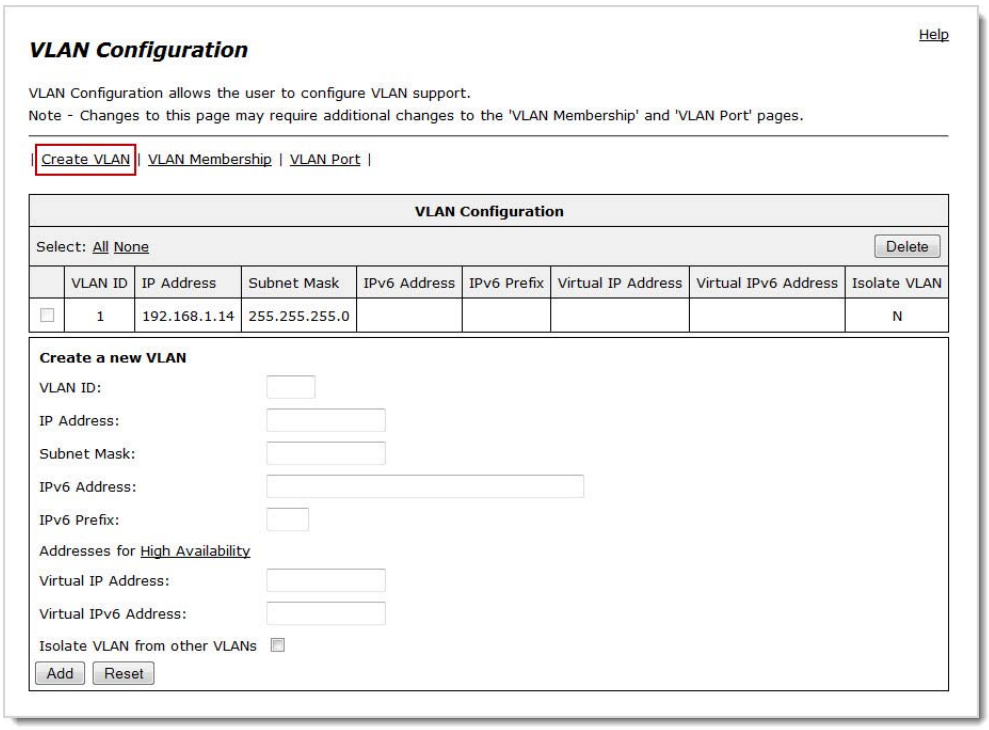
Configures VLAN settings per port. If a drop-down list is empty, no VLANs are assigned to that port. To assign a VLAN to the port, go to the **VLAN Port Membership** page. See Configuring VLAN Ports.

Port number	Specifies the port number.
Packet type	Selects the packet type. By default, both tagged and untagged packet types are accepted on a port.
Port VLAN ID (PVID)	Specifies the port VLAN ID. If a LAN port has multiple VLANs assigned to it, only one of them can be selected as the port's untagged VLAN ID or PVID. By default, a LAN port is assigned to PVID 1. **Note:** If a port is configured to accept tagged packets only, PVID selection is not necessary.

Creating a New VLAN

1. Choose **Network** > **VLAN** (Figure 3-30). The Create a new VLAN page opens by default.
2. If necessary, click **Create a new VLAN** to open the page. Figure 3-31 shows Create a New VLAN input fields.

Figure 3-31 Create a New VLAN Page



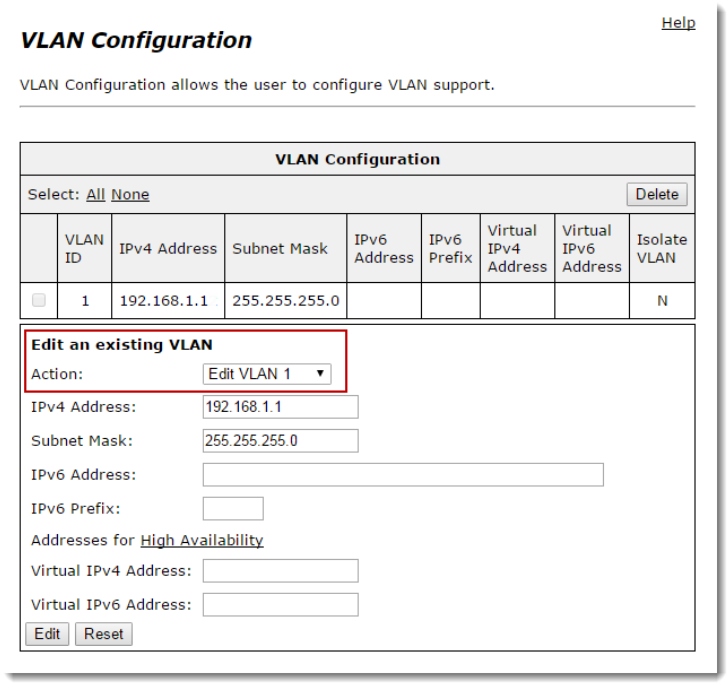
3. In the **VLAN ID** field, enter a number between 2 and 4093.
4. In the **IP Address** field, enter the VLAN IP address.
5. In the **Subnet Mask** field, enter the VLAN subnet mask.
6. In the **IPv6 Address** field, enter the VLAN IPv6 address to uniquely identify the individual network interface.
7. In the **IPv6 Prefix** field, enter a prefix.
8. If High Availability is enabled, enter the VLAN virtual IP address in the **Virtual IP Address** and **Virtual IPv6 Address** fields.

   To configure High Availability, click the **High Availability** link provided on the VLAN Configuration page or choose **Network** > **High Availability** and refer to Configuring High Availability. HA is only available on some EdgeMarc systems.
9. Select the **Isolate VLAN from other VLANs** checkbox to isolate devices on this VLAN from devices on all other VLANs.
10. Click **Add** to add the new VLAN to the VLAN Configuration list.
11. If your system supports VLAN tagging, enter the new VLAN ID, IP address, and network mask. Click **Add**. A new VLAN entry is added to the VLAN configuration.
12. Click **Submit All** to save all changes on the page.
13. Proceed to Configuring VLAN Port Membership.

Editing a VLAN

1. Choose **Network** > **VLAN** (Figure 3-30).
2. In the Create a new VLAN window, select **Edit VLAN *x*** from the **Action** drop-down menu (Figure 3-32).

Figure 3-32 Edit VLAN



3. Edit settings in the fields provided and click **Edit** to save your changes.

Deleting a VLAN

1. Choose **Network** > **VLAN** (Figure 3-30).
2. In the VLAN Configuration table, select the checkbox of the VLAN entry that you want to delete and click **Delete**. Click **OK** to confirm.
3. If a deleted VLAN was previously assigned as the PVID for a port, assign a new PVID to the port on the VLAN Port page. Click **VLAN Port** and refer to Configuring VLAN Ports.

Configuring VLAN Port Membership

The VLAN Configuration page allows you to assign LAN ports as members of a VLAN. If a port is a member of a VLAN, it accepts both tagged and untagged traffic for that VLAN.

Tip
Configure settings on this page before configuring settings in Configuring VLAN Ports.

1. Choose **Network** > **VLAN** (Figure 3-30).
2. Click **VLAN Membership** at the top of the VLAN Configuration page (Figure 3-33) to open the VLAN Port Membership page (Figure 3-34).

Figure 3-33 VLAN Port Membership Link

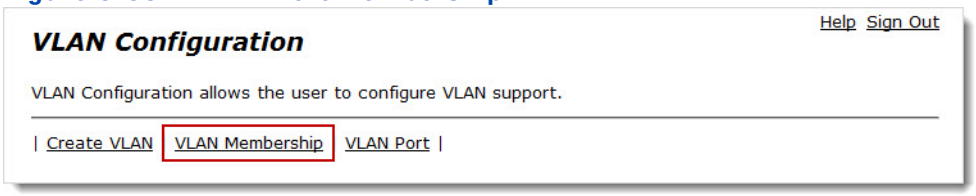
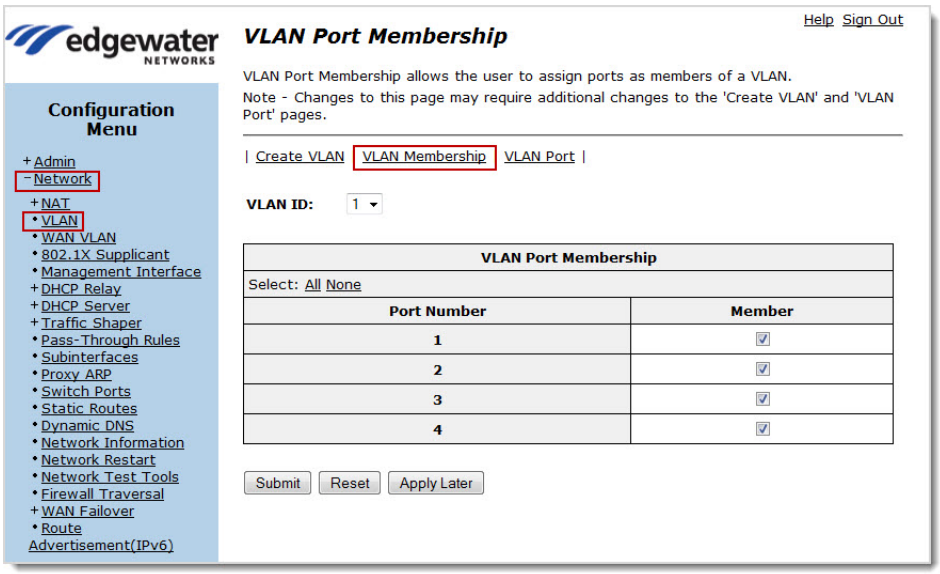


Figure 3-34 VLAN Port Membership Page



3. Choose a VLAN ID from the **VLAN ID** drop-down list.
4. Select the port Member checkboxes that you want to include as members of the selected VLAN. To select all VLANs, click **All**. To clear checked VLANs, click **None**.
5. Click **Submit**.
6. Proceed to Configuring VLAN Ports.

Configuring VLAN Ports

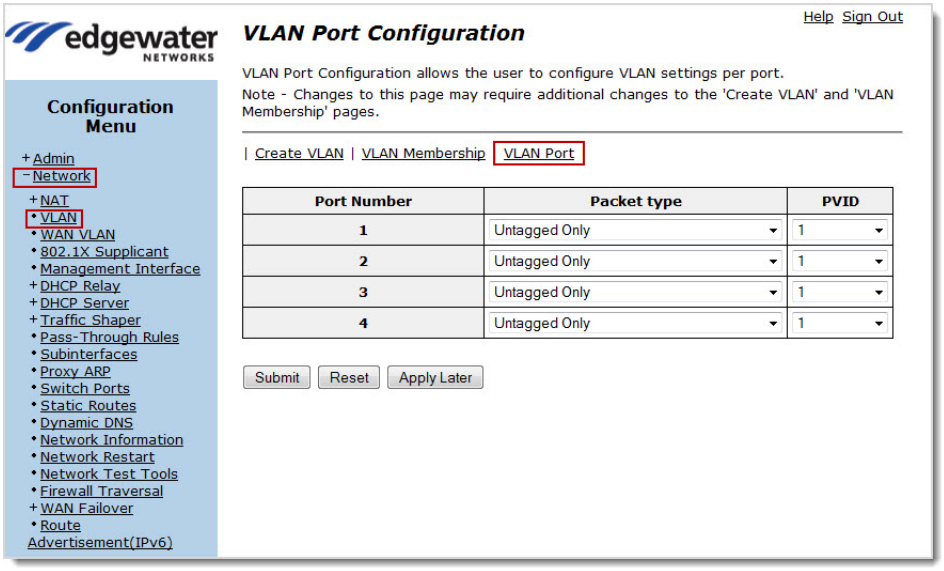
The VLAN Port Configuration page allows you to configure VLAN settings per port. These settings include the packet type accepted on the port and the port Port VLAN ID (PVID).

1. Choose **Network** > **VLAN** (Figure 3-30).
2. Click **VLAN Port** (Figure 3-35) to open the VLAN Port Configuration page (Figure 3-36).

Figure 3-35 VLAN Port Link



Figure 3-36 VLAN Port Configuration Page



3. Configure settings using the information in Table 3-8 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-8 VLAN Port Configuration Parameters

Item	Description
Port Number	Configures VLAN settings per port.
Packet Type	Configures VLAN packet types on the port. Packet type options vary between EdgeMarc models. Choose a packet type for each port from the Packet Type drop-down list: ■ All—Accepts both tagged and untagged packets on the port. ■ Tagged Only—Accepts only VLAN tagged packets on the port and drops untagged packets. The PVID field is disabled. ■ Untagged Only—Accepts only untagged packets on the port and drops tagged packets.
PVID	Assigns a VLAN ID to the port. If you selected Untagged Only in the Packet Type column, choose a Port VLAN ID from the PVID drop-down list. The PVID drop-down list contains all member VLANs to which the port belongs. If a drop-down list is empty, no VLANs were assigned to that port. To assign a VLAN to the port, click **VLAN Membership** and refer to Configuring VLAN Port Membership. If a LAN port has multiple VLANs assigned to it, only one of the VLANs can be selected as the port's untagged VLAN ID. By default, a LAN port is assigned to PVID 1.

Configuring WAN VLAN Settings

Use the WAN VLAN Configuration page to configure the system WAN Ethernet port to support tagged VLANs. By default, all traffic (including data and voice) is tagged with VLAN ID 1.

If WAN VLAN support is disabled on your system, the following message appears at the top of the WAN VLAN Configuration page:

> WAN VLAN is currently not the selected WAN interface. Configuration shown below will not be active until WAN VLAN is selected on the **Network** page.

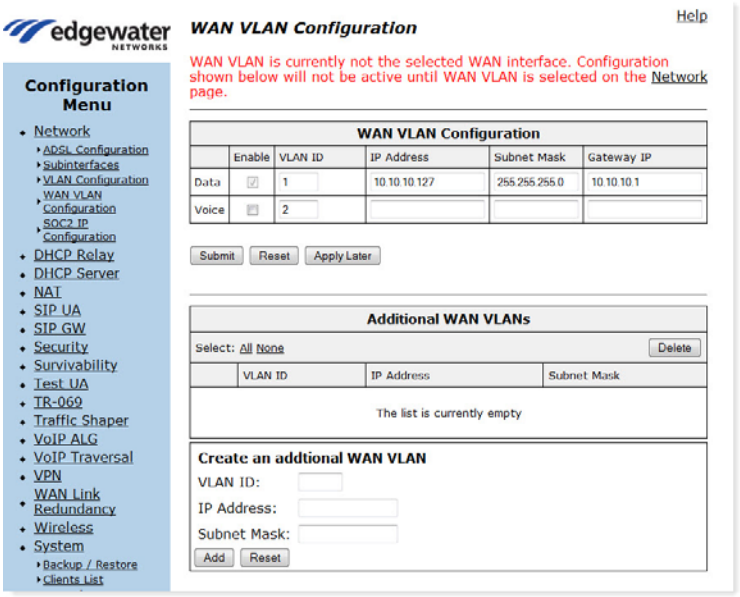
1. Click the **Network** link provided on the WAN VLAN Configuration page.

   Or

2. Choose **Network** from the Configuration Menu (Figure 3).

3. Scroll to **WAN Interface IPv4 Settings** and select the **VLAN** radio button. Refer to IPv4 VLAN for more information.
4. Click the **WAN VLAN Configuration** link provided on the Network page or choose **Network** > **WAN VLAN** to access the WAN VLAN Configuration page (Figure 3-37).

Figure 3-37 WAN VLAN Configuration Page



5. In the Voice section of the WAN VLAN Configuration table, select the **Enable** check box for the Voice VLAN.
6. In the **VLAN ID** field, enter a VLAN ID between 2 and 4094.
7. (Optional) Select the **DHCP** checkbox.
8. Enter the **VLAN IP Address**, **Subnet Mask**, and **Gateway IP** in the fields provided.
9. To configure additional WAN-side VLANs, scroll to **Create an Additional WAN VLAN**:
   a. In the **VLAN ID** field, enter a unique VLAN ID between 2 and 4094.
   b. In the **IP Address** field, enter the VLAN IP address.
   c. In the **Subnet Mask** field, enter a subnet mask.
   d. In the **IPv6 Address** field, enter the IPv6 address.
   e. In the **IPv6 Prefix**, enter the IPv6 prefix.
   f. Click **Add** to add the new VLAN to the Additional WAN VLANs list.
10. Click **Submit All** to save your settings.
11. Restart the network. Choose **Network** > **Network Restart** and refer to Initiating Network Restart.

Deleting a VLAN

To delete a VLAN or multiple VLANs simultaneously from the **Additional WAN VLANs** table:

1. Select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
2. Click **Delete**.



Tip
You must click **Submit All** to save your additional VLAN entries, deletions, and to restart the network with your current VLAN configuration.

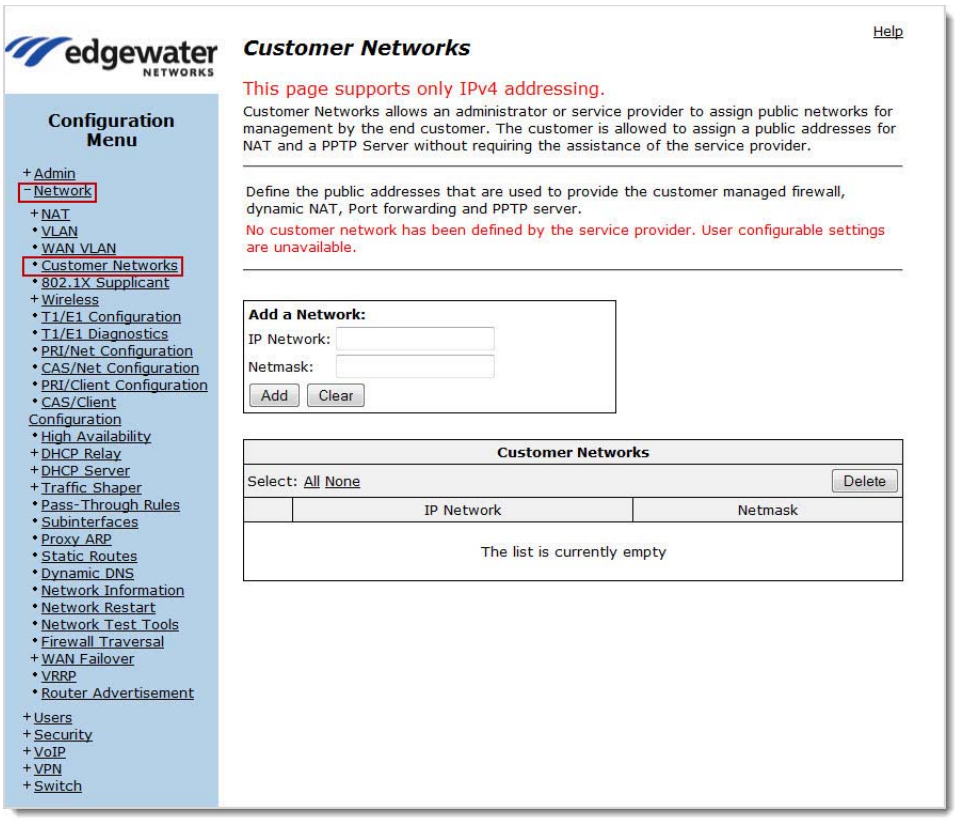
Configuring Customer Networks

Customer Networks allows an administrator or service provider to assign public networks for management by the end customer. Once assigned by the service provider, the customer is allowed to assign the addresses used for NAT and PPTP Server, without requiring the assistance of the service provider.

The Customer Networks page is only available for the root user. The end customer is not allowed to change the networks that can be managed.

1. Choose **Network** > **Customer Networks** (Figure 3-38).

Figure 3-38 Customer Networks Configuration Page



2. Configure settings using the information in Table 3-9 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-9 Customer Networks Configuration Parameters

Item	Description
Customer Network	Defines the public address for the customer managed firewall, dynamic NAT, port forwarding, and the PPTP server. Establish the customer network for the end customer by entering address information in the fields provided:
NAT/Port Forwarding	Enter the address to be used for inbound port forwarding and outbound dynamic NAT connections.
NAT LAN Network	Enter the LAN network address that is associated with the address set in NAT/Port Forwarding. One of the defined LAN networks should be used in this field for NAT to function properly.
NAT LAN Mask	Enter the netmask that is applied to the NAT LAN network.

Table 3-9 Customer Networks Configuration Parameters (continued)

Item	Description
PPTP Server Address	Specifies the address for PPTP VPN connections.
Add a Network Defines a network that the end customer is to allowed to manage.	
IP Network	Enter the network address of the subnet to be managed.
Netmask	Enter the netmask for the IP network. The netmask determines how many addresses are available in the network.
Click **Add** to save your settings.	

Deleting a Customer Network

To delete a network from the Customer Networks table:

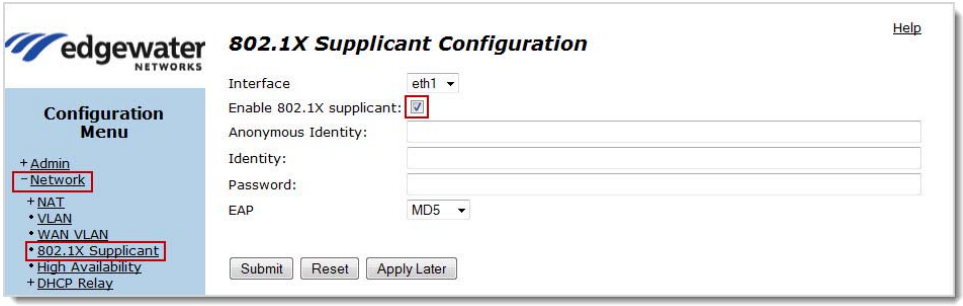
1. Select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
2. Click **Delete**.

Configuring the 802.1X Supplicant

The 802.1x Supplicant Configuration page authenticates the device on a network using 802.1x. 802.1x can be configured to use different authentication mechanisms such as L2 Ethernet for its authentication, but will typically not be able to authenticate over a VLAN.

1. Choose **Network** > **802.1X Supplicant** (Figure 3-39).

Figure 3-39 802.1X Supplicant Configuration Page



2. Configure settings using the information in Table 3-10 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-10 802.1X Supplicant Configuration Parameters

Item	Description
Interface	Select an interface from the **Interface** drop-down list: ■ eth1 (default) ■ eth0 (VID=1) Due to a hardware limitation, authenticating over the LAN port is not supported on the EdgeMarc 4508POE. Refer to 802.1x Supplicant for more information.
Enable 802.1X supplicant	Select the **Enable 802.1X supplicant** checkbox to enable the 802.1X supplicant.
Anonymous Identity	Enter an anonymous ID.
Identity	Enter a username to use with FAST Phase 2 authentication.
Password	Enter a password to use with FAST Phase 2 or MD5 authentication.

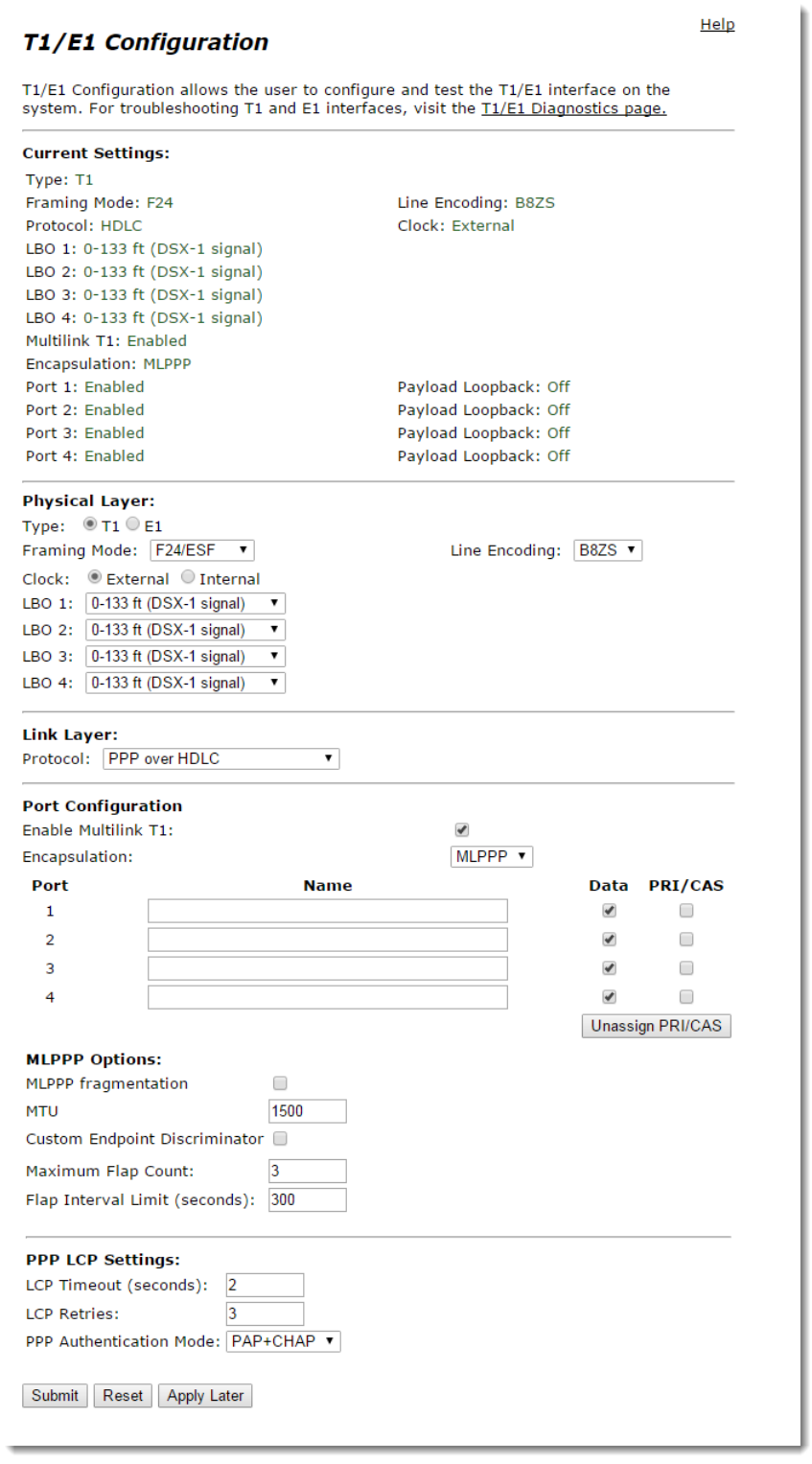
EAP	Selects the Extensible Authentication Protocol (EAP) authentication protocol for your system. Choose an authentication protocol for your system from the **EAP** drop-down list:
	■ MD5—EAP-MD5 password protection only provides authentication of the EAP peer to the EAP server but not mutual authentication. Least secure connection and not suitable for dynamic WEP, or WPA/WPA2 enterprise.
	■ PEAP—Protected Extensible Authentication Protocol (PEAP) with PEAP-MSCHAPv2.
	■ FAST—EAP-FAST (Flexible Authentication via Secure Tunneling) tunnels the authentication data providing more options for security:
	  ■ Phase 1—Validates the tunnel. Only MD5 authentication is supported.
	  ■ Phase 2—Authenticates within the tunnel. The username and password used are “Identity” and “Password.”

Configuring T1/E1 Settings

Use the T1/E1 Configuration page to configure and test the T1/E1 interface on the EdgeMarc.

1. Choose **Network** > **T1/E1 Configuration** (Figure 3-40).
2. Configure settings using the information in Table 4 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Figure 3-40 T1/E1 Configuration Page



Help

T1/E1 Configuration

T1/E1 Configuration allows the user to configure and test the T1/E1 interface on the system. For troubleshooting T1 and E1 interfaces, visit the T1/E1 Diagnostics page.

Current Settings:

Type: T1
Framing Mode: F24 — Line Encoding: B8ZS
Protocol: HDLC — Clock: External
LBO 1: 0-133 ft (DSX-1 signal)
LBO 2: 0-133 ft (DSX-1 signal)
LBO 3: 0-133 ft (DSX-1 signal)
LBO 4: 0-133 ft (DSX-1 signal)
Multilink T1: Enabled
Encapsulation: MLPPP
Port 1: Enabled — Payload Loopback: Off
Port 2: Enabled — Payload Loopback: Off
Port 3: Enabled — Payload Loopback: Off
Port 4: Enabled — Payload Loopback: Off

Physical Layer:

Type: (•) T1 ( ) E1
Framing Mode: F24/ESF — Line Encoding: B8ZS
Clock: (•) External ( ) Internal
LBO 1: 0-133 ft (DSX-1 signal)
LBO 2: 0-133 ft (DSX-1 signal)
LBO 3: 0-133 ft (DSX-1 signal)
LBO 4: 0-133 ft (DSX-1 signal)

Link Layer:

Protocol: PPP over HDLC

Port Configuration

Enable Multilink T1: [x]
Encapsulation: MLPPP

Port	Name	Data	PRI/CAS
1		[x]	[ ]
2		[x]	[ ]
3		[x]	[ ]
4		[x]	[ ]

Unassign PRI/CAS

MLPPP Options:

MLPPP fragmentation [ ]
MTU 1500
Custom Endpoint Discriminator [ ]
Maximum Flap Count: 3
Flap Interval Limit (seconds): 300

PPP LCP Settings:

LCP Timeout (seconds): 2
LCP Retries: 3
PPP Authentication Mode: PAP+CHAP

Submit Reset Apply Later

Figure 4 T1/E1 Configuration Parameters

Item	Description
Current Settings	
Shows information about the current configuration.	
Physical Layer	
See Configuring the T1/E1 Physical Layer.	
Type	Specifies either T1 or E1.
Framing Mode	Defines the number of frames that are grouped together for T1/E1. ■ T1—All T1 Framed modes use a 193-bit frame supporting one framing bit and 24 8-bit channels. There are 8000 frames per second with 1544000 bits per second data rate. ■ ESF—Extended Super Frame groups 24 193-bit frames together, making a 24-bit frame word. Six of the 24 bits are used for the framing pattern, and the other 18 bits are used for other services. ■ SF—Super Frame groups 12 193-bits frames together, making a 12 bit frame word. All 12 bits for the framing word are used for the framing pattern. ■ E1—E1 supports three framing modes and an unframed mode. E1 Framed mode has a 2.048Mbit channel divided into 32 basic channels. Channel 0 is always reserved for framing and cannot be used for media. Channel 16 is the signaling channel and is used for different purposes. E1 frames are 256 bits (32 x 8bits). There are 8000 frames per second with 2048000 bits per second data rate. ■ Double Frame—Basic E1 mode. Two frames are form a 16-bit framing word (2 8bit samples of channel 0). CAS signaling cannot be done in this mode. PRI can be used, and channel 16 is typically used for the D-channel. No cyclic redundancy check (CRC) is performed in this mode. ■ Multi Frame CRC—Groups 16 256-bit frames together creating a 128-bit framing word. Some of the framing bits are used to add a CRC-4 error check. CAS signaling cannot be done in this mode. PRI can be used, and channel 16 is typically used for the D-channel. ■ Multi Frame CRC with CAS—Channel 16 is used for the ABCD CAS signaling bits. This is the only mode that supports CAS signaling. PRI can be used but is not recommended. The D-channel cannot be located on channel 16, and channel 16 cannot be enabled for media. If PRI is used in this mode, a maximum of 29 B-channels can be used (channel 0, channel 16, and the D-channel are not available for media). ■ Unframed—No framing support and can be used for data.
Line Encoding	Defines the bit encoding method used while transmitting data over the line. B8ZS (Bipolar 8 bit zero substitution) and AMI (Alternative Mark Inversion) are currently supported.

Figure 4 T1/E1 Configuration Parameters (continued)

Item	Description
Clock	Displays and sets the timing source for the T1 interface. External—(Default) Retrieves the time from the network. Internal—Generates the time locally. The T1 provider usually provides network timing. Incompatible timing modes can lead to frame slips and temporary loss of data. **Tip:** If PRI is used on one or more of the T1/E1 lines, the clock setting selected in the PRI page is used for that particular T1/E1 line, not the value indicated on the T1/E1 configuration page. All T1/E1 lines that are used for data will use the selection from the T1/E1 Configuration page.
LBO 1 through LBO 4	Line build-out setting (LBO) for T1. Configures the power and attenuation characteristics of the transmit signal from EdgeMarc T1 interfaces. LBO is not available with E1. ■ DS1 level settings are used when connecting an EdgeMarc T1 to a smartjack or T1 provided by the telephone company. The DS1 power levels can be changed depending on the length of the T1 cable from the EdgeMarc to the first T1 repeater. Typical values are 0db and -7.5db. 0db is used for the longest cable lengths while -22.5db is used for the shortest distances. ■ DSX-1 level settings are used when connecting an EdgeMarc T1 to a private line or a co-resident PBX without a CSU/DSU. DSX-1 settings can be changed based on the distance between the EdgeMarc and the terminating device.
Fractional Settings	
These settings are visible if MLPPP is disabled. See Configuring Fractional T1 Links.	
Enable Fractional Support	Enables fractional T1 links. DSO bandwidth configuration fields become active. Fractional support is disabled when Multilink is enabled or when Unframed E1 is configured.
Data DS0 Start	Specifies the starting Digital Signal 0 (DS0) number. The EdgeMarc calculates the total number of contiguous DS0s necessary and configures the line accordingly.
Bandwidth	Specifies the bandwidth for the fractional link as a multiple of 64kbps.
Enable Auto DS0 detection	Automatically configures fractional support based on the IDLE values of unused timeslots.
Auto DS0 IDLE	Sets the Auto DS0 idle time.
Link Layer	
See Configuring the T1/E1 Link Layer.	

Figure 4 T1/E1 Configuration Parameters (continued)

Item	Description
Protocol	Selects T1/E1 layer 2 protocols for the T1/E1 interfaces. **Important:** The protocol must match the protocol sent by the network provider. ■ If multilink is disabled—Supports HDLC, Cisco HDLC, PPP over HDLC, Frame Relay ANSI, and CCITT. Optionally, PPP over Frame Relay may be enabled when ANSI or CCITT is selected as the protocol. The default setting is HDLC. ■ If MLPPP is enabled—Supports HDLC, ANSI, and CCITT. ■ ANSI protocol is PPP over Frame Relay ■ CCITT protocol is PPP over Frame Relay ■ HDLC, PPP operates over the HDLC channels (default) ■ If MLFR is enabled—Supports Frame Relay ANSI and CCITT.
Use PPPoFR	Optional. Enables PPP over Frame Relay when the Frame Relay ANSI or Frame Relay CCITT protocol is selected.
Port Configuration Settings	
See Configuring T1 Ports.	
Enable Multilink T1	Enables Multilink T1 for bundling one or more physical T1 lines together into a single virtual pipe. **Note:** if Multilink T1 is enabled, at least one physical T1 line must also be enabled. All ports selected for data are used in the bundle. MLPPP Options and PPP LCP Settings fields become active. See Configuring T1 Ports.
Encapsulation	Selects either MLPPP or MLFR as the encapsulation method. **Note:** This selection must be the same as the method used by the service provider.
Name	Specifies the interface name to assign to a T1 port. Maximum length is 60 characters. **Note:** This name is not used by the EdgeMarc but is used as a mapping aid for network operators.
Data	Specifies that the port is used for Data. **Note:** Ports used for data can be used for MLPPP bundling.
PRI/CAS	Specifies that the T1 port will be used for PRI/CAS. A maximum of two ports can be used for PRI/CAS. If more than two ports are selected, the lowest numbered licensed ports are used. Use the highest numbered licensed ports for PRI/CAS. T1 data uses the lowest numbered ports, so even if you are not currently using T1 data, using higher numbered ports for PRI will eliminate any port assignment overlap. When T1 PRI/CAS settings in this section are complete, you can configure PRI settings. Refer to Configuring PRI. PRI/CAS is not supported with E1.

Figure 4 T1/E1 Configuration Parameters (continued)

Item	Description
Unassign PRI/CAS	Clears the PRI/CAS checkbox if it was selected. The Data checkbox is re-enabled.

MLPPP Options

Configures Multilink Point-to-Point (MLPPP) load balancing functionality over multiple WAN links. These fields become active when the **Enable Multilink T1** checkbox is selected and Encapsulation is set to MLPP. See Configuring MLPP Settings.

MLPPP fragmentation	Enables data packet fragments to be sent over multiple PPP links to the same IP address.
MTU	Specifies the maximum transmission unit (MTU) size in bytes after which transmission of data to an IP address is fragmented.
Custom Endpoint Discriminator	Specifies the system transmitting the packet and advises the network access server (NAS) that the peer on this link could be the same as the peer on another existing link. Because every client has a unique endpoint discriminator, only multiple links from the same client are bundled into a single unique multilink PPP connection. The **Custom Endpoint Discriminator** field becomes active when the checkbox is selected.
Maximum Flap Count	
Flap Interval Limit (seconds)	

PPP LCP Settings

When in MLPPP, PPPoFR, PPPoMFLR, or MLPoFR modes, the Link Control Protocol (LCP) timeout and retry values can be adjusted for the service provider. The default values which have been optimized for quicker MLPPP link recovery may not work for some service providers. In those instances, recommended values for the timeout and retries are 30 and 3 respectively. In general, higher values may result in more consistent initial link negotiation at the expense of recovery time. If higher values are not required to establish a link, lower values are recommended for great link recovery in multilink connections.

See Configuring PPP LCP Settings.

LCP Timeout	Specifies the timeout for setting up a connection using Link Control Protocol. **Note:** The default values which have been optimized for quicker MLPPP link-recovery may not work for some service providers. The recommended value for retries is 30. In general, lower values are recommended for greater link-recovery in multilink connections.

Figure 4 T1/E1 Configuration Parameters (continued)

Item	Description
LCP Retries	Specifies the number of retries for initiating a connection using LCP. **Note:** The default values which have been optimized for quicker MLPPP link-recovery may not work for some service providers. The recommended value for retries is 3. In general, lower values are recommended for greater link-recovery in multilink connections.
PPP Authentication Settings	Selects the authentication for Peer-to-Peer Protocol (PPP): ■ PAP+CHAP (Password Authentication Protocol and Challenge Handshake Authentication Protocol) ■ CHAP ■ PAP ■ None
Authenticate with PAP only	Specifies that authentication will only occur using a password.
Frame Relay Settings These settings are visible if MLPPP is enabled and one of the PPPoFR protocol options is selected. See Configuring Frame Relay Settings.	
Frame Relay Mode	Specifies data communications equipment (DCE) or data terminal equipment (DTE) mode for frame relay. **Note:** This option is available only for Frame Relay ANSI or CCITT. This value by default is set to DTE. The DLCI value is supplied by the T1/E1 service provider and is used to identify the connection in the link data stream.
Frame Relay DLCI	Specifies the DLCI value, which is a channel number supplied by the T1/E1 service provider that is used to identify the connection in the link data stream. **Restriction:** Values 0-15 and 1023 are reserved and cannot be used. **Note:** When the selected protocol is Frame Relay ANSI or Frame Relay CITTT, a secondary DLCI may also be configured. The secondary DLCI is used for voice services and the Primary DLCI is used for data services. This allows the service provider to provide appropriate treatment to voice and data.
PPPoFR User Name	Specifies the user name for authentication by the PPPoFR switch.
PPPoFR Password	Specifies the password for authentication by the PPPoFR switch.

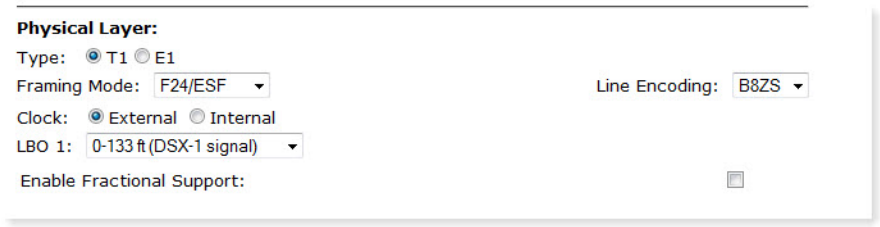
Figure 4 T1/E1 Configuration Parameters (continued)

Item	Description
Frame Relay Secondary Settings	
These settings are visible if MLPPP is disabled and fractional support is enabled. See Configuring Frame Relay Settings.	
Enable Secondary DLCI	Specifies either DCE or DTE mode for frame relay.
Secondary DLCI	Specifies the DLCI value (channel number), which is a channel number supplied by the T1/E1 service provider that is used to identify the connection in the link data stream. **Restriction:** Values 0-15 and 1023 are reserved and cannot be used. **Note:** When the selected protocol is Frame Relay ANSI or CITTT, a secondary DLCI may also be configured. The secondary DLCI is used for voice services and the Primary DLCI is used for data services. This allows the service provider to provide appropriate treatment to voice and data.

Configuring the T1/E1 Physical Layer

1. Choose **Network** > **T1/E1 Configuration** (Figure 3-40).
2. Scroll to **Physical Layer** settings (Figure 3-1).

Figure 3-1 T1/E1 Physical Layer Settings



3. Select the desired protocol Type radio button:
   - T1

     Or
   - E1
4. Select a Framing Mode from the drop-down list:

   Framing Modes for T1

   - F24/ESF—Groups 24 193-bit frames together, making a 24 bit frame word. In extended super frame (ESF) mode, 6 of the 24 bits are used for the framing pattern, and the other 18 bits are used for other services.

- F12/D3/D4—Groups 12 193-bits frames together, making a 12 bit frame word.

Framing Modes for E1

- Double-Frame—Two frames, basic E1 mode
- MultiFrame-CRC-noCAS—16 frames
- MultiFrame-CRC-CAS-only—16 frames, supports CAS signaling
- Unframed—No frames, for data only

5. Select a bit encoding method for transmitting data over the line from the **Line Encoding** drop-down list:
   - AMI (Alternate Mark Inversion) encoding—Available for either T1 or E1
   - B8ZS (Bipolar 8 bit zero substitution)—Default for T1
   - HDB3 (high density bipolar order 3)—Default for E1
6. Select the **Clock** radio button and choose the time source:
   - External—Retrieves the time from the network
   - Internal—Generates the time locally
7. Select an LBO option from the **LBO 1** through **LBO 4** drop-down lists.
   - DS1 level settings are used when connecting an EdgeMarc T1 to a smartjack or T1 provided by a telephone company.
   - DSX-1 level settings are used when connecting an EdgeMarc T1 to a private line or a co-resident PBX without a CSU/DSU.
8. To enable fractional support, proceed to Enabling Fractional Support to enable fractional support.
9. When you are finished configuring all desired settings, click **Submit**.

   A message indicates that service will be interrupted.
10. Click **OK** to confirm.

Configuring Fractional T1 Links

When the protocol is frame relay, additional configuration is needed. The mode value sets the equipment type, either DTE or DCE. Generally, this value is set to DTE for the customer premises. The Data Link Connection Identifier (DLCI) value is supplied by the T1 service provider and is used to identify the connection in the link data stream.

The multi-DLCI enhancement allows two virtual connections over the T1 line with separate IP addresses. This capability is supported in PPP over Frame Relay (either ANSI or CCITT) configuration.

To use this capability, define a permanent virtual circuit (PVC) for data and a secondary PVC for voice, each with a DLCI number. ALG is configured to use the voice PVC, and data is routed through the data PVC. Each has its own user name/password for authentication by the PPPoFR switch during

PPP negotiation. Following authentication, each is assigned its own IP address.

You can assign a contiguous subset of the 24 T1 timeslots to create a fractional T1 link. Specify the starting timeslot (1-24) and bandwidth in increments of 64kbps.

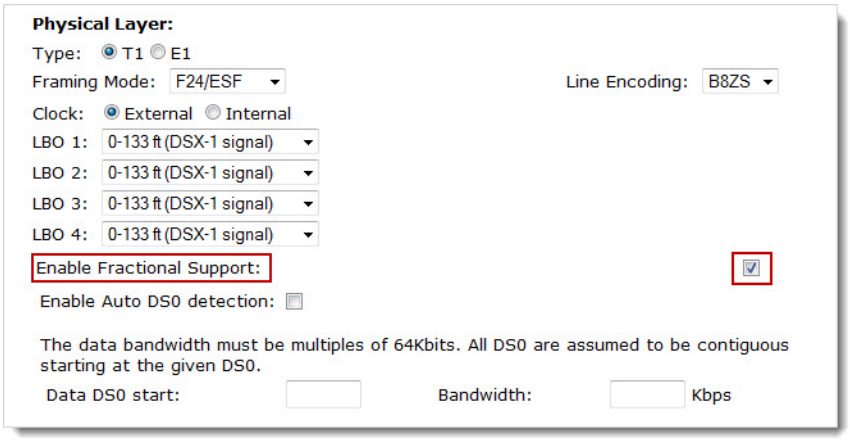
With auto DS0 fractional T1, you can automatically detect the currently-used timeslots based on the pre-configured IDLE value that the T1 service provider provides for unused timeslots.

Enabling Fractional Support

Note
Fractional support is disabled when Multilink is enabled or when Unframed E1 is configured.

1. Select the **Enable Fractional Support** checkbox. DSO configuration fields become active (Figure 3-2).

Figure 3-2 Enable Fractional Support

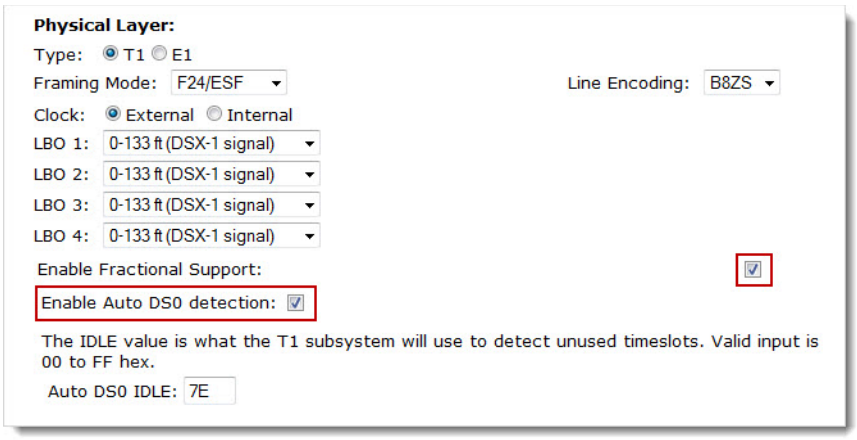


2. In the **Data DSO start** field, enter the starting DS0 number.
3. In the **Bandwidth** field, enter the total bandwidth in increments of 64Kbits. The EdgeMarc calculates the total number of contiguous DS0s necessary and configures the line accordingly.
4. In the **Auto DS0 IDLE** field, enter an idle value in the form 00 to FF hex (for example, 7E to guarantee on-hook switch signaling). The idle value is what the T1 subsystem uses to detect unused timeslots.

   Or

5. Select the **Enable Auto DSO detection** checkbox to set automatic T1 DS0 idle time (Figure 3-3).

Figure 3-3 Enable Auto DS0 Settings



6. When you are finished configuring all desired settings, click **Submit**.
   A message indicates that service will be interrupted.
7. Click **OK** to confirm.

Configuring the T1/E1 Link Layer

1. Choose **Network** > **T1/E1 Configuration**(Figure 3-40).
2. Scroll to **Link Layer** settings (Figure 3-4).

Figure 3-4 Link Layer Settings - HDLC



3. Choose from the following protocol types:
   - HDLC—Default
   - Cisco HDLC
   - PPP over HDLC
   - Frame Relay ANSI—PPP over Frame Relay may be enabled. (Figure 3-5). Select the **Use PPPoFR** checkbox to activate additional configuration fields in Frame Relay Settings and refer to Configuring Frame Relay Settings.

Figure 3-5 Link Layer Settings - ANSI



   - Frame Relay CCITT—PPP over Frame Relay may be enabled. Select the **Use PPPoFR** checkbox to activate additional configuration fields in Frame Relay Settings and refer to Configuring Frame Relay Settings.
4. Click **Submit**.

A message indicates that service will be interrupted.

5. Click **OK** to confirm.

Configuring T1 Ports

1. Choose **Network** > **T1/E1 Configuration** (Figure 3-40).
2. Scroll to **Ports Configuration** (Figure 3-6).

Figure 3-6 Ports Configuration



3. Depending on your service provider settings, select the **Enable Multilink T1** checkbox to allow bundling one or more physical T1 lines together into a single virtual pipe. If Multilink T1 is enabled, at least one physical T1 line must be also enabled. All ports selected for Data are used in the bundle.

   The Encapsulation, MLPPP Options, and PPP LCP Settings fields become active.

4. Choose the **Encapsulation** type from the drop-down list:
   - MLPPP—Supports HLDC, Frame Relay ANSI, and Frame Relay CCITT.

     See Configuring MLPP Settings.
   - MLFR—Supports Frame Relay ANSI and CCITT.

     See Configuring Frame Relay Settings.

   This selection must be the same as the method used by the service provider.
5. Name the configured port for maintaining T1 port mapping. Maximum length is 60 characters.
6. Select the **Data** checkbox to designate a port for data purposes, which is used for MLPPP bundling. E1/T1 Data requires the lowest numbered ports, so even if you are not currently using E1/T1 data, using higher numbered ports for PRI will eliminate any overlap of port assignment.

   Or
7. Select the **PRI/CAS** checkbox to designate a T1 port for configured PRI or CAS (Figure 3-7). Ports assigned for PRI/CAS must be higher than all Data ports and will not be used for MLPPP bundling. Use the highest numbered licensed ports for PRI/CAS.

Figure 3-7 Configuring a T1 Port for PRI/CAS



8. Click **Submit**.

   A message indicates that service will be interrupted.

9. Click **OK** to confirm.

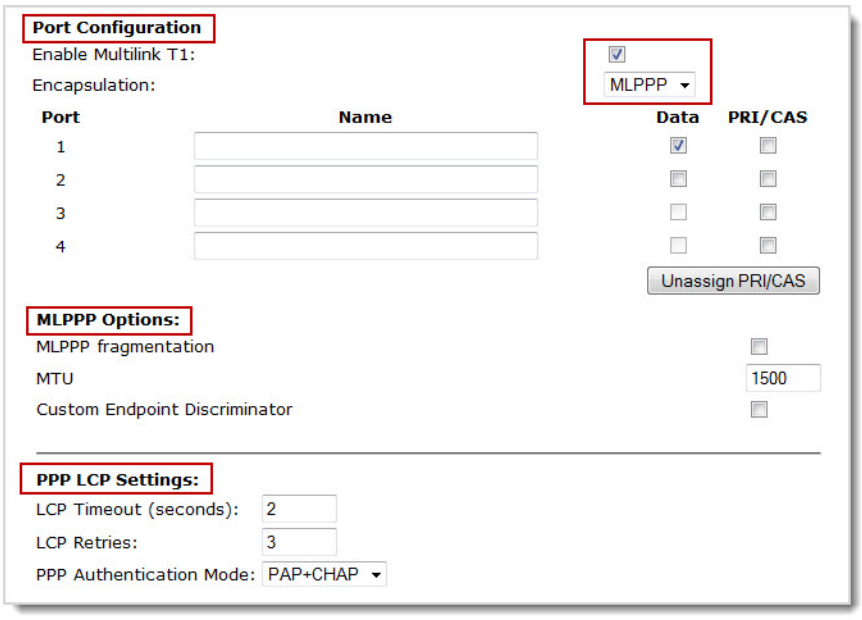
   You can now configure PRI/CAS settings. See Configuring PRI.

10. To clear the PRI/CAS selection, click **Unassign PRI/CAS**.

Configuring MLPP Settings

1. Choose **Network** > **T1/E1 Configuration** (Figure 3-40).
2. Scroll to **Port Configuration** (Figure 3-8).

Figure 3-8 Multilink T1 MLPP Settings



3. Select the **Enable Multilink T1** checkbox.
4. Choose **MLPP** from the **Encapsulation** drop-down list.
5. Assign port Data and PRI/CAS settings as described in Configuring T1 Ports.

6. Select the **MLPPP Options** checkbox.
7. Select the **MLPP fragmentation** checkbox.
8. Enter a value in the **MTU** field.
9. Select the **Custom Endpoint Discriminator** checkbox and enter a value in the field provided.
10. Proceed to Configuring PPP LCP Settings.

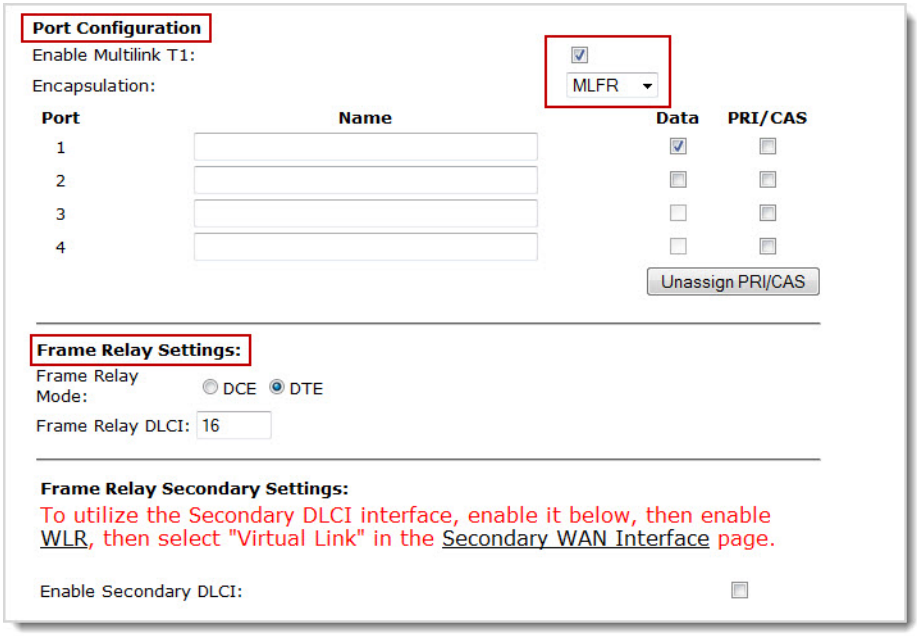
Configuring PPP LCP Settings

1. Choose **Network** > **T1/E1 Configuration** (Figure 3-40).
2. Scroll to **Port Configuration** and enable settings in Configuring T1 Ports and Configuring MLPP Settings.
3. In **PPP LCP Settings**, enter a value in the **LCP Timeout (seconds)** field. Recommended value is 30 seconds.
4. Enter a value in the **LCP Retries** field. Recommended value is 3 retries.
5. Choose an authentication mode from the **PPP Authentication Mode** drop-down list.
6. Click **Submit** to save your settings.

Configuring Frame Relay Settings

1. Choose **Network** > **T1/E1 Configuration**(Figure 3-40).
2. Scroll to **Ports Configuration** (Figure 3-9).

Figure 3-9 Multilink T1 MLFR Settings



3. Select the **Enable Multilink T1** checkbox.
4. Choose **MLFR** from the **Encapsulation** drop-down list.

5. Assign port Data and PRI/CAS settings as described in Configuring T1 Ports.
6. Select the Frame Relay Mode equipment type radio button:
   - DCE
   - DTE—Typical setting
7. Enter a value in the **Frame Relay DLCI** field. The DLCI value is supplied by the T1 service provider and is used to identify the connection in the link data stream. Values 0-15 and 1023 are reserved and should not be used.
8. Click **Submit** to save your settings.

Configuring Frame Relay Secondary Settings

To enable the optional secondary DLCI interface:

1. Select the **Enable Secondary DLCI** checkbox and click **Submit**.
2. On the T1/E1 Configuration page, click the **WLR** link in Frame Relay Secondary Settings and enable settings on the WAN Link Redundancy page. You can also choose **Network** > **WAN Failover** and refer to Configuring WAN Failover.
3. Click **Submit** on the WAN Link Redundancy page.
4. Return to the T1/E1 Configuration page and click the **Secondary WAN Interface** link in Frame Relay Secondary Settings. You can also choose **Network** > **WAN Failover** > **Secondary WAN** and refer to Configuring Secondary WAN Settings.
5. On the Secondary WAN Interface page, select **Virtual Link** and enter the IP address, Network Mask, and gateway for the secondary DLCI.

   The PVC formed by the secondary DLCI is used for voice services and the Primary DLCI is used for data services, allowing the service provider to provide appropriate treatment to voice and data.
6. Click **Submit** on the Secondary WAN Interface page.
7. Return to the T1/E1 Configuration page and enter a value in the **Secondary DLCI** field.
8. Click **Submit**.

   A message indicates that service will be interrupted.
9. Click **OK** to confirm.

Managing the EdgeMarc Daughter Card

Note
Daughter cards are supported on certain EdgeMarc devices.

When you insert the daughter card on EdgeMarc devices that support this type of storage, the status of the card is shown on the following EdgeMarc configuration pages.

Figure 3-10 Daughter Card Ready - T1 Page

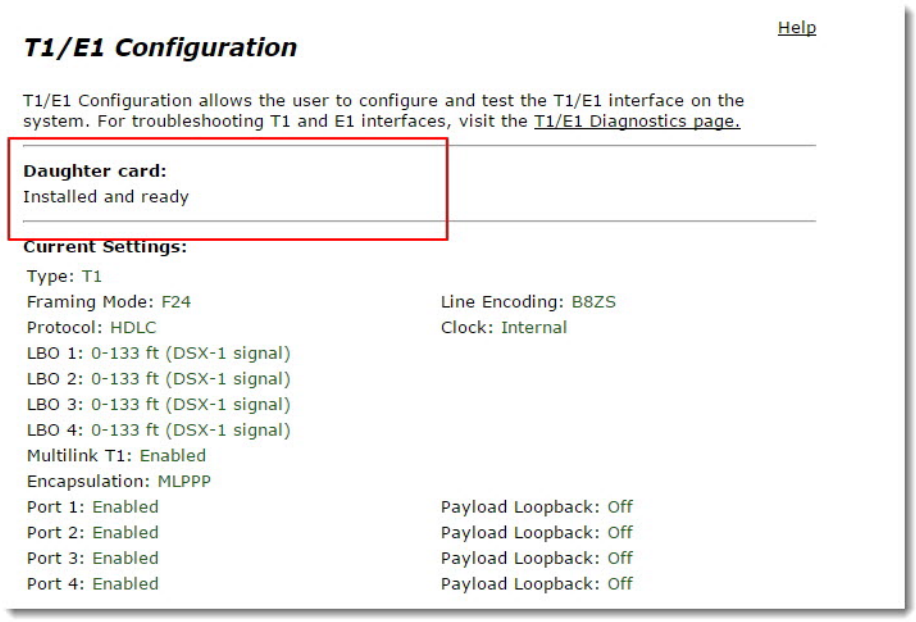
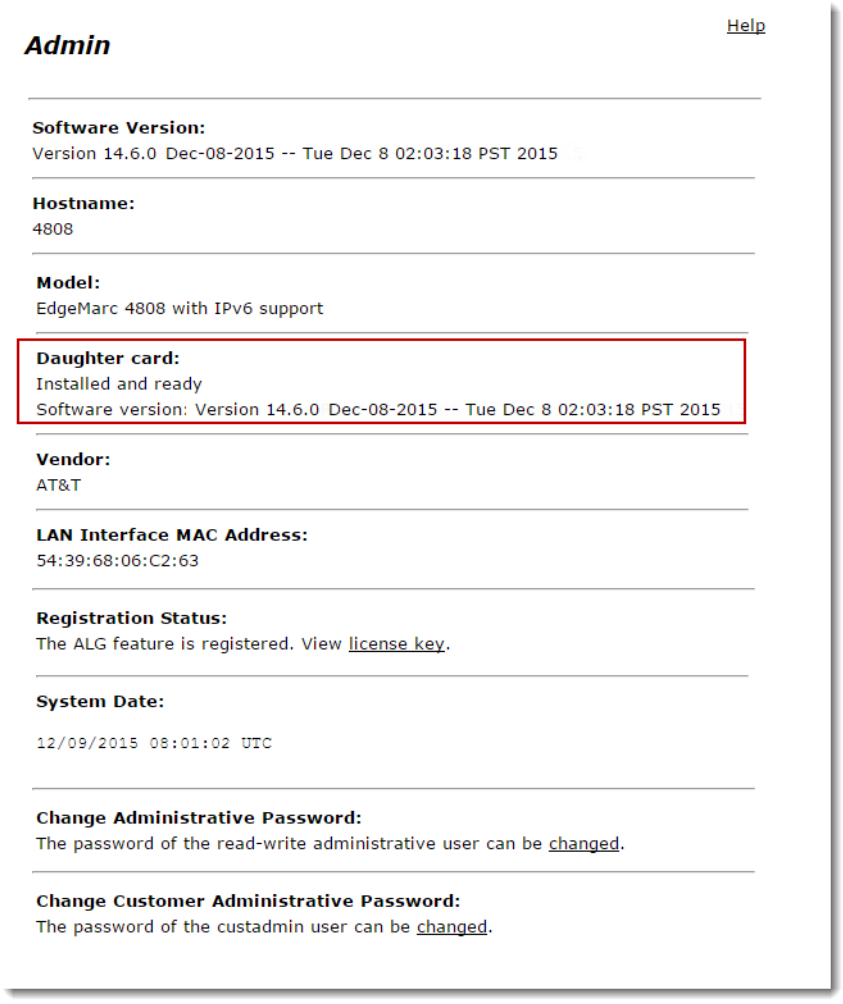


Figure 3-11 Daughter Card Ready - Admin Page



Managing T1/E1 Diagnostics

Use T1/E1 Diagnostics to determine T1 status, retrieve interface statistics and implement loopback and Bit Error Rate Tests (BERT). On platforms that support E1, the T1 properties described on this page also apply to E1 except where noted.

- Using the T1/E1 Diagnostics Page
- T1/E1 Loopback Tests, Alarms, and Counters
- Viewing Advanced T1 Diagnostics

Using the T1/E1 Diagnostics Page

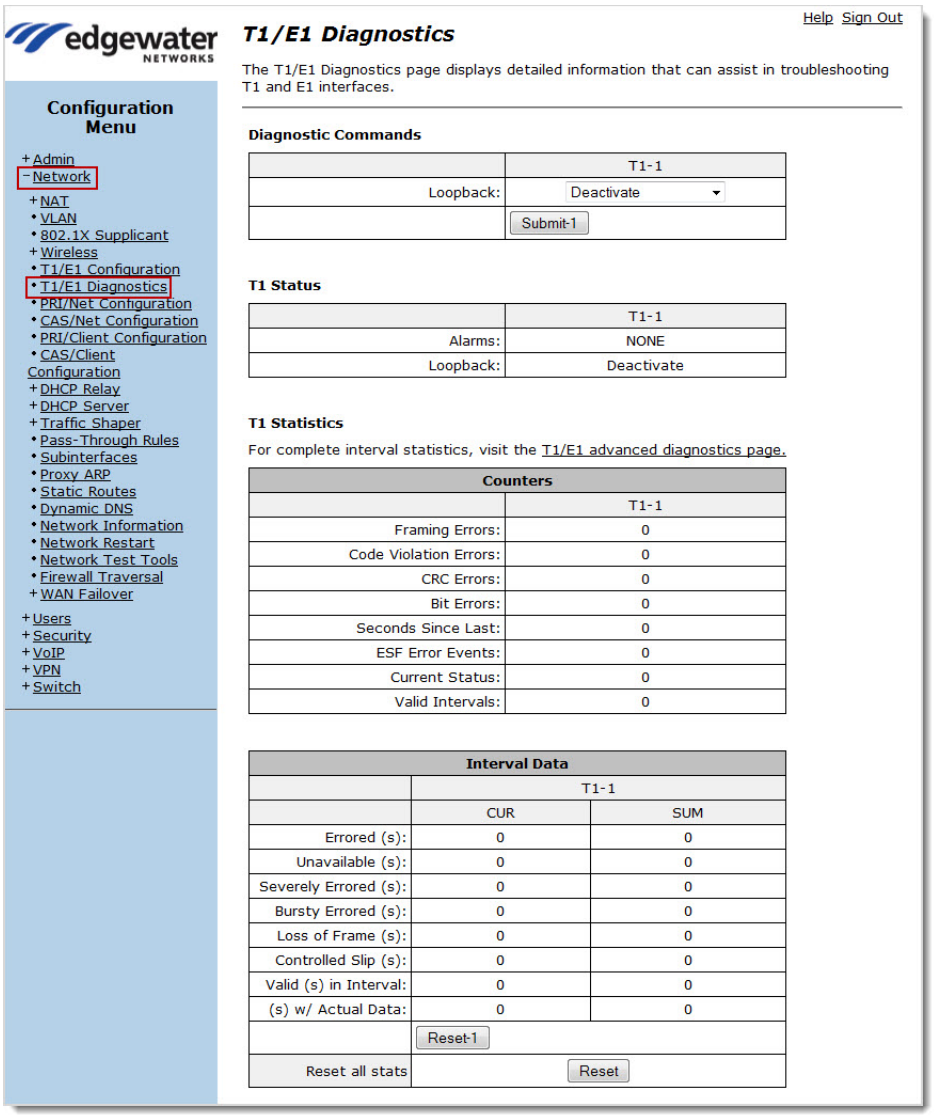
1. Choose **Network** > **T1/E1 Diagnostics** (Figure 3-12).
2. Choose the loopback test you want to run from the **Loopback** drop-down list and click **Submit**. Loopback tests are described in Table 3-11.
3. Select the **BERT** test type from the BERT menu and click **Submit**.

   The BERT test sends a framed Quasi Random Bit Sequence (QRBS) on the T1 link and monitors the receive path for bit errors. A BERT test is usually run in conjunction with a network loopback at the remote end so that the test pattern sent by the EdgeMarc can be compared to the pattern received on the same interface. The EdgeMarc can send a QRBS 2^15-1 and a QRBS 2^20-1 pattern.



Note
The EdgeMarc also responds to network generated, AT&T formatted loop up/down codes. Loopback codes sent from far end equipment loop the T1 interfaces back towards the network. T1/E1 diagnostic counters are described in Table 3-13.

Figure 3-12 T1/E1 Diagnostics Page



T1/E1 Loopback Tests, Alarms, and Counters

- Diagnostic Commands - Loopback Tests
- T1/E1 Status - Alarm Types
- T1/E1 Statistics - Diagnostic Counters
- T1/E1 Interval Data

Diagnostic Commands - Loopback Tests

Several types of loopbacks can be performed on the system T1 interfaces. The system also responds to network generated AT&T formatted loop up/down codes. Loopback codes sent from far-end equipment loop the T1 interfaces back towards the network.

Note
On platforms that support E1, Remote Line and Remote Payload are not supported in E1 mode.

T1/E1 loopback tests are described in Table 3-11.

Table 3-11 Loopback Tests

Item	Description
Local	Tests the inward loopback so that the interface on the EdgeMarc can synchronize on the signal it is sending. Used to verify the proper operation of the T1/E1 interface on the EdgeMarc.
Network line	Loops the data back towards the network before the framer chip in the EdgeMarc.
Network payload	Loops the data back towards the network at the T1/E1 framer chip in the EdgeMarc.
Remote line (AT&T or ANSI)	Sends an AT&T TR 62411 or ANSI T1.403 formatted in-band line loop code to the network. Generating this code causes the remote equipment to loop data back to the EdgeMarc.
Remote payload (AT&T or ANSI)	Sends an AT&T TR 62411 or ANSI T1.403 formatted in-band payload loop code to the network. Generating this code causes the remote equipment to loop data back to the EdgeMarc.
Submit	Implements or deactivates an existing loopback for a specific interface once the desired option is chosen from the Loopback drop-down list.

T1/E1 Status - Alarm Types

T1 Status shows the current alarm state and if there is a loopback or BERT test in progress. T1/E1 alarm types are described in Table 3-12.

Table 3-12 Alarm Types

Type	Description
Red Alarm	The EdgeMarc is not receiving a valid framing pattern from the network. Something is usually broken with the EdgeMarc receiving path of the T1/E1 line or with the sending equipment.
Yellow Alarm	The remote end (network side T1/E1 interface) is not able to synchronize to the signal sent by the EdgeMarc. Something is usually broken with the EdgeMarc transmit path of the T1/E1 line or with the receiving equipment.
Blue Alarm	The EdgeMarc is receiving an unframed all ones signal. This usually indicates a problem with the network side equipment.

T1/E1 Statistics - Diagnostic Counters

The system displays the current 15-minute (CUR) and 24-hour total (SUM) statistics for the T1 interfaces. These statistics provide an easy way to compare results from two different time frames for the network. The system also provides detailed statistics for each 15-minute interval over the last 24 hours on the T1 advanced diagnostics page. The oldest-15 minute interval is deleted from the 24-hour total as a new 15-minute interval is added.

On platforms that support E1, only the first 4 Counters are supported in E1 mode. Interval Data is not supported in E1 mode.

T1/E1 diagnostic counters are described in Table 3-13. For complete interval statistics, click the **T1/E1 Advanced Diagnostics** link and refer to Viewing Advanced T1 Diagnostics.

Table 3-13 T1/E1 Diagnostic Counters

Counter Type	Description
Framing Errors	Incorrect or unexpected framing bit has been received.
Code Violation Errors	Bipolar Violation (BPV) or excessive zero event.
CRC Errors	Received cyclical redundancy check (CRC) code does not match the code that was calculated locally.
Bit Errors	Number of bit errors during Bit Error Rate Tests (BERT)/QRBS test.
Seconds Since Last	Number of seconds since the last performance data event. **Note:** T1.403 and TR54016 standards allow for performance data via FDL. This is the number of seconds since the last receive of FDL performance data.
ESF Error Events	CRC or out of frame event.
Current Status	Current status code.
Valid Intervals	Number of valid 15 minute intervals.

T1/E1 Interval Data

T1/E1 interval data is described in Table 3-14. The **Reset** button resets the statistics in the current interval.

Table 3-14 Interval Data

Interval Data	Description
Errored (s)	Number of seconds with one or more Extended Superframe (ESF) Error events.
Unavailable (s)	Number of seconds during which the T1/E1 interface is unavailable.
Severely Errored (s)	Number of seconds with 320 or more ESF error events.
Bursty Errored (s)	Number of seconds with more than one and fewer than 320 ESF error events.
Loss of Frame (s)	Number of seconds during which an out of frame error is detected.
Controlled Slip (s)	Number of seconds during which there have been one or more controlled slips. A controlled slip occurs when there is a difference between the timing of the EdgeMarc and the received T1/E1 signal.

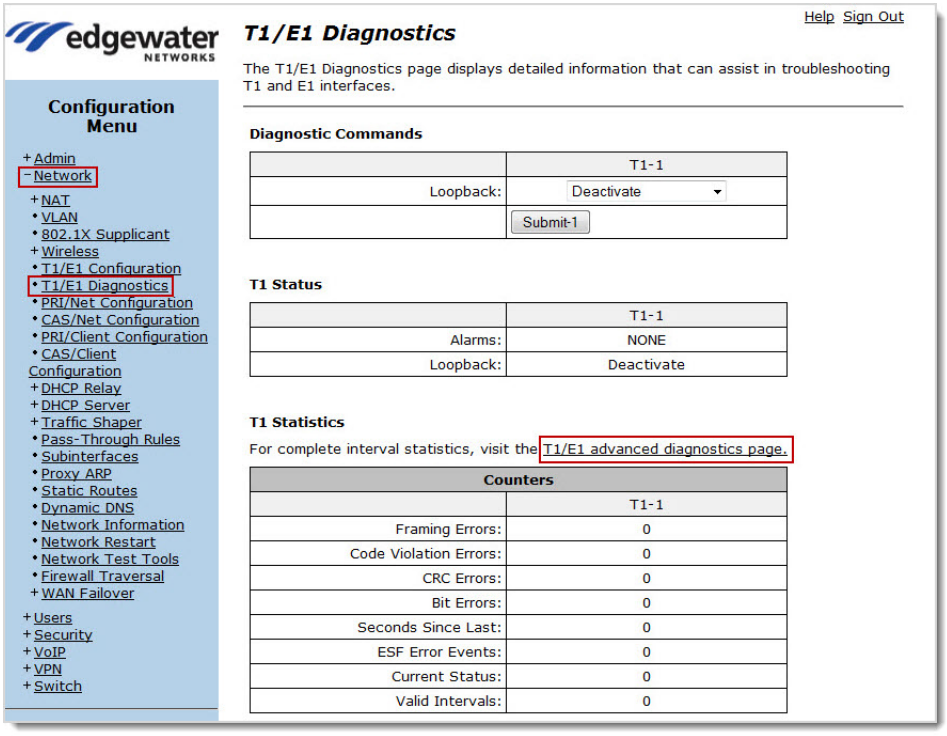
Table 3-14 Interval Data (continued)

Interval Data	Description
Valid Intervals	Number of elapsed seconds in the current interval.
(s) w/ Actual Data	Number of seconds for which there is data.
Reset	Resets the statistics in the current interval.
Reset all stats	Resets all statistics in the current interval.

Viewing Advanced T1 Diagnostics

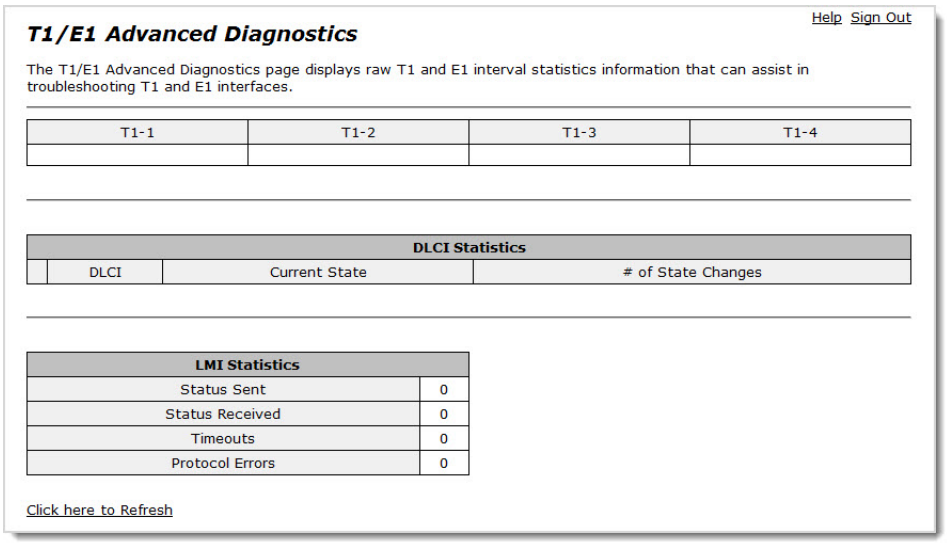
1. Choose **Network** > **T1/E1 Diagnostics** (Figure 3-12).
2. On the T1/E1 Diagnostics page, scroll to **T1 Statistics** and click **T1/E1 Advanced Diagnostics** (Figure 3-13).

Figure 3-13 Advanced Diagnostics Link



The T1/E1 Advanced Diagnostics page displays (Figure 3-14). The page displays data for each 15-minute interval over the last 24 hours. The oldest 15-minute interval is removed from the 24-hour total as each new 15-minute interval is added.

Figure 3-14 T1/E1 Advanced Diagnostics Page



Configuring PRI

This section describes how to configure the ISDN Primary Rate Interface (PRI) on the EdgeMarc:

- Overview
- Configuring Network Side ISDN PRI (PRI/UA)
- Configuring Network Side CAS/UA
- Configuring Client Side ISDN PRI (PRI/GW)
- Configuring Client Side CAS/GW

Overview

The EdgeMarc can be configured to act as a gateway (client device) connecting the IP network to PSTN through to one more T1 or E1 PRI lines. It can also work as a network device connecting a PBX to the IP network. The default configuration enables 23 B channels (bearer channels) at 64 Kbps each and 1 D channel (delta channel) at 64 Kbps each.

The EdgeMarc supports the following PRI features:

- The appliance can be a client device (gateway) or network device, but not both.
- Supports the following switch types:
  - 4ESS
  - 5ESS
  - DMS100
  - EURO

- HK
- NISDN-2 or NI2

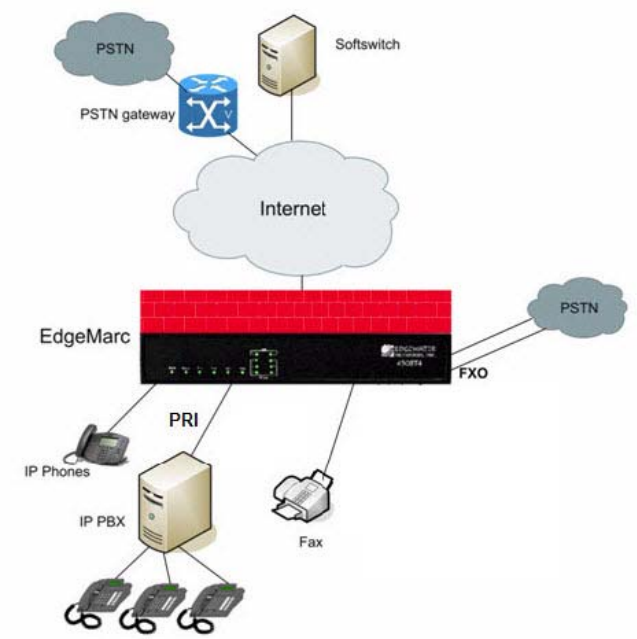
- The highest port numbers of licensed T1/E1 ports should be used for PRI.

Network Side ISDN PRI (PRI/UA)

Network Side PRI enables the SIP_UA(SIP User Agent) to provide a standard ISDN PRI Network-side interface to the PBXs and to mimic the behavior of legacy phone switches. SIP_UA will receive calls from PBXs and connect call on IP network using SIP.

Figure 3-15 shows an example of Network Side PRI.

Figure 3-15 Network Side ISDN PRI (PRI/UA)

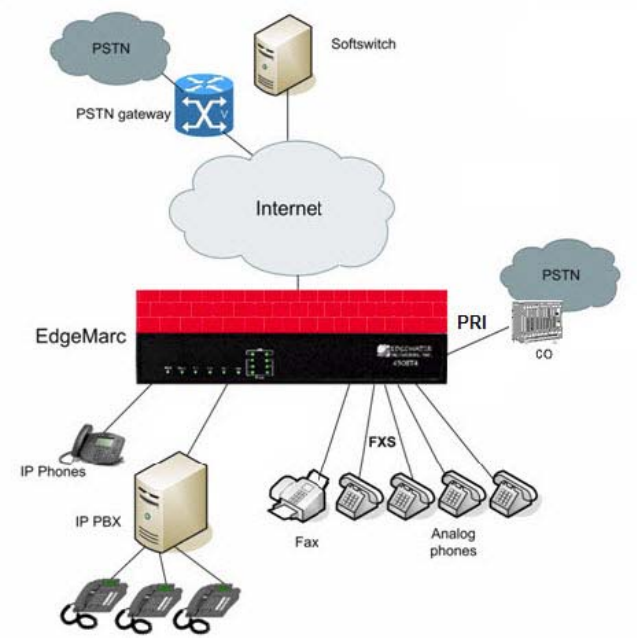


Client Side PRI

Client Side PRI enables the SIP gateway (GW) to provide a standard PRI client-side interface to the PSTN. SIP GW receives calls from the IP side and connects them to the PSTN and vice versa. Enable PRI/GW services

Figure 3-16 shows an example of Client Side PRI.

Figure 3-16 Client Side ISDN PRI (PRI/GW)



PRI Configuration Requirements

Caution
Do not change the IP address unless absolutely necessary. If you change the IP address, make sure that the IP address is in the same subnet as the LAN or VLAN that the VOIP ALG is listening on. Do not use an address that is already in use.

1. Only one type of CAS/PRI interface can be enabled at a time.
   a. Disable the current CAS/PRI configuration by un-checking the "Enable" checkbox on the supporting configuration page
   b. Click **Submit**.
   c. Proceed to one of the following options to configure CAS/PRI:
      - Configuring Network Side ISDN PRI (PRI/UA)
      - Configuring Network Side CAS/UA
      - Configuring Client Side ISDN PRI (PRI/GW)
      - Configuring Client Side CAS/GW
2. To enable service, you must configure the IP trunking device and dial rule to terminate VoIP traffic to the Network or Client side. For example, if Network PRI/UA is bound to 10.1.2.1:1025, you would add a trunking device giving the IP 10.10201 and port 1025. You can pick any name for the trunking device. Once the device is added, define a dial rule that will then truncate to this newly created device.
   a. Create a SIP Trunking device for PRI with the same name as the one used in **VoIP** > **ALG** > **SIP UA** (Network side settings) or **VoIP** >

ALG > **SIP GW** (Client side settings). See Configuring SIP Trunking Devices in Chapter 6, *Configuring VoIP Settings*.

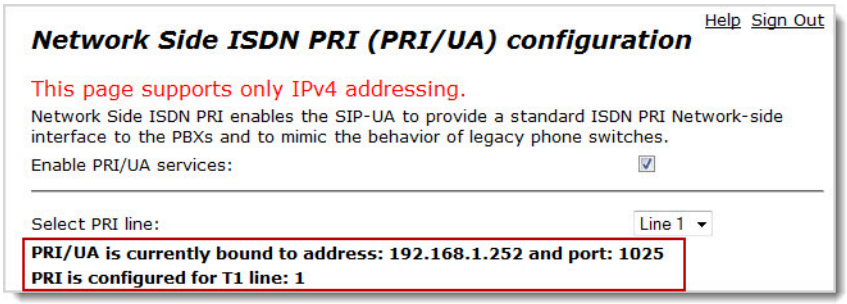
b. Associate an inbound default dial rule with the newly created device. See Configuring Dial Rules in Chapter 6, *Configuring VoIP Settings*.

Note
All inbound traffic coming to CAS/SIP UA is forwarded to the PRI device with the exception of the traffic destined for one of the registered FXS ports.

3. Obtain the SIP UA IP address and port number by going to **VoIP** > **SIP** > **SIP UA** CAS or PRI Network configuration pages and checking for the IP-to-port binding information, for example (Figure 3-17):

"SIP/UA is currently bound to address: <*IP Address*> and port: <*Port Number*>"

Figure 3-17 PRI SIP UA IP Address and Port Binding



IP-to-port binding information is also shown on the FXS/Phone Port Settings - Basic page. Choose **VoIP** > **SIP** > **SIP UA** and refer to Configuring Basic SIP UA FXS Settings in Chapter 6, *Configuring VoIP Settings*.

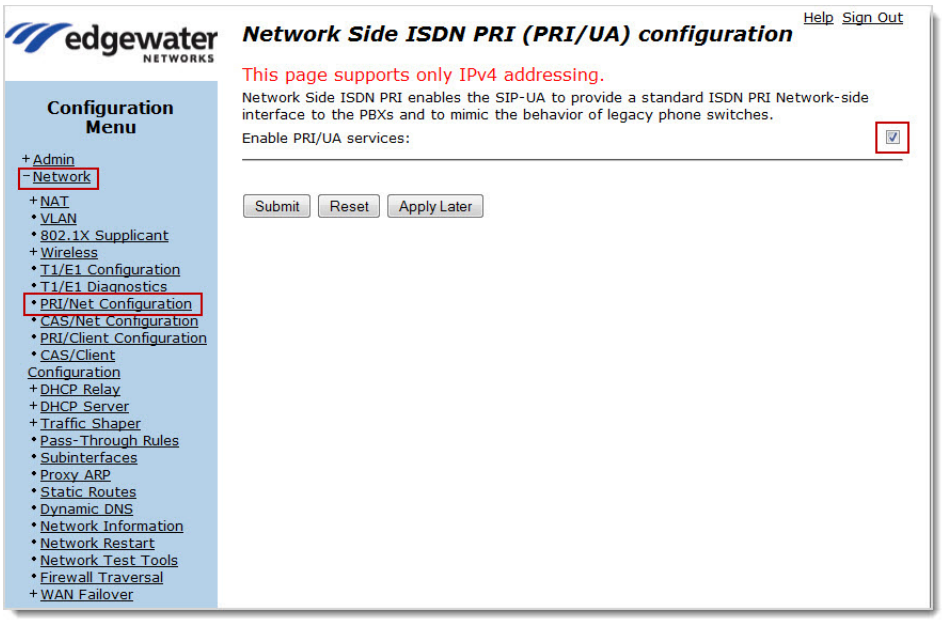
Configuring Network Side ISDN PRI (PRI/UA)

Network side PRI enables SIP UA (SIP User Agent) to provide a standard ISDN PRI network side interface to the PBX, and to mimic the behavior of legacy phone switches. SIP UA receives calls from the PBX and connects calls on the IP network using SIP.

Tip
Complete the steps in PRI Configuration Requirements.

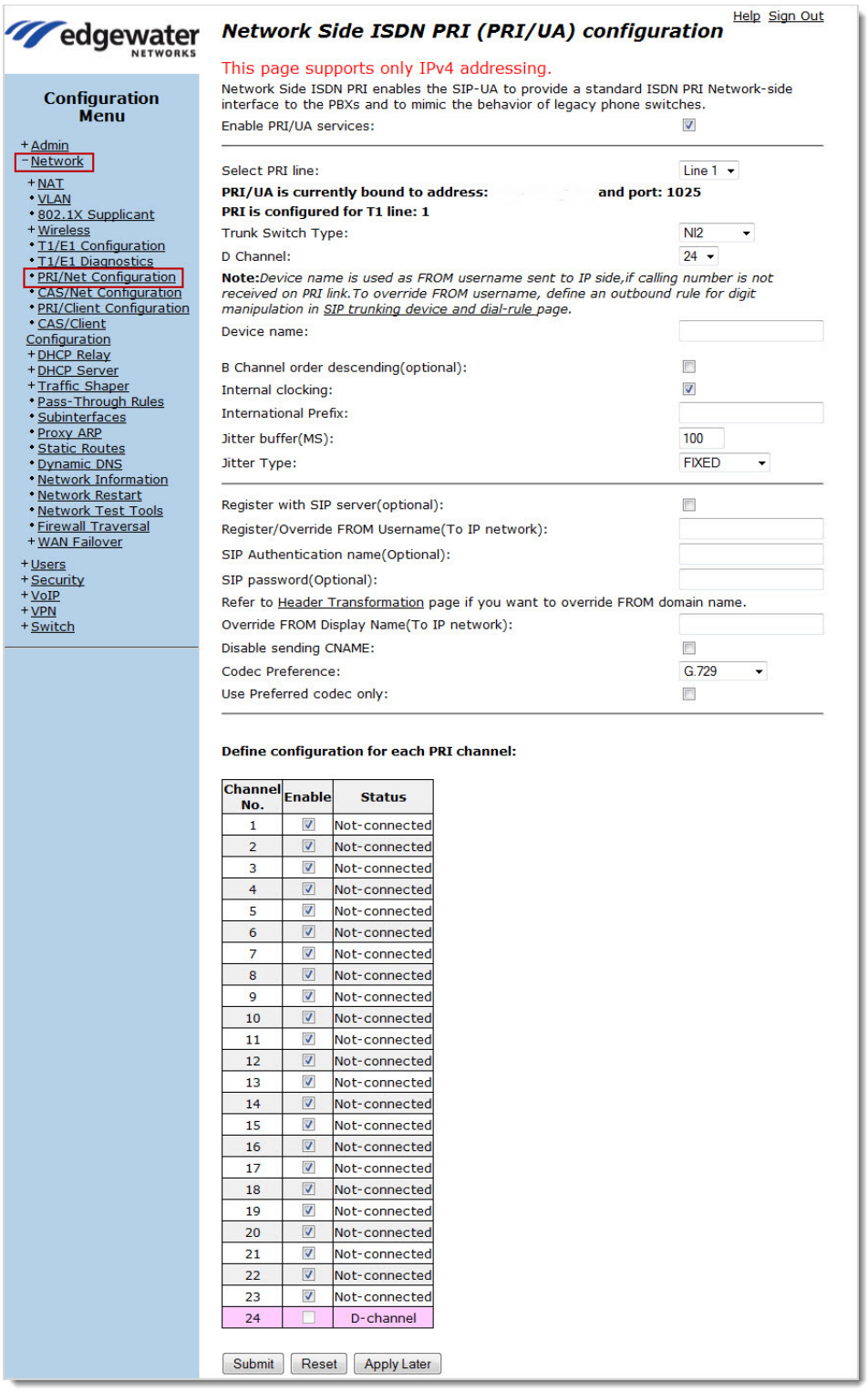
1. Choose **Network** > **PRI/Net Configuration** (Figure 3-18).

Figure 3-18 Enable Network Side ISDN PRI (PRI/UA)



2. Select the **Enable PRI/UA services** checkbox and click **Submit** to activate fields on the Network Side ISDN PRI (PRI/UA) Configuration page (Figure 3-19).

Figure 3-19 Network Side ISDN PRI (PRI/UA) Configuration Page



3. Configure settings using the information in Table 3-15 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.



Tip
TX/RX gains can be set at 2DB increments and the capability is extended to the SD card, if present.

Table 3-15 Network Side ISDN PRI (PRI/UA) Parameters

Item	Description
Enable PRI/UA service	Select the **Enable PRI/UA service** checkbox to enable service.
Select PRI line	Choose a T1 line for ISDN PRI from the **Select PRI line** drop-down list. Valid range is 1-4 based on the number of T1 lines available on a given EdgeMarc platform.
Trunk Switch Type	Enter the switch type that client-side ISDN PRI will be simulating. NI2 is selected by default. It is important that the switch type matches the Network-side switch type to which this interface is connected.
D Channel	Choose a number from the **D Channel** drop-down list to use for Q.931 signaling.
Device name	Enter a device name for the SIP FROM user if caller information is not available in a call coming into the PRI trunk from the remote PRI/T1 link. To override the FROM username, define an outbound rule for digit manipulation from the SIP trunking device and dial rule page. Click the **SIP trunking device and dial-rule** link provided or choose **VoIP** > **SIP** > **ALG** and refer to Configuring VoIP SIP B2BUA Trunking in Chapter 6, *Configuring VoIP Settings*.
B Channel order descending	(Optional) Select the **B Channel** checkbox to change B channel order to descending (24-1). B channel ordering is ascending (1-24) by default when doing a call setup.
Internal clocking	Select the **Internal clocking** checkbox to set the internal clocking mode for PRI. External clocking is used by default.
International Prefix	Enter a value to prepend a prefix to incoming international PRI calls. If the field is empty or a prefix is already part of the called number, no action is taken.

Table 3-15 Network Side ISDN PRI (PRI/UA) Parameters

Item	Description
Jitter buffer (MS)	Enter the jitter buffer value based on the IP network condition. Value is equal to or greater than 40 msecs. Default is 100 msecs.
Jitter Type	Choose the Jitter buffer type from the drop-down list: ■ Fixed—Default ■ Adaptive
SIP Server Settings	
Configure the following settings:	
Register with SIP server	(Optional) Select the **Register with SIP server** checkbox to register with SIP server using the "Register FROM Username" as SIP user name.
Register/Override FROM Username (To IP network)	Enter a name to override the system default DISPLAY name when sending SIP request to IP side. A call coming in Network-side PRI/GW from the PBX is terminated on IP network. By default, the gateway uses the PRI callerID in the FROM field of SIP INVITE message when terminating call on the IP side. If the callerID is not present, the gateway uses the internal name specified.
SIP Authentication name	(Optional) Enter the SIP authentication name used to authenticate the PRI/GW if the gateway registers with name defined in the Register FROM Username field.
SIP password	(Optional) Enter the SIP authentication password used to authenticate the PRI/GW if the gateway registers with the name defined in Register FROM Username field.
Override FROM Display Name (To IP network)	Enter a name to override the DISPLAY name when sending SIP requests to the IP side. An Inbound call coming into PRI/GW from the remote PRI/T1 link is terminated on IP network. By default, the gateway uses this name as part of the DISPLAY name in SIP FROM header. Refer to Header Transformation page if you want to override FROM domain name. Click the **Header Transformation** link provided or choose **VoIP** > **SIP** > **ALG** and refer to Configuring VoIP SIP B2BUA Trunking in Chapter 6, *Configuring VoIP Settings*.

Table 3-15 Network Side ISDN PRI (PRI/UA) Parameters

Item	Description
Disable sending CNAME	Select the **Disable sending CNAME** checkbox to remove the display name from the FACILITY_IE as part of the Q931 SETUP message. By default, the display name of the calling party is sent using the FACILITY_IE in SETUP message. This setting applies to NI2, 5ESS, and 4ESS PRI switch types.
Codec Preference	Select the preferred codec. When making a call, this codec will be the first codec offered. When receiving a call, if this codec is part of the negotiated codec list, then this codec will be used to encode and send voice packets.
Use Preferred codec only	Select the **Use Preferred codec only** checkbox to use your selected codec preference as the only codec offered or responded to in the call setup. All other calls are rejected.
Define configuration for each PRI channel	Configure each PRI channel: ■ Enable—Select the **Enable** checkbox for each PRI channel you want to enable as part of the call. By default, all 23 channels are enabled. ■ Status—In the **Status** column, observe read-only status for a given PRI channel. The status can be Unknown, Idle, Busy, or Not-connected.

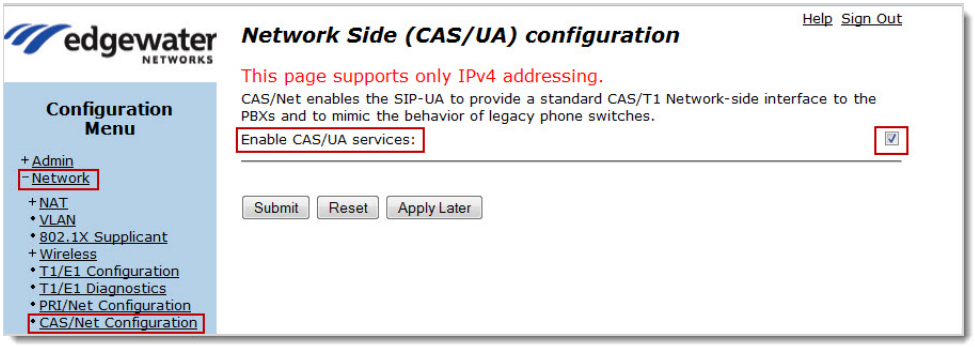
Configuring Network Side CAS/UA

Network Side CAS enables the SIP/UA (SIP User Agent) to provide a standard CAS Network-side interface to the PBXs and to mimic the behavior of legacy phone switches. SIP/UA receives calls from PBXs and connects calls on IP network using SIP.

Tip
Complete the steps in PRI Configuration Requirements.

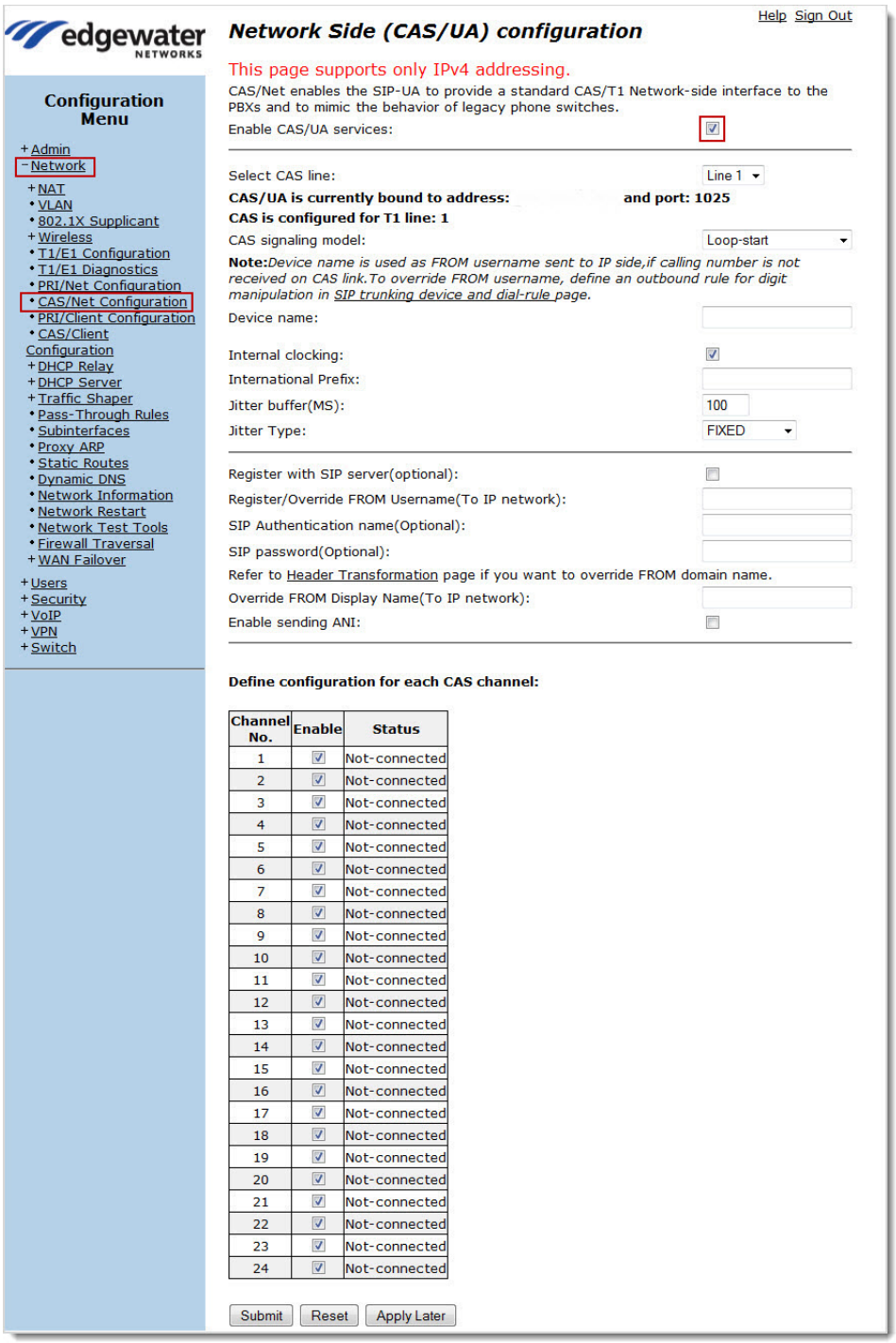
1. Choose **Network** > **CAS/Net configuration** (Figure 3-20).

Figure 3-20 Enable Network Side (CAS/UA)



2. Select the **Enable CAS/UA services** checkbox and click **Submit** to activate fields on the Network Side (CAS/UA) Configuration page (Figure 3-21).

Figure 3-21 Network Side (CAS/UA) Configuration Page



3. Configure settings using the information in Table 3-16 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-16 Network Side (CAS/UA) Parameters

Item	Description
Enable CAS/UA service	Select the **Enables CAS/UA service** checkbox to enable service.
Select CAS line	Choose a T1 line for CAS signaling from the **Select CAS line** drop-down list. Valid range is 1-4 based on the number of T1 lines available on a given EdgeMarc platform.
CAS signaling model	Choose a signaling type from the **CAS signaling model** drop-down list. The CAS signaling type should match the signaling type configured on the PBXs: ■ Ground-Start—T1.403.02-1999 ■ Loop-Start—T1.403.02-1999 ■ GR-303-Ground-Start—GR-303-CORE-Rev3 tables 12-5 and 12-6 ■ GR-304-Loop-Start—GR-303-CORE-Rev3 tables 12-5 and 12-6 ■ Ground-start-sas—T1.403.02-1999, GR-303-CORE-Rev3, and TIA-464-C ■ Loop-start-sas—T1.403.02-1999, GR-303-CORE-Rev3, and TIA-464-C ■ EandMs—T1.403.02-1999
Device name	Enter a device name for the SIP FROM user if caller information is not available in a call coming into the CAS trunk from the remote CAS/T1 link. To override the FROM username, define an outbound rule for digit manipulation from the SIP trunking device and dial rule page. Click the **SIP trunking device and dial-rule** link provided or choose **VoIP** > **SIP** > **ALG** and refer to Configuring VoIP SIP B2BUA Trunking in Chapter 6, *Configuring VoIP Settings*.
Internal clocking	Select the **Internal clocking** checkbox to set the internal clocking mode for PRI. External clocking is used by default.
International Prefix	Enter a value to prepend a prefix to incoming international PRI calls. If the field is empty or a prefix is already part of the called number, no action is taken.
Jitter buffer (MS)	Enter the jitter buffer value based on the IP network condition. Value is equal to or greater than 40 msecs. Default is 100 msecs.

Table 3-16 Network Side (CAS/UA) Parameters

Item	Description
Jitter Type	Choose the Jitter buffer type from the drop-down list: ■ Fixed—Default ■ Adaptive
SIP Server Settings	
Configure the following settings:	
Register with SIP server	(Optional) Select the **Register with SIP server (optional)** checkbox to register with SIP server using the “Register FROM Username” as SIP user name.
Register/Override FROM Username (To IP network)	Enter a name to register with the CAS/GW. A call coming in Network-side CAS/GW from the PBX is terminated on IP network. By default, the gateway uses the PRI callerID in the FROM field of SIP INVITE message when terminating call on the IP side. If the callerID is not present, the gateway uses the internal name specified.
SIP Authentication name	(Optional) Enter the SIP authentication name used to authenticate the CAS/UA when it registers with the name defined in “Register FROM Username” field.
SIP password	(Optional) Enter the SIP authentication password used to authenticate the CAS/UA if the gateway registers with the name defined in “Register FROM Username” field.
Override FROM Display Name (To IP network)	Enter a name to override the DISPLAY name when sending SIP requests to the IP side. An Inbound call coming into CAS/GW from the remote CAS/T1 link is terminated on IP network. By default, the gateway uses this name as part of the DISPLAY name in SIP FROM header. Refer to Header Transformation page if you want to override FROM domain name. Click the **Header Transformation** link provided or choose **VoIP** > **SIP** > **ALG** and refer to Configuring VoIP SIP B2BUA Trunking in Chapter 6, *Configuring VoIP Settings*.

Table 3-16 Network Side (CAS/UA) Parameters

Item	Description
Enable sending ANI	Select the **Enable sending ANI** checkbox to send the calling party number in *ANI*DNIS format on CAS/T1 link to the remote party. Enable only if the remote CAS party is capable of parsing this format to extract the ANI and DNIS.
Define configuration for each CAS channel	Configure each CAS channel: ■ Enable—Select the **Enable** checkbox for each CAS channel you want to enable as part of the call. By default, all 24 channels are enabled. By default all 24 channels are enabled. ■ Status—In the **Status** column, observe read-only status for a given PRI channel. The status can be Unknown, Idle, Busy, or Not-connected.

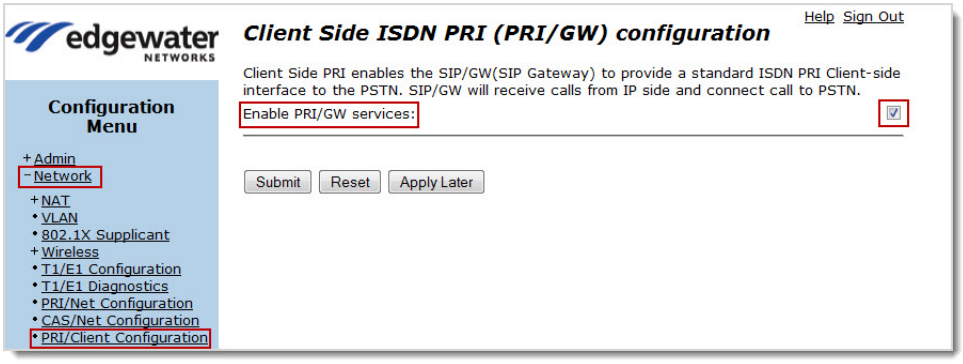
Configuring Client Side ISDN PRI (PRI/GW)

Client Side PRI enables the SIP GW (SIP Gateway) to provide a standard ISDN PRI Client-side interface to the PSTN. The SIP GW receives calls from the IP side and connects calls to the PSTN.

Tip
Complete the steps in PRI Configuration Requirements.

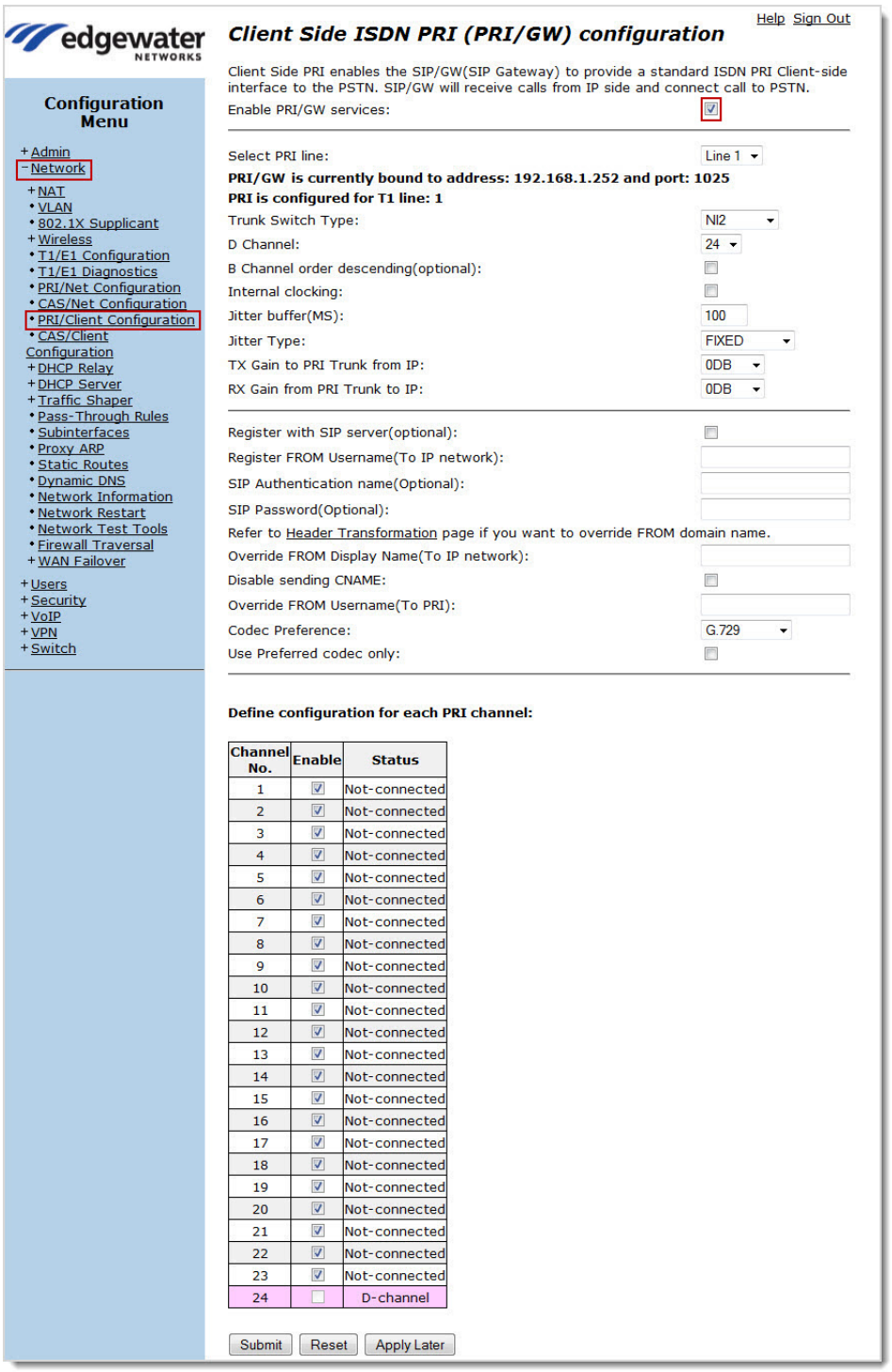
1. Choose **Network** > **PRI/Client Configuration** (Figure 3-22).

Figure 3-22 Enable Client Side ISDN PRI (PRI/GW)



2. Select the **Enable PRI/GW services** checkbox and click **Submit** to activate fields on the Client Side ISDN PRI (PRI/GW) page (Figure 3-23).

Figure 3-23 Client Side ISDN PRI (PRI/GW) Configuration Page



3. Configure settings using the information in Table 3-17 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-17 Client Side ISDN PRI (PRI/GW) Parameters

Item	Description
Enable PRI/GW service	Select the **PRI/GW service** checkbox to enable service.
Select PRI line	Choose a T1 line for ISDN PRI from the **Select PRI line** drop-down list. Valid range is 1-4 based on the number of T1 lines available on a given EdgeMarc platform.
Trunk Switch Type	Enter the switch type that client-side ISDN PRI will be simulating. NI2 is selected by default. It is important that the switch type matches the Network-side switch type to which this interface is connected.
D Channel	Choose a number from the **D Channel** drop-down list to use for Q.931 signaling.
B Channel order descending (optional)	Select the **B Channel** checkbox to change B channel order to descending (24-1). B channel ordering is ascending (1-24) by default when doing a call setup.
Internal clocking	Select the **Internal clocking** checkbox to set the internal clocking mode for PRI. External clocking is used by default.
International Prefix	Enter a value in the **International Prefix** field.
Jitter buffer (MS)	Enter the jitter buffer value based on the IP network condition. Value is equal to or greater than 40 msecs. Default is 100 msecs.
Jitter Type	Choose the Jitter buffer type from the drop-down list: ■ Fixed—Default ■ Adaptive
TX Gain to PRI Trunk from IP	Choose a transmit gain value from the **TX Gain to PRI Trunk from IP** drop-down list.
RX Gain from PRI Trunk to IP	Choose a receive gain value from the **RX Gain from PRI Trunk to IP** drop-down list.
SIP Server Settings	
Configure the following settings:	
Register with SIP server	(Optional) Select the **Register with SIP server (optional)** checkbox to register with SIP server using the “Register FROM Username” as SIP user name.

Table 3-17 Client Side ISDN PRI (PRI/GW) Parameters

Item	Description
Register/Override FROM Username (To IP network)	Enter a name to register with the PRI/GW. A call coming in Network-side PRI/GW from the PBX is terminated on IP network. By default, the gateway uses the PRI callerID in the FROM field of SIP INVITE message when terminating call on the IP side. If the callerID is not present, the gateway uses the internal name specified.
SIP Authentication name	(Optional) Enter the SIP authentication name used to authenticate the PRI/GW if the gateway registers with name defined in the Register FROM Username field.
SIP password	(Optional) Enter the SIP authentication password used to authenticate the PRI/GW if the gateway registers with the name defined in Register FROM Username field.
Override FROM Display Name (To IP network)	Enter a name to override the system default DISPLAY name when sending SIP request to IP side. An Inbound call coming into PRI/GW from the remote PRI/T1 link is terminated on IP network. By default, the gateway uses this name as part of the DISPLAY name in SIP FROM header. Refer to Header Transformation page if you want to override FROM domain name. Click the **Header Transformation** link provided or choose **VoIP** > **SIP** > **ALG** and refer to Configuring VoIP SIP B2BUA Trunking in Chapter 6, *Configuring VoIP Settings*.
Disable sending CNAME	Select the **Disable sending CNAME** checkbox so that the display name is not sent in FACILITY_IE as part of the Q931 SETUP message. The display name of calling party is sent using FACILITY_IE in SETUP message by default. This setting applies to NI2, 5ESS, and 4ESS PRI switch types.
Codec Preference	Select your codec preference from the **Codec Preference** drop-down list. When making a call, the codec is the first offered codec in the codec list. When receiving a call, if that codec is part of the negotiated codec list, that codec is used to encode and send voice packets.

Table 3-17 Client Side ISDN PRI (PRI/GW) Parameters

Item	Description
Use Preferred codec only	Select the **Use Preferred codec only** checkbox to use your selected codec preference as the only codec offered or responded to in the call setup. All other calls are rejected.
Define configuration for each PRI channel	Configure each PRI channel: ■ Enable—Select the **Enable** checkbox for each PRI channel you want to enable as part of the call. By default, all 23 channels are enabled. ■ Status—In the **Status** column, observe read-only status for a given PRI channel. The status can be Unknown, Idle, Busy, or Not-connected.

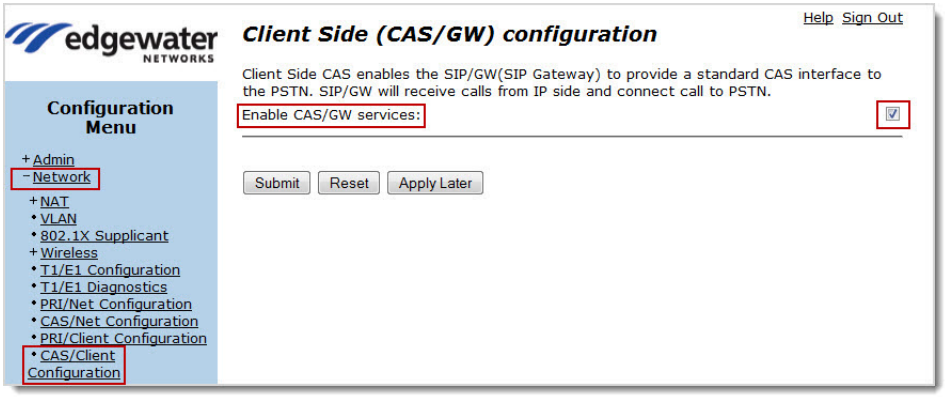
Configuring Client Side CAS/GW

Client Side CAS enables the SIP/GW to provide a standard CAS interface to the PSTN. SIP/GW receives calls from the IP side and connects calls to the PSTN.

Tip
Complete the steps in PRI Configuration Requirements.

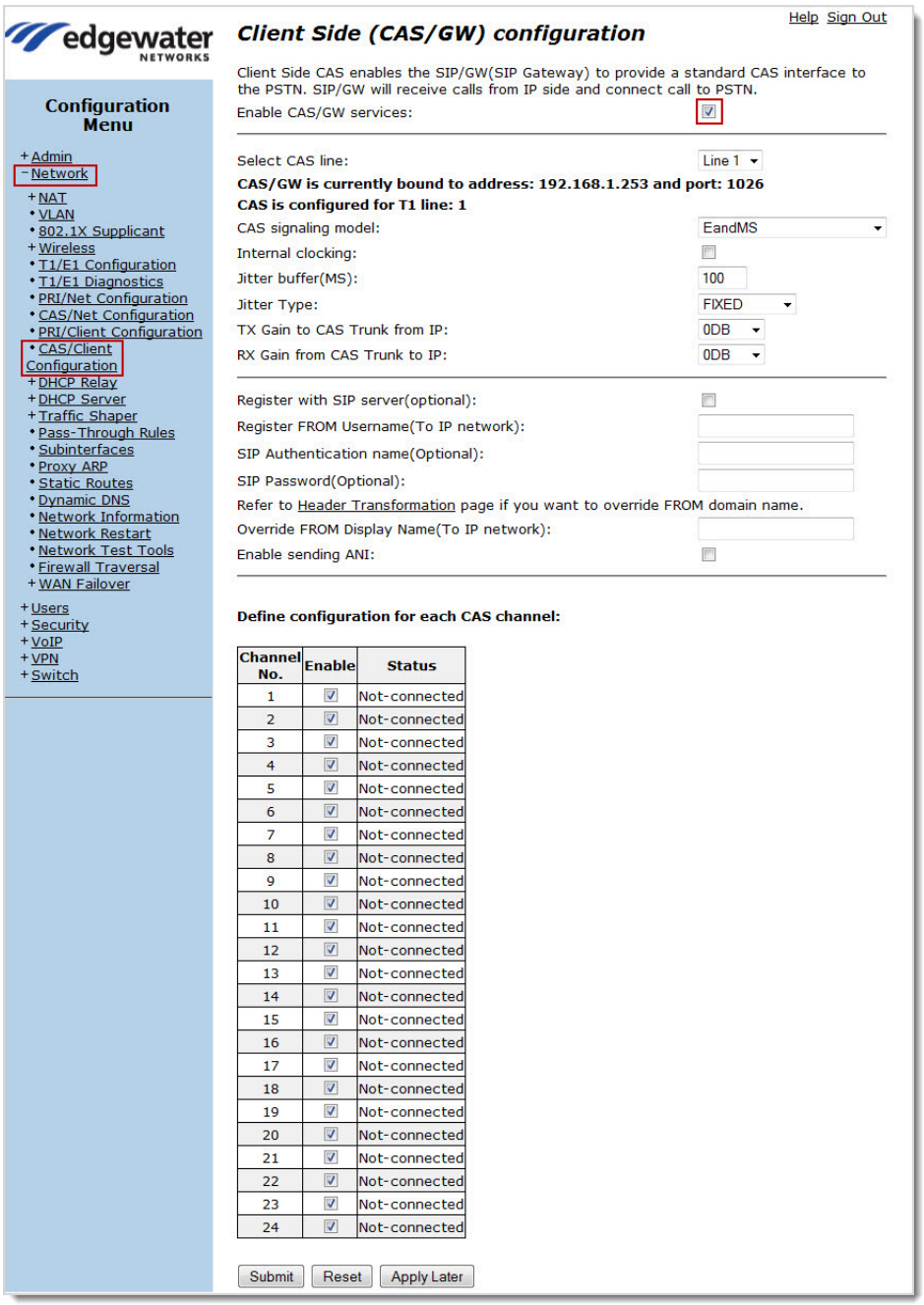
1. Choose **Network** > **PRI/Net Configuration** (Figure 3-24).

Figure 3-24 Enable Client Side (CAS/GW)



2. Select the **Enable CAS/GW services** checkbox and click **Submit** to activate fields on the Client Side (CAS/GW) Configuration page (Figure 3-25).

Figure 3-25 Client Side (CAS/GW) Configuration Page



3. Configure settings using the information in Table 3-18 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-18 Client Side (CAS/GW) Parameters

Item	Description
Enable CAS/GW service	Select the **Enable CAS/GW service** checkbox to enable service.
Select CAS line	Choose a T1 line for CAS signaling from the **Select CAS line** drop-down list. Valid range is 1-4 based on the number of T1 lines available on a given EdgeMarc platform.
CAS signaling model	Choose a signaling type from the **CAS signaling model** drop-down list. E&M synchronous signaling is selected by default. The CAS signaling type should match the signaling type configured on the PBXs: ■ GR-303-Ground-Start—GR-303-CORE-Rev3 tables 12-5 and 12-6 ■ GR-304-Loop-Start—GR-303-CORE-Rev3 tables 12-5 and 12-6 ■ EandM (Pub 43801)— 2- or 4-Wire E & M, According to PUB43801, November 1982 ■ EandMS—T1.403.02-1999 (E&M Synchronous) ■ EandMA—T1.403.02-1999 (E&M Asynchronous)
Internal clocking	Select the **Internal clocking** checkbox to set the internal clocking mode for PRI. External clocking is used by default.
Jitter buffer (MS)	Enter the jitter buffer value based on the IP network condition. Value is equal to or greater than 40 msecs. Default is 100 msecs.
Jitter Type	Choose the Jitter buffer type from the drop-down list: ■ Fixed—Default ■ Adaptive
TX Gain to CAS Trunk from IP	Choose a transmit gain value from the **TX Gain to PRI Trunk from IP** drop-down list.
RX Gain from CAS Trunk to IP	Choose a receive gain value from the **RX Gain from PRI Trunk to IP** drop-down list.
SIP Server Settings	
Configure the following settings:	
Register with SIP server	(Optional) Select the **Register with SIP server** checkbox to register with SIP server using the “Register FROM Username” as SIP user name.

Table 3-18 Client Side (CAS/GW) Parameters

Item	Description
Register/Override FROM Username (To IP network)	Defines a name to register with the CAS/GW. A call coming in Network-side CAS/GW from the PBX is terminated on IP network. By default, the gateway uses the PRI callerID in the FROM field of SIP INVITE message when terminating call on the IP side. If the callerID is not present, the gateway uses the internal name specified.
SIP Authentication name (Optional)	Defines the SIP authentication name used to authenticate the CAS/UA when it registers with the name defined in “Register FROM Username” field.
SIP password (Optional)	Defines the SIP authentication password used to authenticate the CAS/UA if the gateway registers with the name defined in “Register FROM Username” field.
Override FROM Display Name (To IP network)	Enter a name to override the system default DISPLAY name when sending SIP request to IP side. An Inbound call coming into CAS/GW from the remote CAS/T1 link is terminated on IP network. By default, the gateway uses this name as part of the DISPLAY name in SIP FROM header. Refer to Header Transformation page if you want to override FROM domain name. Click the **Header Transformation** link provided or choose **VoIP** > **SIP** > **ALG** and refer to Configuring VoIP SIP B2BUA Trunking in Chapter 6, *Configuring VoIP Settings*.
Enable sending ANI	Select the **Enable sending ANI** checkbox to send the calling party number in *ANI*DNIS format on CAS/T1 link to the remote party Enable only if the remote CAS party is capable of parsing this format to extract the ANI and DNIS.
Define configuration for each CAS channel	Configure each CAS channel: ■ Enable—Select the **Enable** checkbox for each CAS channel you want to enable as part of the call. By default, all 24 channels are enabled. ■ Status—In the **Status** column, observe read-only status for a given PRI channel. The status can be Unknown, Idle, Busy, or Not-connected.

Configuring High Availability

Enable High Availability (HA) to allow a standby system to take control for the active system in the event of a failure. HA is only available on certain EdgeMarc models.



Note
Failover with B2BUA is now supported when High Availability is enabled. When the system is deployed for HA, you must configure the Primary and Backup systems identically for B2BUA features. Configuration mirroring is not supported.

Use HA in conjunction with settings on the VLAN Configuration page. Choose **Network** > **VLAN** and refer to Configuring VLAN Support.

Overview

High Availability is designed to eliminate a single point of failure in a network configuration. Two systems can be configured to act as a redundant pair. One of the systems is the designated Primary system, the other is the designated Secondary system. Normally, the Primary system is the Active system and the Secondary system is the Standby system.

If the Primary system fails because of a network or hardware failure, the Secondary system will take over and become the new Active system.

Stateful Failover

Stateful failover is a high availability feature that transfers state between two systems so that active calls will not be terminated during an activity switch. Stateful failover was designed to support SIP trunking applications only and should only be configured in systems using an Ethernet LAN and WAN. Other applications that require additional call state (for example, multi-line appearances for IP phones as used in Hosted PBX applications) may not work correctly upon an activity switch. For these applications, as well as applications using H.323 over TCP, an activity switch will still occur but the voice or video calls may need to be re-established.

B2BUA High Availability

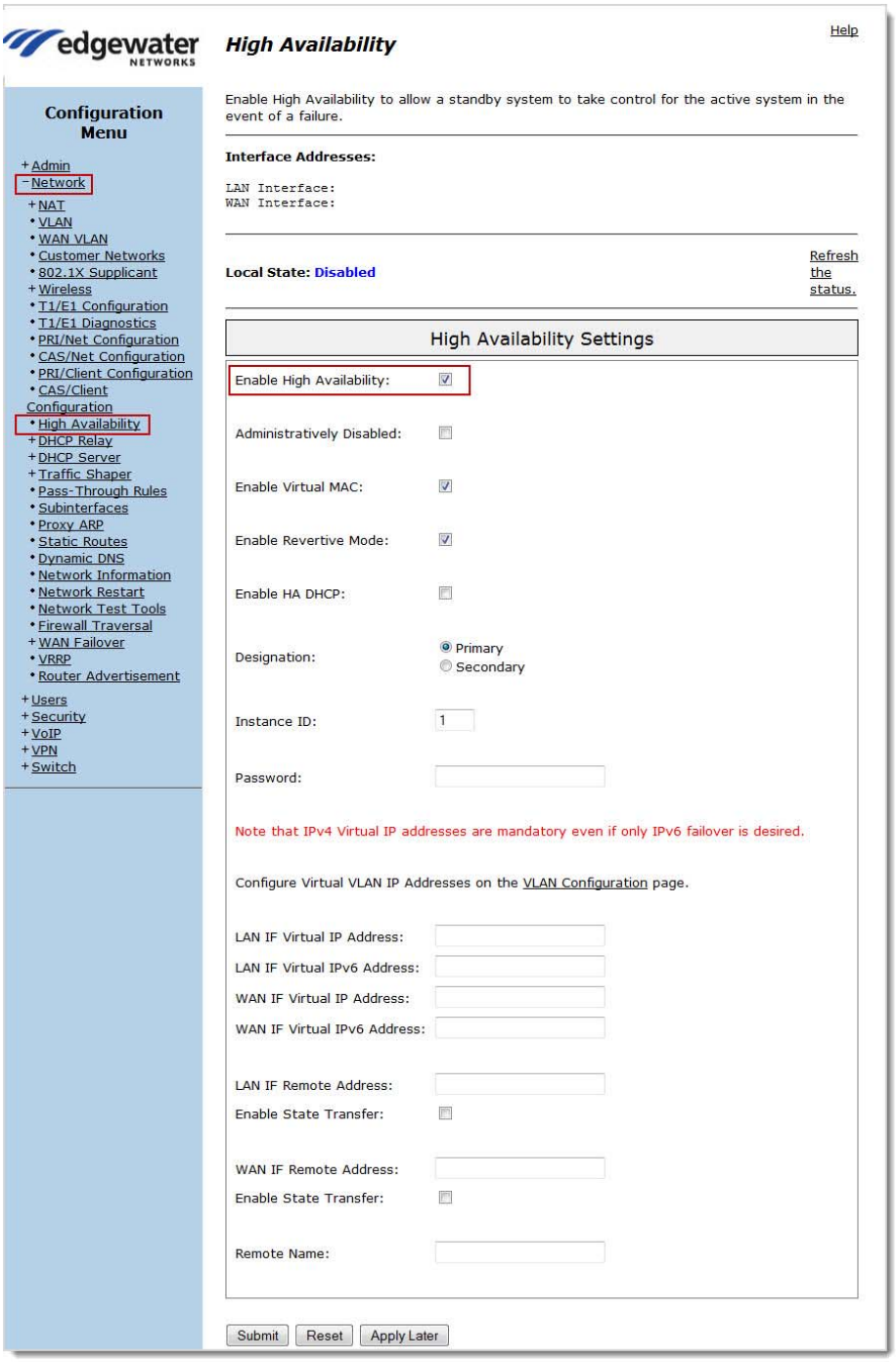
The B2BUA HA feature allows the calls connected via B2BUA to continue seamlessly during and after a system failover. Calls that are already established stay active during system failure. New calls can be established successfully after system failure. This feature works with UDP and TCP protocols, assuming the remote devices supports new TCP connections during a call.

This feature is enabled automatically when HA and state transfer are enabled and is supported on the EdgeMarc 4700, 7000, and 4800 platforms.

Configuring High Availability Settings

1. Choose **Network** > **High Availability** (Figure 3-26). You can also choose **Network** > **VLAN** and click the **High Availability** link provided on the VLAN Configuration page.

Figure 3-26 High Availability Configuration Page



2. Configure settings using the information in Table 3-19 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-19 High Availability Configuration Parameters

Item	Description
Interface Addresses	Displays information about the LAN and WAN interfaces currently running on the system.
Local State	Displays the state of all high availability services. The system is configured to send status updates to the other system by specifying the IP addresses of that other system on a per-link basis. Click **Refresh the status** for updated information.
Administratively Disabled	Sets the system state to be administratively down. This causes the system to give up service and not attempt to retake the active state. This can be used for maintenance, configuration changes, or upgrading and testing the system.
Administratively Disabled	Disables the system administratively. **Note:** Enabling this checkbox causes the other system to take over. If there is no other system, voice services are disrupted. While the system is in this mode, it will not take over for the other system in case of a failure.
High Availability Settings	Controls High Availability behavior. **Note:** Changing these settings disrupts service. Make sure that all systems in the group are configured in a compatible way.
Enable High Availability	Select the **Enable High Availability** checkbox.
Enable Virtual MAC	Select the **Enable Virtual MAC** checkbox to allow hot redundancy switchover to the standby device. **Note:** Virtual MAC (VMAC) is required for IPv6 support. IPv6 HA for VMAC is only supported on some EdgeMarc platforms.
Enable Revertive Mode	Select the **Enable Revertive Mode** checkbox to revert to the higher priority host.

Table 3-19 High Availability Configuration Parameters

Item	Description
Enable HA DHCP	Select the **Enable HA DHCP** checkbox to maintain a single DHCP lease database between the Primary and Secondary systems for seamless failover. This avoids running independent DHCP servers on each system, which could potentially cause IP address conflicts. You must enable State Transfer on at least one interface by selecting the **Enable State Transfer** checkbox.
Designation	Select the Primary or Secondary radio button to designate one system as the primary system or secondary system. ■ Primary ■ Secondary
Instance ID	Enter the instance ID. Both systems in the same group should have the same instance ID and must be unique for that group in order to not cause multiple groups on the same network to disrupt each other. Multiple HA EdgeMarc instances are supported with the same ID on the same network.
Password	Enter a password to be used by the systems in the group. The password must be the same on all systems.

Virtual VLAN Settings

Configure Virtual VLAN IP Addresses on the VLAN Configuration page. Choose **Network** > **VLAN** and refer to Configuring VLAN Support.

Note: IPv4 Virtual IP addresses are mandatory even if only IPv6 failover is desired.

Table 3-19 High Availability Configuration Parameters

Item	Description
LAN IF Virtual IP Address	Enter the virtual IPv4 address to be shared between the two systems. This IPv4 address must be in the same subnet as the physical LAN IPv4 address configured on the Network page. The virtual IPv4 address may also be used to manage the system with HTTPS, HTTPS, Telnet, SSH and SNMP. The system performs a gratuitous ARP for the virtual IP as the physical LAN MAC address of the system when an activity switch occurs and the system assumes the active role. **Note:** Some routers ARP caches may not reflect the new MAC address for the virtual IPv4 address and may require a period of time to store and forward traffic to the active system. In rare cases the upstream router may require the ARP cache to be flushed to store the new MAC address as the virtual IP owner.
LAN IF Virtual IPv6 Address	Enter the virtual IPv6 address to be shared between the two systems.
WAN IF Virtual IP Address	Enter the virtual IPv4 address to be shared between the two systems. This IPv4 address must be in the same subnet as the physical WAN IPv4 address configured on the Network page. The virtual IPv4 address may also be used to manage the system with HTTPS, HTTPS, Telnet, SSH and SNMP. The system performs a gratuitous ARP for the virtual IP as the physical WAN MAC address of the system when an activity switch occurs and the system assumes the active role. **Note:** Some routers ARP caches may not reflect the new MAC address for the virtual IPv4 address and may require a period of time to store and forward traffic to the active system. In rare cases the upstream router may require the ARP cache to be flushed to store the new MAC address as the virtual IP owner.
WAN IF Virtual IPv6 Address	Enter the virtual IPv6 address to be shared between the two systems.
LAN IF Remote Address	Enter the LAN interface remote address or subscriber remote address. This is the actual address of the other system on this interface used to connect to the other system and transfer state information. **Tip:** Select the **Enable State Transfer** checkbox if you want state transfer to take place over this link.

Table 3-19 High Availability Configuration Parameters

Item	Description
Enable State Transfer	Select the **Enable State Transfer** checkbox to select another interface to facilitate stateful failover. If you enable state transfer for multiple links, you have a higher chance of successful state transfer during link failures. **Note:** State transfer causes extra network traffic on that link. For example, if you only enable state transfer on the LAN/Subscriber interface, and this link fails causing the Secondary system to become active, the Primary system will now no longer be able to receive state updates. So if the link is restored, the Primary system takes over without a full state transfer. To prevent this, enable state transfer on the WAN/Provider interface and the management interface as well to ensure that state transfer is successful during link failure.
WAN IF Remote Address	Enter the WAN remote address or provider remote address. This is the actual address of the other system on this interface. This is used to connect to the other system and transfer state information. **Tip:** Select the **Enable State Transfer** checkbox if you want state transfer to take place over this link.
Enable State Transfer	Select the **Enable State Transfer** checkbox if you want state transfer to take place over the WAN remote address link.
Mgmt. Remote Address	(Optional) Enter the actual address of the other system on the management interface. This is used to connect to the other system and transfer state information. **Tip:** Select **Enable State Transfer** if you want state transfer to take place over this link.
Remote Name	(Optional) Enter a string to be used in SNMP traps to identify the remote system by name. It is recommended to use the remote systems hostname, however you can use any character string. If this field is left blank, the IP address of the remote system will be used in the SNMP trap.

Administratively Disabling High Availability

The system can be put in an administrative down state. This causes the system to give up service and not attempt to retake the active state. This can be used for maintenance, configuration changes, or upgrading the system.

To disable HA, select the **Administratively Disabled** checkbox and click **Submit**.

Configuring DHCP Relay

When you enable DHCP relay and point to a valid DHCP server, all DHCP requests are forwarded to that server. Local DHCP and DHCP Relay are mutually exclusive; turning on DHCP Relay automatically turns off local DHCP, and turning on DHCP automatically turns off DHCP Relay.

Note
Use the DHCP Relay page only if DHCP is disabled.

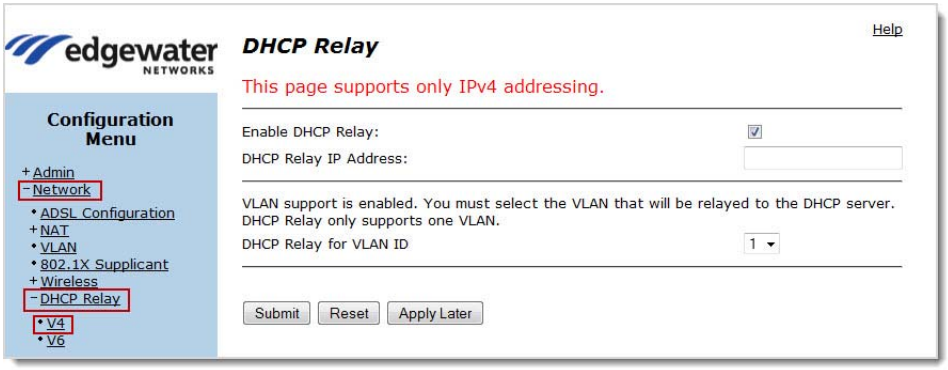
To configure DHCP relay, see the following sections:

- Configuring DHCP Relay IPv4
- Configuring DHCP Relay IPv6

Configuring DHCP Relay IPv4

1. Choose **Network** > **DHCP Relay** (Figure 3-27). The DHCP Relay IPv4 addressing page opens by default.

Figure 3-27 DHCP Relay IPv4 Page



2. Configure settings using the information in Table 3-20 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

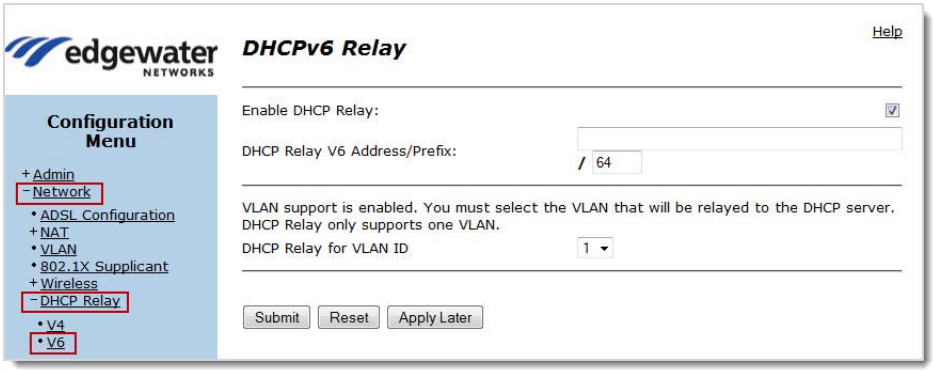
Table 3-20 DHCP Relay IPv4 Parameters

Item	Description
IPv4	
Configures DHCP relay for IPv4.	
Enable DHCP Relay	Select the checkbox to enable DHCP Relay.
DHCP Relay IP Address	Enter the DHCP server IPv4 address where the system forwards traffic.
DHCP Relay for VLAN ID	If VLAN support is enabled, choose the configured VLAN number from the **DHCP Relay for VLAN ID** drop-down list. To enable VLAN support, choose **Network** > **VLAN** and refer to Configuring VLAN Settings. DHCP Relay only supports one VLAN. **Note:** If you delete a VLAN, the DHCP Server must be re-enabled for the remaining VLANs.

Configuring DHCP Relay IPv6

1. Choose **Network** > **DHCP Relay** (Figure 3-27). The DHCP Relay IPv4 addressing page opens by default.
2. Choose **DHCP Relay** > **V6** (Figure 3-28).

Figure 3-28 DHCP Relay IPv6 Page



3. Configure settings using the information in Table 3-21 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-21 DHCP Relay IPv6 Parameters

Item	Description
IPv6	
Configures DHCP relay for IPv6. By setting DHCPv6 relay on, and pointing to a valid DHCPv6 server, all DHCPv6 requests are forwarded to that server.	
Enable DHCP Relay	Select the checkbox to enable DHCP Relay.
DHCP Relay V6 Address/ Prefix	Enter the IPv6 address of the DHCP server where the system forwards traffic.
DHCP Relay for VLAN ID	If VLAN support is enabled, choose the configured VLAN number from the **DHCP Relay for VLAN ID** drop-down list. To enable VLAN support, choose **Network** > **VLAN** and refer to Configuring VLAN Settings. DHCP Relay only supports one VLAN. **Note:** If you delete a VLAN, the DHCP Server must be re-enabled for the remaining VLANs.

Configuring the DHCP Server

Note
Ask your ISP to assign an IP address for the EdgeMarc, an IP address for the gateway, and a preferred and secondary IP address for the DNS server.

Overview

The DHCP Server provides dynamic IP addresses to endpoints on the network and prevents IP address conflicts. It can also provide additional network related configuration such as the default gateway, DNS servers, and other options that endpoints can request.

Tip
Only one DHCP server can be enabled on a network at a time.

DHCP Server Options

You can configure blocks of IP addresses, the default gateway, DNS servers, and other parameters that can be served to requesting devices. Table 3-22 lists the options supported by the DHCP Server.

Table 3-22 DHCP Server Options

Option	Description
1	Subnet Mask—LAN Netmask of the EdgeMarc, Network page
2	Time Offset
3	Router—LAN IP of the EdgeMarc, Network page
6	DNS Server—DNS IP, Network page
42	NTP Servers
51	IP address lease time—Lease duration in seconds, DHCP page
53	DHCP Message Type—Set by DHCP server
54	Server Identifier—LAN IP of the EdgeMarc
66	Server-Name (Polycom uses this for FTP server name)
67	Boot file name
129	Call Server IP Address—VLAN ID Discovery
150	Phone Image TFTP Server IP—LAN IP of the EdgeMarc, Network Page
151	MGCP Control Server IP—LAN IP of the EdgeMarc Network Page
159	Specifies a text string in the form of a FQDN for Polycom phones. It can be used to point the Polycom phones to the domain name of a TFTP server using HTTP.
160	Specifies a text string in the form of a FQDN for Polycom phones. It can be used to point the Polycom phones to the domain name of a TFTP server using HTTPS.

You do not have to enable DHCP on your system if a DHCP server exists elsewhere in your company network, but at least one DHCP server must exist on an accessible network. When you have enabled the DHCP server, you can turn it on or off without having to change other settings by un-checking the **Enable DHCP Server** checkbox.

The DHCP IP Address Ranges table (Figure 3-30) shows the dynamic addresses to use for the LAN devices.

Configuring DHCP Server on the EdgeMarc includes enabling the server and configuring the DHCP IP Address range to be used by LAN devices.

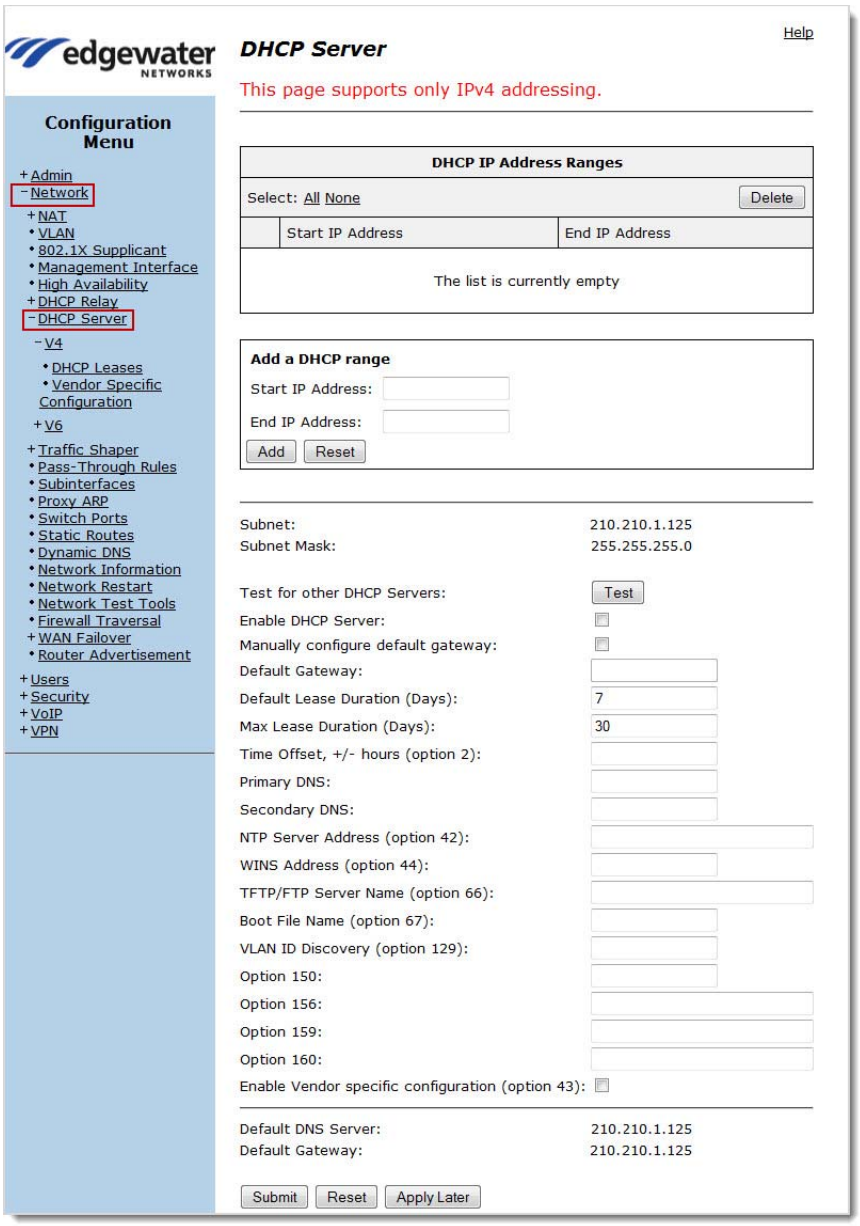
To configure the DHCP server, see the following sections:

- Configuring the DHCP Server IPv4
- Configuring DHCP Server IPv6

Configuring the DHCP Server IPv4

1. Choose **Network** > **DHCP** (Figure 3-29). The DHCP Server IPv4 addressing page opens by default.

Figure 3-29 DHCP Server IPv4 Page



2. Configure settings using the information in Table 3-23 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-23 DHCP Server Parameters

Item	Description
Subnet	
Selects a network to configure for DHCP if multiple networks are configured on the system.	
DHCP IP Address Ranges	
Shows the dynamic addresses to use for the LAN devices. See Managing DHCP IPv4 Address Ranges.	
Add a DHCP Range	
Configures individual DHCP IP addresses or a range of addresses and assigns static IP addresses for any common-access devices, such as printers or fax machines.	
Subnet Subnet Mask	Configures the Subnet and Subnet Mask addresses for the DHCP pool. The default implied values are 192.168.1.1 and 255.255.255.0.
Test for other DHCP Servers	Click the **Test** button to determine whether there are other DHCP servers configured on the system.
DHCP Settings	
See Configuring DHCP Server IPv4 Settings.	
Enable DHCP Server	Select the E**nable DHCP Server** checkbox to enable the DHCP server.
Default Lease Duration (Days)	Configures the default number of days to lease the DHCP service for your system. This is the amount of time a DHCP service remains connected without lapse. Resource allocation and cost might influence the quantity assigned. The value can be 1 day minimum and 30 days maximum.
Max Lease Duration (Days)	Configures the maximum number of days to the lease the DHCP service for your system.
Time Offset, +/- hours (Option 2)	Sets the time offset in hours from Universal time Code (UTC) for your location.
NTP Server Address (Option 42)	Sets the Network Time Protocol (NTP) address that is served out by DHCP.

Table 3-23 DHCP Server Parameters (continued)

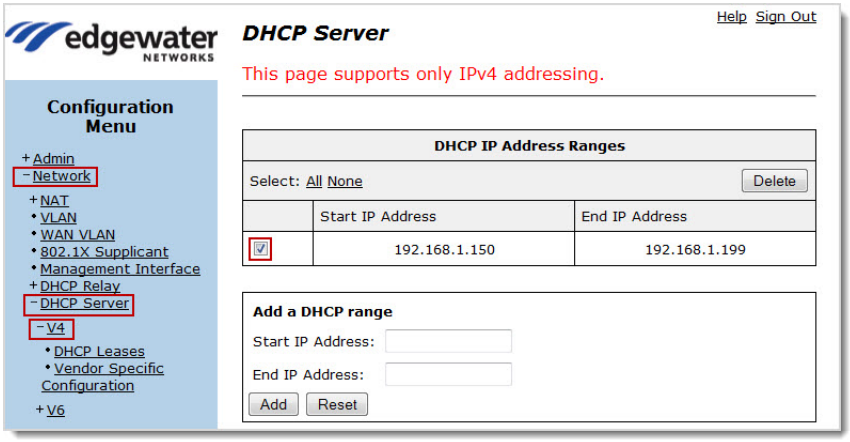
Item	Description
WINS Address (Option 44)	Configures the Windows Internal Naming Service (WINS) service. WINS keeps a database of computer name-to-IP address mappings so that computer names used in Windows environments can be mapped to IP addresses.
TFTP/FTP Server Name (Option 66)	Sets the TFTP/FTP server name that is served out by DHCP. Used by some endpoints to download their configuration via TFTP/FTP. By default, this option is the same as the TFTP server on the ALG page.
Boot File Name (Option 67)	Names boot file used by some endpoints.
VLAN ID Discovery (Option 129)	Configures VLAN ID dynamic discovery. A valid VLAN ID is between 1 and 4094. All EdgeMarc models support a maximum of 16 VLANs, all of which could be associated with the DHCP Server. The following are the default VLAN IDs used on the EdgeMarc: ■ VLAN ID 1 (formerly 2730)—Interface management ■ VLAN ID 500—Voice ■ VLAN ID 600—Data To configure DHCP with VLANS, you must enable VLAN capability. Choose **Network** > **VLAN** and refer to Configuring WAN Interface Settings. **Note:** The Polycom phone boots on the Data (native) VLAN by default and acquires Option 129 automatically. Upon learning Option 129, the phone re-boots with the correct VLAN ID.
Option 150/151	User-defined IP address fields. By default, these options are the same as the LAN IP address on the Network page. See Table 3-22 for a description of these options.
Options 159/160	User-defined text fields.
Enable Vendor specific configuration (Option 43)	Configures the DHCP server to send vendor specific parameters to devices using Option 43. See Managing DHCP IPv4 Vendor Specific Configuration.
Primary DNS Secondary DNS Default Gateway	Describes current DNS and default gateway settings (view only).

3. Configure settings on the DHCP Server page:
   - Managing DHCP IPv4 Address Ranges
   - Configuring DHCP Server IPv4 Settings
   - Managing DHCP IPv4 Leases
   - Managing DHCP IPv4 Vendor Specific Configuration
   - Managing DHCP Vendor Options
   - Configuring Vendor Specific Option Tags

Managing DHCP IPv4 Address Ranges

1. Choose **Network** > **DHCP Server** (Figure 3-29). The DHCP Server IPv4 addressing page opens by default.
2. View and manage DHCP IP addresses in the **DHCP IP Address Ranges** table (Figure 3-30):
   a. Select the checkbox next to a DHCP IP address, or click **All** to select all entries or **None** to select no entries.
   b. Click **Delete** to remove a DHCP IP address from the list.

Figure 3-30 DHCP IPv4 Address Range Settings



3. In Add a DHCP Range, configure additional DHCP IP addresses by entering the **Start IP Address** and the **End IP Address** in the fields provided.
4. Click **Add**.

Configuring DHCP Server IPv4 Settings

1. Choose **Network** > **DHCP Server** (Figure 3-29). The DHCP Server IPv4 addressing page opens by default.
2. If multiple networks are configured on the system, select which network to configure for DHCP from the **Subnet** drop-down list.
3. Test for other DHCP Servers by clicking **Test**.
4. Select the **Enable DHCP Server** checkbox to enable DHCP.

5. Enter the number of days you want to lease the DHCP service in the **Default Lease Duration (Days)** field. Enter a minimum of one day to a maximum of 30 days (recommended).
6. Enter the maximum number of days for the DHCP lease to be valid on your system in the **Max Lease Duration (Days)** field.
7. Enter the UTC time offset (in hours) for your location in the **Time Offset, +/- hours (option 2)** field.
8. In the **Primary DNS** field, enter the address of a Domain Name Server (DNS). If none is specified, the system DNS addresses is used.
9. In the **Secondary DNS** field, enter the address of a secondary DNS.
10. Enter the NTP server address in the **NTP Server Address (option 42)** field.
11. Enter the WINS address in the **WINS Address (option 44)** field to add this computer name to the IP address mapping database.
12. Enter a TFTP/FTP server name in the **TFTP/FTP Server Name (option 66)** field to download your configuration via TFTP/FTP. By default, this option is the same as the TFTP server on the VoIP page. Choose **Network** > **VoIP** and refer to Chapter 6, *Configuring VoIP Settings*.
13. Enter the boot file name in the **Boot File Name (option 67)** field.
14. Enter a VLAN ID in the **VLAN ID Discovery (option 129)** field to enable dynamic VLAN ID discovery.
15. (Optional) Enter an IP address in the Options **150/151** fields. These options are the same as the LAN IP address on the Network page by default.
16. (Optional) Enter text in the Options 156/159/160 fields.
17. In the **Override Default Gateway** field, manually configure the default routing gateway to be something different than the EdgeMarc.



Caution
Most configurations do not use this option; entering incorrect information can leave your DHCP clients unable to reach the Internet.

18. Select the **Enable Vendor specific configuration (option 43)** checkbox to enable the DHCP server to send vendor specific parameters to devices. See Managing DHCP IPv4 Vendor Specific Configuration.
19. Click **Submit** to apply your changes.

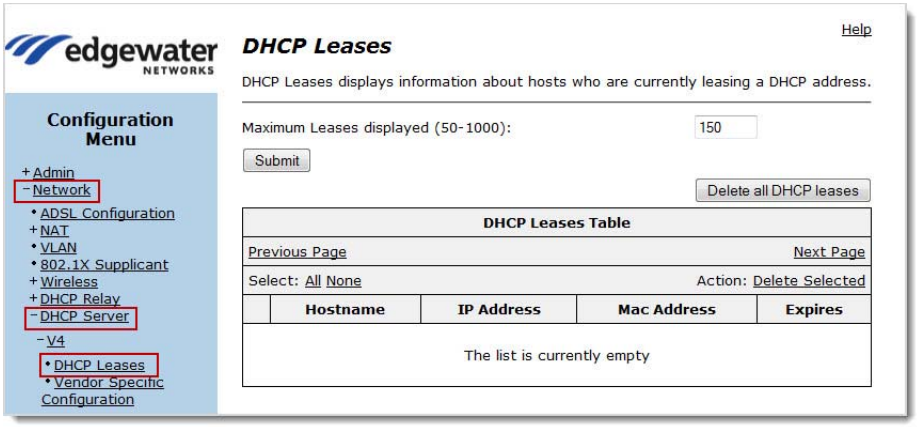
    A message indicates that service will be temporarily interrupted.
20. Click **OK** to confirm.

Managing DHCP IPv4 Leases

The DHCP Leases page displays information about hosts that are currently leasing a DHCP address.

1. Choose **Network** > **DHCP Server** > **V4** > **DHCP Leases** (Figure 3-31).

Figure 3-31 DHCP Leases Page



2. In the **Maximum Leases displayed (50-1000)** field, enter the maximum number of leases to display and click **Submit**.
3. To delete a DHCP lease from the DHCP Leases table, select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
4. Click **Delete Selected**.
5. To delete all entries, click **Delete All DHCP Leases**.

Note
When deleting DHCP lease entries, the DHCP server is restarted. During this brief moment, hosts will not be able to obtain a DHCP IP address.

Managing DHCP IPv4 Vendor Specific Configuration

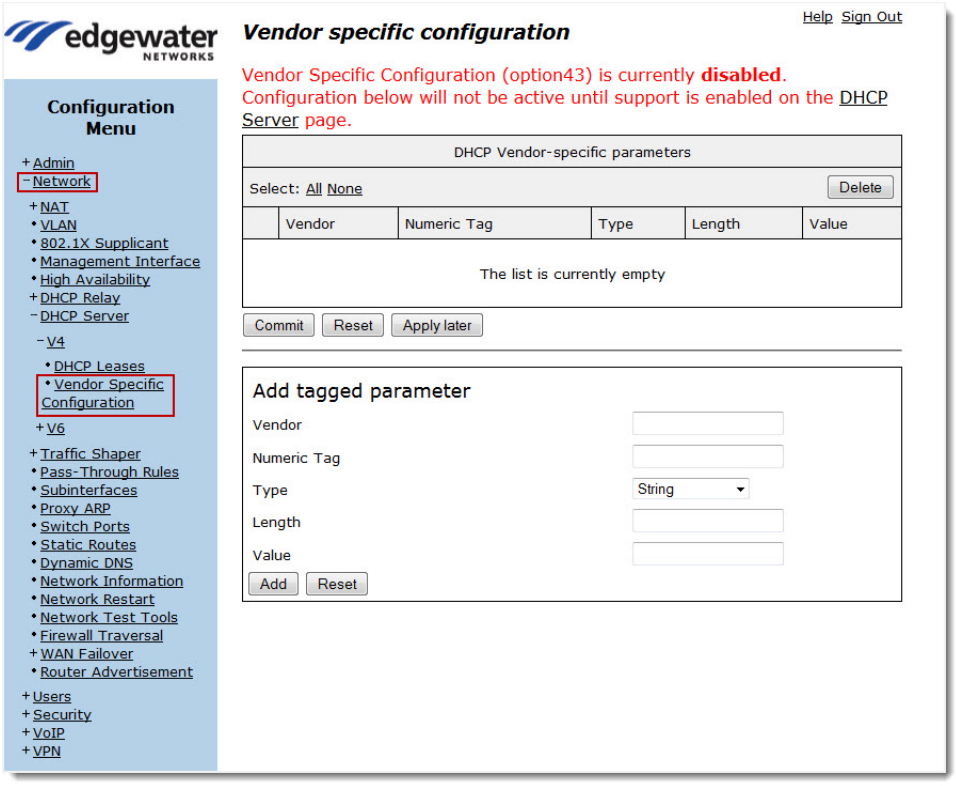
Tip
You must first enable vendor specific configuration (option 43) on the DHCP Server configuration page. Refer to Configuring the DHCP Server.

The DHCP server sends basic vendor specific parameters to devices using Option 43. Parameter definitions are unique to each vendor.

To configure vendor specific configuration:

1. Choose **Network** > **DHCP Server** > **V4** > **Vendor Specific Configuration** (Figure 3-32).

Figure 3-32 Vendor Specific Configuration Page



2. Configure settings using the information in Table 3-24 as a guide. When you have finished configuring settings, click **Add** to make your changes take effect.

Table 3-24 Vendor Specific Parameters

Item	Description
DHCP Vendor Options	Shows unique vendor specific parameters. See Managing DHCP Vendor Options.
Add Option Tag	See Configuring Vendor Specific Option Tags.
Vendor	Configures the vendor name. Vendor names are case-sensitive; if your endpoint identifies itself as “Edgewater,” entering “edgewater” as the vendor means it will not receive your configured parameters.
Tag ID	Configures the tag ID. Tags are vendor unique; if you have defined two vendors they can both use the same tag numbers but a tag can only be used once by a vendor.

Item	Description
Type	Configures an input type. See Table 3-25, “Vendor Specific Input Options,” on page 193 for a description of basic data input types that the EdgeMarc supports.
Length	Configures the parameter length.
Value	Configures the parameter value.

Managing DHCP Vendor Options

1. Choose **Network** > **DHCP Server** > **V4** > **Vendor Specific Configuration** (Figure 3-32).
2. Choose a Vendor ID (VID) from the drop-down list.
3. View and manage Vendors in the DHCP Vendor Options table:
   a. Select the checkbox next to a Vendor, or click **All** to select all entries or **None** to select no entries.
   b. Click **Delete** to remove a Vendor from the list.
4. Click **Commit** to save your settings.

Configuring Vendor Specific Option Tags

1. Choose **Network** > **DHCP Server** > **V4** > **Vendor Specific Configuration** (Figure 3-32).
2. Choose a Vendor ID (VID) from the drop-down list.
3. Enter the following information in the **Add Option Tag** window:
   a. In the **Vendor** field, enter the vendor name.
   b. In the **Tag ID** field, enter a number to identify the vendor in the field provided.
   c. In the **Type** field, enter a value using the information in Table 3-25 as a guide. The **String** field automatically populates with the appropriate number to support the chosen Type.
   d. Enter a **Value** in the field provided using the information in Table 3-25 as a guide.

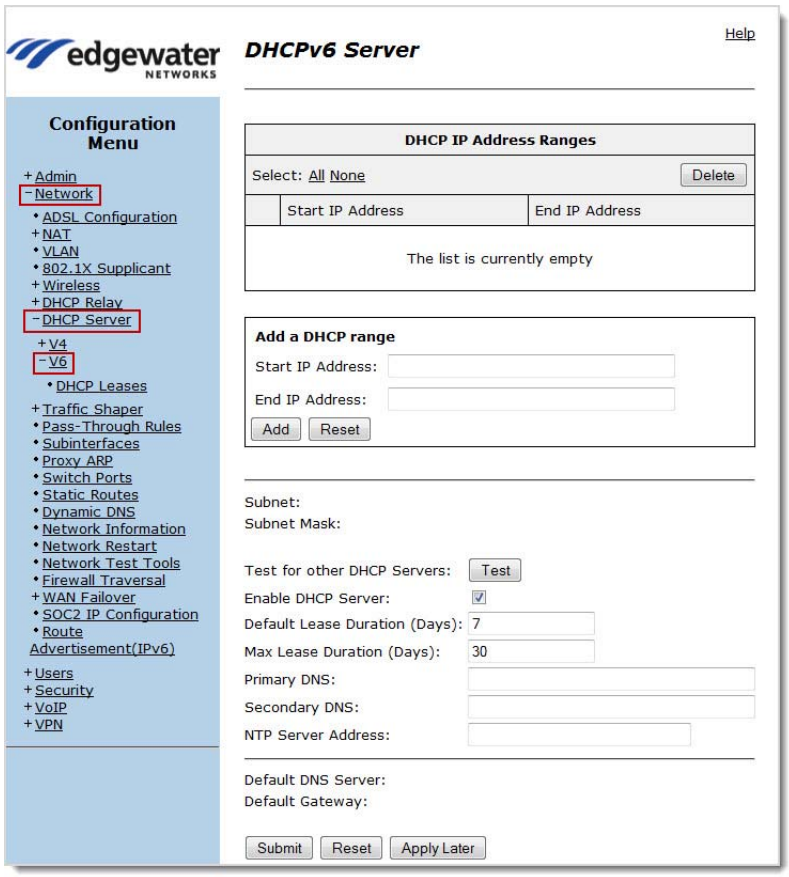
Table 3-25 Vendor Specific Input Options

Item	Description
Input Type ■ String—1 ■ Hex—1 ■ Byte Decimal—1 ■ Byte Hex—1 ■ Long Decimal—4 ■ Log Hex—4 ■ IPv4 address—4 ■ IPv6 address—16	
Strings	Normal strings. The length must be specified to 0, the length of the string, or longer. If the length is set to 0, the string length is calculated. If the string length is longer than the string, the string is zero padded to that length.
Bytes	One-byte unsigned integers which can hold a value between 0 and 255. The only difference between Byte Hex and Byte Long is how they are formatted in the GUI.
Longs	Four-byte unsigned integers which can hold a number between 0 and 4294967295. The only difference between Long Hex and Byte Long is how they are formatted in the GUI.
IPv4 Address	Raw IPv4 address (for example, 142.111.1.1)
IPv6 Address	Raw IPv6 address (for example, daaf::1)
Hex types	Specifies what the DHCP server actually receives. With this data type you can enter anything that the server will understand. The data should be formatted with two hex numbers followed by a colon (for example, 01:23:45:67:89:ab:cd:ef). This string has a length value of 8. Hex types and Strings share the same length rules.
Click **Add** to save your settings.	

Configuring DHCP Server IPv6

1. Choose **Network** > **DHCP** > **V6** (Figure 3-33).

Figure 3-33 DHCP Server IPv6 Page



2. Configure settings using the information in Table 3-26 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-26 DHCP Server IPv6 Parameters

Item	Description
Subnet	Selects a network to configure for DHCP if multiple networks are configured on the system.
DHCP IP Address Ranges	Shows the dynamic addresses to use for the LAN devices. See Managing DHCP IPv4 Address Ranges.

Table 3-26 DHCP Server IPv6 Parameters (continued)

Item	Description
Add a DHCP Range	
Configures individual DHCP IP addresses or a range of addresses and assigns static IP addresses for any common-access devices, such as printers or fax machines.	
DHCP Settings	
Configures the DHCP IPV6 server.	
Subnet Subnet Mask	Describes the Subnet and Subnet Mask addresses for the DHCP pool if multiple networks are configured on the system (view only). If multiple networks are configured on the system, select which network to configure for DHCP from the **Subnet** drop-down list.
Test for other DHCP Servers	Click the **Test** button to search for additional DHCP servers configured on the system. Only one DHCP server can be enabled on a network at a time.
Enable DHCP Server	Select the **Enable DHCP Server** checkbox to enable the DHCP server.
Default Lease Duration (Days)	Enter the default number of days to lease the DHCP service for your system. Default is 7 days.
Max Lease Duration (Days)	Enter the maximum number of days to the lease the DHCP service for your system. Default is 30 days.
Primary DNS	Enter the address of a Domain Name Server (DNS). If none is specified, the system DNS addresses is used.
Secondary DNS	Enter the address of a secondary DNS.
NTP Server	Enter the address of a Network Time Protocol (NTP) server.
Default DNS Server Default Gateway	Describes current DNS and default gateway settings (view only).

3. In the **Add a DHCP range** window:
   a. Enter a DHCP range in the **Start IP Address** and **End IP Address** fields.
   b. Click **Add**.

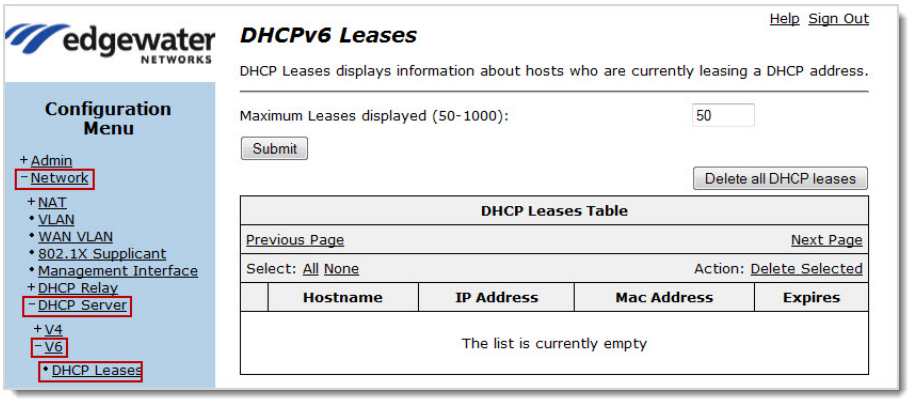
c. To delete a DHCP range, select the desired entry and click **Delete**.

4. Select the **Enable DHCP Server** checkbox to enable the DHCP IPv6 server.
5. Enter the number of days you want to lease the DHCP service in the **Default Lease Duration (Days)** field. Enter a minimum of one day to a maximum of 30 days (recommended).
6. Enter the maximum number of days for the DHCP lease to be valid on your system in the **Max Lease Duration (Days)** field.
7. In the **Primary DNS** field, enter the address of a Domain Name Server (DNS). If none is specified, the system DNS addresses is used.
8. In the **Secondary DNS** field, enter the address of a secondary DNS.
9. Enter the NTP server address in the **NTP Server Address (option 42)** field.
10. Click **Submit**.
11. Proceed to Configuring DHCPv6 Leases.

Configuring DHCPv6 Leases

1. Choose **Network** > **DHCP** > **V6** > **DHCP Leases** (Figure 3-34).

Figure 3-34 DHCPv6 Leases



2. In the **Maximum Leases displayed (50-1000)** field, enter the maximum number of leases to display and click **Submit**.
3. To delete a DHCP lease from the DHCP Leases table, select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
4. Click **Delete Selected**.
5. To delete all entries, click **Delete All DHCP Leases**.

Note
When deleting DHCP lease entries, the DHCP server is restarted. During this brief moment, hosts will not be able to obtain a DHCP IP address.

Configuring Traffic Shaping

This section describes how to configure network traffic control for optimized performance:

- Overview
- Using the Traffic Shaping Page
- Configuring Basic Traffic Shaping
- Configuring Advanced Traffic Shaping

Overview

The traffic management mechanisms provided by the EdgeMarc are designed to ensure that high-priority, real-time voice traffic is processed before lower priority data traffic. At the same time, bandwidth not in use by voice traffic is made available so that data traffic can burst up to full line rate, making efficient use of WAN bandwidth.

Traffic management mechanisms are applied to traffic in both the upstream (LAN to WAN) and downstream (WAN to LAN) direction. Each direction is independent of the other and can support different size priority queues. This is particularly useful in ADSL, where the downstream bandwidth is greater than the upstream bandwidth and it would be undesirable to limit downstream data traffic to the rate of the slower upstream link.

Classifying

High-priority voice traffic generated by endpoint devices such as IP phones and client adaptors is identified by their IP address. The user configures these addresses into a priority list using the traffic shaping features of the EdgeMarc VOS. As the EdgeMarc processes packets they are marked as either high or low priority based on this configuration.

Upstream Traffic Management

The EdgeMarc uses a combination of class-based queuing and simple classless queuing to send data in the upstream direction. The class-based queue (CBQ) consists of two priority classes (high and low), a scheduler to decide when packets need to be sent earlier than others, and a traffic shaper to rate limit by delaying packets before they are sent. Voice traffic is placed in the high-priority class and data traffic is placed in the low-priority class. High-priority data is sent at up to the configured priority data rate. This class is polled before lower priority data to reduce overall latency for voice traffic. Although preferential treatment is given to priority data, it is bounded so that low priority data is not starved. To smooth bursts from high speed data links (typically from the LAN Ethernet segment to the WAN) the EdgeMarc uses a buffer that clocks data out at a rate not exceeding the maximum amount for the slowest link. Any lasting burst condition causes packets to be delayed and then dropped.

Downstream Traffic Management

In the upstream direction (LAN to WAN), QoS mechanisms are applied to voice traffic being sent by the EdgeMarc to guarantee sufficient bandwidth. The EdgeMarc has control over how packets are handed to the WAN interface. In the downstream direction (WAN to LAN), the EdgeMarc is installed at the CPE end of a service provider link and has no control over the amount of voice or data traffic being sent to the WAN interface.

Voice traffic quality is guaranteed by shaping on the egress LAN and egress WAN ports of the EdgeMarc and leveraging the congestion avoidance mechanisms built into TCP to reduce the amount of data traffic on the link. Essentially, data packets received at a rate that exceeds the configured maximum are delayed (then dropped if necessary) when sent to the LAN interface by the EdgeMarc. Similarly, data traffic sent back to the EdgeMarc for transmission to the WAN is also delayed. This results in the end stations slowing down their transmit rate. This technique is effective because end stations usually reduce their transmit rate before VoIP signaling has completed for new call setup.

Excessive UDP traffic must be shaped in the service provider network, because UDP does not provide congestion avoidance mechanisms. The exception is RTP messages for voice traffic. Although RTP is based on UDP, the EdgeMarc provides its own congestion avoidance mechanism for voice traffic using CAC.

Basic Traffic Shaping

Traffic shaping in the system is designed to ensure that high priority real-time data is processed before lower priority non-real-time data. High priority endpoint devices such as VoIP phones are identified by the VoIP ALG function and are automatically marked as high priority. No user configuration is required.

To ensure that some bandwidth is available to non-priority traffic, the system enforces an upper limit on the priority data rate of 90-95% of the slowest link rate. Priority data is bounded so that low priority data is not starved. If low priority clients are starved, they generate retries that may exacerbate congestion during periods of peak usage.

Advanced Traffic Shaping

Advanced traffic shaping is available for use with MPLS-based virtual private networks. Advanced traffic shaping allows you to distinguish between up to eight different traffic classes. You can configure these classes so that they further prioritize traffic using bandwidth specifications and rules which are applied to traffic flows.

Advanced traffic shaping uses the Differentiated Services Coding Point (DSCP) to distinguish between the priority classes. All priority classes can exceed their specified bandwidth if bandwidth is available, otherwise they are restricted to the bandwidth values assigned to them. When multiple classes are exceeding the bandwidth values assigned to them but the WAN

link is not yet saturated, each class is allocated the remaining unused bandwidth equally. This continues until the WAN link becomes congested or saturated, at which point the throughput for any class falls back to its configured bandwidth.

If a class is not created for a DSCP value in use, all packets with that value are sent to the class that has a DSCP Best Effort value. CAC values for Primary and Secondary links specified on the Traffic Shaper page must not exceed the specified bandwidth of the class that is associated with the voice and video traffic.

ToS Byte Setting

Because the Internet itself has no direct knowledge of how to optimize the path for a particular application or user, the IP protocol provides a limited facility for upper layer protocols to convey hints to the Internet Layer about how the trade-offs should be made for the particular packet. This facility is the “Type of Service” or ToS facility.

ToS settings allow the service provider to prioritize time sensitive traffic, such as voice plus video to ensure minimized packet loss and delay through their network. When providing end-to-end QOS, it is important that the voice plus video traffic be placed in the correct queues to deliver a higher QOS than regular traffic. Regular traffic, that is not time sensitive, can be delayed with little or no indication to the user, while the slightest delay in voice plus video can cause audible differences. The ToS byte setting helps prioritize traffic going to the WAN so a provider can prioritize the traffic correctly in its network.

Although the ToS facility has been a part of the IP specification since the beginning, it has been little used in the past. However, the Internet host specification now mandates that hosts use the ToS facility. Additionally, routing protocols (including OSPF and Integrated IS-IS) have been developed which can compute routes separately for each type of service. These new routing protocols make it practical for routers to consider the requested type of service when making routing decisions.

For all RTP traffic (voice and video), the EdgeMarc marks the ToS byte in the IP header as “High Priority,” and strips (set to 0) the ToS byte for all other traffic. un-checking the “Enable ToS Byte Stripping” option means that the ToS byte will not be stripped from non-RTP traffic, but will remain unchanged.

For most situations, you should leave this setting as it is. Only change it if your provider indicates that you should do so.

Traffic Marking

While the Internet maintains no direct knowledge of how to optimize the path for a particular application or user, the IP protocol does provide a limited facility for upper layer protocols to convey hints to the Internet layer about how the trade-offs should be made for the particular packet. This facility is called Type of Service (ToS).

ToS settings allow the service provider to prioritize time sensitive traffic, such as voice plus video, to ensure minimized packet loss and delay through the network. When providing end-to-end quality of service (QoS), it is important that the voice plus video traffic be placed in the correct queues to deliver a higher QoS than regular traffic. Normal traffic that is not time sensitive can be delayed with little or no impact on the user, whereas the slightest delay in voice plus video can cause noticeable differences.

Although ToS has been a part of the IP specification since its inception, it has not been used extensively. However, the Internet host specification now mandates that hosts use ToS. Additionally, routing protocols (including OSPF and Integrated IS-IS) can now compute routes separately for each type of service. These new routing protocols make it practical for routers to consider the requested type of service when making routing decisions.

The Differentiated Services Code Point (DSCP) is the priority value that is encoded in the IP packet header. The DSCP value determines the level of preferred treatment that the packet receives as in travels through the network.

For all real-time transport protocol (RTP) traffic (voice and video), the EdgeMarc marks the ToS byte in the IP header as High Priority, and strips (set to 0) the ToS byte for all other traffic. un-checking the Enable ToS Byte Stripping option means that the ToS byte will not be stripped from non-RTP traffic, but instead will remain unchanged.

Call Admission Control (CAC)

CAC uses a deterministic algorithm to decide when there are insufficient network resources available to adequately support new calls and then return the equivalent of a “fast busy” to new call requests.

The EdgeMarc uses CAC to limit the number of active voice calls over the WAN link. This is necessary because a typical installation uses a ratio of 1:2 or 1:4 active voice calls to voice devices on the assumption that 50% or 25% of all users are on the phone at the same time.

These ratios are guidelines only, and at times the number of concurrent calls may exceed the amount of WAN bandwidth available to process the calls. In this instance existing phone calls will experience poor quality or be dropped altogether. To prevent this from occurring, a typical voice installation will set a threshold for the maximum number of concurrent voice calls supported by the WAN access link. New call requests in excess of this threshold will receive the equivalent of a “fast busy” and the WAN link will not become oversubscribed.

For IP Centrex installations the maximum number of concurrent voice calls is usually configured in the EdgeMarc by enabling CAC. When the EdgeMarc is deployed in IP PBX applications, the maximum number of concurrent calls could be configured in the IP PBX. If the PBX is responsible for this setting, you do not need to configure CAC in the EdgeMarc. Check with your IT administrator to determine if this is the case.

Note
CAC is available in the EdgeMarc for the MGCP and SIP VoIP protocols only.

Determining the Maximum Number of Concurrent Calls

The maximum number of concurrent calls that can be supported by the WAN access link is calculated using the following formula:

Max calls equals the Maximum WAN upstream bandwidth * .85/VoIP codec rate, where the maximum WAN upstream bandwidth equals the value entered in the **WAN Upstream Bandwidth** field (in Kbps)

VoIP codec rate equals 85.6 Kbps for G.711 voice devices or 29.6Kbps for G.729 voice devices.

The maximum WAN upstream bandwidth is multiplied by .85 in this formula to reduce the total bandwidth available for voice calls by 15%. This reduction is necessary because the EdgeMarc automatically reserves 15% of the total WAN bandwidth for low priority data traffic so that data traffic is not starved completely. Starving data traffic completely would increase the number of retry attempts and exacerbate congestion on the link during periods of peak usage. Table 3-27 describes WAN bandwidth calculation examples.

Table 3-27 WAN Bandwidth Calculation Examples

WAN Bandwidth Calculation	Description
(1544*.85)/85.6 = 15.3 or 15 total voice calls.	The maximum number of G.711 voice calls supported by a T1 (1.544 Kbps).
(768*.85)/85.6 = 7.6 or 7 total voice calls	The maximum number of G.711 voice calls supported by a 768Kbps SDSL.
(256*.85)/85.6 = 2.5 or 2 total voice calls	The maximum number of G.711 voice calls supported by an ADSL WAN with 768Kbps downstream WAN bandwidth and 256Kbps upstream.
(256*.85)/29.6 = 7.4 or 7 total voice calls	The maximum number of G.729 voice calls supported by an ADSL WAN with 768Kbps downstream WAN bandwidth and 256Kbps upstream.

Maximum Calls Allowed with Call Admission Control

CAC uses a combination of values to determine the maximum number of calls to allow through the system:

- The maximum number of calls set in the license key
- The maximum number of calls configured on the Primary and Secondary WAN.
- The maximum number of calls support by the hardware platform

The number of calls allowed is the smallest and most restrictive of these values. For example, the system hardware supports 10 calls, the license key allows 5 calls, and the CAC value is set to 8. In this example, the system allows up to simultaneous 5 calls.

To enable Call Admission Control (CAC), first determine the number of calls that can be achieved through the WAN connection. If the codec is G.711, the required bandwidth per call is 85.6 Kbits/sec. If the codec is G.729, the required bandwidth per call is 29.6 Kbits/sec. The data rates apply in both the upstream and downstream directions. The smaller of the upstream and downstream rates should be used to determine how many calls can be supported.

For example, you have a DSL line with physical data rates of 768/128 Kbits. Enter 768 in the WAN Downstream Bandwidth field and 128 in the WAN Upstream Bandwidth field. If CAC is enabled and the codec used is G.711, the maximum number of calls supported is one call. In this case, the upstream bandwidth is the limiting value.

Another example is a T1 line with physical data rates of 1544/1544 Kbits. Enter 1544 in the WAN Downstream Bandwidth field and 1544 in the WAN Upstream Bandwidth field. If CAC is enabled and the codec used is G.711, the maximum number of calls supported is 15 calls.

CAC value when using H.323

H.323 calls use multiple RTP streams for each video call, typically around 6-12 streams. If CAC is enabled and H.323 is used, you must account for the total number of RTP streams that will be created. For example, if your endpoints typically use 8 streams/call, then to allow 3 H.323 calls the CAC must be set to at least 24.



Note
Enabling CAC with H.323 is not recommended. Instead, use the "H.323 Maximum Bandwidth" setting to limit video calls.

Priority IP Addressing

VoIP traffic from devices that use the VoIP ALG function (for example, telephones, video stations, or softphones on PCs) are already marked as high priority and do not need to be manually configured in this list. This list is used to prioritize voice traffic from trunk interfaces of IP PBXs or other high-priority devices that do not use the VoIP ALG function of the EdgeMarc.

SIP Inactivity Monitoring

Dangling RTP occurs when a VoIP call completes but is not properly deallocated and torn down. Not properly tearing a call down can occur due to endpoint power failures, loss of Internet connection, or other abnormal behaviors. To the system, the call is still active (although it is inactive since there is no RTP activity) and the resources needed to maintain the call

persist indefinitely. If CAC is enabled or the number of calls is limited by the license and the max number of allowed calls is reached, the system will prevent additional calls from being placed or received.

The SIP Inactivity Monitor periodically scans all calls and monitors RTP activity. The timeout setting is a timeout period of inactivity (no RTP traffic in either direction) for a SIP call before it is torn down and deallocated by the system. Be cautious of configuring a short timeout value since a call with both parties not speaking (on mute) and silence suppression disabled has the same characteristics of an inactive call: the call was not properly torn down by either endpoint and there is no RTP activity). Should both parties not speak for longer than the timeout value, the system will erroneously tear the call down. The default and recommended timeout value is 90 minutes.

Generalized Random Early Detection (GRED)/ Low Latency Queuing (LLQ)

To improve congestion management, the EdgeMarc supports Low Latency Queuing (LLQ) using Strict Priority Queuing (SPQ). LLQ allows high priority traffic to jump to the front of the queue to improve latency.

The assignment of a strict priority queue is dynamically assigned by the client registration process or by the client configuration process (configuration of a SIP trunking endpoint). Any traffic type may be configured to use the SPQ queue.

When LLQ is enabled, the strict priority queue (SPQ or Q1) is always emptied before all other queues. If multiple traffic policies/classifications are assigned to the strict priority queue, the EdgeMarc treats the packets within those traffic classes as first-in, first-out (FIFO). When LLQ is disabled, all configured queues use the standard priority queuing policies (up to 8) previously supported on the EdgeMarc.

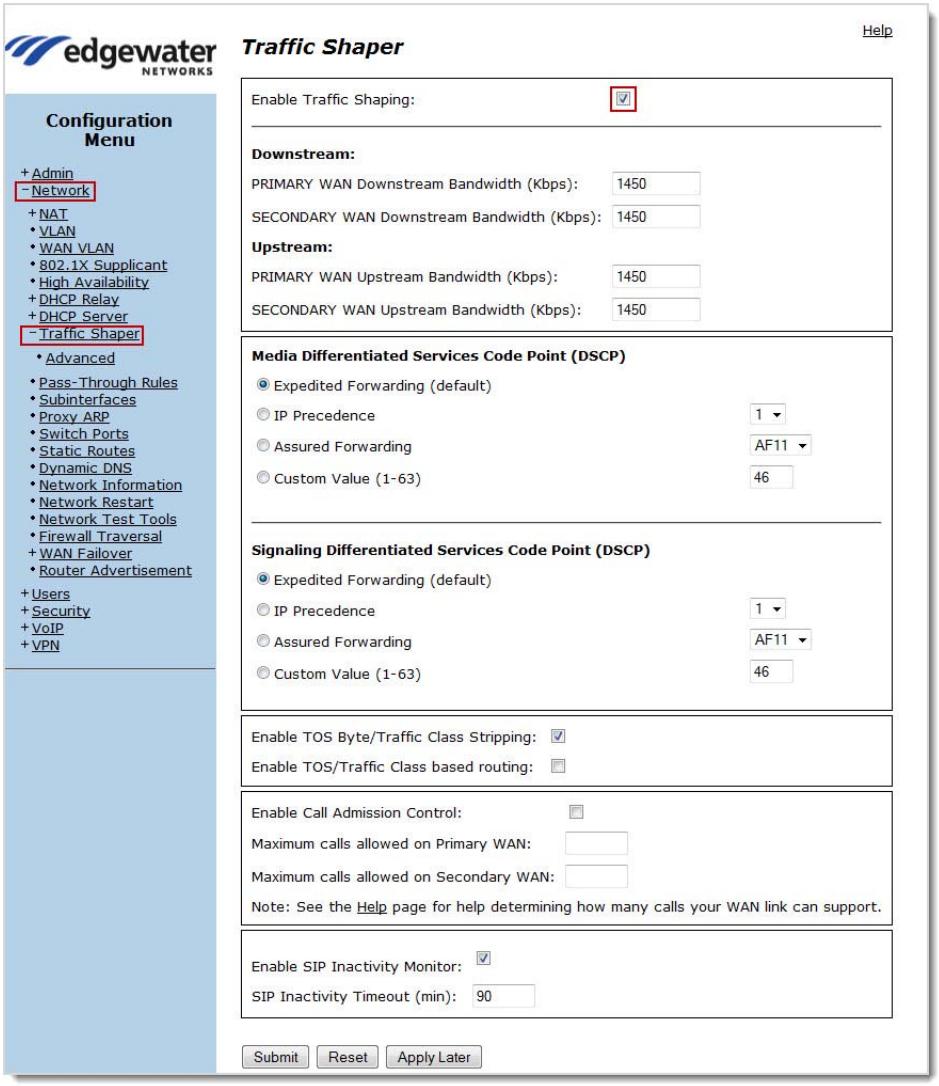
GRED monitors the average queue size and drops packets based on statistical probabilities when a minimum threshold is reached. If the EdgeMarc sends more traffic than the uplink can handle, the second “maximum” threshold is reached and all traffic in that class is dropped.

The EdgeMarc can be configured to support up to eight classes of service. Depending on the number of traffic classes created, multiple classes can be assigned to the LLQ. This allows, for example, a media class and signaling to be assigned to the same high-priority queue. Any traffic classification created can be directed to any of the queues selected on the on the **Network** > **Traffic Shaper** > **Advanced** page. See Configuring Advanced Traffic Shaping.

Using the Traffic Shaping Page

1. Choose **Network** > **Traffic Shaper** (Figure 3-35).

Figure 3-35 Traffic Shaper Page



2. Configure settings using the information in Table 3-28 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-28 Traffic Shaper Parameters

Item	Description
Enable Traffic Shaping	Enables traffic shaping. **NOTE:** With traffic shaping disabled, VoIP devices that are registered to the system ALG still have their layer 3 packets marked as Type of Service (ToS) 0xb8 or DIFFServ.
Enable GRED/LLQ Shaper	(Optional) Enables Low Latency Queuing (LLQ) using Strict Priority Queuing (SPQ) to allow high priority traffic to jump to the front of the queue to improve latency. Choose **Network** > **Traffic Shaper** > **Advanced** and refer to Setting GRED/LLQ Configuration Rules in Configuring Advanced Traffic Shaping.
Downstream Settings	
PRIMARY WAN Downstream Bandwidth (Kbps)	Specifies the total downstream bandwidth for your WAN connection. This value is entered in Kbps; for example, 1024 = 1 Mbps. The value is set to 1450 Kbps for a T1 link by default.
SECONDARY WAN Downstream Bandwidth (Kbps)	Specifies the total downstream bandwidth for your Secondary WAN connection.
Upstream Settings	
PRIMARY WAN Upstream Bandwidth (Kbps)	Specifies the total upstream bandwidth for your WAN connection. This value is entered in Kbps; for example 1024 = 1 Mbps. The value is set to 1450 Kbps for a T1 link by default.
SECONDARY WAN Upstream Bandwidth (Kbps)	Specifies the total upstream bandwidth for your Secondary WAN connection. Default is 1450 Kbps.

Table 3-28 Traffic Shaper Parameters (continued)

Item	Description
ADSL Bandwidth Parameters	Enables auto-configure ADSL Bandwidth Parameters. For systems with an integrated ADSL modem, the bandwidth parameters can be automatically configured with the bandwidth parameters negotiated between the modem and the central office. If this feature is enabled, the configured Downstream and Upstream bandwidth values will be interpreted as maximum values. The bandwidth values never exceed the configured maximum values. This feature is available on the EdgeMarc 250 Series.
Media Differentiated Services Code Point (DSCP)	
Specifies and controls network traffic by class. Media can be configured to use different DSCP values.	
Expedited Forwarding (Default)	Enables the expedited forwarding rule. Provides low-loss, low-latency, low-jitter and guaranteed bandwidth (90%) for real-time voice traffic.
IP Precedence	Enables IP layer packet classification to determine priority. Valid range is 1 through 7.
Assured Forwarding	Configures levels of forwarding assurances for IP packets. Valid range is AF11 through AF43.
Custom Value (1-63)	Specifies a custom rule for non-standard per-hop behavior.
Signaling Differentiated Services Code Point (DSCP)	
Specifies and controls network traffic by class. Signaling can be configured to use different DSCP values.	
Expedited Forwarding (Default)	Enables the expedited forwarding rule. Provides low-loss, low-latency, low-jitter and guaranteed bandwidth (90%) for real-time voice traffic.
IP Precedence	Enables IP layer packet classification to determine priority. Valid range is 1 through 7.
Assured Forwarding	Configures levels of forwarding assurances for IP packets. Valid range is AF11 through AF43.
Custom Value (1-63)	Specifies a custom rule for non-standard per-hop behavior.
Type of Service (ToS) Settings (IPv4 only)	
Sets the ToS byte in the IP header.	

Table 3-28 Traffic Shaper Parameters (continued)

Item	Description
Enable TOS Byte/Traffic Class Stripping	Strips the ToS byte from non-RTP traffic. This option is enabled by default. For all RTP traffic (voice and video) the system marks the ToS byte as High Priority, and strips (sets to 0) the ToS byte for all other traffic. **Caution:** This setting involves non real-time traffic entering the real-time traffic high priority queues. Poorly behaved data may cause voice quality problems.
Enable TOS/Traffic Class based routing	Routes all VoIP packets through the main WAN interface. This option is disabled by default. **Note:** This is used in rare configurations where you want the default route to be other than the WAN interface (for example, VPN) and you want VoIP traffic to still be routed through the WAN. This option should not be enabled for most configurations.
Call Admission Control (CAC)	
Configures a combination of values to determine the maximum number of calls to allow through the system. See Call Admission Control (CAC).	
Enable Call Admission Control	Enables Call Admission Control to ensure that bandwidth allocated to new voice calls does not adversely affect the quality of existing active calls.
Maximum Number of Calls Allowed (Primary and Secondary WAN)	Specifies the total number of VoIP calls allowed to traverse the system. This ensures that the system will not over-subscribe the total amount of WAN bandwidth. For example: ■ If the codec is G.711, the required data rate per call is 85.6 Kbytes/sec. ■ If the codec is G.729, the required data rate per call is 29.6 Kbytes/sec.
SIP Inactivity	
See SIP Inactivity Monitoring for more information.	
Enable SIP Inactivity Monitor	Enables RTP activity monitoring on all calls.
SIP Activity Timeout (min)	Specifies the time in minutes after which SIP activity is timed out. The SIP call is torn down and deallocated by the system. Default timeout value is 90 minutes (recommended).

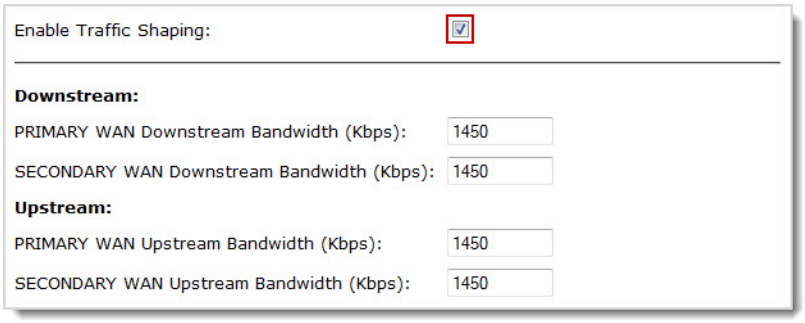
3. Proceed to Configuring Basic Traffic Shaping.

Configuring Basic Traffic Shaping

1. Choose **Network** > **Traffic Shaper** (Figure 3-35).
2. Select the **Enable Traffic Shaping** checkbox (Figure 3-36).

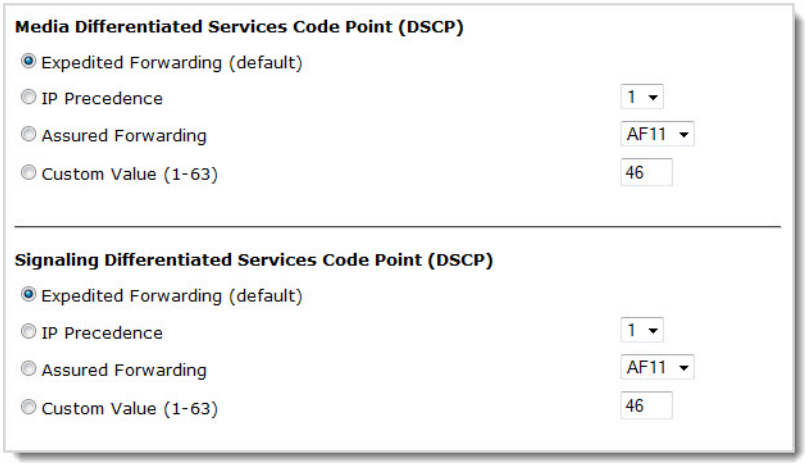
Note
You do not have to enable Enable GRED/LLQ Shaper to use basic traffic shaping features.

Figure 3-36 Basic Traffic Shaping



3. Enter the Downstream and Upstream bandwidth values for your WAN connection in kilobits per second (Kbps). By default, these values are set to 1450 Kbps for a T1 link.
4. Configure Media Differentiated Services Code Point (DSCP) settings (Figure 3-37).

Figure 3-37 Traffic Shaper DSCP Settings



5. **Expedited Forwarding** is set by default (recommended).
   Or select one of the following priority settings:

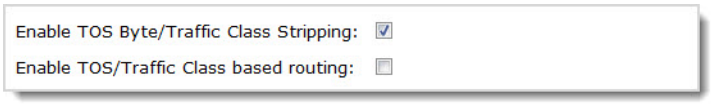
d. Choose a number from the **IP Precedence** drop-down list to enable IP layer packet classification to determine priority.

e. Choose a setting from the **Assured Forwarding** drop-down list to configure levels of forwarding assurances for IP packets.

f. Enter a number between 1 and 63 in the **Custom Value (1-63)** field to specify a custom rule for non-standard per-hop behavior.

6. Configure IPv4 settings (Figure 3-38):

Figure 3-38 Traffic Shaper IPv4 Settings

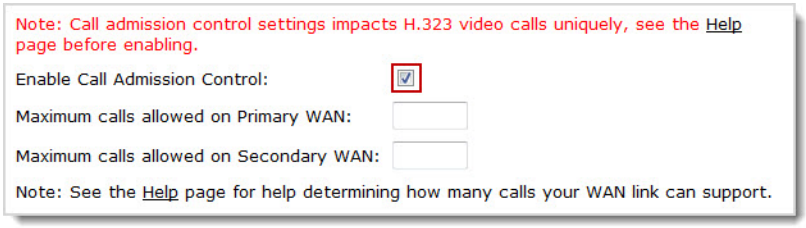


a. Select the **Enable TOS Byte/Traffic Class Stripping** checkbox to strip (set to 0) the ToS byte from non-RTP traffic (default).

b. Select the **Enable TOS/Traffic Class based routing** checkbox to route all VoIP packets through the main WAN interface.

7. Select the **Enable Call Admission Control** checkbox (Figure 3-39) to use a combination of values to determine the maximum number of calls to allow through the system:

Figure 3-39 Traffic Shaper CAC Settings



a. In the **Maximum call allowed on the Primary WAN** field, enter the number of calls that can be achieved through the WAN connection. The maximum number of calls for your system is set in your license key.

b. In the **Maximum calls allowed on the Secondary WAN** field, enter the maximum number of calls that are supported by your hardware platform.

8. Select the **Enable SIP Inactivity Monitor** checkbox to enable RTP activity monitoring on all calls (Figure 3-40).

Figure 3-40 Traffic Shaper SIP Settings



9. Enter a value in the **SIP Inactivity Timeout (min)** field to determine a timeout period of inactivity (no RTP traffic in either direction) for a

SIP call before it is torn down and deallocated by the system. The recommended value is 90 minutes (default).

10. Click **Submit** to save all settings on the page.

    A message indicates that service will be temporarily interrupted.

11. Click **OK** to confirm.

Configuring Advanced Traffic Shaping

To prioritize and guarantee bandwidth for different types of traffic, network traffic must be grouped into classes of service. The Traffic Shaper - Advanced page allows you to create and modify classes of service on the system and allocate a percentage of bandwidth to each class. By default, there are two preconfigured classes:

- Best Effort at 10% bandwidth
- Expedited Forwarding at 90% bandwidth

Support is available for IPv6 Class of Service and IPv4/IPv6 mixed traffic shaping.

See the following sections:

- Configuring Classes of Service
- Configuring Classification Rules
- Setting GRED/LLQ Configuration Rules
- Monitoring GRED/LLQ Traffic Shaping Debug Output

Before You Begin

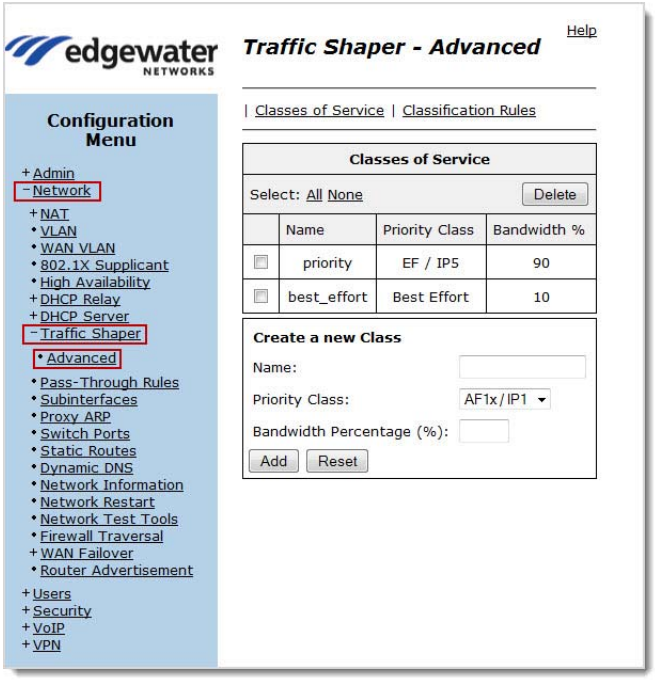
You must first enable traffic shaping:

1. Choose **Network** > **Traffic Shaping** (Figure 3-35) or click the **Traffic Shaper** link provided on the Traffic Shaper - Advanced page.
2. Select the **Enable Traffic Shaping** checkbox.
3. Click **Submit**. See Configuring Basic Traffic Shaping.

Configuring Classes of Service

1. Choose **Traffic Shaper** > **Advanced**. The Classes of Service page opens by default (Figure 3-41).

Figure 3-41 Advanced Traffic Shaping - Classes of Service



2. Configure settings using the information in Table 3-29 as a guide. When you have finished configuring settings, click **Add** to make your changes take effect.

Table 3-29 Advanced Traffic Shaper - Classes of Service Parameters

Item	Description
Classes of Service	
Manages the classes of service list.	
Create a New Class	
Assigns priorities and guarantees bandwidth for different types of traffic. See Creating a New Class of Service.	
Name	Enter the name of the class of service and its associated priority queue.
Priority Class	Choose a class of service from the drop-down list: ■ Best Effort —Default. All unmarked traffic is assigned to this class. This traffic is also the first to be dropped during times of congestion. Examples of best effort traffic include web, email, SNMP, and so on. ■ Assured Forwarding / IP Precedence (1 to 4)—For applications that require better reliability than the best-effort service. There are four Assured Forwarding classes of service: ■ AF1x/IP1 ■ AF2x/IP2 ■ AF3x/IP3 ■ AF4x/IP14 ■ Expedited Forwarding / IP Precedence 5—Provides low-loss, low-latency, low-jitter, and guaranteed bandwidth. For real-time voice traffic: ■ IP Precedence 6 and 7: ■ IP6 ■ IP7
LLQ	Designates traffic as LLQ. LLQ traffic is strictly prioritized and all LLQ traffic is transmitted before any GRED traffic is sent. See Setting GRED/LLQ Configuration Rules.
Bandwidth Percentage	Specifies the guaranteed percentage of bandwidth for the associated class during times of congestion. **Note:** The sum of bandwidth percentages for all configured classes cannot exceed 100 percent.

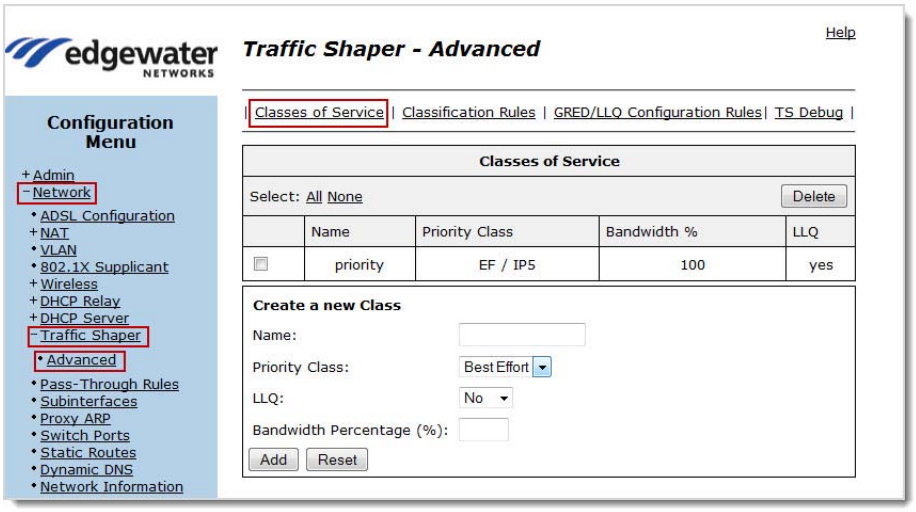
Deleting a Class of Service

1. In the Classes of Service window, select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
2. Click **Delete**.
3. Click **OK** to confirm.

Creating a New Class of Service

1. In the Create a New Class window, enter a name in the **Name** field.
2. Choose a class of service from the **Priority Class** drop-down list (Figure 3-42):
   - Best Effort—Default. All unmarked traffic is assigned to this class. This traffic is also the first to be dropped during times of congestion. For example web, email, and SNMP.
   - Assured Forwarding / IP Precedence (AF/IP 1 to 4)—For applications that require better reliability than best-effort service.
   - Expedited Forwarding / IP Precedence 5—Provides low-loss, low-latency, low-jitter and guaranteed bandwidth for real time voice traffic.
   - IP Precedence 6 and 7

Figure 3-42 Class of Service - Priority Classes



3. If the GRED/LLQ shaper is enabled, choose either **Yes** or **No** from the **LLQ** drop-down list to treat this traffic as LLQ. See Setting GRED/LLQ Configuration Rules.
4. Enter a value in the **Bandwidth Percentage** field. The sum of bandwidth percentages across all configured classes cannot exceed 100%, so you may need to manage the existing Classes of Service list before you can add a new class of service. See Deleting a Class of Service.
5. Click **Add**.

Configuring Classification Rules

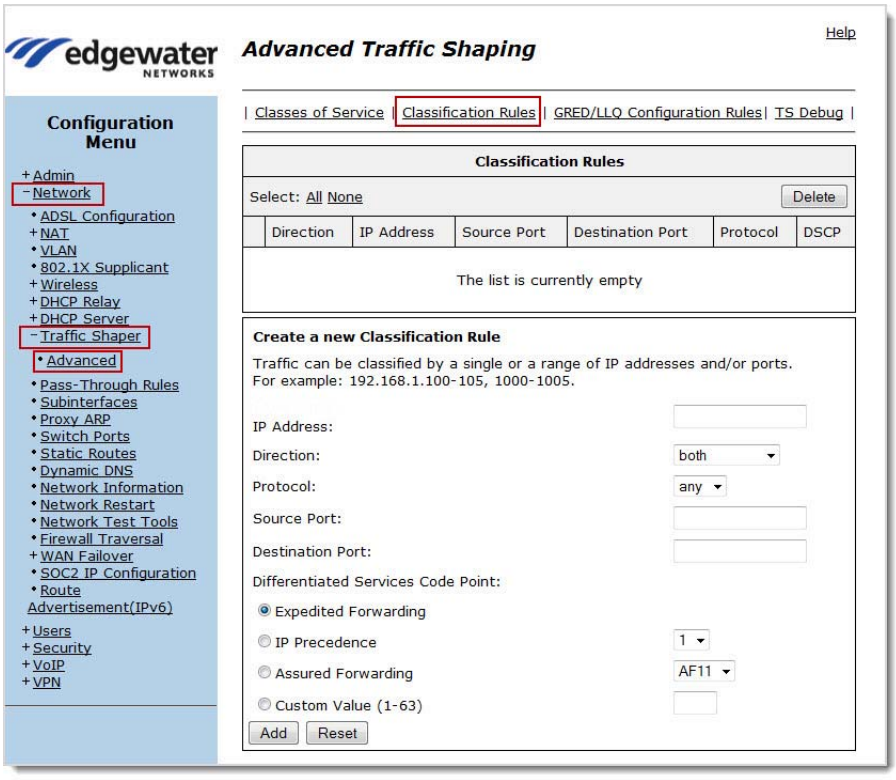
The Classification Rules page allows you to classify a flow of traffic into classes of service based on an IP address, traffic direction, transport protocol, and source and destination ports. Rules are created marking each packet in the flow with the configured DSCP value. The packet then enters the traffic shaper. Based on the DSCP value, the shaper applies the prioritization and bandwidth guarantees of the class of service to which the packet belongs.

Devices that use VoIP ALG (phones, video stations, etc.) are already marked as high priority. All data from IP addresses in the Classification Rules list have the same priority as voice data.

To configure classification rules:

1. Choose **Network** > **Traffic Shaper** > **Advanced**. The Classes of Service page opens by default (Figure 3-41).
2. Click **Classification Rules** to open the Classification Rules configuration page (Figure 3-43).

Figure 3-43 Advanced Traffic Shaping - Classification Rules



3. Configure settings using the information in Table 3-30 as a guide. When you have finished configuring settings, click **Add** to make your changes take effect.

Table 3-30 Advanced Traffic Shaper - Classification Rules

Item	Description
Classification Rules	
Manages the Classification Rules list. See Deleting a Classification Rule.	
Create a New Classification Rule	
Classifies a rule by assigning a single or a range of IP addresses and/or ports. See Configuring Classification Rules.	
IP Address	Specifies the IP address. This can be a single IP address, a range of IP addresses, or can be left blank to signify any IP address.
Direction	Specifies the direction of the traffic. This field only applies if an IP address is entered.
Protocol	Specifies the transport protocol: TCP, UDP, or Any.
Source Port	Specifies the source port. This can be a single port, a range of ports, or the field can be left blank to specify any port number. To specify a range, enter the start port, a '-', then the end port number. For example, 1000-10005. If you configure a port, remember to select a specific transport protocol.
Destination Port	Specifies the destination port. This can be a single port, a range of ports, or the field can be left blank to specify any port number. To specify a range, enter the start port, a '-', then the end port number. For example, 1000-10005. If you configure a port, remember to select a specific transport protocol.
Differentiated Services Code Point	Specifies the DSCP value used to mark the traffic flow.

Deleting a Classification Rule

1. In the Classification Rules window, select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
2. Click **Delete**.
3. Click **OK** to confirm.

Creating a New Classification Rule

1. In the Create a New Classification Rule window, enter a single IP address or a range of IP addresses in the **IP Address** field. Or leave the field blank to signify any IP address. To specify a range, enter the

start IP and the last octet of the end IP in the range separated by a hyphen. For example, 192.168.1.100-105.

If you enter a value in the IP Address field, the Direction field becomes active.

2. Choose the direction of the flow of traffic that you want to mark from the **Direction** drop-down list:
   - Upstream
   - Downstream
   - Both
3. Choose the transport protocol of the flow you wish to mark from the **Protocol** drop-down list:
   - Any
   - UDP
   - TCP

   If you specify a source or destination port, you must select either the UDP or TCP transport protocol.
4. Enter a single port or a range of ports in the **Source Port** and **Destination Port** fields. Or leave the fields blank to specify any port number. To specify a range, enter the start port and destination port separated by a hyphen. For example, 1000-10005.

   If you configure a port, remember to select a specific transport protocol.
5. Configure Media Differentiated Services Code Point (DSCP) settings. **Expedited Forwarding** is set by default (recommended).

   Or select one of the following priority settings:
   - Choose a number from the **IP Precedence** drop-down list to enable IP layer packet classification to determine priority. These classes are for devices that use the top 3 bits of the TOS byte for IP Precedence. There are 8 IP Precedence classes.
   - Choose a setting from the **Assured Forwarding** drop-down list to ensure that packets are forwarded. There are four Assured Forwarding classes and within each class are three drop probabilities: 1 (low), 2 (medium), and 3 (high). For example, AF33 is Assured Forwarding class 3 with a high drop probability.
   - Enter a **Custom Value (1-63)** if your system supports this option. This option is for advanced users only. VoIP services on the system such as the ALG automatically mark VoIP packets with this value. Consult your Internet service provider for the recommended setting.
6. Click **Add**.

Setting GRED/LLQ Configuration Rules

Before You Begin

You must first enable traffic shaping and the GRED/LLQ shaper:

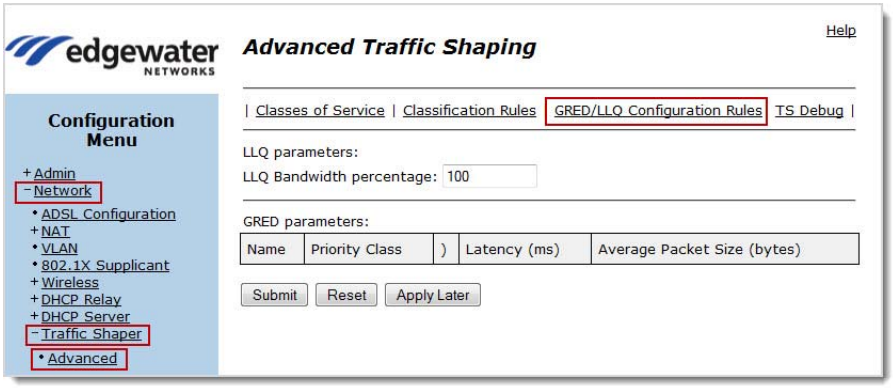
1. Choose **Network** > **Traffic Shaper**.
2. Select the **Enable Traffic Shaping** checkbox.

3. Select the **Enable GRED/LLQ Shaper** checkbox.
4. Click **Submit**.

To configure GRED/LLQ:

1. Choose **Traffic Shaper** > **Advanced**. The Classes of Service page opens by default (Figure 3-41).
2. Click **GRED/LLQ Configuration Rules** (Figure 3-44).

Figure 3-44 Advanced Traffic Shaping - GRED/LLQ Configuration Rules



3. Configure settings using the information in Table 3-31 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-31 Advanced Traffic Shaper - GRED/LLQ Configuration Rules

Item	Description
LLQ Parameters	
Configures LLQ parameters.	
LLQ Bandwidth Percentage	Sets the amount of bandwidth allocated to the LLQ side. If this is set below 100, the low priority traffic is allowed to send data even when there is high priority traffic to be sent. Use the default value of 100.
GRED Parameters	
Configures GRED parameters.	
Name	Specifies the name of the GRED and its associated priority queue.

Table 3-31 Advanced Traffic Shaper - GRED/LLQ Configuration Rules

Item	Description
Priority Class	Specifies the Per-Hop Behavior (PHB) for the associated GRED: ■ Best Effort—Default. All unmarked traffic is assigned to this class. This traffic is also the first to be dropped during times of congestion. Examples of best effort traffic include web, email, SNMP, and so on. ■ Assured Forwarding / IP Precedence (1 to 4)—For applications that require better reliability than the best-effort service. ■ Expedited Forwarding / IP Precedence 5—Provides low-loss, low-latency, low-jitter, and guaranteed bandwidth. For real-time voice traffic. ■ IP Precedence 6 and 7—Protects critical data from being dropped due to congestion. For example, IGP and BGP, which go to the route processor, get priority and have the least chance of getting dropped.
Latency	Sets the desired latency for a packet. More allowed latency means that the packet can remain in the queue longer and is less likely to drop.
Average packet size	Specifies the average sized packet in bytes. ■ Internet Mix (IMIX) traffic—880b ■ Voice traffic—64b

4. In the **LLQ Bandwidth percentage** field, leave the default value of 100 to manage high priority traffic.
5. Set GRED parameters:
   a. In the **Name** field, enter the name of the GRED and its associated priority queue.
   b. In the **Priority Class** field, choose the PHB for the associated GRED:
      - Best Effort—Default
      - Assured Forwarding / IP Precedence (1 to 4)—IP Precedence classes 1 through 4
      - Expedited Forwarding / IP Precedence 5—IP Precedence class 5
      - IP Precedence 6 and 7
   c. In the **Latency** field, enter the latency value for a packet.
   d. In the **Average Packet Size (bytes)** field, choose a value:
      - Internet Mix (IMIX) traffic—880b
      - Voice traffic—64b
6. Click **Submit** to save your settings.

Monitoring GRED/LLQ Traffic Shaping Debug Output

The Traffic Shaper (TS) Debug page provides basic debug output for the GRED/LLQ traffic shaper.

Before You Begin

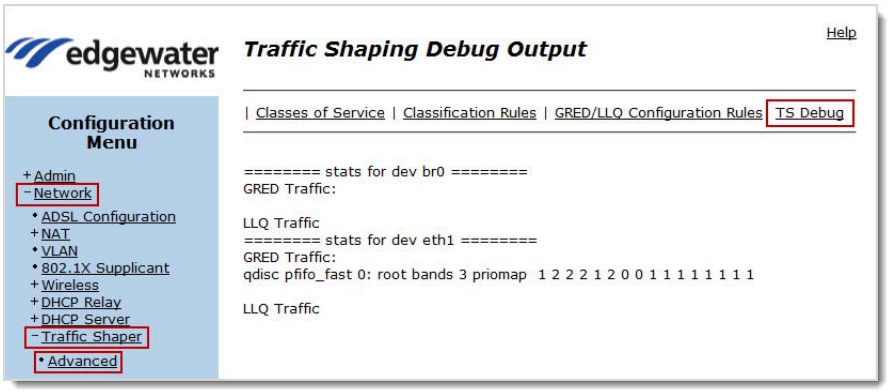
You must first enable traffic shaping and the GRED/LLQ shaper:

1. Choose **Network** > **Traffic Shaper**.
2. Select the **Enable Traffic Shaping** checkbox.
3. Select the **Enable GRED/LLQ Shaper** checkbox.
4. Click **Submit**.

To monitor GRED/LLQ traffic debugging:

1. Choose **Network** > **Traffic Shaper** > **Advanced**. The Classes of Service page opens by default (Figure 3-41).
2. Click **TS Debug** (Figure 3-45).

Figure 3-45 Advanced Traffic Shaping - TS Debug



Configuring Pass-Through Rules

Pass-Through Rules allow you to forward data traffic for a subnet from one interface to another, overriding the firewall default drop rules.

- Overview
- Adding a Pass-Through Rule
- Deleting a Pass-Through Rule

Overview

Subnet forwarding is commonly used when servers with public addresses are placed behind the system. Configuring the network in this way allows

the system to manage and prioritize bandwidth, sharing it between the VoIP services and the servers.

When pass-through traffic is allowed, it is common for one address from the forwarded range of addresses to be assigned to the rule output interface. The system uses this address to act as a gateway router for the subnet. The address is assigned using the **Network** > **Subinterfaces** page. See Configuring Subinterfaces.

Note
The subnet and pass-through addresses are not protected by the firewall.

A similar method for forwarding traffic is provided by Proxy ARP. Proxy ARP is used to “bridge” addresses within a single subnet range from one interface to another. Often this is used to bridge and forward a public address to the protected side of the system without having to subnet the public address range. Proxy ARP does not require an additional gateway address on the System for the subnet, but does not allow port and protocol filtering for pass-through traffic. Choose **Network** > **Proxy ARP** and refer to Configuring Proxy ARP.

Adding a Pass-Through Rule

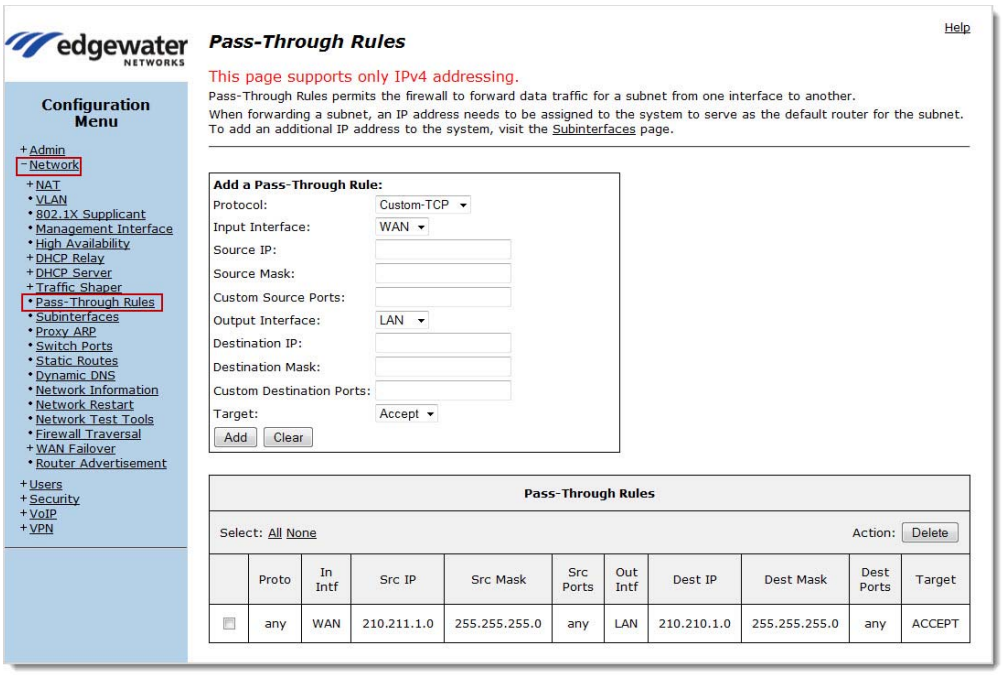
Before You Begin

You must first enable the firewall from the **Security** page for pass-through rules to be applied. See Configuring Basic WAN Firewall Settings in Chapter 5, *Configuring System Security*.

To add a Pass-Through Rule:

1. Choose **Network** > **Pass-Through Rules** (Figure 3-46).

Figure 3-46 Pass-Through Rules Page



2. Configure settings using the information in Table 3-32 as a guide. When you have finished configuring settings, click **Add** to make your changes take effect.

Table 3-32 Custom Rules Fields

Field	Description
Protocol	Choose ports and protocols that are allowed through the system. ■ Custom-UDP—Allows the specified UDP port to pass through the system ■ Custom-TCP—Allows the specified TCP port to pass through the system ■ Any—Allows all ports and protocols through the system. Ports are not required because not all protocols support the concept of ports. For the remaining protocol options, the correct protocol and port is automatically applied for the selected addresses.
Input Interface	Choose the interface where data is received that is destined for the forwarded subnet destination address: ■ WAN ■ LAN ■ VoIP ■ VLAN_1

Table 3-32 Custom Rules Fields (continued)

Field	Description
Source IP	Enter the source address or network to be forwarded through the firewall from the Input Interface to the Output Interface. When left blank or set to 0.0.0.0, all addresses in the subnet are selected.
Source Mask	Enter the network mask that applies to the Source IP to create the host or range of IP addresses that are forwarded through the firewall. When left blank or set to 0.0.0.0, all destination addresses are allowed for this rule.
Custom Source Ports	Enter the source port number that is allowed through the system when either Custom-UDP or Custom-TCP protocol is selected. The Custom Port parameter is not required when Any or a protocol other than Custom-UDP or Custom-TCP is selected. **Note:** For multi-DLCI single T1 Frame Relay links: When VOICE_LAN or VOICE_WAN are selected using the Any rule, traffic is automatically forwarded from VOICE_LAN to VOICE_WAN. Traffic from VOICE_WAN to VOICE_LAN is dropped unless a rule allows it through.
Output Interface	Choose the interface where data is received and then sent from the forwarded subnet destination address: ■ WAN ■ LAN ■ VoIP ■ VLAN_1
Destination IP	Enter the destination address or network to be forwarded through the firewall from the Input Interface to the Output Interface. When left blank or set to 0.0.0.0, all addresses in the subnet are selected.
Destination Mask	Enter the network mask that applies to the Destination IP to create the host or range of IP addresses that are forwarded through the firewall. When left blank or set to 0.0.0.0, all destination addresses are allowed for this rule.

Table 3-32 Custom Rules Fields (continued)

Field	Description
Custom Destination Ports	Enter the destination port number that is allowed through the system when either Custom-UDP or Custom-TCP protocol is selected. The Custom Port parameter is not required when Any or a protocol other than Custom-UDP or Custom-TCP is selected.
Target	Choose the action that is applied to packets that match the rule. The options are ACCEPT or DROP.

Pass-Through Rules

Lists configured Pass-Through Rules.

Click **Add** to save your settings.

A message indicates that service will be temporarily interrupted.

Click **OK** to confirm.

Deleting a Pass-Through Rule

1. Choose **Network** > **Pass-Through Rules** (Figure 3-46).
2. In the **Manage Pass-Through Rules** list, select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
3. Click **Delete**. Click **OK** to confirm.

Configuring Subinterfaces

The Subinterfaces page allows you to assign additional IP addresses to a system interface. These addresses are sometimes referred to as alias or loopback interfaces.

Tip
The Subinterface network can be a subnet of Remote Protected VPN Networks, but it cannot be the same as or a supernet of Remote Protected VPN Networks.

See the following sections:

- Overview
- Adding a Network Subinterface
- Deleting a Subinterface

Overview

A common use for subinterfaces is forwarding a public subnet. A subinterface may be created to support a subnet forwarded through the system. When forwarding a subnet through the system, it is necessary to assign an address for the subnet to act as the system subnet gateway. To configure forwarding rules, choose **Network** > **NAT** > **Port Forwarding** and refer to Configuring Port Forwarding.

When applied to the WAN/Provider interface, these addresses are protected by the same firewall policy that is applied to the WAN/Provider address. Other features in the system automatically create Subinterfaces, Refer to Configuring NAT Settings.

When viewing the **Network** > **Network Information** page, Subinterfaces are designated in the Interface Information section with the device name and number, separated by a colon (for example, eth0:100 or eth0.1:100). Refer to Viewing Network Information.

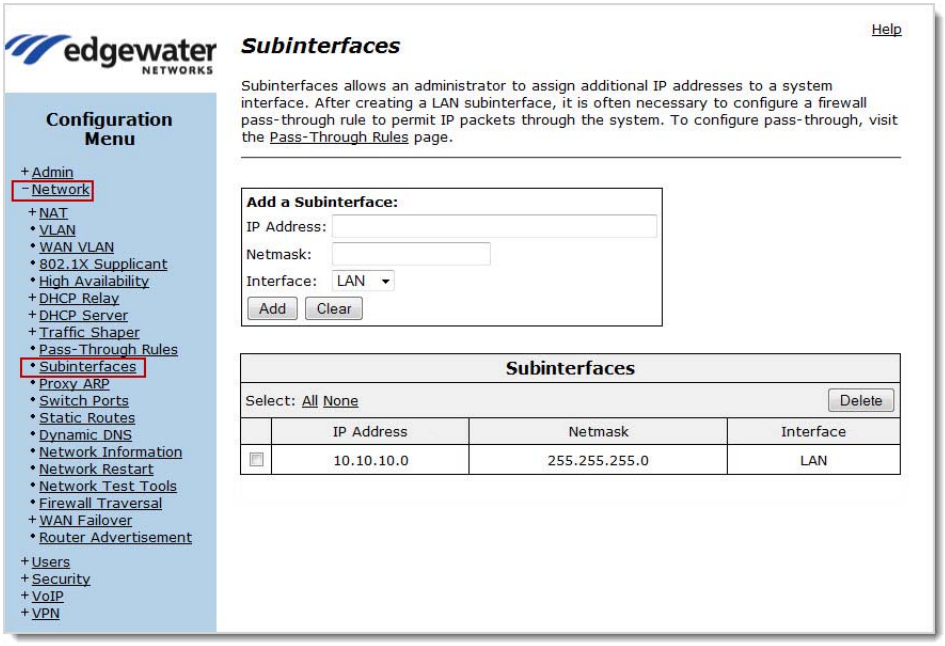


Note
After creating a LAN subinterface, it is often necessary to configure a firewall forwarding rule to permit IP packets through the system. See Configuring Basic WAN Firewall Settings in Chapter 5, *Configuring System Security*.

Adding a Network Subinterface

1. Choose **Network** > **Subinterfaces** (Figure 3-47).

Figure 3-47 Subinterfaces Page



2. Configure settings using the information in Table 3-33 as a guide. When you have finished configuring settings, click **Add** to make your changes take effect.

Table 3-33 Subinterfaces Page Parameters

Item	Description
Add a Subinterface	
Assigns additional IP addresses to interfaces. These addresses are sometimes referred to as alias or loopback interfaces.	
IP Address	Enter the subinterface IP address.
Netmask	Enter the network mask associated with the IP address. The default value is 255.255.255.0. If several addresses are applied to an interface and these addresses are in a common network, they must use a common subnet. The system does not support supernetting.

Table 3-33 Subinterfaces Page Parameters (continued)

Item	Description
Interface	Choose a port location from the **Interface** drop-down list: ■ LAN ■ WAN After creating a LAN subinterface, it is often necessary to configure a firewall pass-through rule to permit IP packets through the system. To configure pass-through rules, choose **Network** > **Pass-Through Rules** and refer to Configuring Pass-Through Rules.
Subinterfaces Manage subinterfaces on the system.	Click **Add**. A message indicates that service will be interrupted. Click **OK** and then **Submit All**. Enter additional subinterfaces as needed.

Deleting a Subinterface

1. Choose **Network** > **Subinterfaces** (Figure 3-47).
2. In the Subinterfaces table, select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
3. Click **Delete**.
4. Click **OK** to confirm.

Configuring Proxy ARP

Use the Proxy ARP page to create a bridge between two interfaces on the system. Addresses and networks that are bridged bypass the firewall and NAT, allowing complete unprotected access to the systems using the addresses.

Overview

Proxy Address Resolution Protocol (ARP) allows the system to respond to ARP requests for the IP address on the specified interface. Without an ARP

response, external devices would be unable to communicate with the requested IP address.

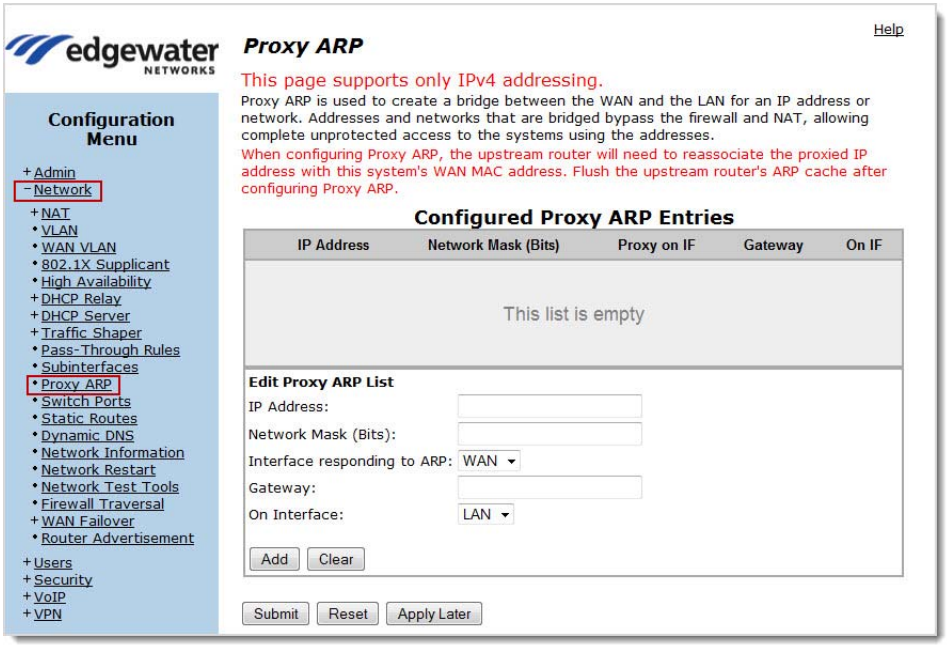
Even though the system responds to ARP requests, it is transparent to the external device and the system using the proxied address. Because the system is transparent, the firewall and NAT features do not affect traffic to and from the proxied address. In addition to proxying individual addresses, a range of addresses can be proxied by specifying a network netmask rather than a host netmask.

Caution
If an address is proxied, the system using the address should have a firewall or it should be not be on the public network.

Using the Proxy ARP Page

1. Choose **Network** > **Proxy ARP** (Figure 3-48).

Figure 3-48 Proxy ARP Page



2. Configure settings using the information in Table 3-34 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-34 Proxy ARP Parameters

Item	Description
Configured Proxy ARP Entries	
Manages a list of configured Proxy ARP entries.	
Edit Proxy ARP List	
Proxy individual addresses or a range of addresses by specifying a network netmask rather than a host netmask.	
IP Address /Bitmask	Enter the IP address and netmask of the subnet to be proxied. For example, 67.40.40.1/32 for this single address. A netmask must be 0 through 32.
Interface responding to ARP	Choose the interface that the system uses to respond to ARP requests. Choose an interface that does not have access to the host system using the proxied address. Usually this is the system WAN interface, which is the default setting.
Gateway	Enter the gateway IP address for the proxy target. The IP address belongs to the subnet of the target interface that is connected to EdgeMarc. The EdgeMarc uses this IP address as the source IP for the ARP requests to the proxy target. This ensures that Proxy ARP works for devices that require that an ARP source IP address belongs to its receiving interface. **Note:** The gateway does not necessarily exist physically. You only need to choose a logical IP address that belongs to the proxy target subnet that does not conflict with existing IP address.
On Interface	Choose the system interface where the proxy target is connected. ■ When VLAN is not enabled, this is always the LAN interface. ■ When VLAN is enabled, choose the VLAN interface to which the target is connected.
Respond to ARP requests on	Enter the interface that the system uses to respond to ARP requests. Use an interface that does not have access to the host system using the proxied address. This interface must be the system WAN interface.
Note: Flush the upstream router ARP cache after configuring Proxy ARP so that the upstream router can reassociate the proxied IP address with this system WAN MAC address.	

Deleting a Proxy ARP Entry

To delete a Proxy ARP entry from the Configured Proxy ARP Entries table:

1. Select checkboxes for the entries that you want to delete; click **All** to choose all entries or click **None** to clear your selections.
2. Click **Delete**.

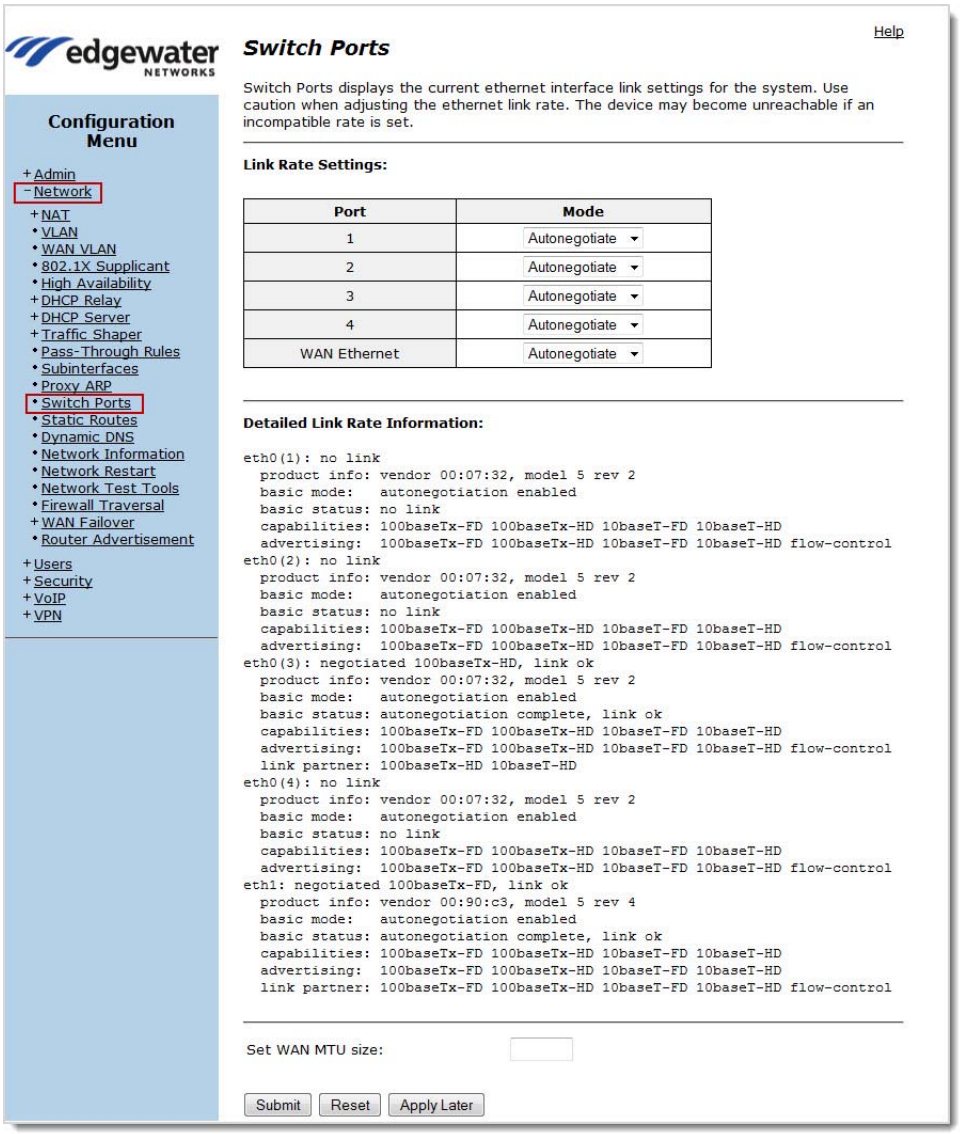
   A message indicates that service will be temporarily interrupted.
3. Click **OK** to confirm.

Managing Switch Ports Settings

Switch Ports displays the current Ethernet interface link settings for the system. If needed, the rate for each interface can be set manually to establish a reliable connection. The MTU size of the WAN interface can be adjusted to reduce the effects of large data packet on media data.

1. Choose **Network** > **Switch Ports** (Figure 3-49).

Figure 3-49 Switch Ports Configuration Page



2. Configure settings using the information in Table 3-35 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-35 Set Link Parameters

Item	Description
Link Rate Settings	Displays the current Port and Mode settings for the LAN and WAN interfaces. **Port**—Ports on the system and WAN Ethernet. **Mode**—Choose the link rate of an interface from the drop-down list: ■ Autonegotiate (default) ■ 10Base T-HD ■ 10Base T-FD ■ 100Base T-HD ■ 100Base T-FD You may want to set the rate manually if autonegotiation fails to select a rate consistently or if it selects a rate that is slower than the maximum rate supported by both interfaces. **Note:** Both sides of the link MUST be set to the same rate. Inconsistent rates may cause “flutter,” leading to intermittent voice outages.
Detailed Link Rate Information	Lists view-only link rate information. If the negotiated rates change intermittently or the link is reported as no link or down, the link rate may need to be set manually. Both sides of the link must be set to the same rate. Inconsistent rates may cause “flutter,” leading to intermittent voice outages.
Set WAN MTU size	Enter a value to set the WAN MTU size to reduce latency when large data packets are sent over a slow link. If this field is left blank, the system determines the most optimal MTU size based on WAN settings. The default setting is 1500 bytes for static IP addresses. PPPoE links negotiate the value automatically although the value can be overridden using this field. If the WAN Upstream Bandwidth is less than 256 Kbps, the MTU size is automatically reduced to 800 bytes. The WAN interface must have an IPv4 address assigned. **Note:** When the link rate is set manually, ensure that the device at the far end of the connection can communicate at the desired rate. Incompatible rates can cause a loss of communication with the system.

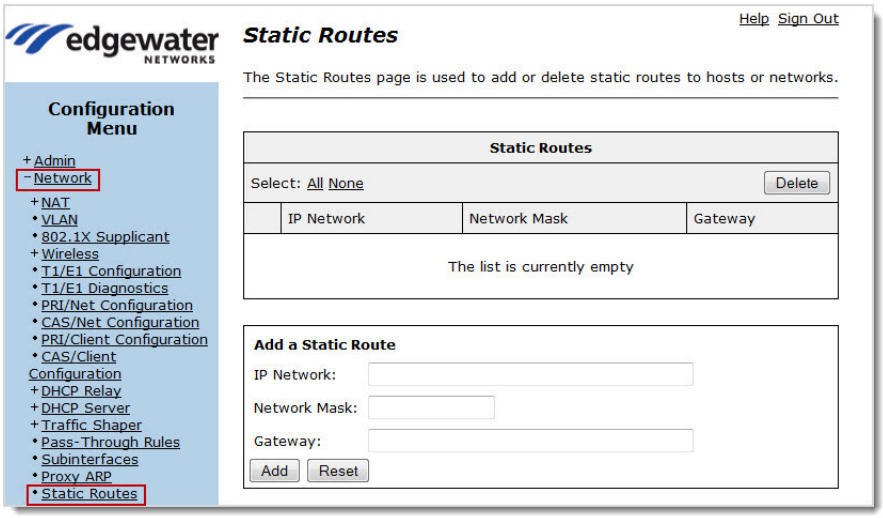
Configuring Static Routes

Use the Route page to create static routes on the system. Static routes may be needed to support network applications (such as a web server) that are allowed through the firewall and directed to a specific IP address or subnet.

Caution
Static routes may prevent the other networking features in the system from functioning properly.

1. Choose **Network** > **Static Routes** (Figure 3-50).

Figure 3-50 Static Routes Page



2. Configure settings using the information in Figure 3-36 as a guide. When you have finished configuring settings, click **Add** to make your changes take effect. Click **Submit All** to save all settings on the page.

Table 3-36 Static Routes

Item	Description
Static Routes	
Manages status routes on the system.	
Add a Static Route	
Creates a static route on the system.	
Apply Route	Activates the route.
IP Network	Enter an Pv4 or an IPv6 address for the remote network in the **IP Network** field.
Network Mask	Enter the subnet mask of the remote network address. ■ For an IPv4 network, this may be defined in the form of a bit mask (for example, 255.255.255.0) or a network mask length (for example, 24). When defining a host route for IPv4, the netmask should be set to 255.255.255.255 or 32. ■ For an IPv6 network, this must be the network mask length (for example, 48). When defining a host route for IPv6, the netmask should be 128.
Gateway	Enter the IPv4 or an IPv6 address of the router on this device's LAN network that is routing for the remote network or host.

Deleting a Static Route

1. In the Static Routes list, select checkboxes for the entries that you want to delete; click **All** to choose all entries or click **None** to clear your selections.
2. Click **Delete**.

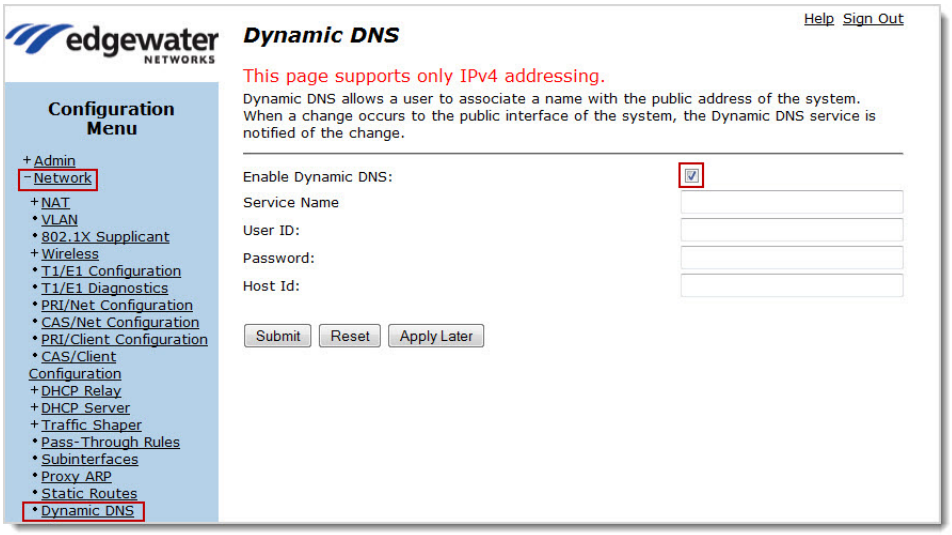
   A message indicates that service will be temporarily interrupted.
3. Click **OK** to confirm.

Configuring Dynamic DNS

Dynamic DNS allows a system administrator to associate a name with the system public address. When a change occurs to the system public interface, the Dynamic DNS service is notified of the change. Dynamic DNS is used in systems with frequently changing public addresses (DHCP or PPPoE). Even systems with static addresses can use dynamic DNS to assign a name to a system.

1. Choose **Network** > **Dynamic DNS** (Figure 3-51).

Figure 3-51 Dynamic DNS Page



2. Configure settings using the information in Table 3-37 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-37 Dynamic DNS Parameters

Item	Description
Enable Dynamic DNS	Select the **Enable Dynamic DNS** checkbox to notify the external DNS server that the system IP address has changed.
Service Name	Enter the system service name. Choose from the following names.

Service Name	URL for Service Provider
dhs	www.dhs.org
dyndns	www.dyndns.org
ods	www.ods.org
tzo	www.tzo.com
easydns	www.easydns.com
justlinux	www.justlinux.com
zoneedit	www.zoneedit.com

User ID	Specifies the user ID to authenticate the DNS name with the service provider. This is usually the information used when a user signs up for Dynamic DNS with one of the service providers shown above.
Password	Enter a password for the User ID.
Host ID	Enter a domain name to identify the system. The name is the fully qualified domain name that can be used to access the system from the public Internet (for example, mysitename.dyndns.org). This name is usually created in the user's portal on the service provider's site.

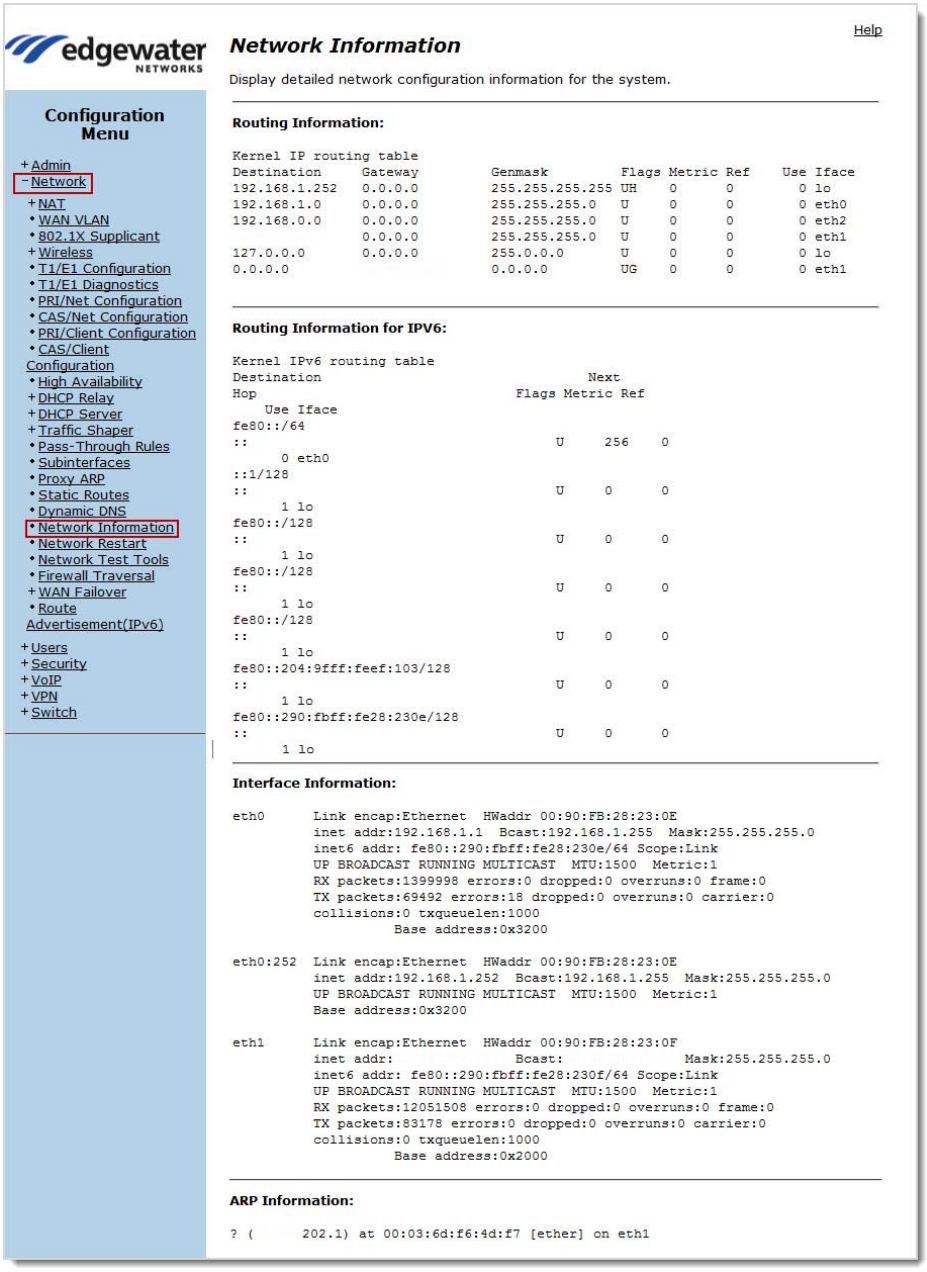
3. Click **Add**.
   A message indicates that service will be interrupted.
4. Click **OK** to confirm.

Viewing Network Information

Displays details of your system network configuration.

1. Choose **Network** > **Network Information** (Figure 3-52).

Figure 3-52 Network Information Page



2. View output descriptions in Table 3-38.

Table 3-38 Network Information Parameters

Item	Description
Routing Information	Displays static routes for hosts and networks configured on the EdgeMarc. The system routing table contains routes for hosts and networks that are configured on the system. When the LAN and WAN settings have been fully configured, there must be four routing lines displayed: ■ Subnet associated with the LAN interface ■ Subnet associated with the WAN interface ■ Loopback interface ■ Network default gateway (most of the time directed to the WAN interface) The order of the lines may vary depending on the subnet masks. Additional lines may be displayed depending on the contents of the static routes entered in the Static Route page. Each of the entries on these pages creates an additional entry in the routing table. Go to **Network** > **Static Route** and refer to Configuring Static Routes.

Table 3-38 Network Information Parameters (continued)

Item	Description
Link Status	Displays status of the Ethernet interfaces. The status of the Ethernet connections is displayed by Link Status. Ethernet autonegotiation is often unreliable, especially between different vendors or old and new networking equipment. Occasionally autonegotiation fails, but this is generally not a cause for concern. However, if the negotiated rates change intermittently, or the link is reported as down or no link, the link rate may need to be set manually on the Switch Ports configuration page. Choose **Switch** from the Configuration Menu and refer to Configuring Switch Ports in Chapter 8, *Configuring Switch Settings*. Intermittent data, and voice outages may be caused by autonegotiation “flutter.” If the link rate is set manually, ensure that the device at the far end of the connection can communicate at the desired rate. Incompatible rates can cause a loss of communication with the system.
Interface Information	Displays status and configuration information for the system interfaces. You may need the interface eth0 MAC address to license the VoIP feature if the license information attached to the system is lost or is unreadable. Interface statistics can point to areas of congestion in the network. If the congestion is not corrected, the voice call quality is affected. Any errors should be examined and your network topology modified to better segment and isolate network traffic.

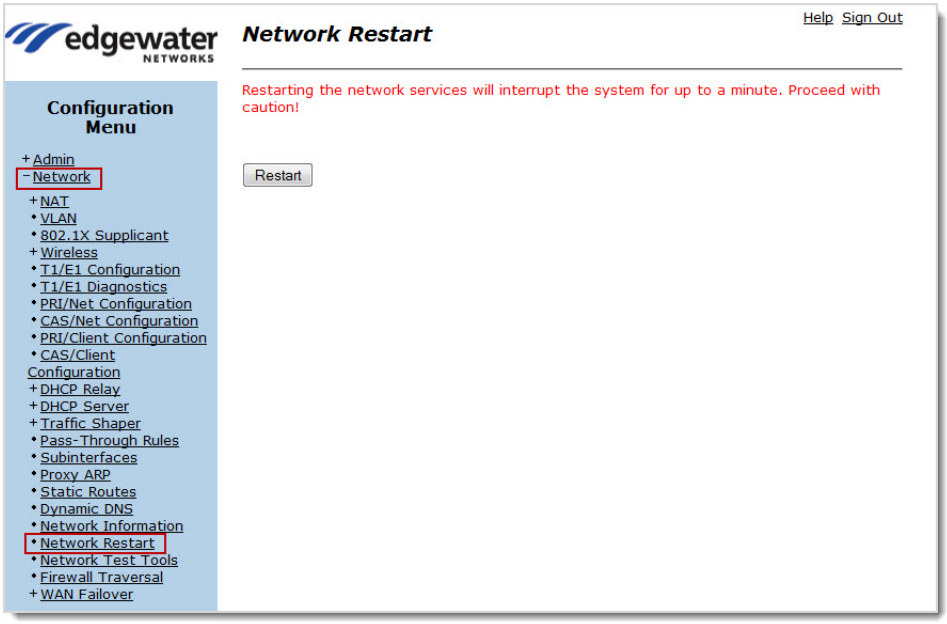
Initiating Network Restart

Use Network Restart to stop and the restart all networking services running on the system. Technical support may request that networking services be restarted during a troubleshooting session.

Caution
Restarting network services will interrupt the system for up to a minute. All voice, video and data sessions currently in progress will be interrupted! Proceed with caution!

1. Choose **Network** > **Network Restart** (Figure 3-53).

Figure 3-53 Network Restart Page



2. Click **Restart**.

   The following warning displays:

   WARNING: All voice and video services will be interrupted. Do you want to continue?

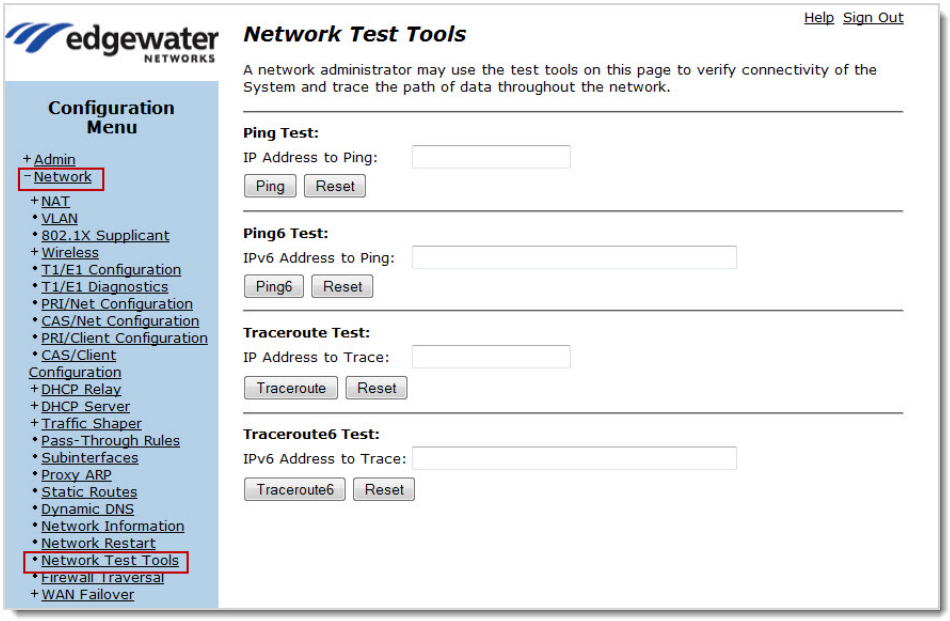
3. Click **OK** to confirm.

Using Network Test Tools

The Network Test Tools page verifies system connectivity and traces the data path throughout the network.

1. Choose **Network** > **Network Test Tools** (Figure 3-54).

Figure 3-54 Network Test Tools Page



2. Configure settings using the information in Table 3-39 as a guide.

Table 3-39 Network Test Tools

Item	Description
Ping Test **Ping6 Test**	See Performing a Ping Test.
IP Address to Ping	Specifies the destination IP address for the ping command.
IPv6 Address to Ping	The ping test is the most common test used to verify basic connectivity to a networking device. Successful ping test results indicate that both physical and virtual path connections exist between the system and the test IP address. Successful ping tests do not guarantee that all data message are allowed between the system and the test IP address.

Table 3-39 Network Test Tools (continued)

Item	Description
Traceroute Test	
See Performing a Traceroute Test.	
IP Address to Trace	Specifies the destination IP address for the traceroute command. The traceroute test is used to track the progress of a packet through the network. The test can be used to verify that data destined for a WAN device reaches the remote IP address via the desired path. Similarly, network paths internal to a company can be traced over the LAN to verify the local network topology. Enter the IP address (IPv4 addresses only) of the device to send a traceroute test to. Select Traceroute to execute the traceroute test. Select Reset to clear the IP address field so you can test a different path.
Interface	Choose the scope of the traceroute change.

3. Proceed to the following sections:
   - Performing a Ping Test
   - Performing a Traceroute Test

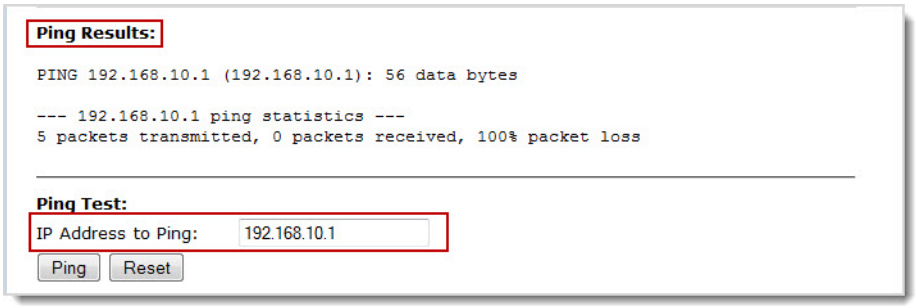
Performing a Ping Test

1. Choose **Network** > **Network Test Tools** (Figure 3-54).
2. Enter an IPv4 address in the **IP Address to Ping** field.
3. Click **Ping**.

   Or
4. Enter an IPv6 address in the **IPv6 Address to Ping** field.
5. Click **Ping6**.

   The Network Test Tools page reopens to display results of the ping test (Figure 3-55). This may take several seconds.

Figure 3-55 Network Test Tools - IPv4 Ping Test



6. Click **Reset** to clear the data or enter another IP address to ping.

Performing a Traceroute Test

1. Choose **Network** > **Network Test Tools** (Figure 3-54).
2. Enter an IPv4 address in the **IP address to Trace** field.
3. Click **Traceroute**.

   Or
4. Enter an IPv6 address in the **IPv6 Address to Trace** field.
5. Click **Traceroute6**.

   The Network Test Tools page reopens to display results of the test at the top of the Network Test Tools page. This may take several seconds.
6. Click **Reset** to clear the data or enter another IP address.

Configuring Firewall Traversal

Firewall Traversal allows you to set up a secure tunnel from a remote client to an external server. All traffic going through this tunnel is encrypted.

- Updating a Certificate
- Using the Firewall Traversal Page
- Configuring Internal Client Mode Settings
- Configuring External Server Mode Settings
- Configuring Remote Client Mode Settings

Updating a Certificate

There are a set of certificates pre-installed on the system to allow quick VoIP Traversal setup and testing. These certificates, however, are not secure for use in production; anyone with a system can connect using the pre-installed certificates. For production use, new certificates should be generated using the Certificate Store page.

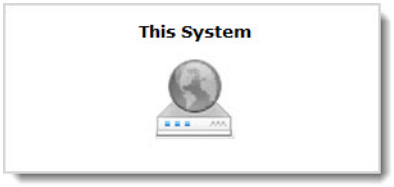
Before You Begin

Before configuring settings on the Firewall Traversal page, generate a new certificate. Choose **Security** from the Configuration Menu and refer to Managing Certificates in Chapter 5, *Configuring System Security*.

Current Status

The current status of the Firewall Traversal sub-system is displayed as a series of Firewall Traversal systems. The image with the text “This System” represents the status of the current system (Figure 3-56).

Figure 3-56 Current Status



By moving the mouse cursor over the image, you can see a more detailed description of the current status. If an error has occurred, the error message will be shown here.

Operating Mode

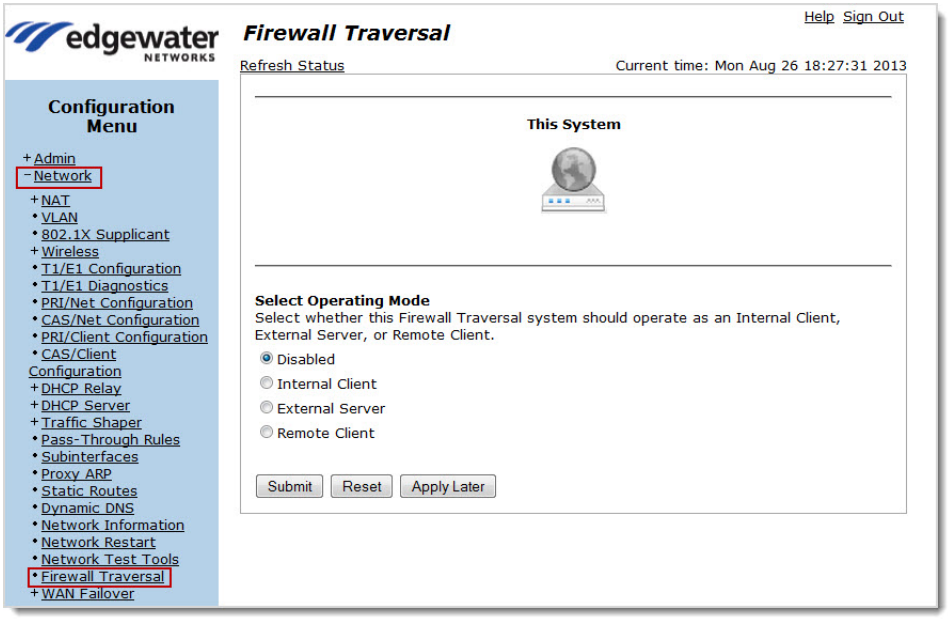
The operating mode determines the location of the system in a Firewall Traversal setup:

- Disabled
- Internal Client—Configuring Internal Client Mode Settings
- External Server—Configuring External Server Mode Settings
- Remote Client —Configuring Remote Client Mode Settings

Using the Firewall Traversal Page

1. Choose **Network** > **Firewall Traversal** (Figure 3-57).

Figure 3-57 Firewall Traversal Page



2. Configure settings using the information in Table 3-40 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-40 Firewall Traversal Parameters

Item	Description
This System	View a detailed description of current status. Move your mouse cursor over the “This System” image to see a detailed description of the current status. If an error has occurred, the error message will be shown here.
Select Operating Mode	In Select Operation Mode, choose an operating mode for the Traversal system by selecting a radio button:
Disabled	Disables firewall traversal (default).
Internal Client	Designates the system for use inside the site firewall. The Internal Client connects through the site firewall to the External Server. See Configuring Internal Client Mode Settings.

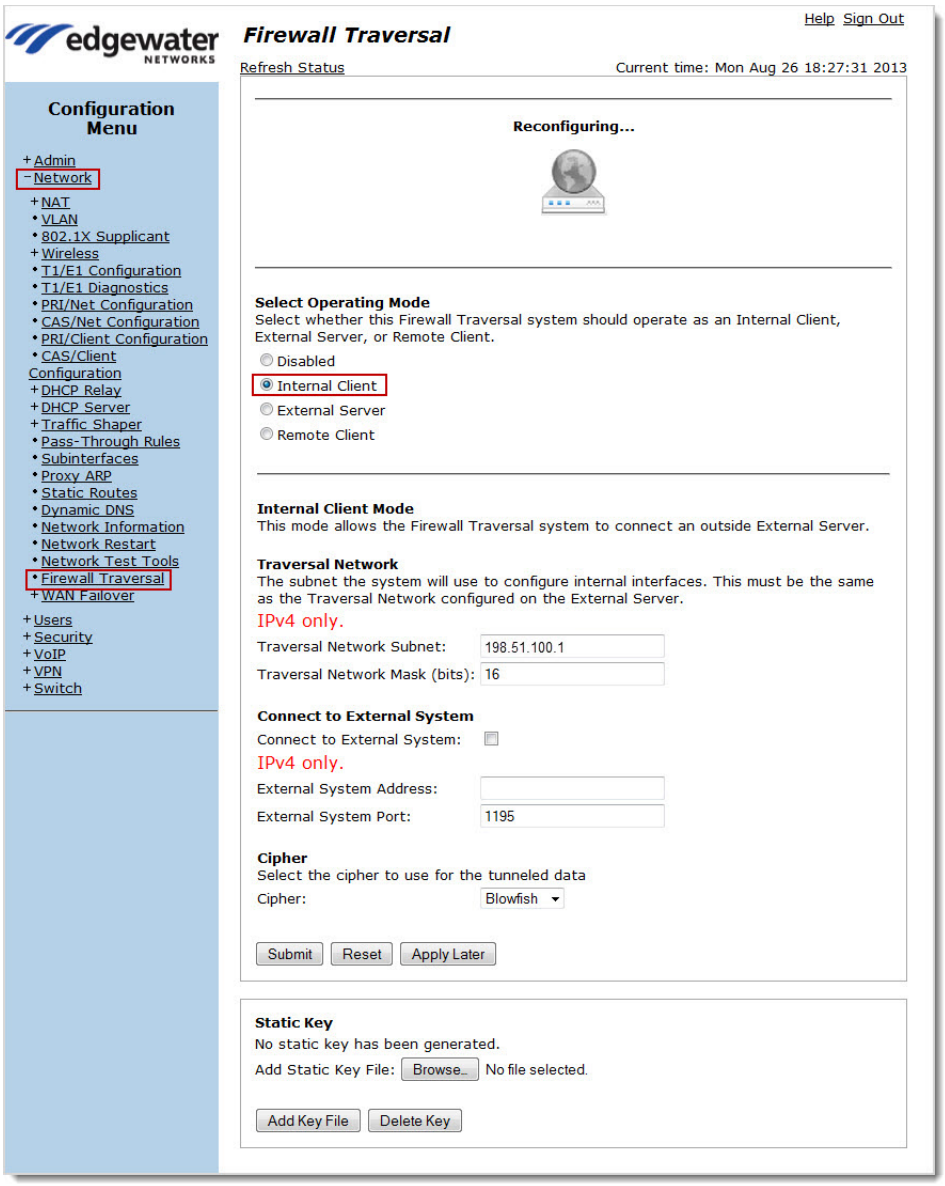
Table 3-40 Firewall Traversal Parameters (continued)

Item	Description
External Server	(Required) Designates is the server that all remote clients connect to. The server must be reachable from the public Internet and is typically set up outside the main site firewall or in parallel with it. The External Server can be connected to an Internal Client. If no Internal Client is used, the External Server must be able to route traffic to the internal network directly. If an Internal Client is used, the External Server routes traffic through a secure tunnel to the Internal Client which in turn sends the traffic to the internal systems. See Configuring External Server Mode Settings.
Remote Client	Connects from a satellite site to the External Server. This allows systems (such as Video Endpoints) to securely connect to other equipment at the main site. See Configuring Remote Client Mode Settings.

Configuring Internal Client Mode Settings

1. Choose **Network** > **Firewall Traversal** (Figure 3-58).
2. Select the **Internal Server** radio button to activate Internal Client Mode configuration fields (Figure 3-58).

Figure 3-58 Firewall Traversal - Internal Server Page



3. Configure settings using the information in Table 3-41 as a guide. Click **Submit** to save your settings.

Table 3-41 Firewall Traversal - Internal Server Parameters

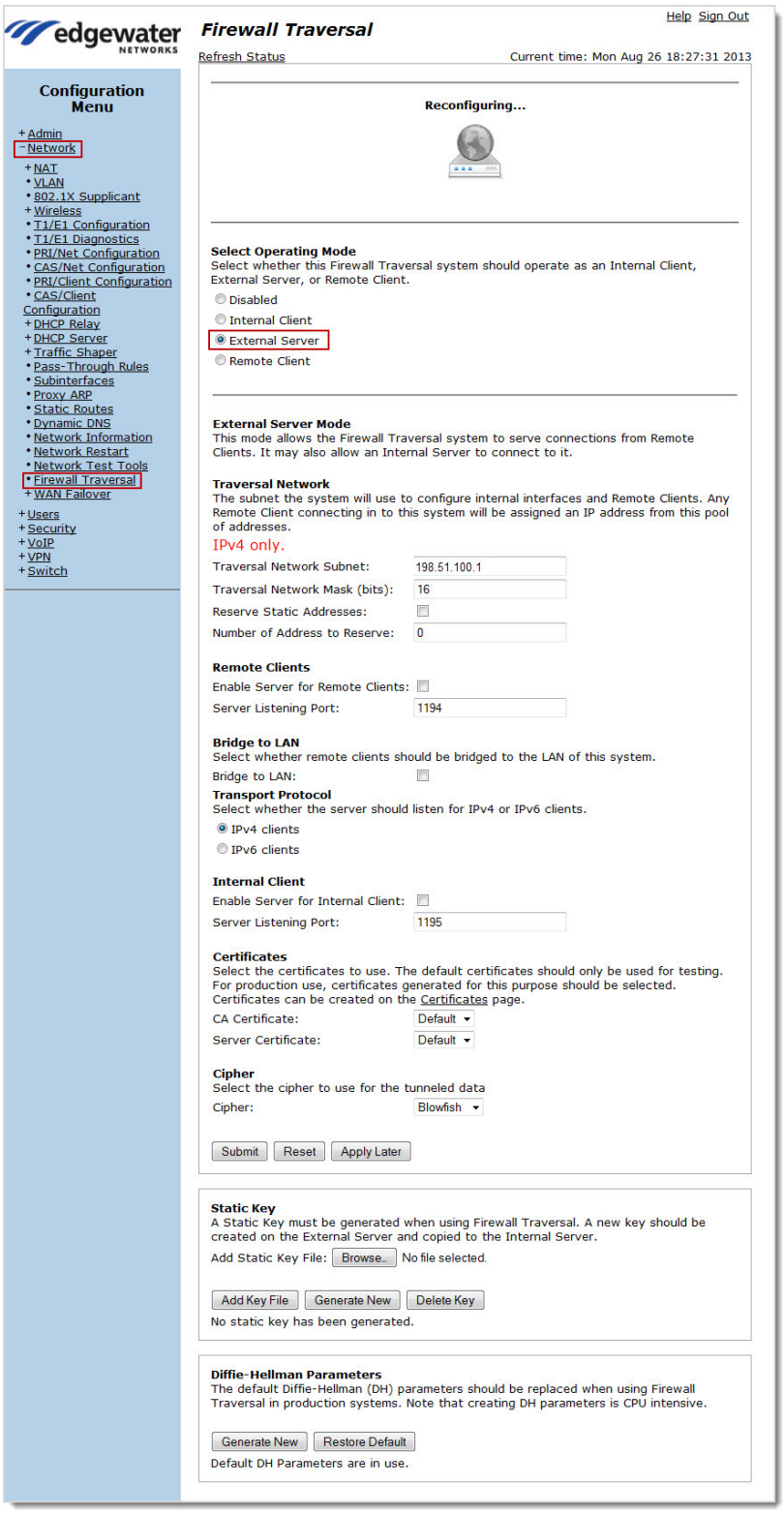
Item	Description
Traversal Network	
	Configures the subnet that the system uses to configure internal interfaces and Remote Clients. Any Remote Client connecting to this system is assigned an IP address from this pool of addresses.
Traversal Network Subnet	Enter the subnet IP address that the system uses to configure internal interfaces. This subnet must be the same as the Traversal Network configured on the External Server. See Configuring External Server Mode Settings.
Traversal Network Mask (bits)	Enter the number of bits for the subnet mask. The subnet must be large enough to support all clients connecting to the server.
Connect to External System	
Connect to External System	Select the **Connect to External System** checkbox.
External system Address	Enter the address of the external server to which you want to connect.
External system Port	Enter the external server port number.
Cipher	
	Selects the cipher to use for tunnel encryption. All systems connecting together must use the same cipher.
Cipher	Choose the cipher to use for encrypted tunneled data from the **Cipher** drop-down list. All systems connecting together must use the same cipher. ■ Blowfish—Security with less resource usage ■ AES-256—Higher security with higher resource usage
Static Key	
	Secures the tunnel from the Internal Client to the External Server; a Static Key is generated on the External Server and copied to the Internal Server. See Configuring the Static Key.

Configuring External Server Mode Settings

External Server Mode allows the Firewall Traversal system to serve connections from Remote Clients. It may also allow an Internal Server to connect to it.

1. Choose **Network** > **Firewall Traversal** (Figure 3-57).
2. Select the **External Server** radio button to activate External Client Mode configuration fields (Figure 3-59).

Figure 3-59 Firewall Traversal - External Server Page



3. Configure settings using the information in Table 3-42 as a guide. Click **Submit** to save your settings.

Table 3-42 Firewall Traversal - External Server Parameters

Item	Description
Traversal Network	
Configure the subnet that the system uses to configure internal interfaces and Remote Clients. Any Remote Client connecting to this system is assigned an IP address from this pool of addresses.	
Traversal Network Subnet	Enter the subnet IP address that the system uses for all clients connecting remotely. Each client connecting through the tunnel gets an IP address from this subnet. This subnet must be the same as the Traversal Network configured on the Internal Server. See Configuring Internal Client Mode Settings.
Traversal Network Mask (bits)	Enter the number of bits for the subnet mask. The subnet must be large enough to support all clients connecting to the server.
Reserve Static Addresses	Select the **Reserve Static Addresses** checkbox to reserve available static IP addresses for add-on hardware.
Number of Address to Reserve	Enter the number of addresses to reserve.
Remote Clients	
Enable Server for Remote Clients	Select the **Enable Server for Remote Clients** checkbox to allow remote clients to connect to this server.
Server Listening Port	Enter the port number to use when listening for client connections. Default is 1194.
Bridge to LAN	
Configures remote bridging to the system LAN.	
Bridge to LAN	Select the **Bridge to LAN** checkbox if you want the clients to be bridged to the protected LAN network. The clients are seen on the same Ethernet segment as the LAN network and get DHCP addresses served by a configured DHCP server on the segment. If the box is not checked, clients are routed to the internal LAN network or the Internal Client. Internal Client fields are disabled when the Bridge to LAN settings are enabled.

Table 3-42 Firewall Traversal - External Server Parameters (continued)

Item	Description
Transport Protocol	
Choose the **Transport Protocol** type by selecting either the **IPv4** or **IPv6** clients radio button:	
IPv4	Configures the server to listen for IPv4 clients.
IPv6	Configures the server to listen for IPv6 clients.
Internal Client	
If an internal client is configured, use this field to configure internal client server settings. If an Internal Client is not enabled, all traffic is routed to the directly attached internal network, or is bridged to the internal network if **Bridge to LAN** is enabled. Refer to Configuring Internal Client Mode Settings.	
Enable Server for Internal Client	Select the **Enable Server for Internal Client** checkbox to enable the Internal Client to connect to this server.
Server Listening Port	Enter the port number to which the Internal Client connects.
Certificates	
In the **Certificates** field, select the certificates to use for the Firewall Traversal server. The server and all clients must have certificates signed by the same Certificate Authority (CA) to be able to connect.	
Tip: To configure certificates, click the **Certificates** link provided or choose **Security** > **Certificates** and refer to Managing Certificates in Chapter 5, *Configuring System Security*.	
CA Certificate	Selects the CA Certificate to use for the server. Choose the Default certificate or a certificate created for this purpose.
Server Certificate	Selects the Server Certificate to use for the server. Choose the Default certificate or a certificate created for this purpose.
Cipher	
Choose the cipher to use for encrypted tunneled data from the **Cipher** drop-down list. All systems connecting together must use the same cipher.	
Cipher	Choose the tunnel encryption cipher: ■ Blowfish—Security with less resource usage ■ AES-256—Higher security with higher resource usage

Table 3-42 Firewall Traversal - External Server Parameters (continued)

Item	Description
Static Key	Secures the tunnel from the Internal Client to the External Server. A Static Key must be generated when using Firewall Traversal. The new is created on the External Server and copied to the Internal Server. See Configuring the Static Key.
Diffie-Hellman Parameters	Sets Diffie-Hellman (DH) parameters. Default DH parameters should be replaced when using Firewall Traversal in production systems. Creating DH parameters is CPU intensive. See Configuring Diffie-Hellman Parameters.

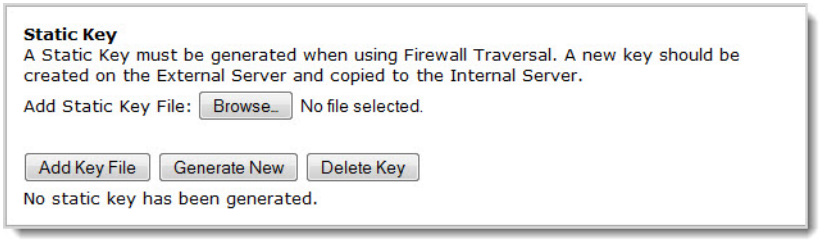
Configuring the Static Key

The Static Key secures the tunnel from the Internal Client to the External Server. The system comes with a default key, but to prevent attackers from connecting to your External Server, it is recommended that you create a new Static Key when setting up VoIP Traversal. A Static Key is generated on the External Server and copied to the Internal Server.

1. Choose **Network** > **Firewall Traversal** (Figure 3-57).
2. Select an operating mode:
   - Internal Client
   - External Server

   Configuration fields for the selected operating mode become active.
3. Scroll to **Static Key** (Figure 3-60).

Figure 3-60 Static Key Configuration



4. Add a static key file:
   - **Browse**—Locate a file key on your system. Or choose a file from the **Choose File** drop-down list and click **Add Key File**.
   - **Generate New** —Generates a new static key. The old static key is overwritten.
     - Click **Generate New**.

- Follow system prompts and return to the Firewall Traversal - External Server page.
- The system prompts you to download your new file key:

"The current static key was generated at Mon Aug 26 21:13:07 2013 (**Download key**)"

- Follow system prompts to open or save the generated key.

- Click **Restore Default**—Restores the default static key to the system.
- **Delete Key**—Deletes the static key on the system.

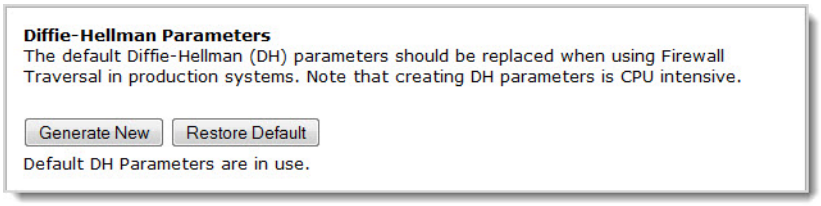
Configuring Diffie-Hellman Parameters

Diffie-Hellman (DH) Parameters are used for VoIP Traversal tunnels. The system comes with default DH parameters, but to prevent attackers from creating attacks specialized for the default DH parameters, it is recommended that you generate new DH parameters when setting up Firewall Traversal.

Note
Creating DH Parameters is CPU intensive and can take quite a long time. During creation, the system may be fully loaded for several minutes. It is therefore not recommended that you do this while the system is in service.

1. Choose **Network** > **Firewall Traversal** (Figure 3-57).
2. Select the **External Server** radio button to activate configuration fields (Figure 3-59).
3. Scroll to **Diffie-Hellman Parameters** (Figure 3-61).

Figure 3-61 Diffie-Hellman Configuration



4. Choose an action:
   - **Generate New**—Click to generate new DH Parameters. The old DH Parameters are overwritten. Once created, the DH Parameters do not need to be changed.

     The following message is displayed:

     "WARNING: Creating Diffie-Hellman Parameters requires a lot of CPU resources and should not be done while the system is in service. This will take quite some time."

     Click **OK** to accept.

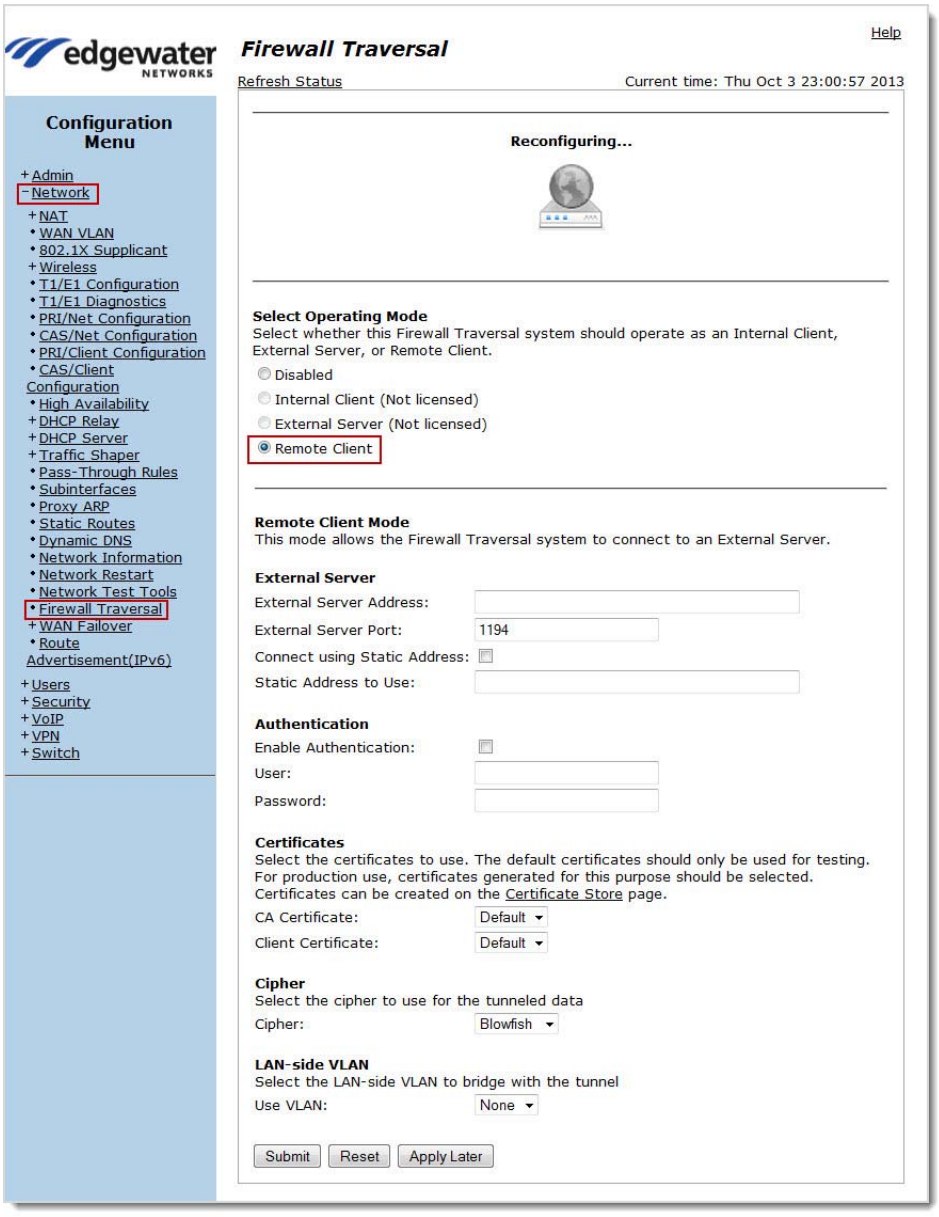
- **Restore Default**—This button restores the default DH Parameters to the system.

Configuring Remote Client Mode Settings

Remote Client Mode allows the Firewall Traversal system to connect to an External Server.

1. Choose **Network** > **Firewall Traversal** (Figure 3-57).
2. Select the **Remote Client** radio button to activate configuration fields (Figure 3-62).

Figure 3-62 VoIP Firewall Traversal - Remote Client Page



3. Configure settings using the information in Table 3-43 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-43 Firewall Traversal - External Server Parameters

Item	Description
External Server	
Configures external server settings.	
External Server Address	Enter the server IP address of the external server to which you want to connect.
External Server Port	Enter the external server port number to which you want to connect. Default is 1194.
Connect using Static Address	Select the **Connect Using Static Address** checkbox to use a static address.
Static Address to Use	Enter a static IP address.
Authentication	
Configures authentication settings.	
Enable Authentication	Select the **Enable Authentication** checkbox.
User	Enter the username for authentication.
Password	Enter a password for the authentication user.
Certificates	
Select the certificates to use for the VoIP Traversal server. The server and all clients must have certificates signed by the same Certificate Authority (CA) to be able to connect.	
To configure certificates, click the **Certificates** link provided or choose **Security** > **Certificates** and refer to Managing Certificates in Chapter 5, *Configuring System Security*.	
CA Certificate	Selects the CA Certificate to use for the server. Choose the Default certificate or a certificate created for this purpose.
Server Certificate	Selects the Server Certificate to use for the server. Choose the Default certificate or a certificate created for this purpose.
Cipher	
Selects the cipher to use for tunnel encryption. All systems connecting together must use the same cipher.	
Cipher	Enables the tunnel encryption cipher: ■ Blowfish—Security with less resource usage ■ AES-256—Higher security with higher resource usage

Table 3-43 Firewall Traversal - External Server Parameters (continued)

Item	Description
LAN-side VLAN	
If you have VLANs enabled, select the LAN-side VLAN to bridge with the tunnel from the **Use VLAN** drop-down list.	
Use VLAN	Choose a VLAN from the drop-down list.
Tip: For more information about tunneling, see Chapter 7, *Configuring VPN Settings*.	

Configuring WAN Failover

This section describes how to configure the EdgeMarc to support WAN failover (WAN Link Redundancy, or WLR) to ensure WAN link switchover if an active WAN link fails:

- Overview
- Configuring WAN Failover Settings
- Configuring WAN Failover Advanced Settings
- Configuring Secondary WAN Settings

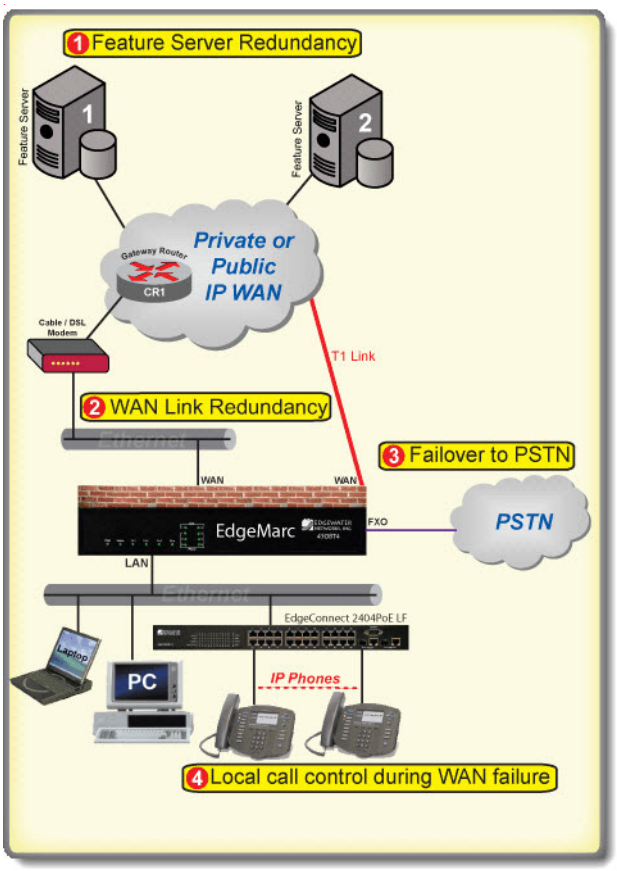
Note
Priority calling services cannot be configured when WAN Link Redundancy is enabled.

Overview

WAN failover relies on two separate physical routes to the WAN network, Primary and Secondary. If a communication failure is detected on the Primary route, the EdgeMarc switches to the secondary route, reducing the risk of the WAN link being the single point of failure. Figure 3-63 shows WLR configured with Survivability, which allows the EdgeMarc to provide robust and reliable voice services for Enterprise and Service Provider deployment.

For more information about Survivability, choose **VoIP** > **Survivability** and refer to Configuring Survivability in Chapter 6, *Configuring VoIP Settings*.

Figure 3-63 WAN Failover with Survivability



Automatic WLR Switchover

Revertive behavior instructs the data or voice interface to revert based on configured priority values. If Revertive mode has been turned on for WLR, the module invokes a switchover as soon as the default data interface (Primary) or configured voice interface (Primary/Secondary) is marked operationally up. This takes into account both IOCTL-based as well ping-based polling mechanisms in addition to the usual active Link failure-related switchover.

Supported WLR Interfaces

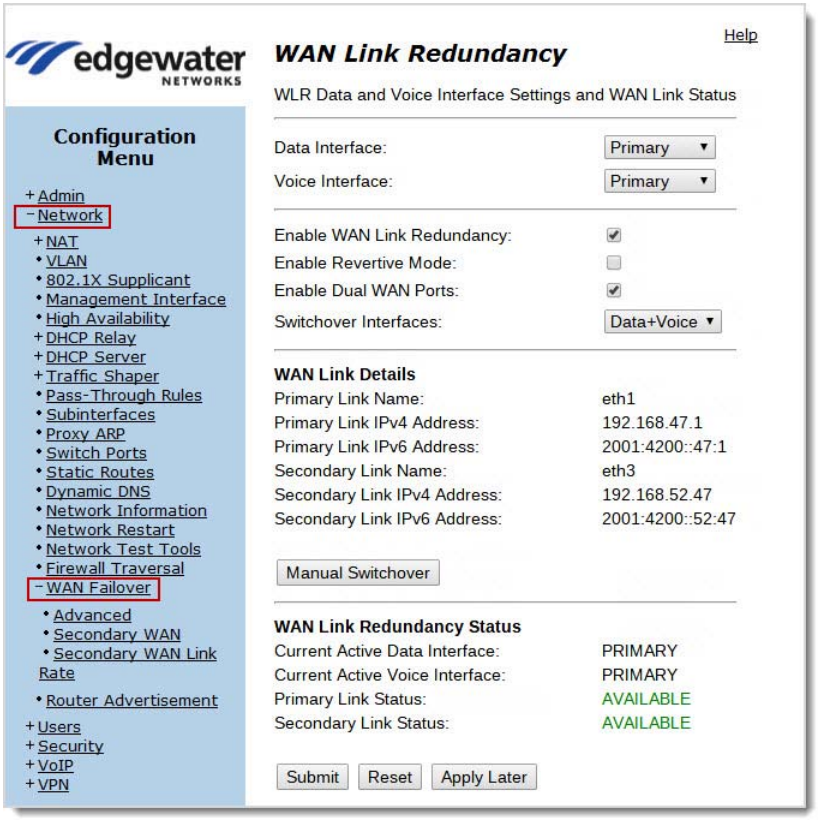
WAN Link Redundancy can be implemented using two different physical interfaces on the same EdgeMarc (for example, T1 interface and Ethernet) or one physical interface with two gateways to the WAN via an intermediate LAN. Any interface or gateway can either be primary or secondary.

See Configuring Dual WAN Ports.

Configuring WAN Failover Settings

1. Choose **Network** > **WAN Failover** (Figure 3-64).

Figure 3-64 WAN Link Redundancy Configuration Page



2. Configure settings using the information in Table 3-44 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-44 WAN Link Redundancy Parameters

Item	Description
Data Interface	Choose an option from the **Data Interface** drop-down list: ■ Primary ■ Secondary Designate either the Primary or Secondary interface as the active interface for data. You can assign the same interface link type for both data and voice or choose different interface types for load balancing data and voice traffic across multiple links. By default, the data and voice interfaces are assigned to the Primary link.
Voice Interface	Choose an option from the **Voice Interface** drop-down list: ■ Primary ■ Secondary Designate either the Primary or Secondary interface as the active interface for voice. You can assign the same interface link type for both data and voice or choose different interface types for load balancing data and voice traffic across multiple links. By default, the data and voice interfaces are assigned to the Primary link.
Enable WAN Link Redundancy	Select the checkbox to enable WAN Link Redundancy. WLR is disabled if the check box is cleared. **Note:** Priority calling services cannot be configured when WAN Link Redundancy is enabled. When you click **Submit**, the Manual Switchover button and WAN Link Redundancy Status field become active.
Enable Revertive Mode	Select the checkbox to activate automatic switchback between Primary and Secondary interfaces. Un-check the box to disable. (Optional) Non-revertive switchover for the Primary interface. If the Secondary interface is functioning as the active interface and the Primary interface becomes available, the system continues to use the Secondary interface and no switchover occurs.

Table 3-44 WAN Link Redundancy Parameters (continued)

Item	Description
Enable Dual WAN Ports	For the EdgeMarc 4750 and 7300 Series. Select the checkbox to enable the second Ethernet WAN port (Port 4) for dual WAN support: ■ EdgeMarc 7300, EdgeMarc 7301: eth3 When enabled, two devices configured for Ethernet DHCP can be used as the Primary/Secondary WAN. See Configuring Dual WAN Ports.
Switchover Interfaces	Applies WLR to specified interfaces: ■ Data+Voice—Default ■ Data Only—Only the data interface switches over between the Primary and Secondary links, while the voice interface is fixed to its configured link. ■ Voice Only
WAN Link Details	
Displays Primary and Secondary interface names and IP addresses: ■ Primary Link Name ■ Primary Link IPv4 Address ■ Primary Link IPv6 Address ■ Secondary Link Name ■ Secondary Link IPv4 Address ■ Secondary Link IPv6 Address	
Manual Switchover	Switches voice and data services from their currently active interfaces to their inactive interfaces when revertive mode is disabled. This results in a network restart. **Note:** Manual Switchover is only available when the system is configured in non-revertive mode. If the Secondary interface is functioning as the active interface, and the Primary interface becomes available, the system automatically switches back to the Primary interface as the active interface (making the Secondary interface inactive). For more information about restarting the network, choose **Network** > **Network Restart** and refer to Initiating Network Restart.

Table 3-44 WAN Link Redundancy Parameters (continued)

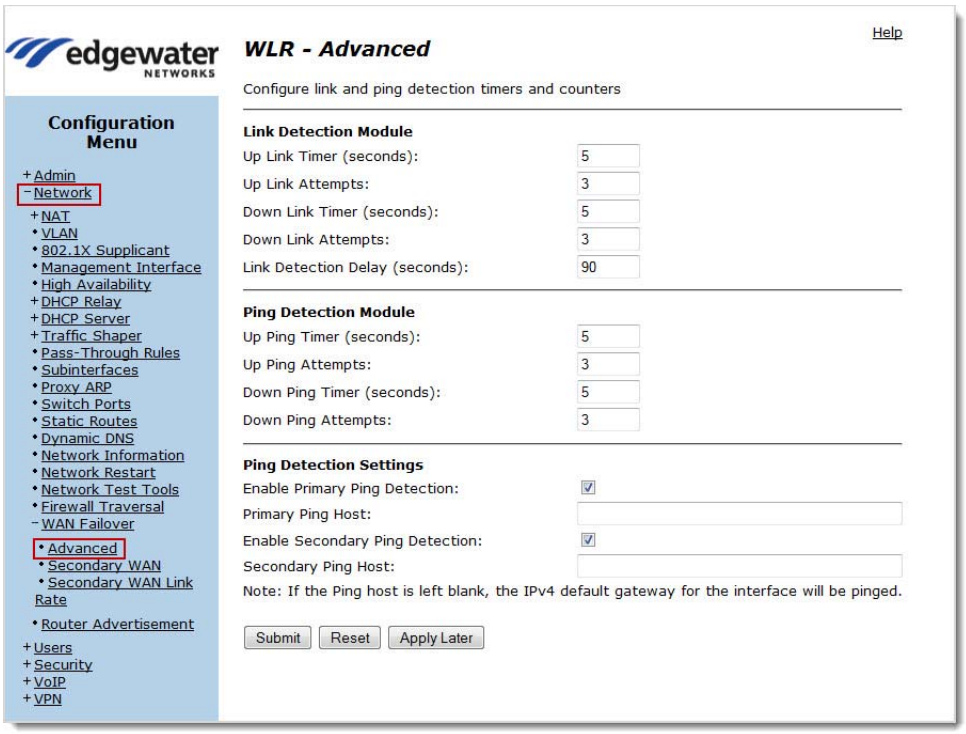
Item	Description
WAN Failover Status	Shows currently active voice and data information and describes whether the Primary and Secondary interfaces are up or down. The status is only visible when the WAN failover feature is enabled on the system. The status is displayed on the basis of link detection via IOCTL and the optional ping link detection mechanism: ■ Current Active Data Interface—Primary or Secondary ■ Current Active Voice Interface—Primary or Secondary ■ Primary Link Status—Available or Unavailable ■ Secondary Link Status—Available or Unavailable

Configuring WAN Failover Advanced Settings

Use the WLR - Advanced page to configure Layer 1 link detection and Layer 3 ping detection to determine the availability of a WAN link. Each method has configurable up and down interval times between keepalive attempts and the number of attempts before a link is considered available or unavailable.

1. Choose **Network** > **WAN Failover** > **Advanced** (Figure 3-65).

Figure 3-65 WLR - Advanced Configuration Page



2. Configure settings using the information in Table 3-45 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-45 WLR - Advanced Configuration Parameters

Item	Description
Link Detection Module	
Configure Link Detection Module settings:	
Up Link Timer (seconds)	Enter the number of seconds between keepalive attempts when determining if a link is back up or leave the default value.
Up Link Attempts	Enter the number of consecutive successful keepalive attempts before a WAN link is considered back up or leave the default value
Down Link Timer (seconds)	Enter the number of seconds between keepalive attempts when determining if a link has gone down or leave the default value.
Down Link Attempts	Enter the number of consecutive failed keepalive attempts before a WAN link is considered down or leave the default value.
Link Detection Delay	Specifies the number of seconds to wait before making switchover decisions when the link first comes up. There are certain WAN types whose Data Link Layer takes time to establish. These types include Frame Relay over T1. If the time to establish exceeds the Link and Ping Detection Down timers, WLR considers the WAN link unavailable and switches over to the backup link. If revertive mode is disabled and the link becomes available soon after, WLR will not assign it as the active link. This parameter can be tuned so that WLR waits for the link to come up before marking an interface as down and switching over to another link. This delay occurs as the system starts up or after a switchover, when the module restarts. This should not affect switchover time under working conditions. Link Detection Delay only applies to non-PPP Frame Relay WAN types. It should be set to the maximum acceptable time for a Frame Relay link to establish. Range is 1 to 180 seconds. Default is 90 seconds.
Ping Detection Module	
Configure Ping Detection Module settings:	
Up Ping Timer	Enter the time interval in seconds before the module sends an Internet Control Message Protocol (ICMP) echo request packet on a physically up link to the Ping Host.

Item	Description
Up Ping Attempts	Enter the number consecutive responses for ICMP requests from the Ping Host on a previously down link before the link can be declared as up.
Down Ping Timer	Enter the time interval in seconds before the module sends an ICMP request on a down link with physically up interface.
Down Ping Attempts	Enter the number of consecutive ICMP requests with no responses from the Ping Host on a physically up interface with a previously up link status.

Ping Detection Settings

Configure Ping Detection Settings:

Enable Primary Ping Detection	Select the **Enable Primary Ping Detection** checkbox to activate the layer 3 ICMP-based ping detection mechanism. WLR will send periodic keepalive pings to the configured host to monitor the status of the WAN Link.
Primary Ping Host	Enter the host IP to periodically send keepalive pings to. If unspecified, the default gateway becomes the ping host by default. If the Ping host is left blank, the IPv4 default gateway for the interface will be pinged.
Enable Secondary Ping Detection	Select the **Enable Secondary Ping Detection** checkbox to enable a secondary ping detection mechanism for WLR to send periodic keepalive pings.
Secondary Ping Host	Enter the secondary host to periodically send keepalive pings to.

Configuring Secondary WAN Settings

WAN failover enables the system to be configured with two WAN interfaces simultaneously: one as Primary and the other as Secondary. The following Primary/Secondary interfaces combinations are supported:

Two Physical Devices

- Ethernet Static IP and T1/ADSL
- Ethernet DHCP and T1/ADSL
- Ethernet PPPoE and T1/ADSL
- Ethernet DHCP and Ethernet DHCP—Available only when Dual WAN Ports is enabled.

Two Networks Over a Single Ethernet Device

- Ethernet Static IP and Ethernet Static IP
- Ethernet Static IP and Ethernet DHCP
- Ethernet Static IP and Ethernet PPPoE

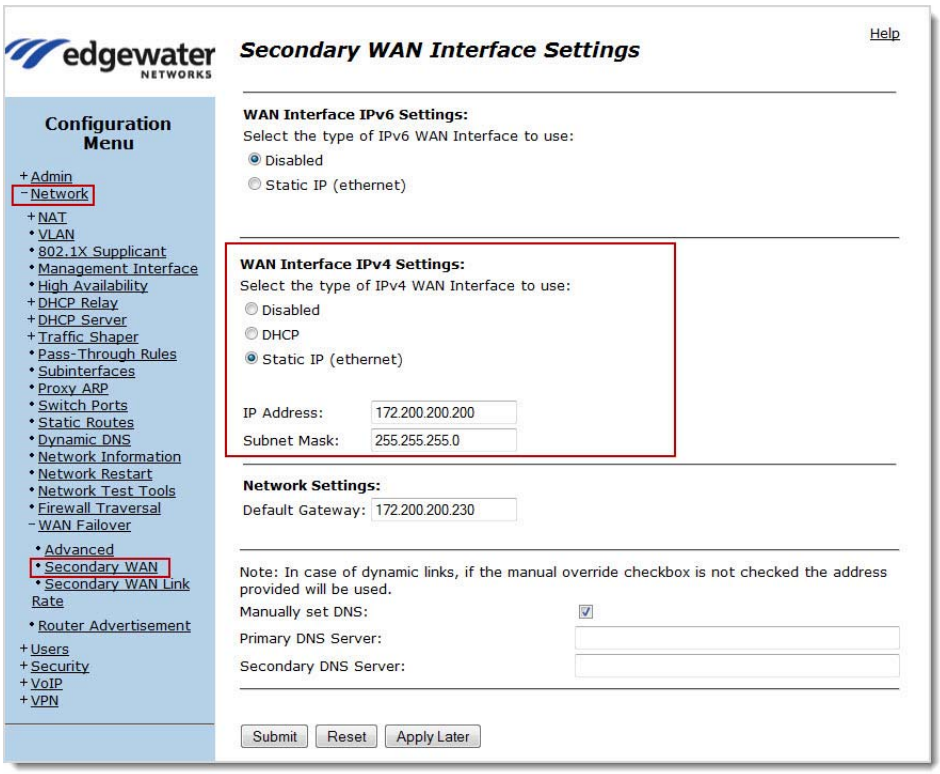
To exclude an interface from Primary/Secondary combination, select the default system configuration for that interface:

- Interface Type—Ethernet-Static IP
- IP Address—<empty>

To configure Secondary WAN interface settings:

1. Choose **Network** > **WAN Failover** > **Secondary WAN Config** (Figure 3-66).

Figure 3-66 Secondary WAN Interface Settings Page



2. Configure settings using the information in Table 3-46 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-46 Secondary WAN Interface Settings

Item	Description
WAN Interface IPv6 Settings	

Selects the type of IPv6 WAN interface to use to connect to the Internet.
■ Disabled—Secondary WAN interface settings are disabled (default).
■ Static IP—Configures the Secondary WAN interface with a static IP address:
  ■ IPv6 Address/Prefix
  ■ IPv6 Default Gateway	

WAN Interface IPv4 Settings	

Selects the type of IPv4 WAN interface to use to connect to the Internet. See Configuring WAN Interface IPv4 Settings for configuration information.
■ **ADSL**—Configures the integrated ADSL modem (available only on certain models):
  ■ ADSL-PPPoE
  ■ ADSL-PPPoATM—Only on ADSL WAN based models.
See IPv4 ADSL for configuration information.
■ **DHCP**—Configures the device to obtain the WAN-side IP address using a DHCP server available from the WAN side of the network. See IPv4 DHCP for configuration information.
■ **Static IP Address**—Configures the WAN interface with a static IP address (default). See IPv4 Static IP for configuration information.
■ **VLAN**—Selects the VLAN defined in Configuring WAN Interface Settings. See IPv4 VLAN for configuration information.
■ **T1/E1**—Configures the WAN interface with a static IP address and tests the T1/E1 interface on the system using the T1/E1 Configuration page. T1/E1 configuration options are only available on certain models. See IPv4 T1/E1 and Configuring T1/E1 Settings for configuration information.	

IP Address	Manually assigns an IP address.
Subnet Mask	Manually assigns a subnet mask. Default is 255.255.255.0.
Network Settings	
See Configuring Secondary WAN Network Settings.	
Default Gateway	Specifies the default gateway. This gateway is on the same IP subnet as the IP address.
Primary DNS	Specifies the primary DNS server supplied by the ISP.

Table 3-46 Secondary WAN Interface Settings

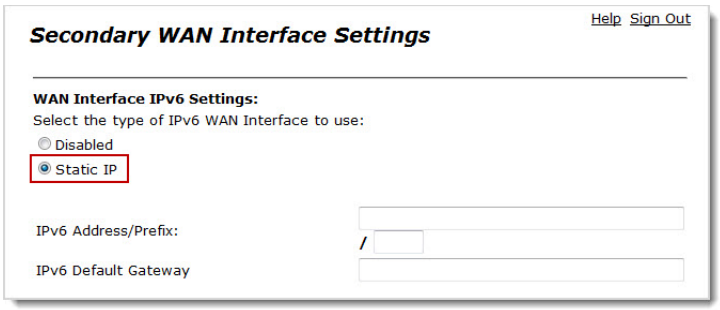
Item	Description
Secondary DNS	Specifies the Secondary DNS server supplied by the ISP. Used if the Primary server is unavailable.
Secondary WAN Redundancy Settings	
Enable Ping based status detection	Enables ping-based link detection for the Primary interface if WLR is enabled. The system periodically sends pings to the specified host to monitor the status of the Primary interface. If no response is received, the link is declared down.
Ping Host	Specifies the ping host. If Ping Based Status Detection is enabled, pings are periodically sent to the ping host specified in this field. If no ping host is specified, pings are sent to the Primary Default Gateway.

3. Proceed to the following sections:
   - Configuring Secondary WAN Interface IPv6 Settings
   - Configuring Secondary WAN Interface IPv4 Settings
   - Configuring Secondary WAN Network Settings
   - Configuring Dual WAN Ports

Configuring Secondary WAN Interface IPv6 Settings

1. Choose **Network** > **WAN Failover** > **Secondary WAN Interface Settings** (Figure 3-66).
2. In **WAN Interface IPv6 Settings**, click the **Static IP** radio button. The WAN IPv6 fields become active (Figure 3-67).

Figure 3-67 Secondary WAN Interface IPv6 Fields

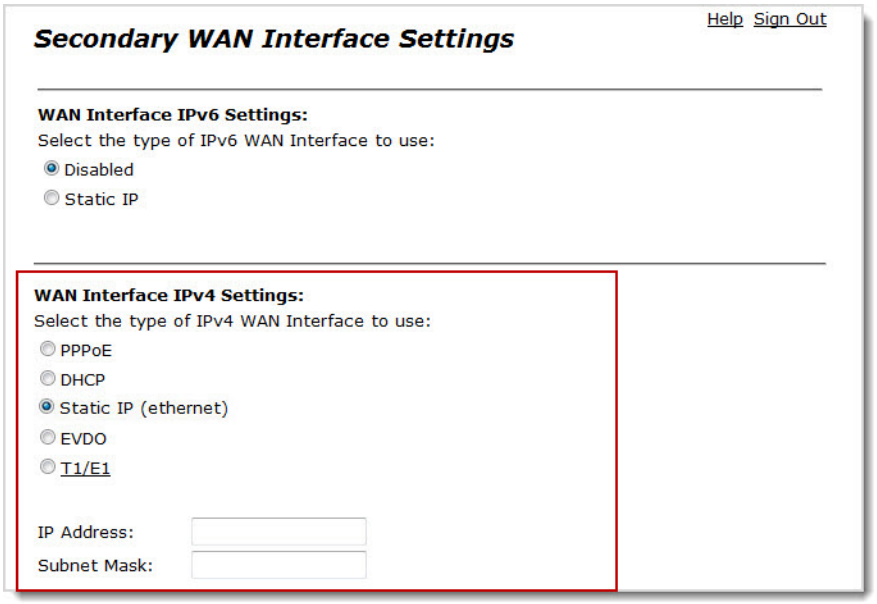


3. In the **IPv6 Address/Prefix** field, enter the IPv6 address and prefix.
4. In the **IPv6 Default Gateway** field, enter the IPv6 default gateway.
5. Click **Submit** to save your settings.

Configuring Secondary WAN Interface IPv4 Settings

1. Choose **Network** > **WAN Failover** > **Secondary WAN Interface Settings** (Figure 3-66).
2. Scroll to **WAN Interface IPv4 Settings** (Figure 3-68) and refer to Configuring WAN Interface IPv4 Settings for configuration information.

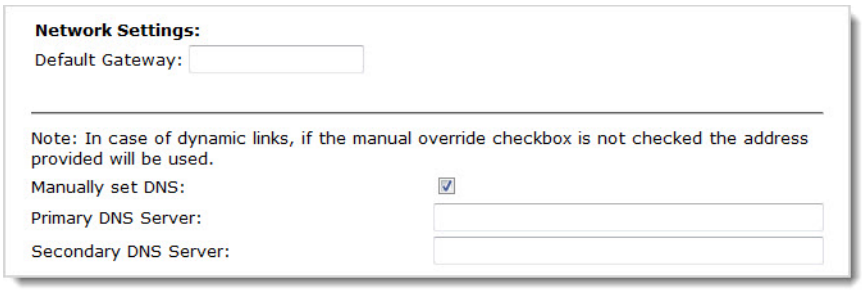
Figure 3-68 Secondary WAN Interface IPv4 Fields



Configuring Secondary WAN Network Settings

1. Choose **Network** > **WAN Failover** > **Secondary WAN Interface Settings** (Figure 3-66).
2. Scroll to **Network Settings** (Figure 3-69) and refer to the following sections for configuration information:
   - Configuring Network Default Gateway Settings
   - Configuring DNS Servers

Figure 3-69 Secondary WAN Interface Network Settings Fields



Configuring Dual WAN Ports

For the EdgeMarc 4750, EdgeMarc 7300, and EdgeMarc 7301.

Select the checkbox to enable the second Ethernet WAN port for dual WAN support:

- EdgeMarc 4750: eth1
- EdgeMarc 7300, EdgeMarc 7301: eth3

When enabled, two devices configured for Ethernet DHCP can be used as the Primary/Secondary WAN. Traffic Shaper is configured on the Secondary WAN Ethernet.

When Data and Voice are set for the Primary/Secondary WAN interfaces, the WLR daemon monitors the active WAN link interface, using link detection or ping detection. When the active WAN link loses connectivity, the WLR daemon switches services to the backup WAN link

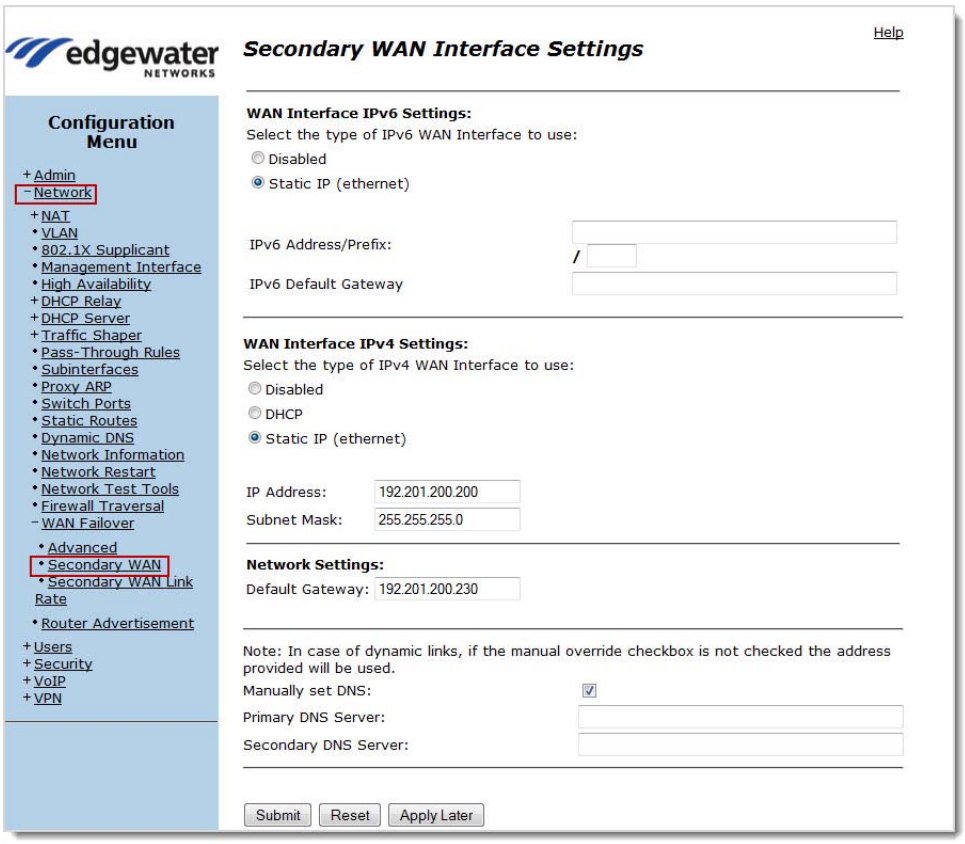
When Revertive mode is set, the WLR daemon monitors both the Primary and Secondary interfaces. When the default interface comes back up, the WLR daemon switches services back to the main/default WAN link.

To configure Dual WAN Ports:

1. Choose **Network** > **WAN Failover**. The WAN Link Redundancy page displays (Figure 3-64).
2. Select the **Enable WAN Link Redundancy** checkbox.
3. Select the **Dual WAN Ports** checkbox.
4. Click **Submit**.

   The system displays eth1 and its IP information in WAN Link Details on the WAN Link Redundancy page. Now you can configure the Secondary interface.
5. Choose **Network** > **WAN Failover** > **Secondary WAN Interface Settings** (Figure 3-70).

Figure 3-70 Dual WAN Ports - Secondary WAN Settings



6. Select **Static IP** to configure the WAN interface manually:
   a. Enter an IP Address.
   b. Enter the Subnet Mask (default is 255.255.255.0).
   c. Enter the Default Gateway and DNS addresses.
   d. Click **Submit**.
7. Choose **Network** > **WAN Failover**. Information for eth1 as well as eth3 are displayed in WAN Link Details.
8. Choose from the drop-down list whether Data and Voice should be on the Primary or Secondary interface.
9. Choose from the drop-down list whether Data or Voice or both should be switched if the Active Interface goes down.
10. Click **Submit** to save your settings.
11. To test your configuration, click **Manual Switchover**. This switches the data and/or voice interfaces from one link to the other.

Managing the Secondary WAN Link Rate

The Secondary WAN Link Rate page displays the current Secondary WAN Ethernet interface link settings for the system. If needed, the rate for each interface can be set manually to establish a reliable connection. The MTU size of the WAN interface can be adjusted to reduce the effects of large data packets on media data.

Before You Begin

You must first enable Dual WAN Ports to use the Secondary WAN Link Rate page. The following message prompts you to enable Dual WAN Ports:

> You cannot configure Secondary Interface Link Rate because Dual WAN Ports are not enabled. To enable Dual Wan Ports, click **here**.

1. Click the link provided.

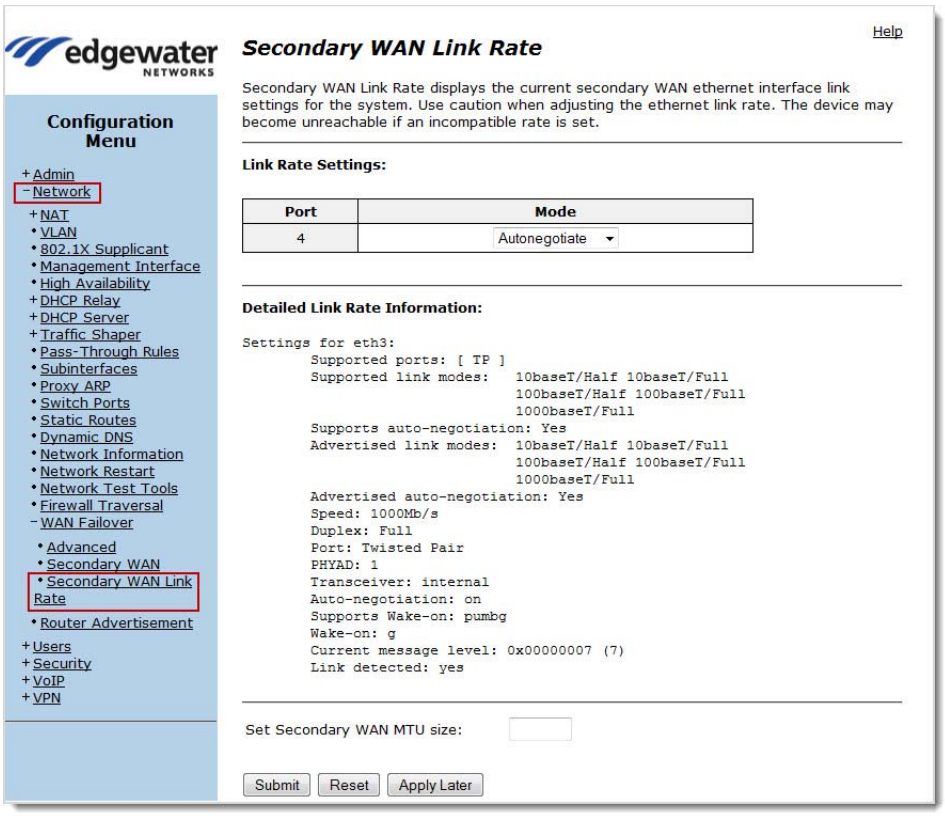
   Or

2. Choose **Network** > **WAN Failover** (Figure 3-64).
3. Select the **Enable Dual WAN Ports** checkbox and click **Submit**.
4. Proceed to Manage Secondary WAN Link Rate Settings.

Manage Secondary WAN Link Rate Settings

1. Choose **Network** > **WAN Failover** > **Secondary WAN Link Rate** (Figure 3-71).

Figure 3-71 Secondary WAN Link Rate Page



2. Manage settings using the information in Table 3-47 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-47 Secondary WAN Link Rate Parameters

Item	Description
Link Rate Settings	Displays the current settings for the Secondary WAN interface. The default setting is auto-negotiate. **Port** Displays the ports configured on the system. Port 4 supports a Secondary WAN. See Configuring Dual WAN Ports for more information. **Mode** Choose an negotiation mode from the drop-down list. The link rate of an interface can be set to static values, it is recommended to statically set the values on both, the system and devices connecting to any port when applicable. When connecting a device to the system that cannot be hard coded, leave these ports on the system set to auto-negotiate.
Detailed Link Rate Information	Ethernet auto-negotiation is often unreliable, especially between different vendors or old and new networking equipment. Failure of auto-negotiation is generally not a cause for concern. However, if the negotiated rates change intermittently or the link is reported as no link or down, the link rate may need to be set manually. Both side of the link MUST be set to the same rate. Inconsistent rates may cause “flutter,” leading to intermittent voice outages.
Set Secondary WAN MTU size	Enter a secondary WAN MTU size to reduce the latency that is introduced when large data packets are sent over a slow link. If left blank, the system determines the most optimal MTU size based on WAN settings. **Note:** This option is not available on all platforms. The default setting is 1500 bytes for static IP addresses. PPPoE links negotiate the value automatically although the value can be overridden using this field. This only applies if the WAN interface has an IPv4 address assigned. When the link rate is set manually, ensure that the device at the far end of the connection can communicate at the desired rate. Incompatible rates can cause a loss of communication with the system.

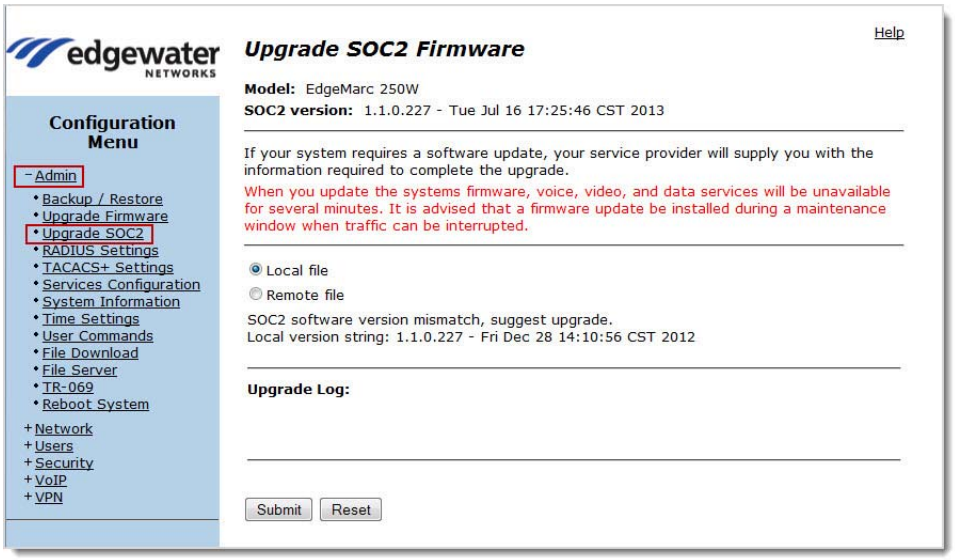
Configuring SOC2 IP Settings

The EdgeMarc 250 DSP runs on SOC2, which communicates to the controller host (SOC1) via a private IP network. This network is a /30 subnet and only has two hosts (the DSP and controller-host) as part of this private network. By default, no configuration is needed, as default addresses Controller-Host (10.199.200.2) and DSP (10.199.200.1) are used on the 10.199.200.1/30 network. If these addresses conflict with any existing network on your device, your configurations can be changed after first consulting Edgewater support to avoid any disruption in service.

Warning
Do not change the IP address on the SOC2 (DSP) unless specified by Edgewater Networks personnel. Changing it to an IP within your network will cause issues and stop network traffic.

1. Choose **Network** > **SOC2 IP Configuration** (Figure 3-72).

Figure 3-72 SOC2 IP Settings Page



2. In the **SOC2(DSP) IP Address** field, enter a new SOC2 IP address.

   This defines a DSP address in a /30 subnet. The System automatically calculates the peer controller-host IP in that subnet. Once configuration is applied, a new addresses is shown as the current configuration.

3. Click **Submit** to save all settings on the page.

Where to Go Next

See Upgrading SOC2 Firmware in Chapter 2, *System Administration*.

Configuring Router Advertisement (IPv6)

The Router Advertisement (RA) Server configuration page manages Neighbor Discovery Protocol (NDP) information exchange. Routers that are active on the link respond by sending a Router Advertisement with their address to all nodes on the group. Router advertisements provide the hosts a path out of the local link and other information necessary for NDP operation.

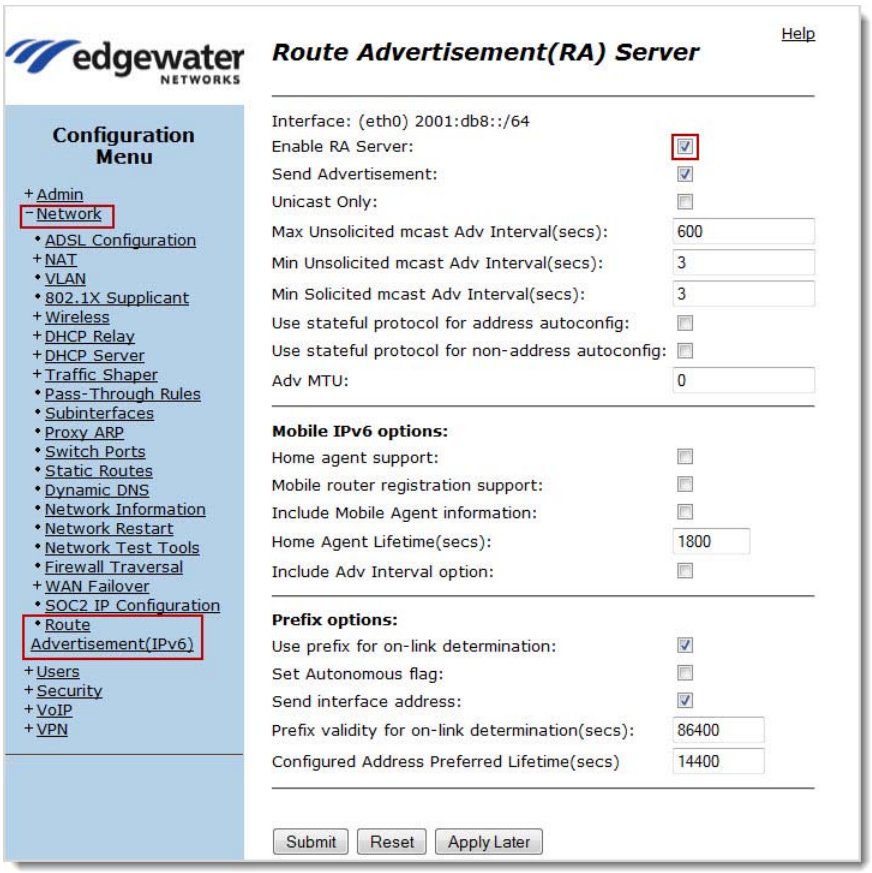
Before You Begin

To configure Router Advertisement settings, you must first configure IPv6 on your LAN/LAN VLAN interfaces. Choose **Network** from the Configuration Menu and refer to Using the Network Page.

To configure router advertisement:

1. Choose **Network** > **Router Advertisement (IPv6)** (Figure 3-73).

Figure 3-73 Router Advertisement Configuration Page



2. Configure settings using the information in Table 3-48 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 3-48 Router Advertisement Server Parameters

Item	Description
Interface	Displays the IPv6 interface for which options are being configured.
Enable RA Server	Select the **Enable RA Server** checkbox to enable RA services for the IPv6 interface.
Send Advertisement	Select the **Send Advertisement** checkbox to designate whether the router should send periodic router advertisements and responses to router solicitations.

Table 3-48 Router Advertisement Server Parameters (continued)

Item	Description
Unicast Only	Select the **Unicast Only** checkbox to designate whether interface link type only supports unicast. This prevents unsolicited advertisements from being sent and causes solicited advertisements to be unicast to the soliciting node. This option is necessary for non-broadcast, multiple-access links such as the IPv6 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP).
Max Unsolicited mcast Adv Interval (secs)	Enter the maximum time allowed between sending unsolicited multicast router advertisements from the interface. Range is 4 to 1800 seconds.
Min Unsolicited mcast Adv Interval (secs)	Enter the minimum time allowed between sending unsolicited multicast router advertisements from the interface. Range is 3 to (0.75 * Max Unsolicited mcast Adv Interval) seconds.
Min Solicited mcast Adv Interval (secs)	Enter the minimum time allowed between sending multicast router advertisements from the interface.
Use stateful protocol for address autoconfig	Select the **Use stateful protocol for address autoconfig** checkbox to use the administered (stateful) protocol for address autoconfiguration and any addresses autoconfigured using stateless address autoconfiguration.
Use stateful protocol for non-address autoconfig	Select the **Use stateful protocol for non-address autoconfig** checkbox to use the administered (stateful) protocol for autoconfiguration of other (non-address) information.
Adv MTU	Enter a value to insure that all nodes on a link use the same MTU value in those cases where the link MTU is not well known. Range is 1280 to 1500. A value of 0 indicates not to send an MTU value in router advertisement messages.
Mobile IPv6 Options	
Configure Mobile IPv6 options:	
Home agent support	Select the **Home agent support** checkbox to indicate that the sending router is able to serve as Mobile IPv6 Home Agent. Minimum and maximum limits for the router advertisement interval are specified by your Mobile IPv6 settings.

Table 3-48 Router Advertisement Server Parameters (continued)

Item	Description
Mobile router registration support	Select the **Mobile router registration support** checkbox to indicate that the Home Agent signals it supports Mobile Router registrations. You must also select the **Include Mobile Agent information** checkbox.
Include Mobile Agent information	Select the **Include Mobile Agent information** checkbox to indicate that the Home Agent Information Option (specified by Mobile IPv6) is included in Router Advertisements. You must also select the **Home agent support checkbox**.
Home Agent Lifetime (secs)	Enter the length of time in seconds (relative to the time the packet is sent) that the router is offering Mobile IPv6 Home Agent services. The maximum lifetime is 65520 seconds (18.2 hours). The value 0 is not used.
Include Adv Interval option	Select the **Include Adv Interval option** checkbox to indicate that Advertisement Interval Option (specified by Mobile IPv6) is included in router advertisements.
Prefix Options	
Configure Prefix Options:	
Use prefix for on-link determination	Select the **Use prefix for on-link determination** checkbox to indicate that this prefix can be used for on-link determination. When not set the advertisement makes no statement about on-link or off-link properties of the prefix. When not set the advertisement makes no statement about on-link or off-link properties of the prefix. For example, the prefix might be used for address configuration with some of the addresses belonging to the prefix being on-link and others being off-link.
Set Autonomous flag	Select the **Set Autonomous flag** checkbox to indicate that this prefix can be used for autonomous address configuration as specified in RFC 4862.
Send interface address	Select the **Send interface address** checkbox to indicate that the address of interface is sent instead of the network prefix, as is required by Mobile IPv6.

Table 3-48 Router Advertisement Server Parameters (continued)

Item	Description
Prefix validity for on-link determination (secs)	Enter the length of time in seconds (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination.
Configured Address Preferred Lifetime (secs)	Enter the length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred.

4

Managing System Users

This chapter describes how to manage user settings and administrative user accounts from the **Users** tab in the Configuration Menu.

- Configuring Session/User Management
- Session/User Management - Enabling Session Management
- Session/User Management - Enabling User Management
- Using the User Management Page
- Configuring System Audit Settings
- Configuring the Message of the Day (MOTD)

Configuring Session / User Management

The Session/User Management page provides configuration settings for session management, user account management, and password management.

Before You Begin

Session management must be enabled first. Once session management is enabled, all fields pertaining to session management will be visible. User management can only be enabled once session management is enabled.



Note
Enabling user management will prevent the root user from accessing the GUI and activates a default administrative user “admin.” A new password for the user “admin” must be entered in order to enable user management if user management was not already enabled.

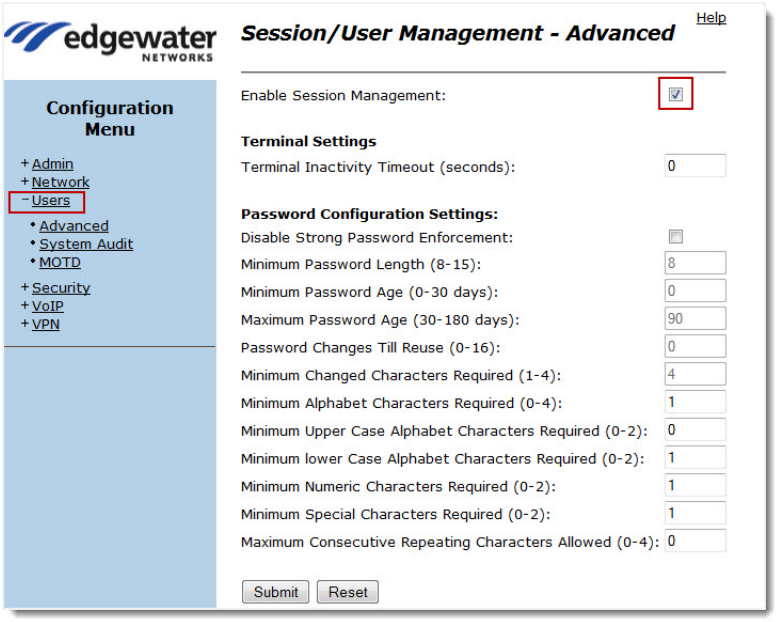
Proceed to the following sections:

- Session/User Management - Enabling Session Management
- Session/User Management - Enabling User Management

Session/User Management - Enabling Session Management

1. Choose **Users** from the Configuration Menu. The Session/User Management - Advanced page opens by default (Figure 4-1).

Figure 4-1 Enable Session Management

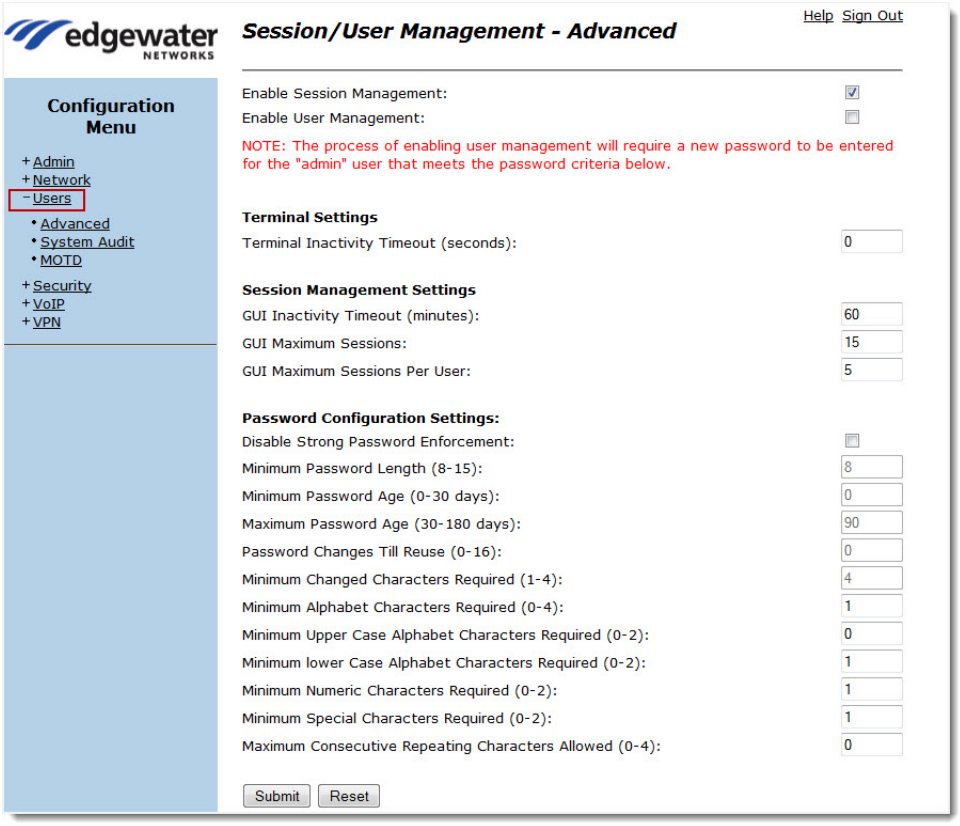


2. Select the **Enable Session Management** checkbox and click **Submit**.

Note
The process of enabling user management requires you to enter a new password; you are automatically directed to the Change Password page once you click **Submit**.

3. Enter your username and password and click **Submit**. Session management fields become active (Figure 4-2).

Figure 4-2 Session Management Enabled - Advanced Settings Page



4. Configure settings using the information in Table 4-1 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 4-1 Session/User Management - Advanced Parameters

Field	Description
Enable Session Management	Enables session management for the web user interface. You must enable Session Management before you can use the User Management configuration page.
Enable User Management	Enables user management configuration parameters. See Session/User Management - Enabling User Management.
Terminal Settings	
Sets the length of inactivity allowed before login sessions are terminated.	

Table 4-1 Session/User Management - Advanced Parameters (continued)

Field	Description
Terminal Inactivity Timeout (seconds)	Enter a timeout value between 0 (disabled) and 86400 seconds. This timer applies to Console, Telnet, and SSH logins. Changes to this value do not affect sessions that are already open. The timer starts counting when the session is available to receive a command. The timer is not reset until a complete command is entered. An empty command resets the timer (for example, clicking **Enter**). The timer is not active when a command is running (for example, continuous ping). A value of '0' disables the inactivity timer. The largest allowed timeout value is 86400 seconds. The default is '0'.
Session Management Settings	
Configure GUI session settings.	
GUI Inactivity Timeout (minutes)	Enter the time in minutes after which a GUI session will expire. Range is 5 to 60 minutes.
GUI Maximum Sessions	Enter the maximum allowed number of GUI sessions for the system. Range is 1 to 100.
GUI Maximum Sessions Per User	Enter the maximum allowed GUI sessions for a single user. Range is 1 to 10.
Password Configuration Settings	
Disable Strong Password Enforcement	Box is un-checked by default: Strong Password Enforcement is enabled to require that new passwords be complex. ■ When the box is un-checked, you can configure password enforcement parameters. ■ When the box is checked, new passwords are not required to be complex. **Note:** If user management is enabled, this checkbox is not available on the configuration page and you have the option to edit all of the password enforcement parameters. Refer to Default Password Change and Strong Password Enforcement.

Table 4-1 Session/User Management - Advanced Parameters (continued)

Field	Description
Minimum Password Length	Minimum number of required characters a password must contain. Note: Maximum password length is 32 characters. Configurable range is 8-15 characters.
Minimum Password Age	Minimum number of days before a password can be changed. Range is 0 to 30 days.
Maximum Password Age	Maximum number days after which the password will expire. Range is 30 to 180 days. Once a user password has reached the maximum age, the user is forced perform a password change prior to gaining system access. A user account will be disabled if the user fails to perform a password change after three notifications of password expiration.
Password Changes Till Reuse	To prevent password flipping, the user is denied the ability to re-use recently used passwords. Range is 0 to 16 previous passwords.
Minimum Changed Characters Required	Minimum number of characters that must be changed from the previously used password. Range is 1 to 4.
Minimum Alphabet Characters Required	Range is 0 to 4.
Minimum Upper Case Alphabet Characters Required	Range is 0 to 2.
Minimum lower Case Alphabet Characters Required	Range is 0 to 2.
Minimum Numeric Characters Required	Range is 0 to 2.

Table 4-1 Session/User Management - Advanced Parameters (continued)

Field	Description
Minimum Special Characters Required	Range is 0 to 2. Special characters are the non alphabet or numeric ASCII characters between codes 33 and 127.
Maximum Consecutive Repeating Characters Allowed	Range is 0 to 4.

Default Password Change and Strong Password Enforcement

Administrators can now configure the EdgeMarc to require users to change their default password the first time they log in. The password must adhere to the strong password policy configured by the administrator.

When this feature is enabled and a root or read-only (rouser) user tries to log into the EdgeMarc GUI with the default password, they will be redirected to the Change Password page to change their password.

CLI (SSH or Serial) users are also prompted to change their password. This feature is enabled by default.

A user is not allowed to access the system until they create a strong password that meets the following criteria:

- 6-8 (for root) total characters
- 1 lower case alphabet
- 1 numeric
- 1 special

To enable or disable Strong Password Enforcement from the EdgeMarc configuration GUI:

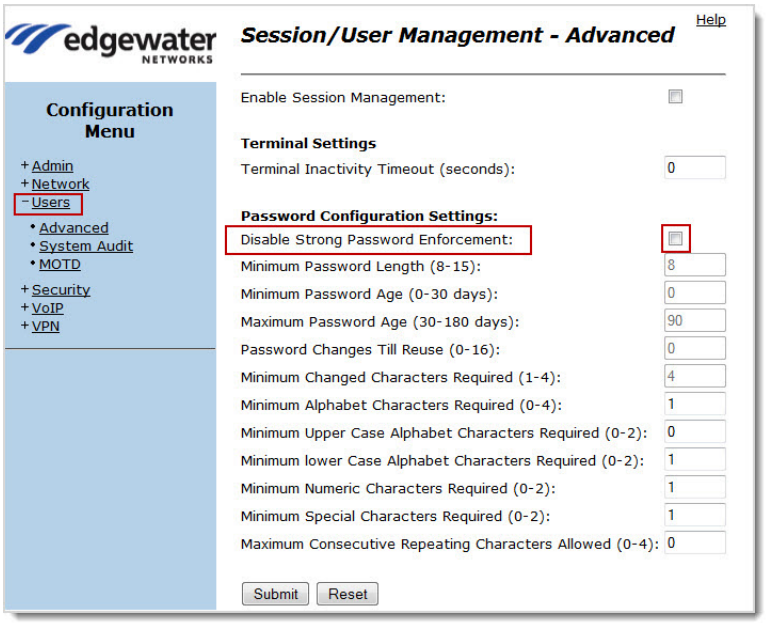
1. Choose **Admin** > **Users**. The Session/User Management - Advanced configuration page displays by default (Figure 4-3).

   The **Disable Strong Password Enforcement** checkbox is un-checked by default: Strong Password Enforcement is enabled and configuration fields are active.



Note
If User Management is enabled, Strong Password Enforcement settings are not available on the Session/User Management - Advanced configuration page.

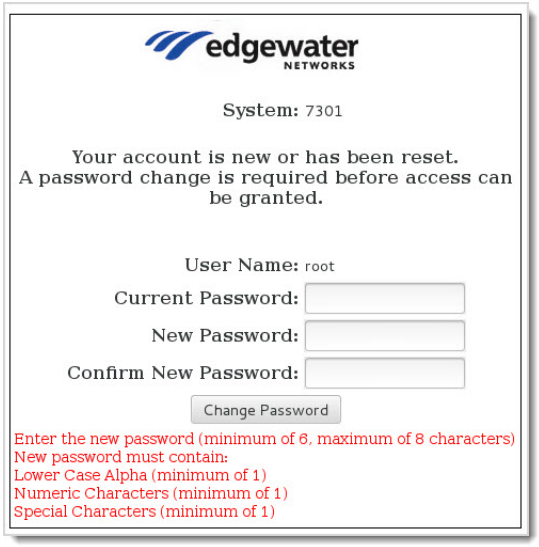
Figure 4-3 Enable Strong Password Enforcement



2. Enter required password information in the following active Password Configuration Settings fields:
   - Minimum Alphabet Characters Required (0-4)
   - Minimum Upper Case Alphabet Characters Required (0-2)
   - Minimum lower Case Alphabet Characters Required (0-2)
   - Minimum Numeric Characters Required (0-2)
   - Minimum Special Characters Required (0-2)
   - Maximum Consecutive Repeating Characters Allowed (0-4)
3. Click **Submit**.

   When the user logs in to the system for the first time with their default password, they are directed to the Change Password page (Figure 4-4).

Figure 4-4 Change Password Page



4. To disable Strong Password Enforcement, check the **Disable Strong Password Enforcement** checkbox on the Session/User Management - Advanced configuration page. Password Configuration Settings fields become inactive (grayed out) on the page.

   Strong Password Enforcement can also be configured through the CLI by setting parameters in the **user_mgmt.conf** file. Two new **PASSWD** configuration commands are added, as described in Table 4-2.

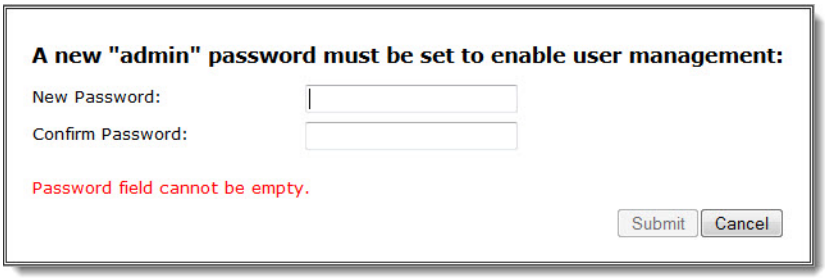
Table 4-2 Strong Password Enforcement CLI

Command	Description
DISABLE_STRONG_PASSWORD_ENFORCEMENT =off	The Strong Password Enforcement feature is on.
PASSWD_MIN_UPPER_ALPHABET_CHARS=0	Sets the minimum number of upper case letters required.
PASSWD_MIN_LOWER_ALPHABET_CHARS=1	Sets the minimum number of lower case letters required.

Session/User Management - Enabling User Management

1. Choose **Users** from the Configuration Menu. The Session/User Management - Advanced page opens by default (Figure 4-5).
2. Enable Session Management by selecting the **Enable Session Management** checkbox and clicking **Submit**. Refer to Session/User Management - Enabling Session Management.
3. Select the **Enable User Management** checkbox. The change admin password window pops up automatically, you do not have to click **Submit** at this time.
4. Enter a new admin password in the pop-up window (Figure 4-5). The password must meet the criteria that you have set in Configuring Session/User Management.

Figure 4-5 Change Admin Password

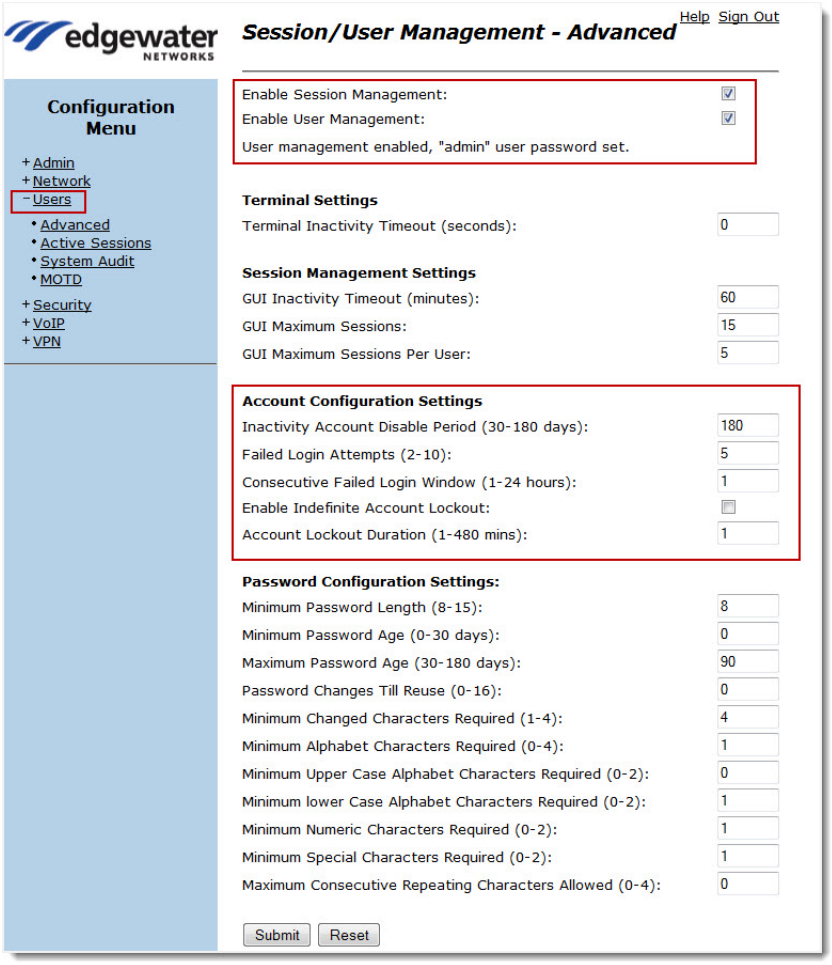


5. Click **Submit** in the password pop-up. You are returned to the Session/User Management - Advanced page.
6. Click **Submit** again at the bottom of the Session/User Management - Advanced page to activate User Management configuration fields.

   A message indicates that service will be interrupted and the following warning is displayed:

   “You are attempting to enable user management. Enabling user management will activate the default administrative user 'admin'. The GUI 'root' user will subsequently be prevented from accessing the GUI. Are you sure?”
7. Click **OK** to accept the change and return to the Session/User Management - Advanced page with User Management enabled (Figure 4-6)

Figure 4-6 Session/User Management - User Management Enabled



8. Configure settings using the information in as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 4-3 Session/User Management - Advanced Parameters

Field	Description
Terminal Settings	
Refer to Session/User Management - Enabling Session Management.	
Session Management Settings	
Refer to Session/User Management - Enabling Session Management.	
Account Configuration Settings	
The fields are active when User Management is enabled.	

Table 4-3 Session/User Management - Advanced Parameters (continued)

Field	Description
Inactivity Account Disable Period (30-180 days)	Enter the number of days after which inactive accounts will be disabled.
Failed Login Attempts (2-10)	Enter the number of allowed failed login attempts due to invalid passwords before a user account is locked. Configurable range is 2-10 attempts.
Consecutive Failed Login Window (1-24 hours)	Enter the time period for which the failed login counter is maintained. The failed login count for users is reset to zero when the failed login window expires.
GUI Maximum Sessions Per User	Select the **Enable Indefinite Account Lockout** checkbox to keep a user locked out for excessive failed login attempts. The administrator can unlock the account. When disabled, the configured account lockout duration setting is applied. The default admin user cannot be locked out, so indefinite lockout does not apply to the default administrator.
Account Lockout Duration (1-480 mins)	Enter the number of minutes that a user account will be locked out due to excessive failed login attempts. This setting is not applicable when the Indefinite Account Lockout setting is enabled.
Password Configuration Settings	
Refer to Session/User Management - Enabling Session Management.	

Using the User Management Page

This page provides information and dialogs to create, edit, disable, delete, and reset user-defined management user accounts and access server user accounts.



Tip
Both Session Management and User Management must be enabled to use the User Management page

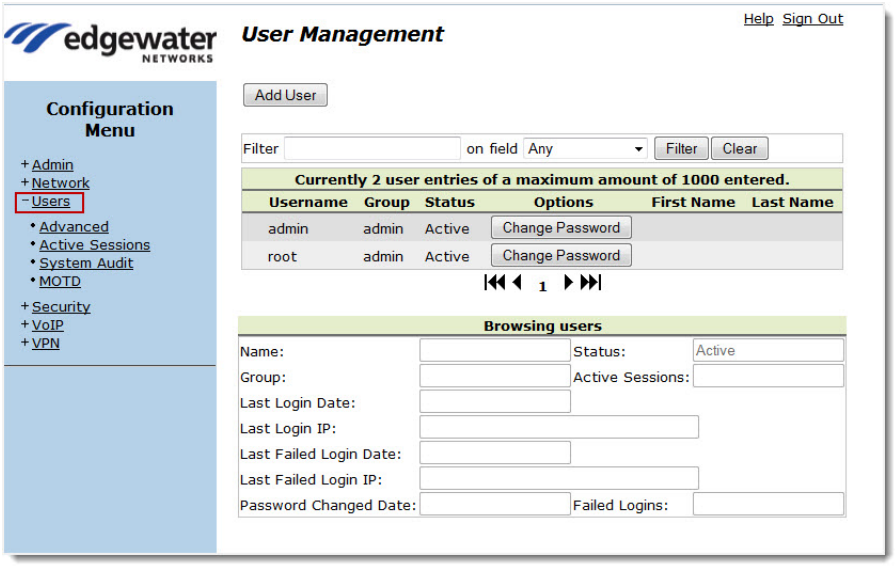
1. Enable Session Management as described in Configuring Session/User Management.
2. Enable User Management as described in Session/User Management - Enabling User Management.

3. Manage users using the information in the following sections:
   - Viewing a User
   - Changing a User Password
   - Adding a User
   - Managing Active User Sessions
   - Disabling User Management

Viewing a User

1. Choose **Users** from the Configuration Menu (Figure 4-7). The User Management page opens by default when user management is enabled.
2. On the User Management page, roll your mouse over the username in the list of users. Details for the selected user are displayed in the Browsing/Viewing Users window.

Figure 4-7 List of Users - View User

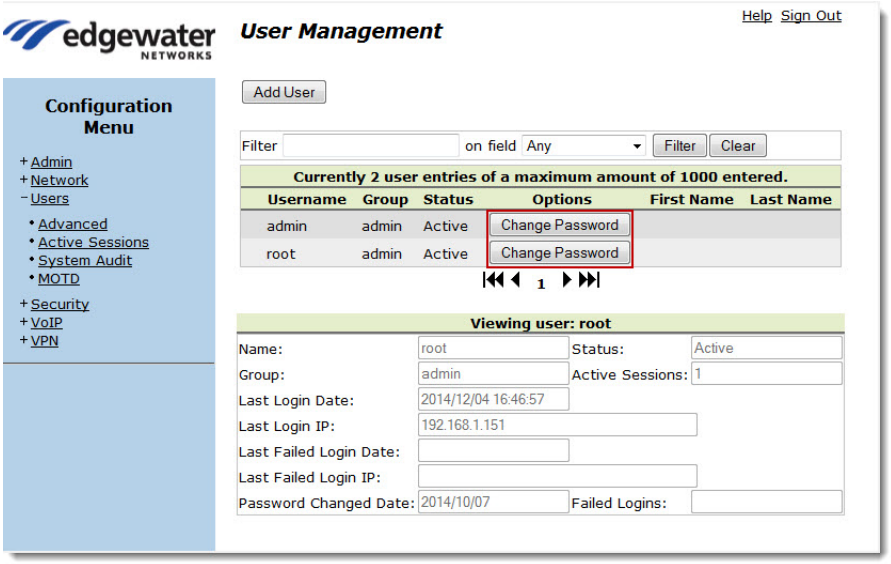


Changing a User Password

The change password action is available for the administrator account that is currently logged in. It is also available for the 'admin' account and the 'root' account. Clicking on this action provides a pop-up for changing the password of the user. The current password is required for a password change. A user may only change the password once until the minimum password age is exceeded. Password complexity restrictions must be followed for administrator users accounts. Refer to Management User Password Field Information.

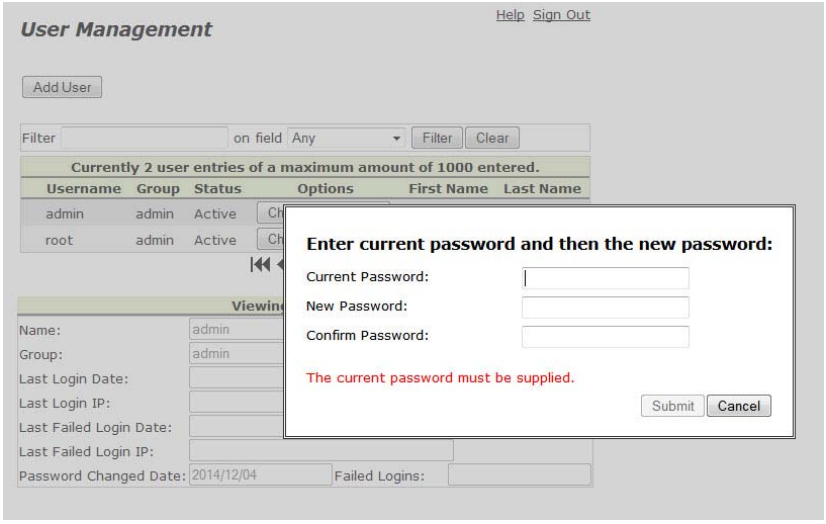
1. Choose **Users** from the Configuration Menu (Figure 4-8). The User Management page opens by default when user management is enabled.
2. On the User Management page, click **Change Password** in the Options column for the admin user.

Figure 4-8 User Management Page



3. Enter your current password in the field provided (Figure 4-9).
4. Enter and confirm your new password in the fields provided.

Figure 4-9 Changing a User Password



5. Click **Submit**.

Management User Password Field Information

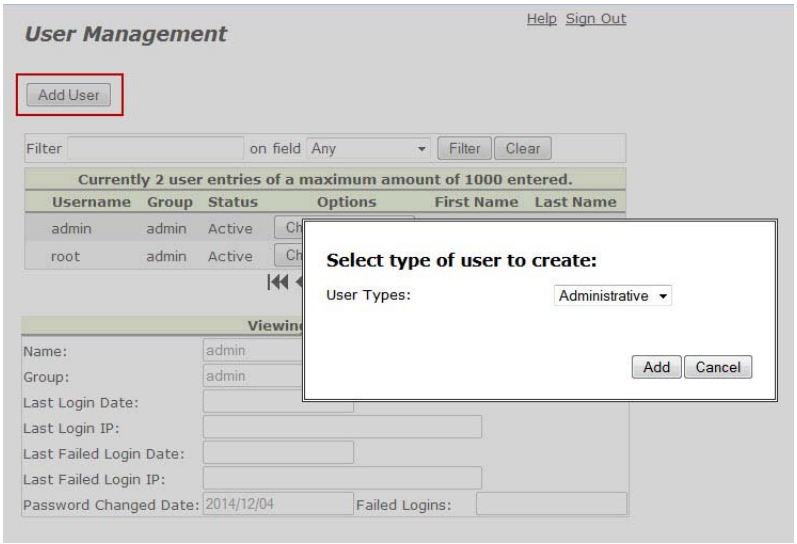
The following user account password requirements are for admin/management users only. Passwords can be 8 to 32 alphanumeric or special characters. Passwords must meet the following complexity requirements:

- Must have a minimum length in the range of 8-15 characters.
- Must contain the minimum configured number of alphanumeric and special characters. Configurable range is 1-2 characters for each character class.
- Must not exceed the maximum number of consecutive repeating characters that are allowed in the password. Configurable range is 1-4 repeating characters.
- Must contain the minimum configured number of changed characters from the previously used password. Configurable range is 1-4 characters.
- Must not be identical to configured number of previously used password. Configurable range is 8-16 previously used passwords.

Adding a User

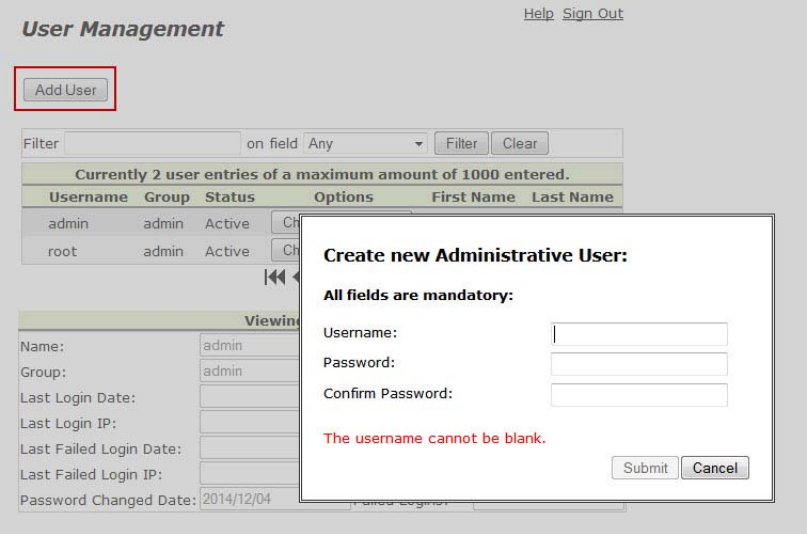
1. Choose **Users** from the Configuration Menu. The User Management page opens by default when user management is enabled.
2. On the User Management page, click **Add User**. The User Types window is displayed (Figure 4-10).

Figure 4-10 Selecting a New User Type



3. Select a user type from the **User Types** drop-down list.
4. Click **Add** to activate configuration fields. Figure 4-11 shows the Create New Administrative User window.

Figure 4-11 Adding an Administrator User



5. Configure settings for the new Administrative User using the information in Table 4-4 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 4-4 Adding a User

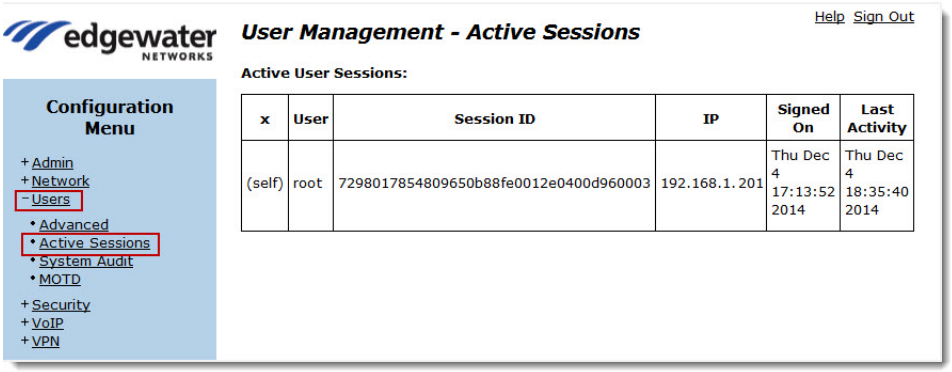
Field	Description
Adding An Administrative/Management User	
Adds new management user accounts that can be configured to be in the administrative users (admin) group. The group cannot be changed after you create it. Select **Administrative** from the **User Types** drop-down list and click **Add**.	
Username	Enter a user account name. This name can be up to 30 characters long and can only contain lowercase letters (a-z), digits (0-9), or an underscore (_).
Group	Select the group the user belongs to as Admin.
Password	Enter the initial password for the new management user account. Refer to the password parameters in Management User Password Field Information.
Confirm	Enter the initial password a second time for confirmation.

Managing Active User Sessions

When User Management is enabled from the Session/User Management - Advanced configuration page, you can manage active user sessions.

1. Choose **Users** > **Active Sessions** (Figure 4-12).

Figure 4-12 User Management - Active Sessions Page



2. View active users using the information in Table 4-5 as a guide.

Table 4-5 List of Active Sessions

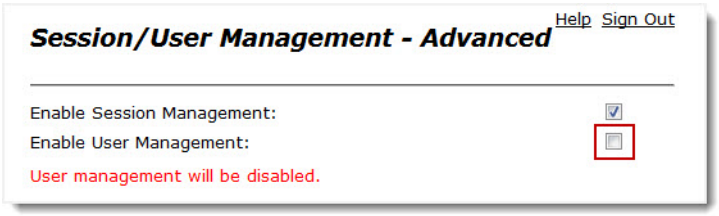
Item	Description
Active User Sessions	
View and manage a list of active sessions on the system.	
User	Displays the user account name. A “self” identifier indicates that the session information belongs to the current session.
Session ID	Displays session identification.
IP Address	Displays the session IP address.
Signed On	Displays the login time stamp; the time the session was created.
Last Activity	Displays the time stamp of the last session activity.
Deleting an Active Session	
To delete a session, select a session from the List of Active Sessions and click the trash can icon. Click **OK** to confirm.	
Note: A currently active session cannot be deleted; end the session to delete it from the list.	

Disabling User Management

Tip
You must first disable System Audit. Choose **Users** > **System** Audit and refer to Configuring System Audit Settings.

1. Choose **Users** > **Advanced** and un-check the **Enable User Management** checkbox (Figure 4-13).

Figure 4-13 User Management - Disable



2. Click **Submit** at the bottom of the Session / User Management - Advanced page. A message indicates that service will be interrupted and the following warning is displayed:

   "You are attempting to disable user management. System auditing must also be disabled. Disabling user management will deactivate the "admin" user and all user defined accounts. The GUI 'root' user will be activated. Are you sure?"

3. Click **OK**.

Configuring System Audit Settings

The System Audit Configuration page provides configuration settings for the audit logging facility, and dialogs for viewing audit logs. Audit users are also permitted to download and clear audit logs.

Before You Begin

1. Enable Session Management. See Configuring Session/User Management
2. Enable User Management. See Using the User Management Page.

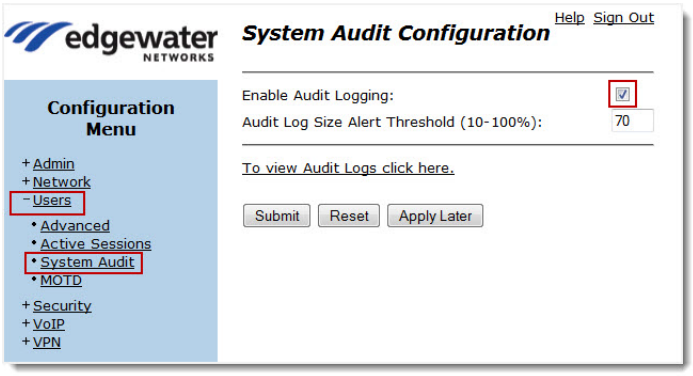
Proceed to the following sections:

- Enabling System Audit
- Viewing Audit Logs
- Disabling System Audit

Enabling System Audit

1. Choose **Users** > **System Audit** (Figure 4-14).

Figure 4-14 System Audit Configuration Page



2. Configure settings using the information in Table 4-6 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 4-6 System Audit Configuration Parameters

Item	Description
Enable Audit Logging	Select the **Enable Audit Logging** checkbox.
Audit Log Size Alert Threshold (10-100%)	Set the log file size alert by entering a value from 10% to 100% in the **Audit Log Size Alert Threshold (10-100%)** field.
Audit Log Fields	
Opens a new window to view audit log information. See Viewing Audit Logs.	
Date	Time stamp of event occurrence.
User	User performing the event.
Event Type	Type of event: ■ User-authorization ■ Config-change—Changes to the device configuration ■ System-alert—Miscellaneous system alerts (for example, log size alert)
Event Severity	Severity of the event: ■ INFO—Informational ■ WARN—Warning ■ ERROR—Error

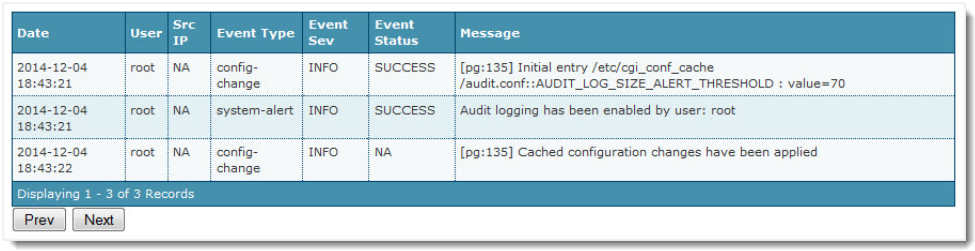
Table 4-6 System Audit Configuration Parameters

Item	Description
Event Status	Event success or failure. A failure or success may apply, in which case an NA indicator is displayed.
Message	Additional details about the entry.

Viewing Audit Logs

1. Click the **To view Audit Logs click here** link to view audit logs (Figure 4-15). Audit log parameters are described in Table 4-6.

Figure 4-15 View Audit Logs



2. Click **Prev** or **Next** to see additional audit logs.
   - **Clear Audit logs**—Available for audit users only. Follow the link to clear audit logs. Audit logs can only be cleared when all records have been backed up via download.
   - **Download Audit logs**—Available for audit users only. Follow the link to download audit logs. Audit logs can only be cleared when all records have been backed up via a download. The download link is only available when there are entries in the log file.

Disabling System Audit

You must disable System Audit to turn off User Management.

1. Choose **Users** > **System Audit** (Figure 4-14).
2. Un-check the **Enable System Logging** checkbox and click **Submit**.
3. Click **OK** at the system prompt.
4. Refer to Disabling User Management.

Configuring the Message of the Day (MOTD)

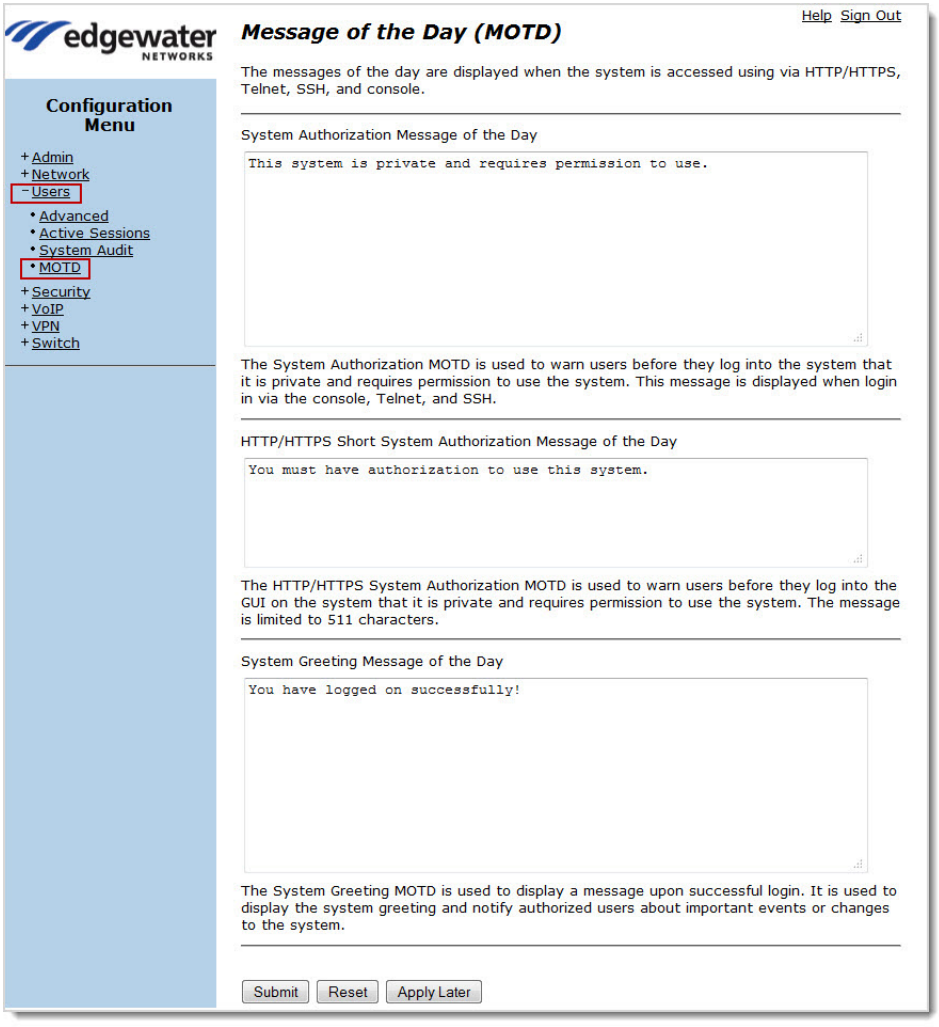
Administrators who log in to the system console can configure custom messages of the day (MOTD). Refer to the following sections for supported message types and login methods:

- Message Types
- Login Methods

To configure the message of the day:

1. Choose **Users** > **MOTD** (Figure 4-16).

Figure 4-16 Message of the Day Configuration Page



2. Enter message text in the fields provided using the information in Table 4-7 as a guide.
3. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 4-7 Message of the Day Parameters

Item	Description
System Authorization Message of the Day	Enter a message for users before they log into the system from the console. A typical message warns users that access is private and requires permission. This message allows unauthorized users the opportunity to terminate their login session before they access the system. System Authorization MOTD is supported only on logins from the console. Telnet, SSH and HTTP/HTTPS protocols do not allow the transfer of MOTDs in the protocol while establishing a session.
HTTP/HTTPS Short System Authorization Message of the Day	Enter a message warning users before they log into the system GUI that the system is private and requires permission to use. The message is limited to 511 characters.
System Greeting Message of the Day	Enter a message that is displayed following successful login. A typical message includes a system greeting along with notification about important events or changes to the system.

Message Types

The following message types are supported:

- System Authorization Message of the Day
- HTTP/HTTPS Short System Authorization Message of the Day
- System Greeting Message of the Day

Login Methods

Several login methods are supported to access the EdgeMarc:

- Command line access through serial console connection—System Authorization and System Greeting messages are displayed.
- Telnet or SSH access—System Greeting message is displayed, but not the System Authorization message.
- HTTP/HTTPS—Neither the System Authorization nor System Greeting message is displayed.

5

Configuring System Security

The following sections describe how to configure security features on the EdgeMarc using the **Security** tab in the Configuration Menu.

- Overview
- Configuring Basic WAN Firewall Settings
- Forwarding WAN Firewall Settings
- Managing Certificates
- Configuring HTTPS
- Configuring Outbound Settings
- Configuring Trusted Hosts
- Limiting the Number of SSH Attempts

Overview

The EdgeMarc can act as a firewall for voice, video, and data traffic. A firewall restricts and controls the traffic between networks, typically between a corporate network and the Internet. If an external firewall is used, the firewall configuration can be set to pass or block data traffic depending on whether the system is placed in series or in parallel with the external firewall.

The EdgeMarc provides a full layer 7 gateway for voice traffic and a stateful packet inspection firewall for data traffic. You can define policies to filter traffic that traverses the device or administration traffic that is destined to the device. Voice and video firewalls are implemented by VoIP Proxy.

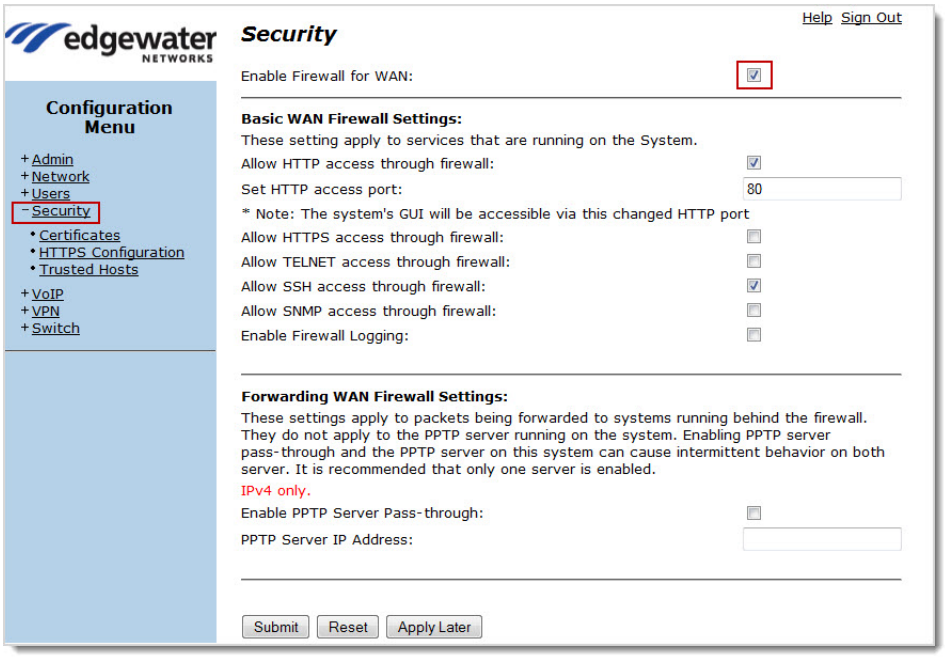
For more information about VoIP Proxy, see Chapter 6, *Configuring VoIP Settings*.

Configuring Basic WAN Firewall Settings

The Firewall configuration page allows you to enable or disable firewall functions and set firewall log parameters.

1. Choose **Security** from the Configuration Menu (Figure 5-1).

Figure 5-1 Firewall Configuration Page



2. Configure settings using the information in Table 5-1 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 5-1 Standard Firewall Parameters

Item	Description
Enable Firewall for WAN	Select the **Enable Firewall for WAN** checkbox.
Basic WAN Firewall Settings Enable or disable the management services allowed to the system from the WAN: ■ WAN access to the firewall—Management access from the LAN to these services is still enabled even if all checkboxes are deselected. ■ Provider/Subscriber access to the system—Management services to the system apply to both the provider and the subscriber interfaces. Deselecting a management service causes loss of access to the system from both the provider and the subscriber interfaces.	
Allow HTTP Access Through the Firewall	Select the **Enable Firewall Logging** checkbox to log information about packets to and through the system. **Tip:** To configure the system to use an external syslog server: ■ Choose **Admin** > **System Configuration**. ■ Select the **Remote System Logging** checkbox and configure settings in the Remote System Logging window. Refer to Configuring Remote System Logging in Chapter 2, *System Administration*.
Set HTTP access port	Enter the HTTP connection port to connect to the system and use the system GUI.
Allow HTTPS Access Through the Firewall	Select the checkbox to allow HTTPS system management from the WAN interface.
Allow TELNET Access Through Firewall	Select the checkbox to allow Telnet system management from the WAN interface.
Allow SSH Access Through Firewall	Select the checkbox to allow SSH (version 2) system management from the WAN interface.

Table 5-1 Standard Firewall Parameters (continued)

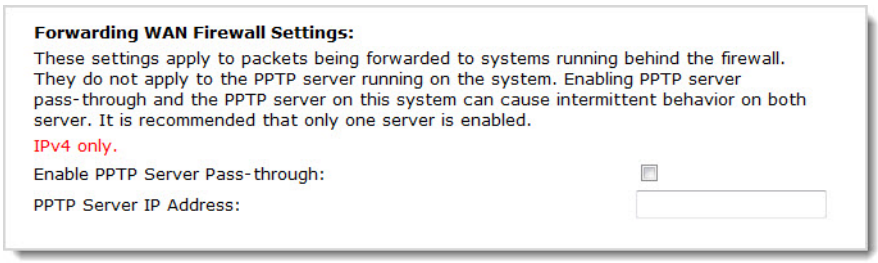
Item	Description
Allow SNMP Access Through Firewall	Select the checkbox to allow SNMP V1 and V3 system management from the WAN interface.
Enable Firewall Logging	Select the checkbox to enable logging for packets to and through the system. **WARNING:** Because port scanning and login attacks are common when connected to a public network, logging is disabled by default. When enabling logging, use caution! Firewall logging may affect call quality and system performance. It may also use network bandwidth if system logging is enabled over the WAN.

Forwarding WAN Firewall Settings

You can configure settings to allow packets to be forwarded to systems running behind the firewall. These settings are for systems using IPv4.

1. Choose **Security** from the Configuration Menu (Figure 5-1).
2. Scroll to **Forwarding WAN Firewall Settings** (Figure 5-2).

Figure 5-2 Forwarding WAN Firewall Settings



3. Configure settings using the information in Table 5-2 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 5-2 Forwarding WAN Firewall Parameters

Item	Description
Forwarding WAN Firewall Settings **Tip:** Use CLI to view the active firewall logs in **/var/log/messages**.	
Enable PPTP Sever Pass-Through	Select the **Enable PPTP Server Pass-through** checkbox to allow TCP port 1723 to be forwarded through the system to the defined PPTP Server IP Address. The server is placed on the LAN side with a private IP address, which allows Windows PPTP to pass through to a Windows server, but firewalls the server from other traffic. **Caution:** Enabling PPTP server pass-through and the PPTP server on this system can cause intermittent behavior on both servers. It is recommended that only one server be enabled at a time.
PPTP Server IP Address	Enter the private PPTP server IPv4 IP address. All outside users will use the system's public IP address to access the PPTP server. The Windows server has a private IP address, which is handled by the system using NAT.

Managing Certificates

The Certificates page manages certificates in the Certificate Store. The Certificate Store contains certificates for use with HTTPS and VoIP Traversal. All certificates are kept in the Certificate list and can be downloaded from the list. See the following sections for more information about certificates:

- Understanding the Certificate List
- Understanding HTTPS Usage
- Understanding VoIP Traversal Usage
- Creating a New Certificate
- Downloading a Certificate or Key File
- Adding a Local Certificate

Understanding the Certificate List

The certificate list shows all certificates available on the system. The following certificate types are supported:

- HTTPS—Self-signed or generated by Certificate Authority (CA). Used for secure connections.
- CA Certificate—Used to sign other certificates.
- VoIP Traversal Server—Used by a VoIP Traversal server.
- VoIP Traversal Client—Used by a VoIP Traversal client.



Tip
Refer to Chapter 6, *Configuring VoIP Settings* for more information about VoIP Traversal.

A certificate entry can be a normal certificate or a Certificate Signing Request (CSR). CSRs cannot be used for normal operation and can only be downloaded for CA signing. Once the CA has signed the CSR, the resulting certificate can be added to the system and used.

For each entry, the certificate (or certificate signing request) as well as the corresponding key can be downloaded. If there is no key available for a given certificate, the key download field is empty. Refer to Downloading a Certificate or Key File.

Understanding HTTPS Usage

When generating a certificate for use with HTTPS, it is typically self-signed or generated by an external CA. It is possible to sign the HTTPS certificate with a locally generated CA certificate, but there is no need to do this extra step. Once an HTTPS certificate is created or uploaded, go to the HTTPS Configuration page to select which HTTPS certificate to use for the Web Server.

Understanding VoIP Traversal Usage

The VoIP Traversal feature needs at least three certificates to function:

- A locally available CA certificate is needed on both the server and the remote clients.
- A VoIP Traversal Server certificate is needed on the server.
- A VoIP Traversal Client certificate is needed on each client You can use the same client certificate on each client, or a unique client certificate for each client.

Typically, you generate a CA certificate and a server certificate that is signed by that CA certificate. Then you would generate one or more client certificates signed by the same CA certificate. Once these certificates are created on the server, you can download the CA certificate, the client certificates and key, and upload them on each client (the CA key does not

need to be transferred to the client). Once this is done, go to the VoIP Traversal page to select the certificates to use for VoIP Traversal.



Note

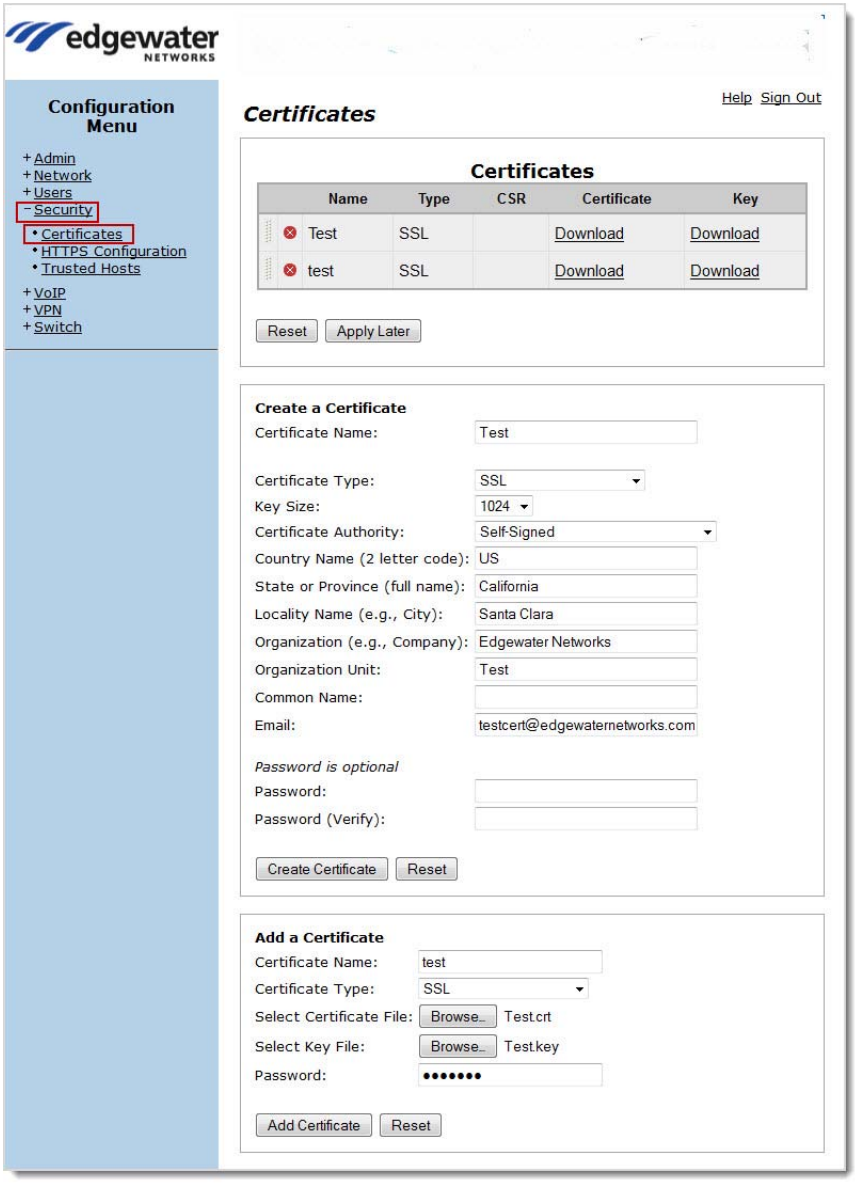
If you delete a VoIP Traversal CA or Server certificate, no VoIP Traversal clients using certificates signed by that CA certificate can connect to the server again. You must generate a new CA, Server and Client certificate and install these certificates on the clients to be able to establish the tunnels again.

See Chapter 6, *Configuring VoIP Settings* for more information.

Creating a New Certificate

1. Choose **Security** > **Certificates** (Figure 5-3).

Figure 5-3 Certificates Configuration Page



2. Configure settings using the information in Table 5-3 as a guide. When you have finished configuring settings, click **Create Certificate** to make your changes take effect.

Table 5-3 Certificates Configuration Parameters

Item	Description
Certificates	
Lists certificates and certificate keys currently on the system available for download. If there is no key available for a given certificate, the key download cell will be empty. Refer to Downloading a Certificate or Key File.	
Create a Certificate	
Creates a new certificate to add to your certificate store.	
Certificate Name	Enter the certificate name. This name is used for certificate management only and is displayed in the Certificate list.
Certificate Type	Choose the certificate type from the drop-down list: ■ SSL ■ CA Certificate ■ VoIP Traversal Server ■ VoIP Traversal Client
Key Size	Choose the key size from the drop-down list: ■ 1024 ■ 2048
Certificate Authority	Choose a certificate authority type from the drop-down list: ■ Self-signed ■ CSR
Country Name	Enter the two-letter code of the country where the certificate is to be used. For example, “US.”
State or Province (full name)	Enter the full name of the state or province where the certificate is to be used. For example, “California.”
Locality Name	Enter the name of the city where the certificate is to be used.
Organization	Enter the company name. For example, “Edgewater Networks.”
Organization Unit	Enter the company department.

Table 5-3 Certificates Configuration Parameters (continued)

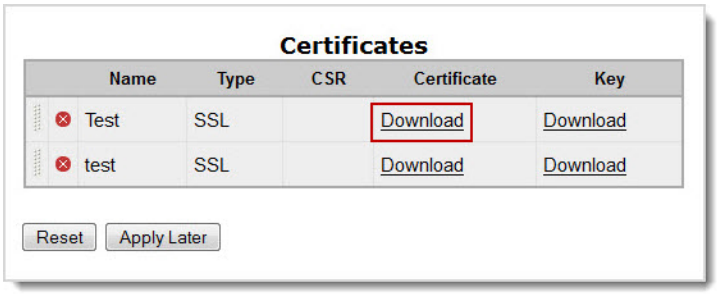
Item	Description
Common Name	Enter the FQDN assigned to the WAN IP of the system, or the DNS A record name. When creating a CSR to obtain a signed VeriSign or Go-Daddy certificate, this name must be the FQDN of the system. Security scanners pick up the public certificate and do a reverse lookup to make sure the CN: field has a DNS that matches the IP of this system. If it does not, the security scanner will fail this portion of the scan.
Email	Enter the email to contact regarding the certificate.
Password Password Verify	(Optional) Enter a password for HTTPS certificates only or optionally used to secure the key. If a password was used when generating the key, the same password must be specified here.

3. Click **Create Certificate**.
   The system displays the following message:
   WARNING: Creating a certificate may require a lot of CPU resources and should not be done while the system is in service.
4. Click **OK**. The new certificate is added to the Certificates list.

Downloading a Certificate or Key File

1. Choose **Security** > **Certificates** (Figure 5-3).
2. To download a certificate or key file, click **Download** for the selected file from the Certificates list (Figure 5-4).

Figure 5-4 Download a Certificate



3. Click **Save File** in the download pop-up to save the certificate or key file to your computer.
4. Double click your certificate or key file or right-click the file and choose **Install Certificate**.
5. Follow the prompts in your Certificate Import Wizard to add the certificate or key to your certificate store.

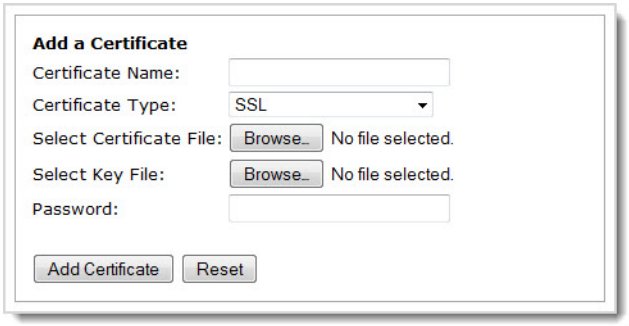
Adding a Local Certificate

When adding a certificate you must select two files, the actual certificate and the corresponding key file.

Note
CA certificates may be added without a corresponding key file. However, they cannot be used to sign other certificates.

1. Choose **Security** > **Certificates** (Figure 5-3).
2. Scroll to **Add a Certificate** (Figure 5-5).

Figure 5-5 Add a Certificate



3. Configure settings using the information in Table 5-4 as a guide. When you have finished configuring settings, click **Add Certificate** to make your changes take effect.

Table 5-4 Adding a Certificate

Item	Description
Add a Certificate	
Adds a local certificate from your certificate store or elsewhere on your system.	
Certificate Name	Enter the certificate name. This name is used for certificate management only and is displayed in the certificate list.
Certificate Type	Choose one of the following options from the **Certificate Type** drop-down list: ■ HTTPS ■ CA Certificate ■ VoIP Traversal Server ■ VoIP Traversal Client
Select Certificate File	Click **Browse** to find the local certificate file to add to the list of certificates.
Select Key File	Click **Browse** to find the local key file that goes with the certificate.
Password	Optional for HTTPS certificates only. Enter the password with which the key file is encrypted.
Click **Add Certificate**. A message indicates that service will be interrupted. Click **OK**. The certificate and associated key are added to the Certificates list.	

Configuring HTTPS

The HTTPS Configuration page configures the certificate used by HTTPS for secure remote management as well as any alternate HTTPS port to use. Access to the system from the WAN or public interface requires HTTPS access, which is enabled on the Firewall page.

Before You Begin

1. Access from the LAN or private interface using HTTPS is not enabled by default on some platforms. Verify your requirements and check current firewall settings on the Firewall page:

   Choose **Security** from the Configuration Menu and refer to Configuring Basic WAN Firewall Settings.

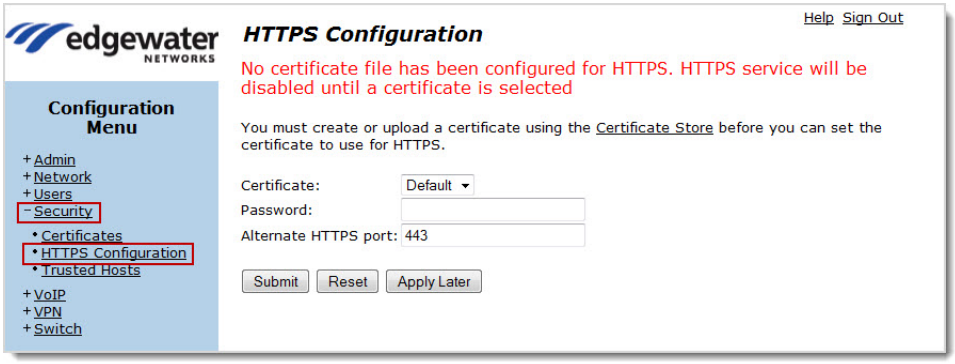
2. You must create or upload a certificate using the Certificate Store before you can set the certificate to use HTTPS:

Tip
Choose **Security** > **Certificate Store** to create or upload a certificate (refer to Managing Certificates).

Configure HTTPS

1. Choose **Security** > **HTTPS Configuration** (Figure 5-6).

Figure 5-6 HTTPS Configuration Page



2. Configure settings using the information in Table 5-5 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 5-5 HTTPS Configuration Parameters

Item	Description
Certificate	Choose a certificate from the **Certificate** drop-down list. If you need to create or upload a certificate, click the **Certificate Store** link or choose **Security** > **Certificates** and refer to Managing Certificates.
Password	(Optional) Enter the password that protects the private key file.
Alternate HTTPS port	Enter the port number that the system web server uses to listen for inbound management HTTPS requests. By default this port is 443. **Note:** If you change the default connection port 443 to another port, you must update your browser URL to the following format: **https:/ /** [**ip-of-device**] **:** [**alternate-https-port**]

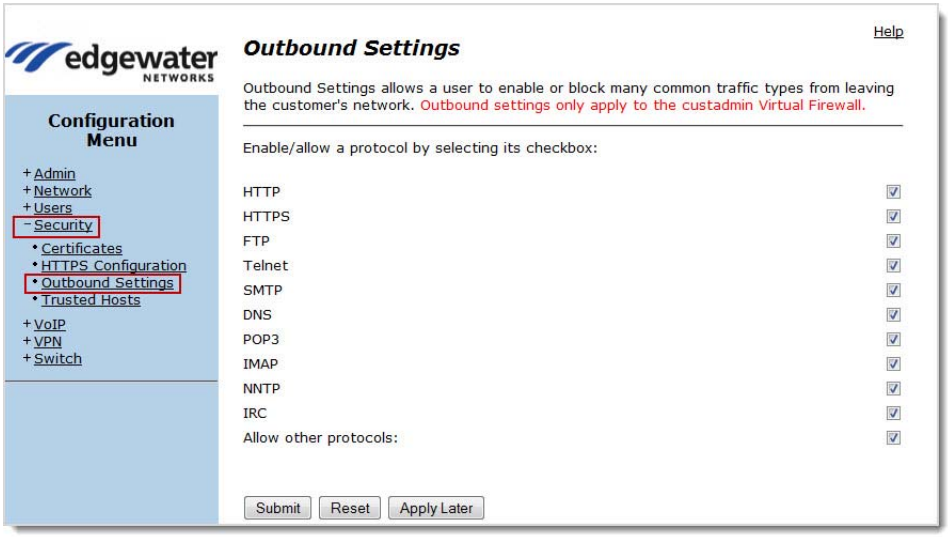
Configuring Outbound Settings

The checkboxes on the Outbound Settings page allows you to configure the policy for several of the most common outbound protocols. When checked, the protocol will be allowed through the system. If un-checked, the protocol will be blocked from LAN to WAN.

The protocols shown only apply to the custadmin user's dynamic NAT settings.

1. Choose **Security** > **Outbound Settings** (Figure 5-7).

Figure 5-7 Outbound Settings Configuration Page



2. Select the checkboxes for the protocols that you want to allow through the system. If a protocol is un-checked, the protocol is blocked from LAN to WAN.
3. Click **Submit** to save your settings.

Configuring Trusted Hosts

The Trusted Hosts page defines a list of hosts or networks that are able to access the system using management protocols. These management protocols are configured using the settings on the Basic WAN Firewall Settings page. Choose **Security** from the Configuration Menu and refer to Configuring Basic WAN Firewall Settings.

Before You Begin

1. Once a trusted address is defined, only hosts in the trusted list are allowed to access the system. Before proceeding, verify that the firewall settings are configured to allow the desired management protocols. Click the **Firewall page** link provided or choose **Security**

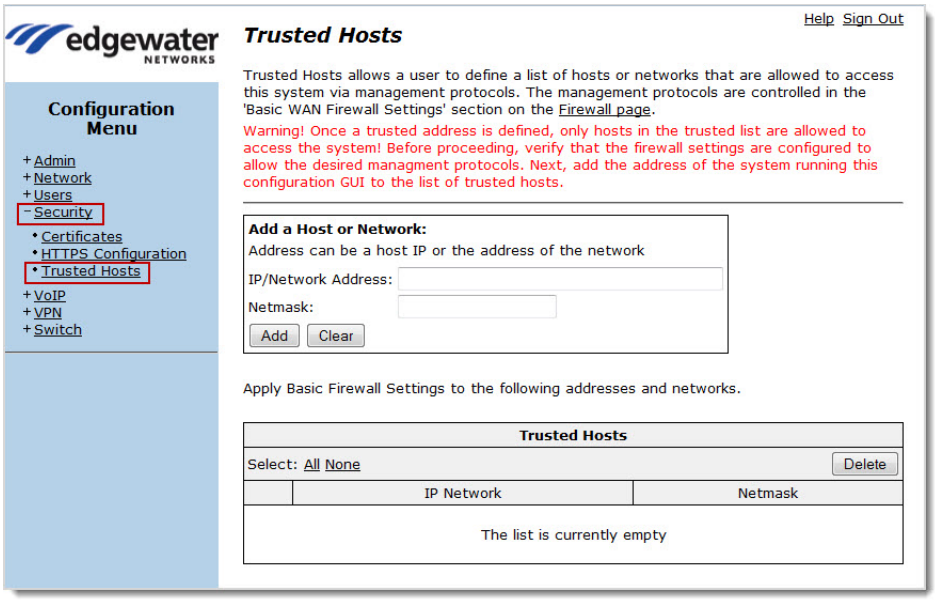
from the Configuration Menu and refer to Configuring Basic WAN Firewall Settings.

2. Make sure to add the IP address of this system (the system running your configuration GUI) to the list of trusted hosts.

Adding a Host or Network

1. Choose **Security** > **Trusted Hosts** (Figure 5-8).

Figure 5-8 Trusted Hosts Page



2. Configure settings using the information in Table 5-6 as a guide. When you have finished configuring settings, click **Add** to make your changes take effect.

Table 5-6 Trusted Hosts Configuration Parameters

Item	Description
Add a Host or Network	
IP/Network Address	Enter the IP address or network address of the subnet to be managed.
Netmask	Enter the netmask to apply to the IP/Network Address. The netmask determines how many addresses are available in the network.
Trusted Hosts	
Lists addresses and networks to which basic firewall settings have been applied.	
Click **Add**. A message indicates that service will be temporarily interrupted. Click **OK** to confirm.	

Deleting a Trusted Host

1. Choose **Security** > **Trusted Hosts** (Figure 5-8).
2. In the **Trusted Hosts** list select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
3. Click **Delete**.
4. Click **OK** to confirm.

Limiting the Number of SSH Attempts

The Intrusion Prevention page allows a user to set a number of unsuccessful login attempts a remote host may have during a period of time before that remote host is locked out from being able to attempt to login. The user will be locked out from the time of the first unsuccessful login to the lockout duration.

For example, if the number of attempts specified is 3 and the lockout duration is 5 minutes, a user who unsuccessfully logs in at time 0, at 1 minute, and at 3 minutes will be locked out until the time of 5 minutes because that is the time of the lockout duration since the initial failed attempt.

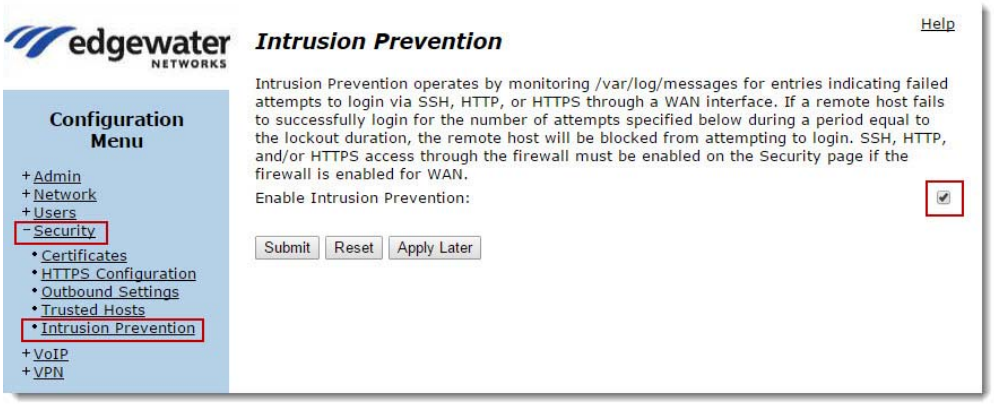
The user will then have one attempt available to login. At the 6 minute mark, the user will have another attempt to login, if needed. Failed attempts essentially “expire” after the lockout duration from the time of the failed attempt.

When the feature is disabled or if the system reboots, all records of failed attempts are deleted and all users can attempt to login. When the feature is re-enabled, the record keeping starts again. This feature works for SSH, HTTP, & HTTPS for IPv4 & IPv6.

To enable the feature:

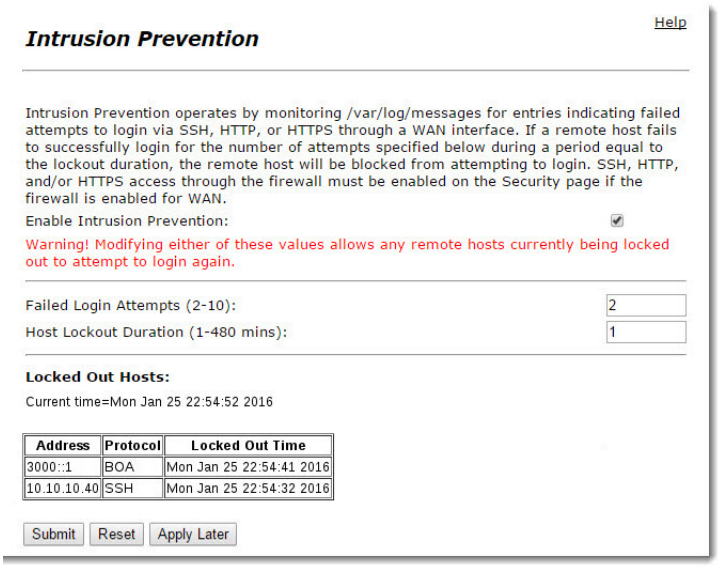
1. Choose **Security** > **Intrusion Prevention** from the Configuration Menu (Figure 5-1).

Figure 5-1 Intrusion Prevention Page



2. Select the **Enable Intrusion Prevention** checkbox and click **Submit**. Additional fields become active (Figure 5-1).

Figure 5-1 Intrusion Prevention Configuration



3. Enter a value in the **Failed Login Attempts (2-10)** field.
4. Enter a value in the **Host Lockout Duration (1-480 mins)** field.

The Locked Out Hosts section displays hosts that have exceeded the number of attempts to log in.

6

Configuring VoIP Settings

The following sections describe how to configure the Voice over IP (VoIP) Application Layer Gateway (ALG) on the EdgeMarc to recognize and register network devices using the **VoIP** tab in the Configuration Menu.

- Overview
- Configuring VoIP ALG Settings
- Configuring H.323 Settings
- Configuring MGCP Settings
- Configuring SIP Settings
- Configuring Survivability
- Configuring the Clients List
- Managing Test UA
- Configuring IP Phones, IADs, or Softphones

Overview

A VoIP Application-Layer Gateway (ALG) provides basic proxy features. Serving as an ALG proxy, the system maps many network appliances into one or more public IP addresses and provides the connectivity and management for IP phones. The ALG must first recognize and register a network appliance before it presents the IP telephone or data device through its public WAN port.

The system contains an MGCP, SIP and H.323 call control proxy ALG. VoIP phones and client adapters have to be configured to point to the system, which serves as a call control server, proxy, gatekeeper or gateway.

For corporate customers with high-end routers and firewalls, the system can be configured as a VoIP Application Layer Gateway only. This allows all of the normal data traffic to continue to be handled by the existing network devices, and voice/video traffic to be handled by the system. For this configuration, the system WAN Ethernet port is connected to the internet. The system LAN Ethernet port is connected to a port on the desired LAN

Ethernet switch. The system can reside on one subnet and be accessed by VoIP devices on other subnets through the router.

Alias Manipulation and Prefix Routing

Alias manipulation and prefix routing both make use of regular expressions to match a particular string in an alias and act on that match.

Alias manipulation is done immediately when a message (for example, an Automatic Repeat reQuest or ARQ, Location Request or LRQ, or a Setup) is received. Any matching pattern is replaced with a given string. All normal call look-up is done after the alias manipulation stage. This allows you to replace characters or strings that are hard or impossible to dial on certain endpoints. For example, in order to accomplish Annex O style dialing on an endpoint that cannot enter the '@' and/or the '.' character, you can create the following rules

Pattern Replace

* .

@

(Note that '*' has a special meaning in regular expressions and therefore must be escaped with a preceding '\'.)

Prefix routing is similar but here the regular expression determines where to send a matching alias. This call decision is done after the alias manipulation and is therefore acting on the modified string similar to other call lookup processes (for example, look-up of registered clients). H.323 prefixes can be used to route calls based on a matching prefix in the destination alias of the call. Each prefix is associated with a domain name or IP address to send the call to in case the prefix matches.

Regular Expressions and Expression Examples

Alias manipulation patterns and prefixes use regular expressions to match a string in the destination alias. A regular expression can be a string of literal characters to match or a number of special expressions.

Alias manipulation patterns can match a sub-string anywhere and multiple times within the alias. Prefixes are always searched from the left of the alias and cannot match a middle part or the end of the alias. Table 6-1 describes supported expressions.

Table 6-1 Regular Expressions

Symbol	Description
.	Matches any single character.
[ ]	Matches any single character listed between the [ ]. For example, [abc], [123]. If the characters are separated by a -, all characters between the two are matching, for example [a-z], [0-9]
( )	Matches the literal string given, for example (abc).
|	Matches the block on either side of the |, for example a **|** b.
?	Matches 0 or 1 of the preceding block.
*	Matches 0 or more of the preceding block.
+	Matches 1 or more of the preceding block.
\	Escapes the special meaning of the next character.
{a}	Matches exactly 'a' numbers of the preceding block.
{a,}	Matches 'a' or more of the preceding block.
{a,b}	Matches between 'a' and 'b' (inclusive) of the preceding block.
$	Matches the end of the alias.

Table 6-2 describes example expressions.

Table 6-2 Regular Expression Examples

Expression	Description
100	Matches the string 100.
(555)?123	Matches 555123 or 123.
(408|555)	Matches 408 or 555.
555[0-9]{3}	Matches 555 followed by exactly 3 digits.
#	Matches the character '#'.
*	Matches the character '*'. Note that '*' by itself is a regular expression and must therefore be escaped with a '\' to match the character itself.
[a-z]{1,30}@ example.net$	Matches from one to thirty lower-case letters followed by @example.net.

SIP Trunking

If an enterprise has multiple offices with associated PBXs in geographically separated locations, the EdgeMarc can help provide lower cost service between the offices.

For multiple office connection support, an EdgeMarc is installed with each PBX. As in the single office case, the PBXs provide local call processing. However, calls between the different offices are handled through the service provider, rather than through the PSTN. The process employs SIP trunking to make connections through the service provider's IP network. SIP handles the call set-up, control, and disconnect between PBXs.



Note
With SIP trunking, it may still be desirable to keep a single FXO port connected to the PSTN to support Survivability.

SIP trunking is used to configure dial-plans or rules to route calls to and from the softswitch/IP-PBX to client devices that do not register. A number of trunking devices are configured and rules are set up to route calls from the softswitch/IP-PBX to these devices (Inbound rules), manipulate dial strings in calls from these devices to a softswitch/IP-PBX (Outbound rules), or redirect calls from other local devices to these trunking devices without routing the call to the softswitch/IP-PBX first (Redirect rules).

Each rule contains matching criteria for how to match the calls and points to a target trunking device that the call should be routed to (for Inbound and Redirect rules) or trunking device that the rule should be applied to (for Outbound rules).

When an incoming softswitch/IP-PBX SIP message is received, it is always matched against the list of currently registered clients first. If no registered client matches the destination of the call, these rules are tried. If a rule matches, the device that the rule points to will receive the call. If no rule matches, a configured default rule (if any) is used to match the call.



Tip
Messages from SIP clients (including trunking devices) are always forwarded to the SIP ALG configured softswitch/IP-PBX unless there is a matching redirect rule.

Dial String Manipulation

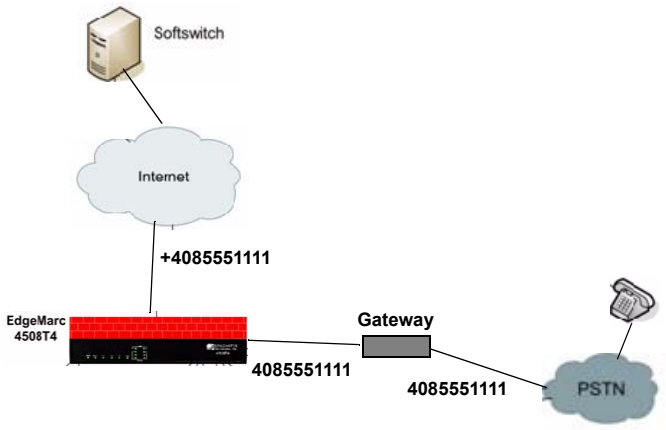
Outbound SIP trunking rules support dial string manipulation for outbound calls sent to a network softswitch. Outbound rules allow a gateway to direct calls through the EdgeMarc to a softswitch using appropriate dialing conventions, even if the gateway itself does not support the required conventions.

For example, if a softswitch requires use of a + sign that is not normally supported by a particular gateway, you can define an outbound SIP

trunking rule that appends a + sign to outbound calls that come from the gateway.

Figure 6-1 shows how the SIP trunking rule works. A call comes in from the PSTN through a gateway to the EdgeMarc. The gateway does not support + dialing, so the EdgeMarc applies an outbound SIP trunking rule to prepend a + sign before forwarding the call to the softswitch.

Figure 6-1 Outbound Dial String Manipulation



If you assign a particular gateway to multiple outbound SIP trunking rules. The EdgeMarc applies the first matching rule that applies to that gateway.

Priority Redirection

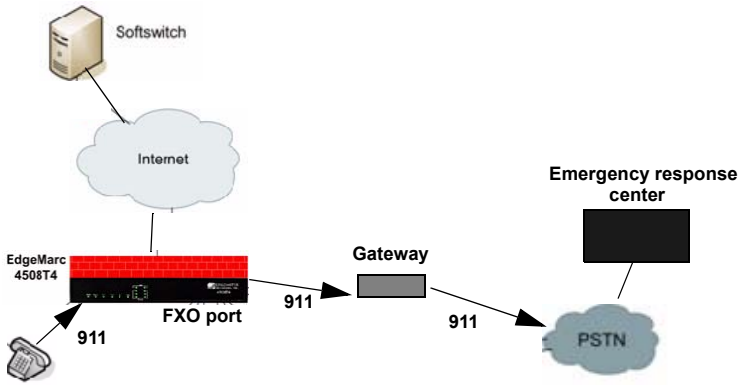
You can apply SIP trunking rules to redirect local calls through any of the FXO ports on the EdgeMarc to a matching trunking device without having to direct the call to a network softswitch. Any call that matches a specified pattern is automatically routed to a specified gateway, thereby bypassing the network softswitch.

You can also tag redirection rules as having a priority designation. If a priority-tagged call comes in while all FXO ports are in use with non-priority calls, one of the in-progress calls is dropped and the priority call is connected. Priority calls do not interrupt other priority calls, however.

Priority redirection can be used to improve handling of 911 calls, as shown in Figure 6-2. If a SIP trunking rule is defined for 911 pattern match and tagged as priority, then a local 911 call is sent directly from the local phone through an FXO port on the EdgeMarc to the designated gateway. If all FXO ports are in use and at least one of the ports is not tagged for priority, then a non-priority call is dropped and the 911 call is connected.

Priority redirection can help emergency responders speed identification of a caller's location.

Figure 6-2 Priority Redirection



Note
Priority calls do not support dial string manipulation. They must be sent through as-is.

Configuring VoIP ALG Settings

Note
VoIP ALG requires that a SIP server is configured on the system. See Configuring SIP Settings for support information.

1. Choose **VoIP** from the Configuration menu (Figure 7).
2. Configure settings using the information in Table 6-3 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Figure 7 VoIP Configuration Page

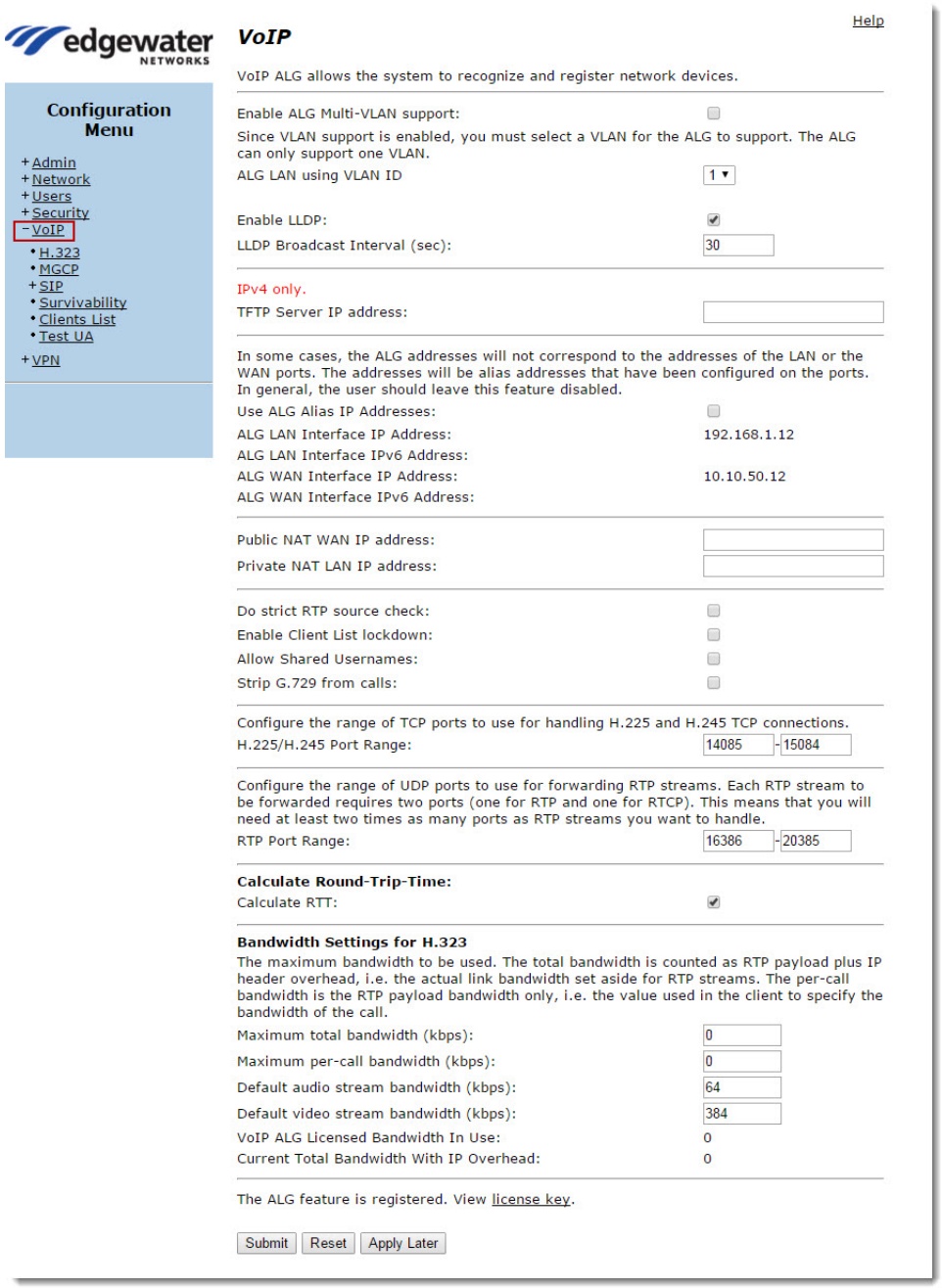


Table 6-3 VoIP ALG Parameters

Item	Description
Enable ALG Multi-VLAN support	Select the **Enable ALG Multi-VLAN support** checkbox to supporting Multiple VLANs with certificate for VLANs.
ALG LAN using VLAN ID	If VLAN support is enabled, you must select a VLAN for the ALG to support. Choose an option from the **ALG LAN using VLAN ID** drop-down list. The ALG can only support one VLAN. This feature allows the system to recognize and register a network appliance before it presents the IP telephone or data device through its public WAN port.
Enable LLDP	Select the **Enable LLDP** checkbox to allow the Application Layer Gateway (ALG) to use the Link Layer Discovery Protocol (LLDP) to send periodic broadcasts to advertise information about the sending device.
LLDP Broadcast Interval	Enter the interval in seconds between each LLDP frame information broadcast.
TFTP server IP address	Enter the TFTP IPv4 server address to allow the system to act as a TFTP server providing subsequent configuration information to other VoIP phones or devices.
ALG Settings	
Use ALG Alias IP Address	Select the **Enable ALG IP Addressing** checkbox and choose one of the following based on your system configuration: ■ ALG LAN Interface IP Address (IPv4) ■ ALG LAN Interface IPv6 Address ■ ALG WAN Interface IP Address (IPv4) ■ ALG WAN Interface IPv6 Address **Note:** In some cases, the ALG addresses do not correspond to the addresses of the LAN or the WAN ports. The addresses are alias addresses that have been configured on the ports. In general, you should leave this feature disabled.
ALG LAN Interface IP Address	Enter the IPv4 address on the LAN that endpoints communicate with. Generally, this is the same as the LAN IP address
ALG LAN Interface IPv6 Address	Enter the IPv6 address on the LAN that endpoints communicate with.

Table 6-3 VoIP ALG Parameters (continued)

Item	Description
ALG WAN Interface IP Address	Enter the IPv4 address on the WAN that communicates with the softswitch. Generally, this is the same as the WAN IP address.
ALG WAN Interface IPv6 Address	Enter the IPv6 address on the WAN that communicates with the softswitch
NAT Addressing	
Configure public and private NAT addressing.	
Public NAT WAN IP address	Enter the public IPv4 address the perimeter security appliance provides for static one-to-one mapping: Public NAT Subscriber IP address—The public IPv4 address that the perimeter security appliance provides for static one-to-one mapping. This allows incoming traffic to the public IP to be translated to the system internal IP. This is typically called a private demilitarized zone (DMZ) which allows devices in this DMZ to be configured with a private RFC 1918 address. The NAT configuration must be a Public IPv4 address configured for a one-to-one NAT translation without any port-mapping to the Video Border Proxy (VBP)-E internal DMZ WAN IPv4 address.
Private NAT LAN IP address	Enter the private IPv4 address the perimeter security appliance provides for static one-to-one mapping. This allows incoming traffic to the private IP to be translated to the system internal IP. This is typically called a private DMZ which allows devices in this DMZ to be configured with a specific DMZ internal address. The NAT configuration must be an IPv4 address configured for a one-to-one NAT translation to the VBP-E internal DMZ LAN IPv4 address. Typically, this interface is not placed in a NAT environment but can be used in advanced security scenarios.

Table 6-3 VoIP ALG Parameters (continued)

Item	Description
Private NAT Provider IP address	Enter the private IPv4 address the perimeter security appliance provides for static one-to-one mapping. This allows incoming traffic to the private IP to be translated to the system internal IP. This is typically called a private DMZ which allows devices in this DMZ to be configured with a specific DMZ internal address. The NAT configuration must be an IPv4 address configured for a one-to-one NAT translation to the VBP-ST internal DMZ Provider IPv4 address. Typically, this interface is not placed in a NAT environment but can be used in advanced security scenarios.
Public NAT Subscriber IP address	Enter the public IPv4 address the perimeter security appliance provides for static one-to-one mapping. This allows incoming traffic to the public IP to be translated to the system internal IP. This is typically called a private DMZ which allows devices in this DMZ to be configured with a private RFC 1918 address. The NAT configuration must be a public IPv4 address configured for a one-to-one NAT translation without any port-mapping to the VBP-ST internal DMZ Subscriber IPv4 address.
Do strict RTP source check	Select the **Do Strict RTP Source Check** checkbox to protect against specific Real-time Transport Protocol (RTP)-based denial-of-service attacks and controls address network based gateways that periodically continue to send an RTP stream after a call ends. If the source of an inbound RTP stream does not match the IP address and port for an existing outbound RTP stream, it is assumed that the inbound stream is “rogue RTP.” When rogue RTP is detected, a syslog message is generated and the inbound stream is dropped.
Enable Client List lockdown	Select the **Enable Client List Lockdown** checkbox to prevent new clients from registering. **Tip:** You must first configure the Client List. Choose **VoIP** > **Client List** and refer to Configuring the Clients List. **Caution:** Do not use Client List Lockdown and Allow Shared Usernames at the same time.

Table 6-3 VoIP ALG Parameters (continued)

Item	Description
Allow Shared Usernames	Select the **Allow Shared Username** checkbox to allow multiple clients to register using the same username. A new entry and a unique contact field are generated for each client. **Caution:** Do not use Client List Lockdown and Allow Shared Usernames at the same time; new phones using an existing username will not be added to the Clients List and will fail to work.
Strip G.729 from calls	Select the **Strip G.729 From Calls** checkbox to improve codec compatibility for legacy and newer networks by removing all references to the G.729 in codec lists for calls made using SIP and MGCP. The codecs in the signaling protocols are listed in the session description protocol (SDP). When you enable the G.729 feature, the codecs are removed from the SDP.
TCP Port Range Configure the range of TCP ports to use for handling H.225 and H.245 TCP connections. Specifies the range of Transmission Control Protocol (TCP) ports to use for handling H.225 and H.245 TCP connections. If there is a firewall in front of the system, that firewall must allow TCP connections to this range to reach this system. A smaller range means that less ports must be opened on the firewall; however, each H.323 call may require up to 3 ports each and if the range is too small, the number of H.323 calls that the system can process may be restricted. Port numbers specified are inclusive: Range is 10000 to 65535, default values are 14085 to 15084. The range must contain a minimum of 999 ports.	

Table 6-3 VoIP ALG Parameters (continued)

Item	Description
RTP Port Range	Configure an RTP port range for non-translated RTP MOS scoring and traffic shaping. This licensed option allows you to MOS score a non-SIP call and prioritize traffic over these ports to the far end. Without this setting, voice traffic over the IPsec VPN tunnel will not be prioritized and you may experience choppy audio. Port numbers specified are inclusive and are limited and checked against the platform the licensed number of calls allowed. The minimum number of ports required is two times the number of licensed streams or the Call Admission Control (CAC) value from the Traffic Shaping page, whichever is smaller. Choose **Network** > **Traffic Shaper** and refer to Configuring Traffic Shaping in Chapter 3, *Network Deployment*. While the minimum number of ports is two per stream, some endpoints may open multiple streams. For H.323 calls, the number of ports per call depends on the number of individual RTP streams the endpoints may use. In some cases, an H.323 client may request a separate stream for video, audio, content sharing, and data/camera control. In that case, eight ports are needed per H.323 endpoint. Enter ports to be scored as comma-separated port numbers or ranges of port numbers. For example: 2000,30000-32000,40002,45000-46000 **Note:** This option is available only on some versions of VOS with a special license.
Calculate Round-Trip-Time	Enables Round-Trip-Time (RTT) calculation. RTCP packets, LSR, and DLSR values are used to calculate an RTT value for each RTP stream. RTCP packets can be sent on behalf of phones if they do not send RTCP themselves.
Calculate Round-Trip-Time	Select the **Calculate RTT** checkbox to enable the feature.

Table 6-3 VoIP ALG Parameters (continued)

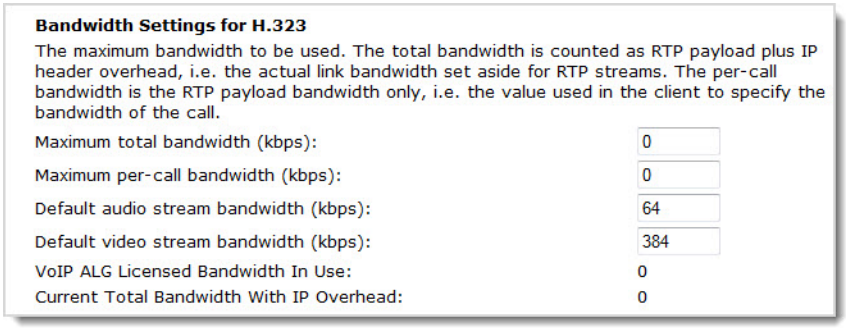
Item	Description
Bandwidth Settings for H.323	The maximum bandwidth to be used. The total bandwidth is counted as RTP payload plus IP header overhead, for example, the actual link bandwidth set aside for RTP streams. The per-call bandwidth is the RTP payload bandwidth only, for example, the value used in the client to specify the bandwidth of the call. See Configuring Bandwidth Settings for H.323.
ALG registration	Displays current ALG registration status. The registration status for the ALG feature is displayed to ensure that the feature is enabled. If the feature is not registered, no calls will be allowed to pass. **Note:** The ALG registration code is available on a sticker on the bottom of the device or from your service provider. To view your license key, click the **license key** link provided to access the License page or choose **Admin** from the Configuration Menu and click the **license key** link in Registration Status. Refer to Managing the License Key in Chapter 2, *System Administration*.

3. Proceed to Configuring Bandwidth Settings for H.323.

Configuring Bandwidth Settings for H.323

1. Choose **VoIP** from the Configuration Menu (Figure 7).
2. Scroll to **Bandwidth Settings for H.323** (Figure 6-1).

Figure 6-1 VoIP Configuration Page - Bandwidth Settings for H.323



3. Configure bandwidth settings using the information in Table 6-4 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 6-4 VoIP ALG Parameters- H.323 Bandwidth Settings

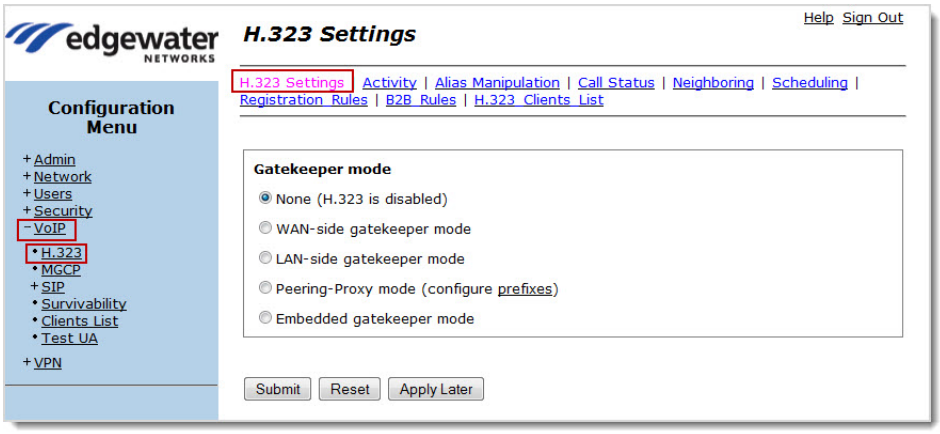
Item	Description
Bandwidth Settings for H.323	
Maximum total bandwidth (kbps)	Enter the maximum available bandwidth. Bandwidth includes the RTF payload plus the IP header overhead. If the bandwidth is set to 0, bandwidth management is not enforced Only calls with media traversing the system is counted towards the bandwidth maximum. This number applies to the total bandwidth maximum (payload + overhead); the actual payload amount allowed through is 20% lower than this number. For example, if Maximum Bandwidth is set to 1000k, only 800k of actual voice/video is allowed through.
Maximum per-call bandwidth (kbps)	Enter the maximum available per call bandwidth, which is the bandwidth available for the RTP payload (value that the client uses to specify call bandwidth). The IP overhead is not specified here, but rather the value used in an H.323 endpoint when making a call.
Default audio stream bandwidth (kbps)	Enter the bandwidth available for streaming audio traffic when an endpoint does not specify the call bandwidth in the SDP.
Default video stream bandwidth (kbps)	Enter the bandwidth available for streaming video traffic when an endpoint does not specify the call bandwidth in the SDP.
VoIP ALG Licensed Bandwidth In Use	Displays the sum of RTP payloads of all current calls. For example, if two 384k calls are present, this field displays 768. The system uses the field to subtract against the system licensed value as Video Bandwidth in the license key page.
Current Total Bandwidth With IP Overhead	Displays the RTP payload of current calls and add the estimated IP overhead. Use this value to budget the requirements for video traversing the customer WAN connection. The value is calculated by the RTP payload divided by .8 to add the IP overhead use to the total. For example, 384k/.8 = 480k of estimated bandwidth usage.

Click **Submit** to apply your changes.

Configuring H.323 Settings

1. Choose **VoIP** > **H.323** (Figure 6-2).

Figure 6-2 H.323 Settings Page



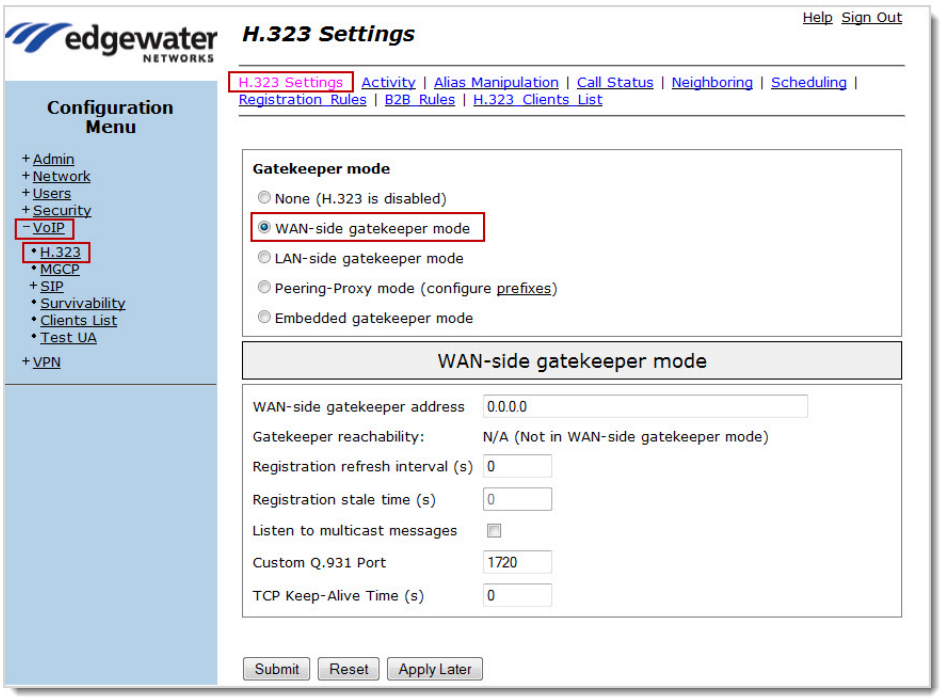
Note
The **None** radio button in the Gatekeeper mode window is selected by default: H.323 processing is disabled.

2. Select a gatekeeper mode by clicking a radio button to activate configuration fields and refer to the following:
   - Configuring WAN/Provider-Side Gatekeeper Mode Settings
   - Configuring LAN/Subscriber-Side Gatekeeper Mode Settings
   - Configuring Peering-Proxy Mode Settings
   - Configuring Embedded Gatekeeper Mode Settings

Configuring WAN/Provider-Side Gatekeeper Mode Settings

1. Choose **VoIP** > **H.323** (Figure 6-2).
2. Click the **WAN/Provider-side gatekeeper mode** radio button in the Gatekeeper Mode window. The WAN/Provider-side gatekeeper mode settings fields become active (Figure 6-3).

Figure 6-3 H.323 Settings - WAN/Provider-Side Gatekeeper Mode



3. Configure settings using the information in Table 6-5 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 6-5 WAN/Provider-Side Gatekeeper Mode Parameters

Item	Description
WAN/Provider-Side Gatekeeper Mode	
Allows LAN side devices to forward H.323 Remote Access Services (RAS) and Q.931 signaling messages to a WAN gatekeeper for registration and call processing. Use this mode when designing a centralized gatekeeper solution in which the headquarters location provides the H.323 gatekeeper functionality; all remote locations can deploy the system configured for WAN-side gatekeeper to the headquarters location for call control. H.323 registration and call setup messages are processed by the headquarters gatekeeper, while the RTP media takes the shortest and most direct path between the two WAN-side gatekeeper locations.	
WAN/Provider-side GK address	Enter the IPv4 or IPv6 address of the WAN gatekeeper to which client messaging will be forwarded for registration and call control.
Gatekeeper reachability	Displays whether the gatekeeper specified can be reached.
Registration refresh interval	Enter the registration refresh interval or time to live (TTL) field in the RAS RCF message sent to the LAN side client. The client sends keepalive registrations to reset the gatekeeper client entry from becoming stale and being deleted from the gatekeeper Clients List. Endpoints typically send a keep-alive registration before this value. For example, if you enter 30 seconds, most endpoints will send a keep-alive registration at 29 seconds or as early as 19 seconds. The endpoint keepalive registration interval minus the value set in this field can vary depending on the endpoint vendor. The default value of 0 is used to pass through the original value set from the WAN side gatekeeper. Most WAN side gatekeepers set the TTL field to 300 seconds when deploying the system in WAN-side gatekeeper mode.

Table 6-5 WAN/Provider-Side Gatekeeper Mode Parameters (continued)

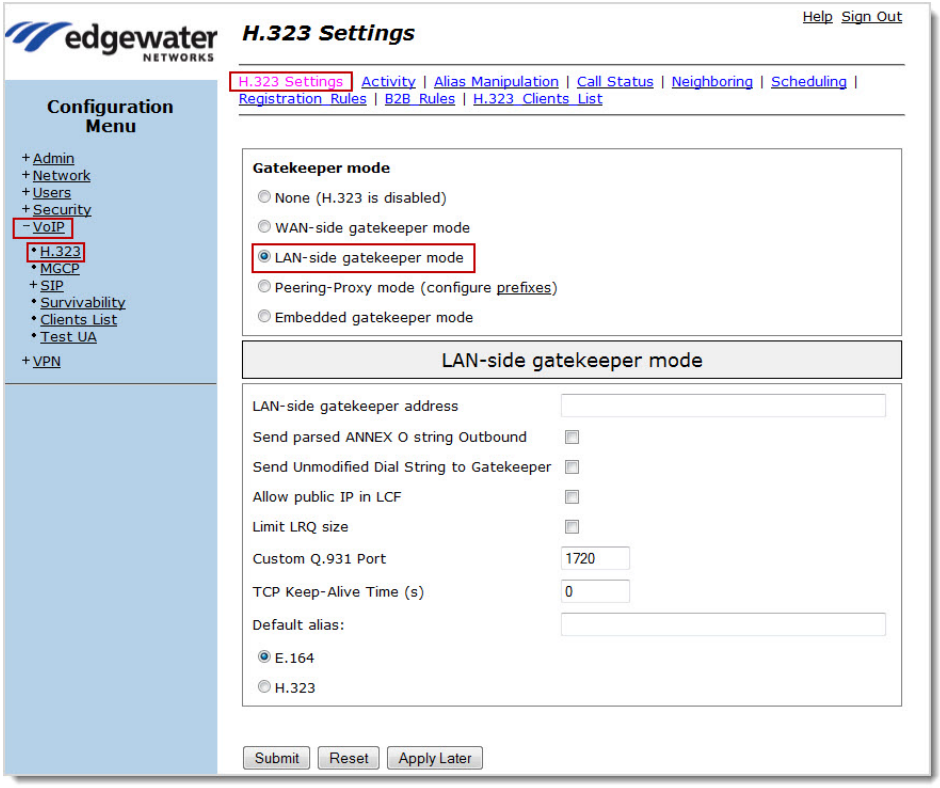
Item	Description
Registration stale time	Enter the time a client entry is valid on the system. Each LAN side endpoint has a system client list entry with activity timers to determine if the client is actively sending keepalive registration messages. When a LAN side client fails to update its registration entry on the system within the time specified in this field, the system removes the client from the H.323 Clients List and sends an unregistration request (URQ) to the WAN side gatekeeper.
Listen to multicast messages	Select the **Listen to multicast messages** checkbox to enable the system LAN side UDP 1718 multicast listener for gatekeeper discovery and registration procedures described in H.225.0.
Custom Q.931 Port	Enter the port that will be returned in Admission Confirm (ACF) messages. If no Custom Q.931 port is set, the default port of 1720 is used. Remote NAT devices can intercept H.323 messages and modify these messages which results in call failure. Changing the TCP call setup port to something other than TCP 1720 can help with call completion in these cases. For example, modifying this field to port 5000 modifies the RCF message to instruct the registered WAN side clients to use this port for call signaling. TCP 1720 will still be a system listening port for B2B calls. **Note:** Ensure the alternate port is not being used for other services.
TCP Keep-Alive Time	Enter the time in seconds between TCP keep-alive messages. If this value is zero, no keep-alive messages are sent. If no response is received, the TCP stack assumes the connected endpoint is no longer listening, and ends the connection. This field sends TCP keepalives to clients connected to the systems well known TCP 1720 port. Default is 0 (disabled); the minimum setting is 120 seconds.

Click **Submit** to apply your changes.

Configuring LAN/Subscriber-Side Gatekeeper Mode Settings

1. Choose **VoIP** > **H.323** (Figure 6-2).
2. Click the **LAN/Subscriber-side gatekeeper mode** radio button. The LAN/Subscriber-side gatekeeper mode fields become active (Figure 6-4).

Figure 6-4 H.323 Settings - LAN/Subscriber-Side Gatekeeper Mode



3. Configure settings using the information in Table 6-6 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 6-6 LAN/Subscriber-Side Gatekeeper Mode Parameters

Item	Description
LAN/Subscriber-Side Gatekeeper Mode	
Allows WAN side H.460/H.323 clients to proxy register and provide H.460 traversal methods to the system WAN interface. The system forwards all RAS and Q.931 messages to the LAN gatekeeper for registration and call control. The system maintains an H.323 client list for all WAN side devices that have been registered by the LAN gatekeeper. Also allows B2B calls to proxy through to the LAN gatekeeper for call processing. Certain LAN gatekeepers can be configured to forward offnet or public IP or ANNEX O (URI-Dialing) WAN-side destination calls for B2B calling.	
LAN/Subscriber-side GK address	Enter the IPv4, IPv6, or FQDN address of the LAN gatekeeper that all client messaging is forwarded to for registration and call control.
Send parsed ANNEX O string Outbound	Select the **Send parsed ANNEX O string Outbound** checkbox to remove the host portion of the destination address. For example, when the incoming destination address from the LAN is formatted as a H.323 URL 1234@example.com, the outgoing destination address will be parsed and sent as dialedDigits 1234 to the resolved example.com host address.
Send Unmodified Dial String to Gatekeeper	Select the **Send Unmodified Dial String to Gatekeeper** checkbox to forward all destination address information to the LAN gatekeeper unmodified. For example, when the incoming destination address to the WAN is 9876@example.com, the system forwards this destination address to the LAN gatekeeper unmodified as 9876@example.com. When this option is not used, the host portion is stripped off and is forwarded to the LAN gatekeeper as destination address 9876. **Note:** If the host part of the Annex O address resolves to the LAN gatekeeper device, routing loops can occur. When this option is selected, ensure the gatekeeper receiving the full ANNEX O string is properly configured and capable of receiving the full destination unresolved ANNEX O address. Some older gatekeepers cannot receive this unresolved string and the call will fail.

Table 6-6 LAN/Subscriber-Side Gatekeeper Mode Parameters (continued)

Item	Description
Allow public IP in LCF	(Optional) Select the **Allow public IP in LCF** checkbox to allow public IP addresses to be returned in an LCF. This option should usually not be enabled. When this option is set, the system does not ALG the address in the Location_Confirm (LCF) to the system WAN IP. This allows the public IP WAN gatekeeper to send call setup directly to the public IP of the LAN gatekeeper. By allowing public IP addresses to be returned in an LCF, the gatekeeper may be able to do more complex policy decisions. This field should usually not be enabled; only use when the system has public IPs on both the WAN and LAN interfaces.
Limit LRQ size	Decreases the TTL in the LCF to prevent LCF looping when **Allow public IP in LCF** is enabled.
Custom Q.931 Port	Sets the port returned in Admission Confirm (ACF) messages. If no Custom Q.931 port is set, the default port of 1720 is used. Remote NAT devices can intercept H.323 messages and modify these messages which results in call failure. Changing the TCP call setup port to something other than TCP 1720 can help with call completion in these cases. For example, modifying this field to port 5000 modifies the RCF message to instruct the registered WAN side clients to use this port for call signaling. TCP 1720 will still be a system listening port for B2B calls. **Note:** Ensure the alternate port is not being used for other services.
TCP Keep-Alive Time	Enter the time in seconds between TCP keep-alive messages. If this value is zero, no keep-alive messages are sent. If no response is received, the TCP stack assumes the connected endpoint is no longer listening, and ends the connection. This field sends TCP keepalives to clients connected to the systems well known TCP 1720 port. Default is 0 (disabled); the minimum setting is 120 seconds.

Table 6-6 LAN/Subscriber-Side Gatekeeper Mode Parameters (continued)

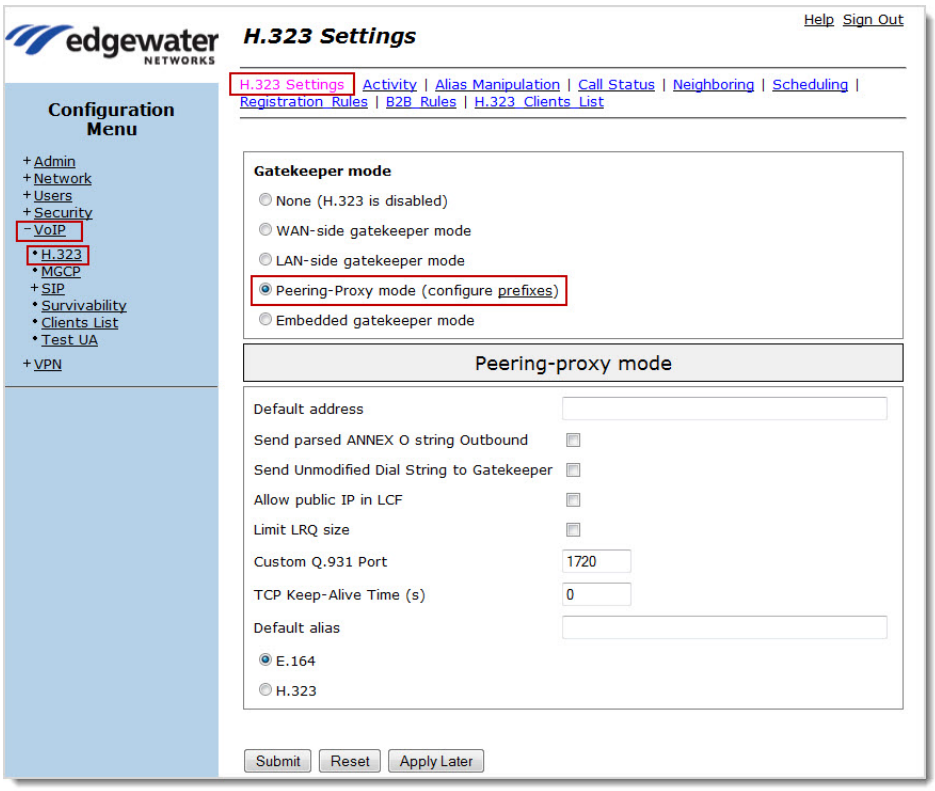
Item	Description
Default Alias	Select a default alias to be added to incoming calls without a destination message in the Q.931 Setup message: ■ E.164 ■ H.323 This alias allows the embedded gatekeeper or a LAN/Subscriber-side gatekeeper to route the call to a default endpoint. For example, when a B2B call is placed to the system and the user only dialed the IP or FQDN of the WAN interface, the system adds this alias to the H.323 call setup message and forwards it to the LAN gatekeeper for call processing. This alias can be any alias actively registered to the LAN gatekeeper. You may add a H.323 static client in the H.323 Clients List and configure this client as the default alias. The static H.323 client should be locked to prevent the client entry from being deleted. A typical configuration scenario is to configure this field with an MCU IVR alias or a default MCU meeting room alias. Default is E.164, no alias is set.

Click **Submit** to apply your changes.

Configuring Peering-Proxy Mode Settings

1. Choose **VoIP** > **H.323** (Figure 6-2).
2. Click the **Peering-Proxy mode (configure prefixes)** radio button. The Peering-Proxy mode fields become active (Figure 6-5)

Figure 6-5 H.323 Settings - Peering-Proxy Mode



3. Configure settings using the information in Table 6-7 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 6-7 Peering-Proxy Mode Parameters

Item	Description
Peering-Proxy mode	
Provides call routing for inbound calls to the WAN interface with configured prefixes when the Default Address is not set. The system relies on prefix routing to forward the call to the LAN side destination. With no prefixes configured, the system only forwards LAN to WAN calls with ANNEX O destinations. This mode is typically deployed in networks with multiple internal NAT boundaries to provide prefix routing between gatekeeper zones. Click the **configure prefixes** link or click **Neighboring** in the navigation panel at the top of the H.323 Settings page and refer to Configuring Peering-Proxy Mode Settings. When you have finished configuring prefixes on the H.323 Neighboring page, return to the H.323 Settings page by clicking **H.323 Settings** in the navigation panel at the top of the H.323 Neighboring page.	
Default Address	Enter the IPv4, IPv6, or FQDN address of the default location that all client messaging is forwarded to on the LAN side.
Send parsed ANNEX O string Outbound	Select the **Send parsed ANNEX O string Outbound** checkbox to remove the host portion of the destination address. For example, when the incoming destination address from the LAN is formatted as a H.323 URL 1234@example.com, the outgoing destination address will be parsed and sent as dialedDigits 1234 to the resolved example.com host address.

Table 6-7 Peering-Proxy Mode Parameters (continued)

Item	Description
Send Unmodified Dial String to Gatekeeper	Select the **Send Unmodified Dial String to Gatekeeper** checkbox to forward all destination address information to the LAN gatekeeper unmodified. For example, when the incoming destination address to the WAN is 9876@example.com, the system forwards this destination address to the LAN gatekeeper unmodified as 9876@example.com. When this option is not used, the host portion is stripped off and is forwarded to the LAN gatekeeper as destination address 9876. **Note:** If the host part of the Annex O address resolves to the LAN gatekeeper device, routing loops can occur. When this option is selected, ensure the gatekeeper receiving the full ANNEX O string is properly configured and capable of receiving the full destination unresolved ANNEX O address. Some older gatekeepers cannot receive this unresolved string and the call will fail.
Allow public IP in LCF	(Optional) Select the **Allow public IP in LCF** checkbox to allow public IP addresses to be returned in an LCF. This option should usually not be enabled. When this option is set, the system does not ALG the address in the Location Confirm (LCF) to the system WAN IP. This allows the public IP WAN gatekeeper to send call setup directly to the public IP of the LAN gatekeeper. By allowing public IP addresses to be returned in an LCF, the gatekeeper may be able to do more complex policy decisions. This field should usually not be enabled; only use when the system has public IPs on both the WAN and LAN interfaces.
Limit LRQ size	Decreases the TTL in the LCF to prevent LCF looping when **Allow public IP in LCF** is enabled.

Table 6-7 Peering-Proxy Mode Parameters (continued)

Item	Description
Custom Q.931 Port	Sets the port returned in Admission Confirm (ACF) messages. If no Custom Q.931 port is set, the default port of 1720 is used. Remote NAT devices can intercept H.323 messages and modify these messages which results in call failure. Changing the TCP call setup port to something other than TCP 1720 can help with call completion in these cases. For example, modifying this field to port 5000 modifies the RCF message to instruct the registered WAN side clients to use this port for call signaling. TCP 1720 will still be a system listening port for B2B calls. **Note:** Ensure the alternate port is not being used for other services.
TCP Keep-Alive Time	Enables TCP keep-alive messages and sets the interval between messages in seconds. If this value is zero, no keep-alive messages are sent. If no response is received, the TCP stack assumes the connected endpoint is no longer listening, and ends the connection. This field sends TCP keepalives to clients connected to the systems well known TCP 1720 port. Default is 0 (disabled); the minimum setting is 120 seconds.

Table 6-7 Peering-Proxy Mode Parameters (continued)

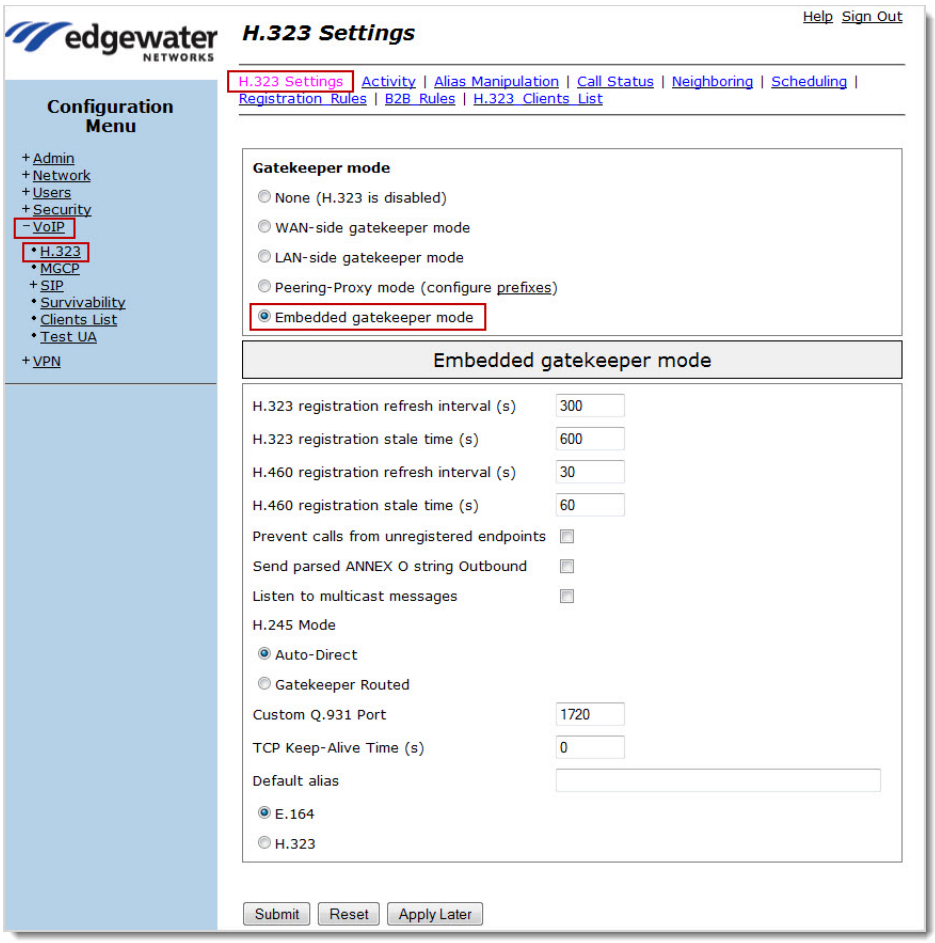
Item	Description
Default Alias	Enter a default alias to be added to incoming calls without a destination message in the Q.931 Setup message: ■ E.164 ■ H.323 This alias allows the embedded gatekeeper or a LAN/Subscriber-side gatekeeper to route the call to a default endpoint. For example, when a B2B call is placed to the system and the user only dialed the IP or FQDN of the WAN interface, the system adds this alias to the H.323 call setup message and forwards it to the LAN gatekeeper for call processing. This alias can be any alias actively registered to the LAN gatekeeper. You may add a H.323 static client in the H.323 Clients List and configure this client as the default alias. The static H.323 client should be locked to prevent the client entry from being deleted. A typical configuration scenario is to configure this field with an MCU IVR alias or a default MCU meeting room alias. Default is E.164, no alias is set.

Click **Submit** to apply your changes.

Configuring Embedded Gatekeeper Mode Settings

1. Choose **VoIP** > **H.323 Settings** (Figure 6-2).
2. Click the **Embedded gatekeeper mode** radio button. The Embedded gatekeeper mode fields become active (Figure 6-6).

Figure 6-6 H.323 Settings - Embedded Gatekeeper Mode



3. Configure settings using the information in Table 6-8 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 6-8 Embedded Gatekeeper Mode Parameters

Item	Description
Embedded Gatekeeper Mode	
Allows the system to act as the gatekeeper for WAN and LAN side devices. All WAN or LAN RAS, Q.931, and H.245 messages are processed by the system.	
H.323 registration refresh interval	Enter the registration refresh interval or TTL field in the RAS RCF message sent to the WAN or LAN side H.323 client. The client sends keepalive registrations to reset the gatekeeper client entry from becoming stale and being deleted from the gatekeeper Clients List. Endpoints typically send a keepalive registration before this value. For example, if you enter 300 seconds, most endpoints will send a keepalive registration at 299 seconds or as soon as 199 seconds. The endpoints keepalive registration interval minus the value set in this field can vary depending on the endpoint vendor. Range is 30 to 9999 seconds, default is 300.
H.323 registration stale time	Enter the time a H.323 client entry is valid on the system. Each WAN or LAN side registered H.323 endpoint has a H.323 Clients List entry with registration activity timers to determine if the client is actively sending keepalive registrations messages. When a WAN side client fails to update its registration entry on the system within the time specified in this field, the system removes the client from the H.323 Clients List. The default range for this timer is two times the H.323 registration refresh interval to 9999. For example, when the H.323 registration refresh interval is set to 300, the range for the H.323 registration stale time is 600 to 9999. Default is 600.

Table 6-8 Embedded Gatekeeper Mode Parameters (continued)

Item	Description
H.460 registration refresh interval	Enter the registration refresh interval for the TTL field in the RAS RCF message sent to the WAN side H.460 client. The client sends keepalive registrations to reset the gatekeeper client entry from becoming stale and being deleted from the gatekeeper Clients List. Endpoints typically send a keepalive registration prior to this value. For example, if you enter 30 seconds, most endpoints will send a keepalive registration at 29 seconds and as soon as 19 seconds. The endpoints keepalive registration interval minus the value set in this field can vary depending on the endpoint vendor. Range is 30 is 9999 seconds, default is 30.
H.460 registration stale time	Enter the time an H.460 client entry is valid on the system. Each WAN side registered H.460 endpoint has a H.323 Clients List entry with registration activity timers to determine if the client is actively sending keepalive registrations messages. When a WAN side H.460 client fails to update its registration entry on the system within the time specified in this field, the system removes the client from the H.323 Clients List. The default range for this timer is two times the H.460 registration refresh interval to 9999. For example, when the H.460 registration refresh interval is set to 30, the range for the H.460 registration stale time is 60 to 9999.
Prevent calls from unregistered endpoints	Select the **Prevent calls from unregistered endpoints** checkbox to block unregistered LAN-side endpoints from making calls through the device. Calls can still be made from registered clients to unregistered endpoints. Default is disabled.

Table 6-8 Embedded Gatekeeper Mode Parameters (continued)

Item	Description
Send parsed ANNEX O string Outbound	Select the **Send parsed ANNEX O string Outbound** checkbox so that outbound LAN to WAN Annex O calls will have the host part of the destination address removed. For example, when the incoming destination address from the LAN is formatted as a H.323 URL 1234@example.com, the outgoing destination address will be parsed and sent as dialedDigits 1234 to the resolved example.com host address.
Multicast Messages	Select the **Multicast Messages** checkbox to enable the system LAN side UDP 1718 multicast listener for gatekeeper discovery and registration procedures described in H.225.0.

Table 6-8 Embedded Gatekeeper Mode Parameters (continued)

Item	Description
H.245 Mode	Enables firewall traversal support by conveying information needed for multimedia communication, such as encryption, flow control, jitter management, preference requests, as well as opening and closing logical channels used to carry media streams. It also defines separate send and receive capabilities and the means to send these details to other devices that support H.323: ■ Auto-Direct—Auto-Direct mode allows the system to determine if the WAN or LAN call model needs to be routed or direct. When two H.323 registered LAN clients place a call to each other, the call model is direct. H.460 WAN clients placing calls will always use a routed call model for signaling and RTP media traversal. If the solution includes two remote locations configured for WAN-side gatekeeper mode or if two public WAN H.323 clients are registered to the system and call each other then, the Embedded gatekeeper allows a direct call signaling model and shortest path RTP media. ■ Gatekeeper Routed—Forces all Q.931 and H.245 messaging through the Embedded gatekeeper. RTP can be sent directly between the clients if both H.323 clients are on the LAN or WAN. H.460 clients always use a routed call model. ■ Gatekeeper Routed, Force RTP through Gatekeeper—Functions like the Gatekeeper Routed option but always forces RTP media traversal through the system.

Table 6-8 Embedded Gatekeeper Mode Parameters (continued)

Item	Description
Custom Q.931 Port	Sets the port returned in Admission Confirm (ACF) messages. If no Custom Q.931 port is set, the default port of 1720 is used. Remote NAT devices can intercept H.323 messages and modify these messages which results in call failure. Changing the TCP call setup port to something other than TCP 1720 can help with call completion in these cases. For example, modifying this field to port 5000 modifies the RCF message to instruct the registered WAN side clients to use this port for call signaling. TCP 1720 will still be a system listening port for B2B calls. **Note:** Ensure the alternate port is not being used for other services.

Table 6-8 Embedded Gatekeeper Mode Parameters (continued)

Item	Description
TCP Keep-Alive Time	Enables TCP keep-alive messages and sets the interval between messages in seconds. If this value is zero, no keep-alive messages are sent. If no response is received, the TCP stack assumes the connected endpoint is no longer listening, and ends the connection. This field sends TCP keepalives to clients connected to the systems well known TCP 1720 port. Default is 0 (disabled); the minimum setting is 120 seconds.
Default Alias	Enter a default alias to be added to incoming calls without a destination message in the Q.931 Setup message: ■ E.164 ■ H.323 This alias allows the embedded gatekeeper or a LAN/Subscriber-side gatekeeper to route the call to a default endpoint. For example, when a B2B call is placed to the system and the user only dialed the IP or FQDN of the WAN interface, the system adds this alias to the H.323 call setup message and forwards it to the LAN gatekeeper for call processing. This alias can be any alias actively registered to the LAN gatekeeper. You may add a H.323 static client in the H.323 Clients List and configure this client as the default alias. The static H.323 client should be locked to prevent the client entry from being deleted. A typical configuration scenario is to configure this field with an MCU IVR alias or a default MCU meeting room alias. Default is E.164, no alias is set.

Click **Submit** to apply your changes.

Managing H.323 Settings

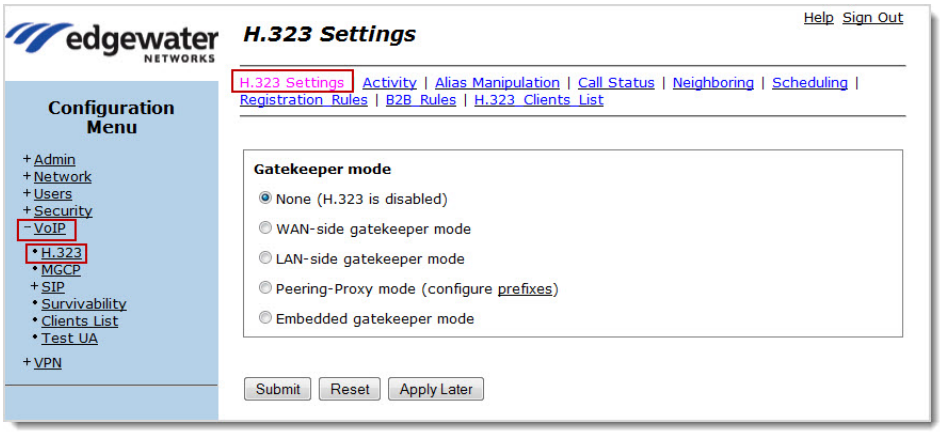
This section describes how to manage H.323 settings using the navigation menu at the top of the H.323 Settings page. Choose **VoIP** > **H.323** and refer to the following sections:

- Managing H.323 Activity
- Configuring H.323 Alias Manipulation
- Managing H.323 Call Status
- Configuring H.323 Neighboring
- Configuring H.323 Bandwidth Scheduling
- Configuring Registration Rules
- Configuring H.323 B2B Rules
- Configuring the H.323 Clients List

Managing H.323 Activity

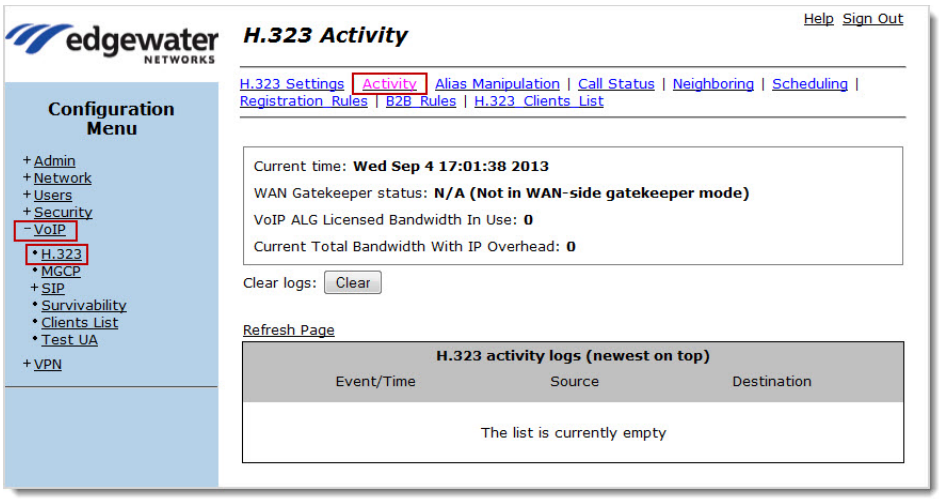
1. Choose **VoIP** > **H.323** (Figure 6-7).

Figure 6-7 H.323 Settings Page



2. Click **Activity** in the H.323 Settings navigation panel at the top of the page to open the H.323 Activity page (Figure 6-8).

Figure 6-8 H.323 Activity Page



3. View H.323 activity using the information in Table 6-9 as a guide.

Table 6-9 H.323 Activity Parameters

Item	Description
H.323 Current Activity	
Shows current H.323 activity.	
Current time	Shows the current date and time.
WAN Gatekeeper status	Describes the current gatekeeper mode settings.
VoIP ALG Licensed Bandwidth In Use	Displays the sum of RTP payloads of all current calls. For example, if two 384k calls are present, bandwidth use is 768. The system uses the field to subtract against the system licensed value as Video Bandwidth on the License page. To view the License page, choose **Admin** from the Configuration Menu and click **license key** under Registration Status. You can also choose **VoIP** from the Configuration Menu and click **View license key** at the bottom of the page.
Current Total Bandwidth With IP Overhead	Displays the RTP payload of current calls and adds the estimated IP overhead. This allows you to budget the requirements for video traversing a customer WAN connection. The value is calculated by the RTP payload divided by .8 to add the IP overhead use to the total. For example, 384k/.8 = 480k of estimated bandwidth usage.

Table 6-9 H.323 Activity Parameters

Item	Description
H.323 Activity Logs	
Shows recent H.323 events such as call terminations and registration rejects. Abnormal events display specific information in red. Refer to H.323 Call Activity Messages.	
Event/Time	Type of event and the time that it occurred.
Source	Source of the event as an IP address and an alias (when available).
Destination	Destination of the event as an IP address and an alias (when available).
To clear H.323 activity logs, click **Clear**. To refresh current status, click **Refresh Page**.	

H.323 Call Activity Messages

- H.323 Call Status Messages
- H.323 Call Termination Messages

H.323 Call Status Messages

Call status shows the last state of the call at the time of the event. Each call progresses through a number of states while being established. Table 6-9 lists call status messages.

Table 6-10 Call Status Messages

Message	Description
Caller admission request received	Received an admission request from the source endpoint and forwarded it to the gatekeeper.
Caller admission response received	Received an admission response (either confirm or reject) from the gatekeeper and forwarded it to the source endpoint.
Incoming Q.931 TCP connection established	Received an incoming Q.931 TCP connection from the source.
Attempting to establish outgoing Q.931 TCP connection	Successfully resolved the destination of the call and attempting to establish an outgoing Q.931 TCP connection to the destination.
Q.931 signaling received and forwarded	Both Q.931 TCP connections have been successfully established and Q.931 signaling has been received and forwarded.

Table 6-10 Call Status Messages (continued)

Message	Description
Callee admission request received	Received an admission request from the destination endpoint and forwarded it to the gatekeeper.
Callee admission response received	Received an admission response (either confirm or reject) from the gatekeeper and forwarded it to the destination endpoint.
Incoming H.245 TCP connection established	Received an incoming H.245 TCP connection from the source.
Attempting to establish outgoing H.245 TCP connection	Attempting to establish an outgoing H.245 TCP connection to the destination.
H.245 signaling received and forwarded	Both H.245 TCP connections have been successfully established and H.245 signaling has been received and forwarded. At this point, the call is considered established, even though no media channels have been opened up yet.
Outgoing media channel established	An outgoing media channel (from the LAN/subscriber side to the WAN/provider side) has been opened.
Incoming media channel established	An incoming media channel (from the WAN/provider side to the LAN/subscriber side) has been opened.
Bidirectional media channels established	Media channels have been opened in both directions. This is a normal call where media is being sent in both directions.

H.323 Call Termination Messages

Call termination messages can help troubleshoot the cause of the call failure. Table 6-11 lists call termination messages.

Table 6-11 Call Termination Messages

Message	Description
Out of system resources	The call could not be completed because the system did not have enough resources.
Client owning the call has been deleted	The call could not be completed because the client that made this call was deleted during the call setup.

Table 6-11 Call Termination Messages (continued)

Message	Description
Connection to destination could not be established	TCP connection to the destination could not be established.
Connection refused by destination	The call could not be completed because the destination refused the incoming TCP connection.
No route to destination	A TCP connection to the destination could not be established because the destination could not be reached. This could happen if there is no route to the destination or, if the destination is on the same subnet, the destination does not answer to ARP requests.
Connection to destination timed out	The TCP connection attempt to the destination timed out before it could be established.
Call ended by source	The call was gracefully terminated by H.323 signaling from the source. This usually indicates that the endpoint intended to terminate the call.
Call ended by destination	The call was gracefully terminated by H.323 signaling from the destination. This usually indicates that the endpoint intended to terminate the call.
Connection terminated by source	The call was terminated because the source terminated the TCP connection without prior call termination signaling.
Connection terminated by destination	The call was terminated because the destination terminated the TCP connection without prior call termination signaling.
No admission confirm received	The call could not be established because the admission response was not received from the gatekeeper.
Cannot resolve destination	The call could not be established because the destination could not be resolved.
At maximum bandwidth usage	The call could not be established because the system already is at the maximum allowed bandwidth.
Call exceeds maximum per-call bandwidth	The call could not be established because the bandwidth requested for the call exceeds the configured per-call maximum.
Received admission reject	The call was terminated because an admission reject was received from the gatekeeper.

Table 6-11 Call Termination Messages (continued)

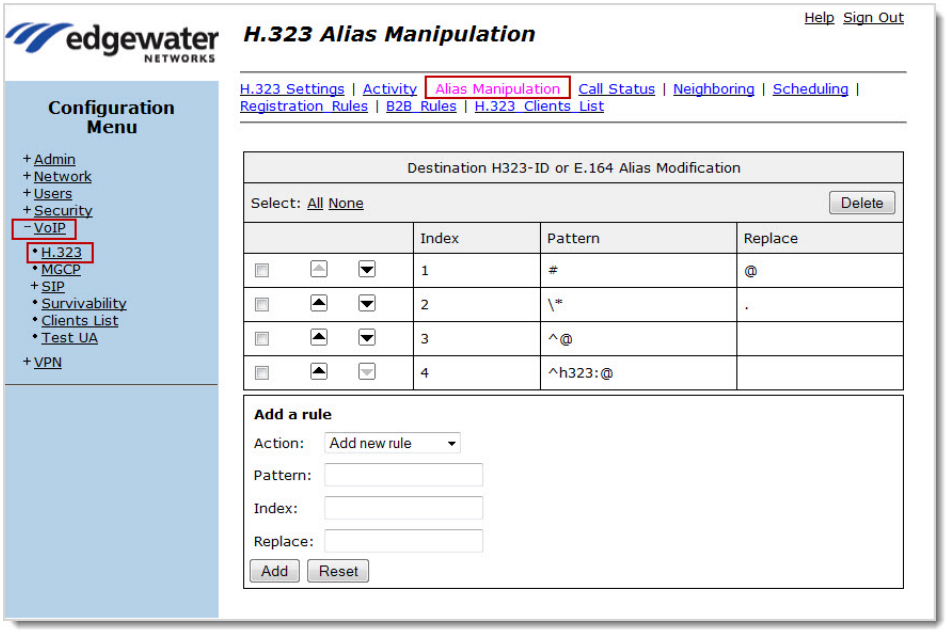
Message	Description
Received disengage request	The call was terminated because the endpoint requested to tear down the call.
Received invalid data	The call could not be established because the system received invalid data on the signaling channel.
Cannot find client	The call could not be established because the called client could not be found.

Configuring H.323 Alias Manipulation

Alias manipulation is performed immediately when a message such as an ARQ, LRQ, or a Setup is received. Any matching pattern is replaced with the specified string, allowing you to replace characters or strings that are hard or impossible to dial on certain endpoints. Normal call lookup is performed following alias manipulation.

1. Choose **VoIP** > **H.323** (Figure 6-7).
2. Click **Alias Manipulation** in the H.323 Settings navigation panel at the top of the page to open the H.323 Alias Manipulation page (Figure 6-9).

Figure 6-9 H.323 Alias Manipulation Page



3. Configure settings using the information in Table 6-12 as a guide.

Tip
Rules are executed in the order in which they are listed. Use the arrows to move entries up and down, or use the Index field to specify where a new or edited rule falls in the list.

Table 6-12 H.323 Alias Manipulation Parameters

Item	Description
Destination H323-ID or E.164 Alias Modification	Shows all alias manipulation rules configured on the system. All rules are applied to each alias being processed. The rules are applied in the order they are listed. Each rule consists of a pattern to match and a string to replace the matching pattern with.
Add a Rule	Allows you to add new prefixes to the Prefix Routing and Gatekeeping Neighboring table. See Configuring Peering-Proxy Mode Settings.
Action	Specifies whether the rule is to be added or edited: ■ Add new rule ■ Edit 1: "#" ■ Edit 2: "*" ■ Edit 3: "^@" ■ Edit 4: "^h323:@"
Pattern	Enter the pattern to be matched. See Regular Expressions and Expression Examples for a list of valid patterns.
Index	Determines the order in which the rule is scanned in the Destination H323-ID or E.164 Alias Modification table. To add a rule between two rules with consecutive indexes (n and m), use the higher index (m).
Replace	Enter the string that replaces the matched pattern. See Regular Expressions and Expression Examples for a list of valid patterns.

4. Manage rules in the Destination H323-ID or E.164 Alias Modification table:
   a. Select checkboxes for the entries that you want to move up or down in the list or delete. Click **All** to choose all the entries or **None** to clear your selections.
   b. Click the up or down arrows to move entries in the list.
   c. Click **Delete** to remove an entry.

   Or

d. Click **OK** to confirm

5. To add a new rule:

   a. Choose **Add a new rule** from the **Action** drop-down list (Figure 6-10).

Figure 6-10 Add a New Alias Rule



   b. In the **Pattern** field, add a regular expression for matching against the destination alias. See Regular Expressions and Expression Examples for a list of valid patterns.

   c. In the **Index** field, add a position that the rule occupies in the Destination H323-ID or E.164 Alias Modification list.

   d. In the **Replace** field, enter a string to replace the matching pattern. See Regular Expressions and Expression Examples for a list of valid patterns.

   e. Click **Add** to save your changes.

6. To edit a rule:

   a. Choose an edit action from the **Action** drop-down list (Figure 6-11).

Figure 6-11 Edit an Alias Rule



   b. In the **Pattern** field, edit the regular expression for matching against the destination alias.

   c. In the **Index** field, edit the position that the rule occupies in the Destination H323-ID or E.164 Alias Modification list.

   d. In the **Replace** field, enter a string to replace the matching pattern. See Regular Expressions and Expression Examples for a list of valid patterns.

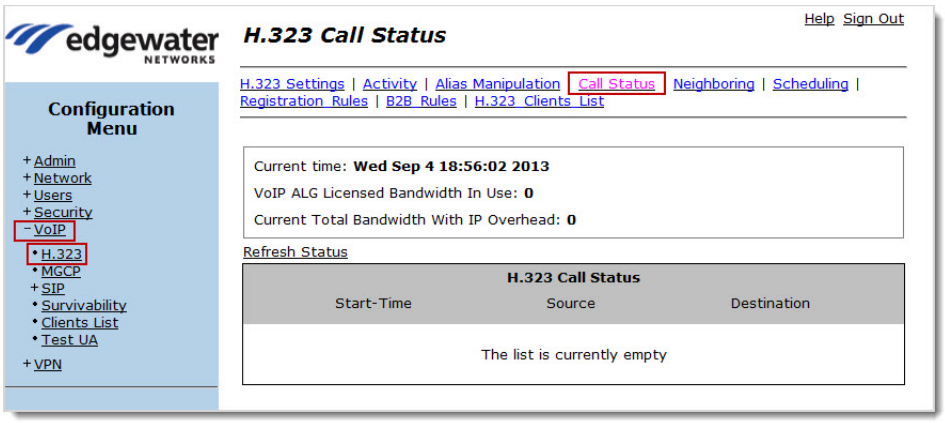
   e. Click **Edit** to save your changes.

Managing H.323 Call Status

The H.323 Call Status page displays information about active H.323 calls.

1. Choose **VoIP** > **H.323** (Figure 6-7).
2. Click **Call Status** in the H.323 Settings navigation panel at the top of the page to open the H.323 Call Status page (Figure 6-12).

Figure 6-12 H.323 Call Status Page



3. View H.323 in-progress call status using the information in Table 6-13 as a guide.

Table 6-13 H.323 Call Status Parameters

Item	Description
Current time	Shows the current date and time.
VoIP ALG Licensed Bandwidth In Use	Displays the sum of RTP payloads of all current calls. For example, if two 384k calls are present, bandwidth use is 768. The system uses the field to subtract against the system licensed value as Video Bandwidth on the License page. To view the License page, choose **Admin** from the Configuration Menu and click **license key** under Registration Status. You can also choose **VoIP** from the Configuration Menu and click **View license key** at the bottom of the page.
Current Total Bandwidth With IP Overhead	Displays the RTP payload of current calls and adds the estimated IP overhead. This allows you to budget the requirements for video traversing a customer WAN connection. The value is calculated by the RTP payload divided by .8 to add the IP overhead use to the total. For example, 384k/.8 = 480k of estimated bandwidth usage.
H.323 Call Status Logs Shows current H.323 call status. Refer to H.323 Call Activity Messages.	

Table 6-13 H.323 Call Status Parameters

Item	Description
Start Time	The time the call was initiated.
Source	Source of the event as an IP address and an alias (when available).
Destination	Destination of the event as an IP address and an alias (when available).
To refresh current status, click **Refresh Page**.	

4. Terminate specific calls by clicking the delete icon next to the call.



Note
No notification is given to the participants in the call when you terminate a call in this manner.

Only calls where the Q.931 (and H.245) TCP connections are routed through this system can be terminated. If no Q.931 TCP connection has been received for a call, this call cannot be terminated using the H.323 Call Status page.

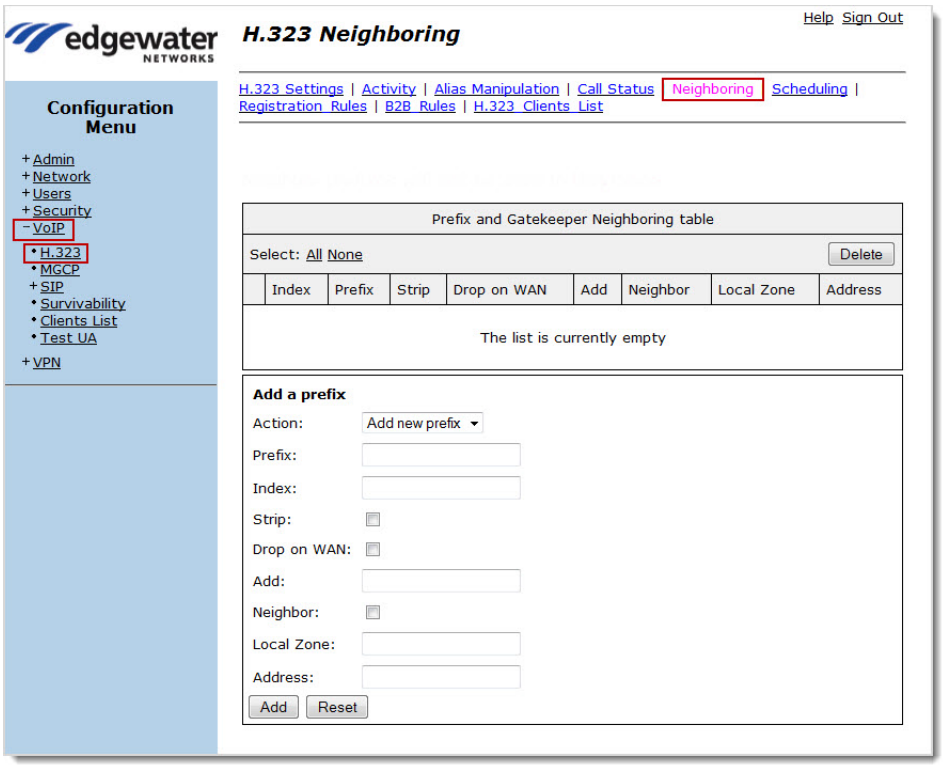
Some calls (for example, Gatekeeper-routed calls between two clients to this system) may show up as two calls. This is because each client has a call leg established to the outside system. In this case, terminating one of the call-legs will eventually lead to both calls disappearing, but this will not be shown immediately.

Configuring H.323 Neighboring

Use the H.323 Neighboring page to route calls based on a matching prefix in the destination alias of the call. Each prefix is associated with a domain name or IP address that is used if the prefix matches.

1. Choose **VoIP** > **H.323** (Figure 6-7).
2. Click **Neighboring** in the H.323 Settings navigation panel at the top of the page to open the H.323 Neighboring page (Figure 6-13).

Figure 6-13 H.323 Neighboring Configuration Page



3. Manage settings using the information in Table 6-14 as a guide. When you have finished configuring settings, click **Add** to make your changes take effect.

Table 6-14 H.323 Neighboring Parameters

Item	Description
Prefix and Gatekeeper Neighboring	Shows all prefix routing configured on the system. The prefixes are searched in the order they are entered. Each prefix consists of the prefix pattern, a strip prefix flag, Drop on WAN flag, add string, neighbor flag, and the target IP or domain for that prefix. Normally, the prefix is used to route the Q.931 Setup message at the time it is received. However, if the neighbor flag is set, the prefix is only applicable in the admission request (ARQ) look-up stage. If the prefix matches at this stage, a location request (LRQ) is sent to the target neighbor in order to resolve the call destination. Each prefix can be moved up or down in the list.
Add or Edit a Prefix	Allows you to add new prefixes to the Prefix Routing and Gatekeeping Neighboring table. See Configuring Peering-Proxy Mode Settings.
Action	Specifies whether the rule is to be added or edited.
Prefix	Specifies the prefix for the system to match with a destination pattern and forward the call to the configured address. Regular expressions can be used in the field. Prefixes are typically matched from the left side of the destination string when received by the system unless a regular expression is used to find the match anywhere in the string. Refer to Regular Expressions and Expression Examples.
Index	Determines where the rule is placed in the table. Prefixes are processed by the system from top to bottom so it maybe necessary to move rules around during testing. Edit the rule and enter the new index number as desired.
Strip	Removes the matching prefix from the destination string and forwards the call to the configured address.

Table 6-14 H.323 Neighboring Parameters (continued)

Item	Description
Drop on WAN	Creates a policy to drop incoming WAN side calls when this prefix matches the destination string on the WAN side only. When configuring a prefix and selecting the Drop on WAN option, all other fields are considered Invalid combinations. This feature is supported with LAN-side gatekeeper and Embedded gatekeeper modes. All other prefixes without Drop on WAN selected are processed and routed by the system to the configured address.
Add	Specifies a digit or string of digits to be added to the destination string. The added digit(s) are inserted at the beginning or left side of the string before forwarding to the configured address.
Neighbor	Sends a location request (LRQ) to the configured address only when the system is configured for Embedded gatekeeper mode. When the system receives an admission request (ARQ) and makes a prefix match on the destination string and this flag is set, the system sends an LRQ before forwarding the call setup message. LAN-side gatekeeper mode performs prefix routing but does not send an LRQ to the configured address.
Local Zone	Configures a zone name for older Cisco Multimedia Conference Manager (MCM) gatekeepers. A zone name must be present in the LRQ that matches the Cisco MCM configured remote zone name. The zone name entered replaces the H323-ID in the LRQ sent to the Cisco MCM for LRQ verification by the MCM before the call setup is accepted by the MCM.
Address	Specifies the IPv4 address or system domain name to route the prefix to. The system only provides a DNS A-record lookup on the configured domain.

4. Manage prefixes in the Prefix and Gatekeeper Neighboring table:
   a. Select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
   b. Click **Delete**.
   c. Click **OK** to confirm
5. Proceed to Add a New Prefix

Add a New Prefix

1. Choose **Add a New Prefix** from the Action drop-down list.

   In the **Prefix** field, enter a prefix pattern. The prefix pattern is the regular expression to use when matching against the destination alias. See Regular Expressions and Expression Examples.
2. In the **Index** field, enter an index location. The index is the position in the list where the prefix is inserted.
3. Select the **Strip** checkbox to specify whether the matching prefix should be removed from the destination string.
4. Select the Drop on WAN checkbox to drop incoming WAN-side calls when this prefix matches the destination string on the WAN side only.
5. In the **Add** field, specify a particular string to prepend to the alias in case of a match.
6. Select the **Neighbor** checkbox to specify whether the prefix should result in a neighbor request or just route the call to the destination.
7. In the Local Zone field, enter a zone name to replace the H323-ID in the LRQ sent to the Cisco MCM for LRQ verification by the MCM before the call setup can be accepted by the MCM.
8. In the **Address** field, enter the IP address or domain of the target to send the call to.
9. Click **Add**.

Configuring H.323 Bandwidth Scheduling

Bandwidth can be reserved for a time interval for calls from or to an endpoint or between two endpoints. An endpoint is identified by its H.323 ID and E.164 aliases. The amount of bandwidth to reserve is taken from the endpoint ARQ message at the beginning of the call and is not specified here in a reservation.

If a call is scheduled but there is not enough bandwidth for it, first unscheduled calls and then scheduled calls past their stop time are terminated. The call is rejected if there is still not enough bandwidth (scheduled calls within their reserved times are never terminated). A reservation does not specify or imply the number of calls for which bandwidth is reserved.

Reservation Tips

Specifying both aliases is useful for point-to-point calls where the aliases of both parties are known. For presentations, it may be useful to just reserve bandwidth for the presenter by specifying his or her endpoint's alias and leaving the other alias field blank. Leaving both alias fields blank matches all calls. If both time fields are blank, the reservation is forever—no time

constraint is applied. Reservations are not recurring, for example, every week at 14:00; however, you can edit a reservation and update the time.

The schedule entry shown in Figure 6-14 reserves bandwidth for any number of calls to or from an endpoint whose ARQ contains an H.323 ID or E.164 alias beginning with 5612.

Figure 6-14 Bandwidth Scheduling Example



The 5612 alias could have been specified in the Alias 2 field, instead. Because an alias expression is used as a prefix, this matches any alias that begins with 5612. In most cases, this subtlety does not matter; there is little to no risk of there being another endpoint on the network with the alias of 561230, for example.

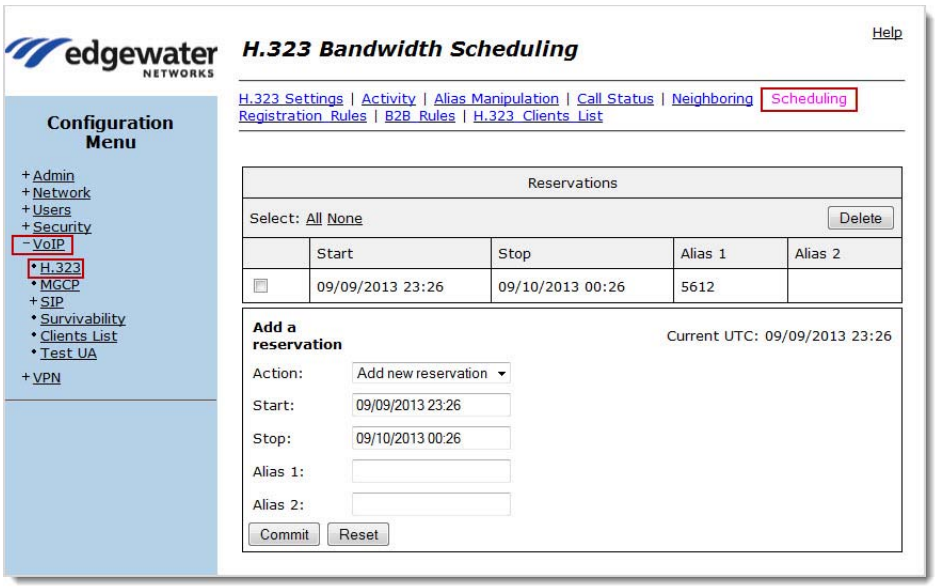
However, if you want to be extra careful, you could follow 5612 with a special character like the dollar sign, for example “5612$.” The special character indicates the end of the expression. Conversely, if you didn’t want your alias expression to be treated as a prefix, you could include the asterisk character at the beginning, for example, “*@example.net.” This indicates any number of any kind of character.

The Reservations table lists reservations in chronological order according to start time. All “forever” reservations are listed first. There are no duplicate entries. An ARQ may match multiple reservations, so the first reservation is used. The only impact is that the call's reservation ends based on the stop time for that reservation. The call is not terminated just because its reservation has expired; however, if there is a new scheduled call, it might be terminated to make room for the new call.

Configure H.323 Bandwidth Scheduling

1. Choose **VoIP** > **H.323** (Figure 6-7).
2. Click **Scheduling** in the H.323 Settings navigation panel at the top of the page to open the H.323 Scheduling page (Figure 6-15).

Figure 6-15 H.323 Bandwidth Scheduling Page



3. Configure settings using the information in Table 6-15 as a guide. When you have finished configuring settings, click **Commit** to make your changes take effect.

Table 6-15 H.323 Scheduling Parameters

Item	Description
Reservations	Lists reservations in chronological order according to start time. All “forever” reservations are listed first. There are no duplicate entries.
Start time Stop time	Describes the date and time in Coordinated Universal Time (UTC), no time-zone offset is applied. Fields use the format, mm/dd/yyyy hh:mm. Leading zeroes are allowed, the year must be four digits, the time uses a 24-hour clock.

Table 6-15 H.323 Scheduling Parameters (continued)

Item	Description
Alias 1	(Optional) Identifies the two endpoints in a call.
Alias 2	An alias field contains a regular expression for matching at least one H.323 ID or E.164 alias in the list of source or destination aliases in an ARQ. An alias expression is always treated as a prefix; matching begins at the beginning of an alias. ARQ source and destination aliases are searched using Alias 1 and Alias 2, respectively, or Alias 2 and Alias 1, respectively. It is not necessary to specify the direction of the call—who is the called party and who is the calling party. A blank alias field is a wildcard; it matches all aliases,
Add a Reservation	
Action	Adds or edits a reservation.
Start	Specifies the start date and time in the format mm/dd/yyyy hh:mm. Leading zeroes are allowed, the year must be four digits, the time uses a 24-hour clock.
Stop	Specifies the stop date and time in the format mm/dd/yyyy hh:mm. Leading zeroes are allowed, the year must be four digits, the time uses a 24-hour clock.
Alias 1	(Optional) Specifies the two endpoints in a call.
Alias 2	An alias field contains a regular expression for matching at least one H.323 ID or E.164 alias in the list of source or destination aliases in an ARQ. An alias expression is always treated as a prefix; matching begins at the beginning of an alias.

4. Manage the bandwidth schedule in the Reservations table:
   a. Select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
   b. Click **Delete**.
   c. Click **OK** to confirm
5. Proceed to Add a Reservation.

Add a Reservation

1. Choose **Add a New Reservation** from the Action drop-down list.
2. Enter the start and stop times in the **Start Time** and **Stop Time** fields. Enter values in mm/dd/yyyy hh:mm format. Leading zeroes are allowed, the year must be four digits, the time uses a 24-hour clock.

3. (Optional) Enter an alias value in the **Alias 1** and **Alias 2** fields to identify the two endpoints in a call.

   Regular expressions are listed in Table 6-1. Regular expression examples are listed in Table 6-2. See Regular Expressions and Expression Examples.

4. Click **Commit** to save your settings.

Configuring Registration Rules

The Registration Rules page is used to selectively program the system firewall to control registration access to the system for H.323 UDP port 1719. The H.323 Registration Rules only apply to clients registering from the WAN side.

The whitelist/blacklist is used to block H.323 calls to your device based on IP addresses. First, a default policy is defined and a list of exceptions to this policy is created. If a whitelist is selected, all calls are blocked by default except for calls from the listed addresses. If a blacklist is selected, all calls are allowed by default except for calls from the listed addresses.

Note
The Firewall must be enabled for this feature to function. Choose **Security** from the Configuration Menu and refer to Configuring Basic WAN Firewall Settings in Chapter 5, *Configuring System Security*.

1. Choose **VoIP** > **H.323** (Figure 6-7).
2. Click **Registration Rules** in the H.323 Settings navigation panel at the top of the page to open the H.323 Registration Rules page (Figure 6-16).

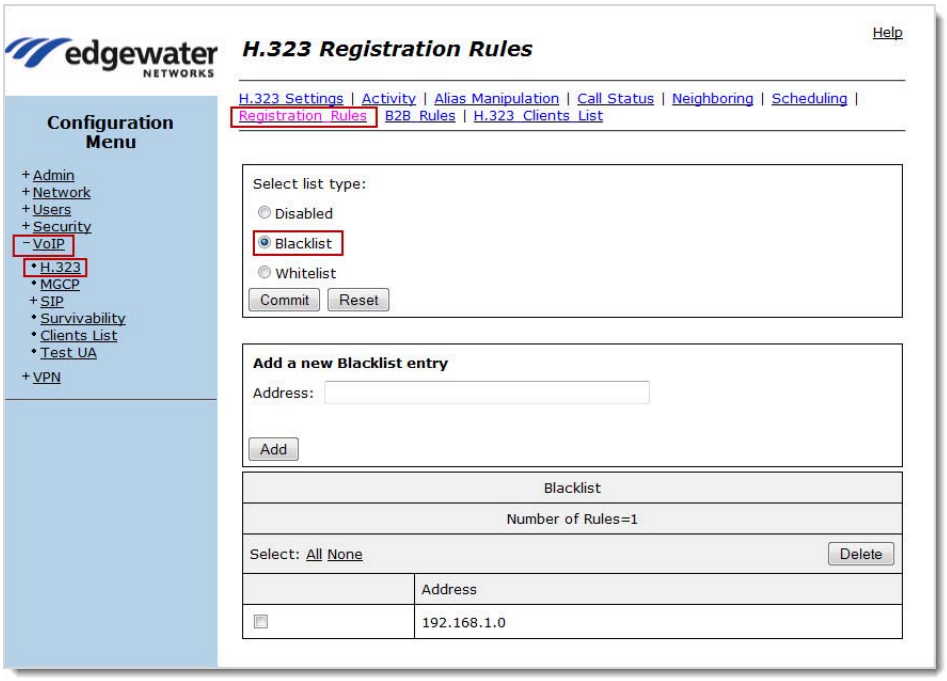
Figure 6-16 H.323 Registration Rules Configuration Page



3. Select a list type radio button:
   - **Disabled** (default)
   - **Blacklist**
   - **Whitelist**

4. Click **Commit** to activate H.323 Registration Rules Whitelist or Blacklist configuration fields. The example in Figure 6-17 shows Blacklist fields; Whitelist fields are identical when you select the **Whitelist** radio button. Calls are not interrupted on the system when you click **Commit**.

Figure 6-17 Blacklist Configuration Fields



5. Configure settings using the information in Table 6-16 as a guide.

Table 6-16 H.323 Registration Rules Parameters

Item	Description
Disabled	Default setting is disabled and all H.323 devices are allowed to register.
Blacklist	Creates a blacklist policy to allow all H.323 registrations into the system. The Blacklist table allows administrators to enter selected blocked IP addresses. Adding or deleting entries to the list does not affect ongoing calls through the system.
Whitelist Static-Only	Creates a whitelist policy to block all H.323 registrations into the system. The Whitelist table allows the administrator to enter allowed IP addresses. Adding or deleting entries to the list does not affect ongoing calls through the system.

Table 6-16 H.323 Registration Rules Parameters (continued)

Item	Description
Add a New Whitelist/Blacklist Entry	
Address	Specifies the IP address or IP address/bitmask. If an IP address/bitmask is entered, it must be entered in the format a.b.c.d/xx, where xx has a range of 0 to 32. Once the new address is added to the list, the policy is immediately changed to include the new address.
Delete	Deletes one or more IP addresses from the list. Once the address is deleted from the list, the policy is immediately changed to exclude the address.
Add a New Whitelist Static/Dynamic Entry	
Creates a static and dynamic whitelist policy to block all H.323 registrations into the system. The whitelist static/dynamic option generates two lists of clients. The first list is the static list, which is modified exactly as the static-only option described above. The second list is automatically generated when clients authenticate to the Access Proxy. Access Proxy must be enabled to have clients added dynamically. No action can be performed on the dynamic clients from this page; the page only displays a list of the authenticated clients; the user cannot modify/add/delete any of the clients directly in the dynamic list. When this option is enabled, the firewall first searches the static list, then the dynamic list. As with the whitelist static-only option, if no match is found in either list, the request is dropped.	

6. Manage entries in the H.323 Registration Rules Whitelist or Blacklist table:
   a. Select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
   b. Click **Delete**.
   c. Click **OK** to confirm
7. Add a new Whitelist or Blacklist entry by entering an IP address in the **Address** field.
8. Click **Add** for each address that you add to the list.
9. Click **Submit All** to save all settings on the page.

Configuring H.323 B2B Rules

The H.323 B2B Rules page is used to selectively program the system firewall to control call access to the system for H.323 TCP port 1720 from

unregistered clients. The B2B Rules only apply to calls originating from the WAN side.

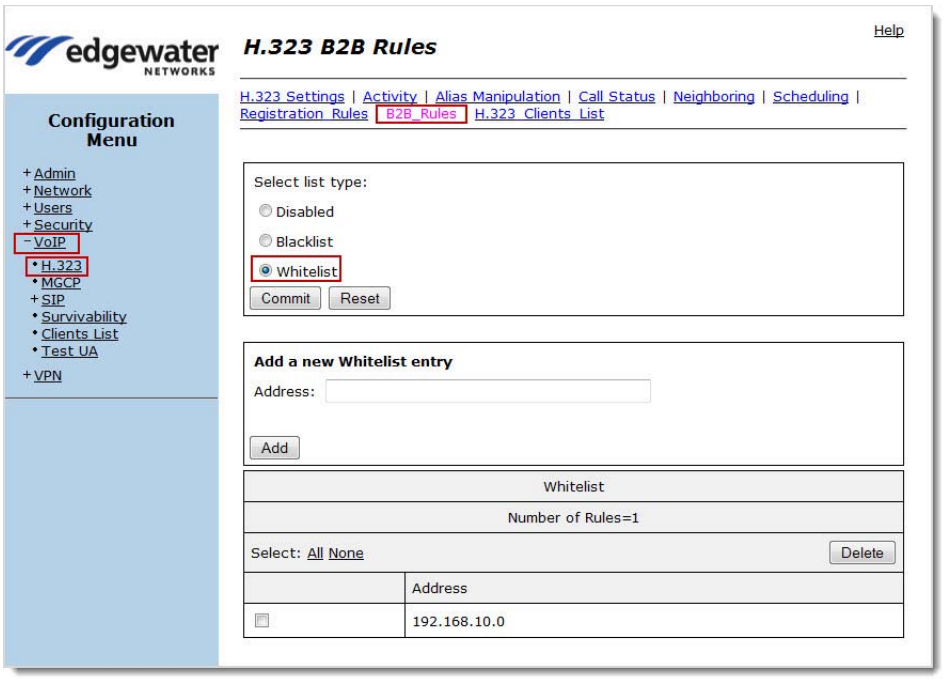
1. Choose **VoIP** > **H.323** (Figure 6-7).
2. Click **B2B_Rules** in the H.323 Settings navigation panel at the top of the page to open the H.323 B2B Rules configuration page (Figure 6-18).

Figure 6-18 H.323 B2B Rules Configuration Page



3. Select a list type radio button:
   - **Disabled** (default)
   - **Blacklist**
   - **Whitelist**
4. Click **Commit** to activate H.323 B2B Rules Whitelist or Blacklist configuration fields. The example in Figure 6-19 shows Whitelist fields; Blacklist fields are identical when you select the **Blacklist** radio button. Calls are not interrupted on the system when you click **Commit**.

Figure 6-19 H.323 B2B Rules Configuration Page



5. Configure settings using the information in Table 6-17 as a guide.

Table 6-17 H.323 B2B Rules Parameters

Item	Description
Disabled	Default setting is disabled and all H.323 B2B calls are allowed in.
Blacklist	Creates a blacklist policy to allow all H.323 B2B calls into the system from unregistered clients. The Blacklist table allows administrators to enter selected blocked IP addresses. Adding or deleting entries to the list does not affect ongoing calls through the system.
Whitelist	Creates a whitelist policy to block all H.323 B2B calls into the system from unregistered clients. The Whitelist table allows administrators to enter selected blocked IP addresses. Adding or deleting entries to the list does not affect ongoing calls through the system.
Add a New Whitelist/Blacklist Entry	

Table 6-17 H.323 B2B Rules Parameters (continued)

Item	Description
Address	Specifies the IP address or IP address/bitmask. If an IP address/bitmask is entered, it must be entered in the format a.b.c.d/xx, where xx has a range of 0 to 32. Once the new address is added to the list, the policy is immediately changed to include the new address.
Delete	Deletes one or more IP addresses from the list. Once the address is deleted from the list, the policy is immediately changed to exclude the address.

6. Manage entries in the H.323 B2B Rules Whitelist or Blacklist table:
   a. Select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
   b. Click **Delete**.
   c. Click **OK** to confirm
7. Add a new Whitelist or Blacklist entry by entering an IP address in the **Address** field.
8. Click **Add** for each address that you add to the list.
9. Click **Submit All** to save your settings.

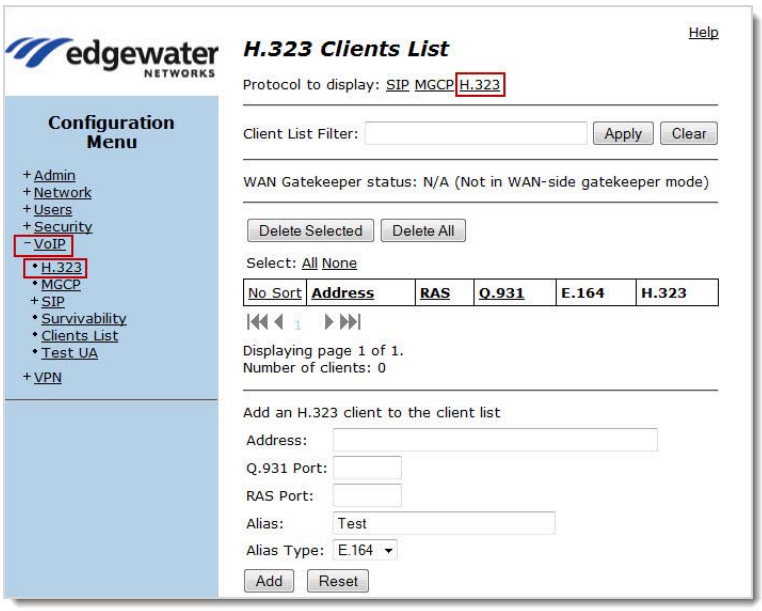
Configuring the H.323 Clients List

Use H.323 Clients List configuration page to configure the entries for devices that have registered with the EdgeMarc.

Tip
See also Configuring the Clients List.

1. Choose **VoIP** > **H.323** (Figure 6-7).
2. Click **H.323 Clients List** in the H.323 Settings navigation panel at the top of the page to open the H.323 B2B Rules configuration page (Figure 6-20).

Figure 6-20 H.323 Clients List Configuration Page



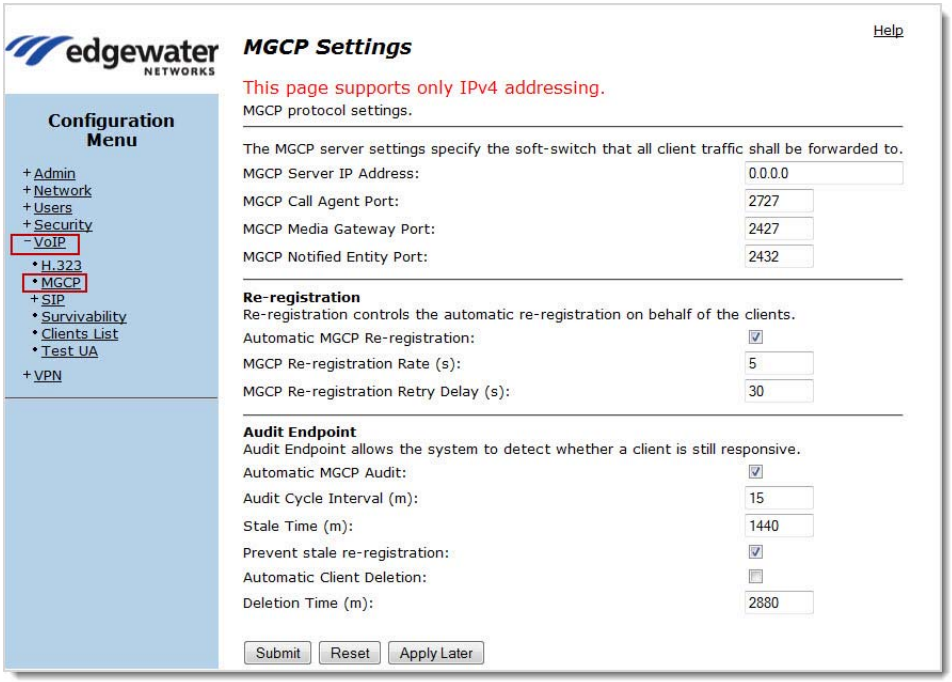
3. Configure settings using the information in Configuring the Clients List as a guide. When you have finished configuring settings, click **Add** to make your changes take effect.

Configuring MGCP Settings

Use the MGCP Settings configuration page to manage the MGCP protocol for VoIP ALG.

1. Choose **VoIP** > **MGCP** (Figure 6-21).

Figure 6-21 MGCP Settings



2. Configure settings using the information in Table 6-18 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 6-18 MGCP Parameters

Item	Description
MGCP Protocol Settings	
Manages MGCP IPv4 server settings to specify the softswitch that all client traffic shall be forwarded to. See Configuring MGCP Protocol Settings.	
MGCP Server IP Address	Specifies the IP address for the MGCP Server. The MGCP server provides media gateway control protocol service to IP phones, client adapters, and gateways.
MGCP Call Agent Port	Specifies the port number that the Call Agent softswitch listens to for messages from the phones. Default is 2727.

Table 6-18 MGCP Parameters

Item	Description
MGCP Media Gateway Port	Specifies the port number that the Media Gateway phones listen to for messages from the softswitch. Default is 2427.
MGCP Notify Entity Port	Specifies the port number that the softswitch uses for notifications from the phones. For example, hook up, hook down, and digits. Default is 2432
Re-registration	
Configures automatic client re-registration. See Re-Registering Clients.	
Automatic MGCP Re-registration	Enables MGCP endpoint re-registration every time the network or system restarts. Automatically synchronizes the softswitch and phones immediately after a restart. Default is Enabled.
MGCP Re-Registration Rate (s)	Sets the number of MGCP RSIP messages to send per second to the Media Gateway Controller when re-registration is needed. Range is 1 to 5 seconds, default is 5 messages per second. Generally, this value does not need to be modified.
MGCP Re-Registration Retry Delay (s)	Specifies the number of seconds to wait before retrying re-registration. The system makes a maximum of 10 re-registration requests for failed attempts. Range is 30 to 60 seconds, default is 30 seconds. Generally, this value does not need to be modified.
Audit Endpoint	
Sets an audit endpoint to help the appliance detect whether a client is still responsive. See Configuring the Audit Endpoint.	
Automatic MGCP Audit	Specifies that MGCP clients are automatically audited by sending a message to each client and waiting for a response.
Audit Cycle Interval (m)	Specifies in minutes how often these messages should be sent to the clients. At each cycle, all endpoints are audited so the rate of messages being sent is dependent upon the number of clients currently registered.
Stale Time (m)	Specifies in minutes when a client is deemed stale or unavailable.
Prevent Stale Registration	Disables automatic MGCP re-registration for stale clients.

Table 6-18 MGCP Parameters

Item	Description
Automatic Client Deletion	Deletes clients that have been unavailable for the specified period of time.
Deletion Time (m)	Specifies the period of time in minutes for automatic client deletion.

3. Configure the following settings on the MGCP Settings configuration page:
   - Configuring MGCP Protocol Settings
   - Re-Registering Clients
   - Configuring the Audit Endpoint

Configuring MGCP Protocol Settings

MGCP server settings specify the softswitch that all client traffic is forwarded to.

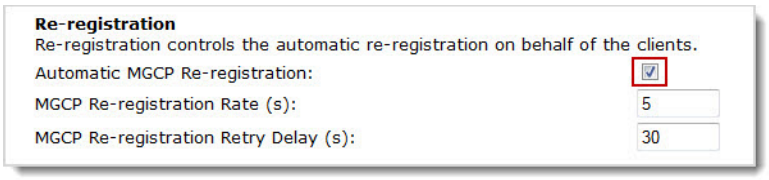
1. Choose **VoIP** > **MGCP** (Figure 6-21).
2. In the **MGCP Server IP Address** field, enter the IP address for the MGCP server.
3. In the **MGCP Call Agent Port** field, enter the port number that the Call Agent softswitch listens to for messages from the phones. Default is 2727.
4. In the **MGCP Media Gateway Port** field, enter the port number that the Media Gateway phones listen to for messages from the softswitch. Default is 2427.
5. In the **MGCP Notified Entity Port** field, enter the port number that the softswitch uses for notifications from the phones, for example, hook up, hook down, and digits. Default is 2432.
6. Proceed to Re-Registering Clients.

Re-Registering Clients

Configure MGCP endpoint automatic re-registration to synchronize the softswitch and the phones immediately upon network or system restart. Re-registration is enabled by default.

1. Choose **VoIP** > **MGCP** (Figure 6-21).
2. Select the **Automatic MGCP Re-registration** checkbox (Figure 6-22).

Figure 6-22 Automatic MGCP Re-Registration



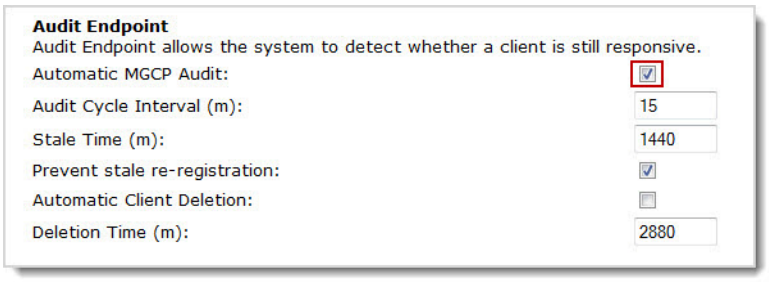
3. In the **MGCP Re-registration Rate** field, enter a value between 1 and 5 to set the number of MGCP RSIP messages to send per second to the Media Gateway Controller when re-registration is needed. The default is 5 messages per second. Generally, this value does not need to be modified.
4. In the **MGCP Re-registration Retry Delay** field, enter a value between 30 and 60 to set the number of seconds that the system waits to retry a failed re-registration. Default is 30 seconds. Generally, this value does not need to be modified.
5. Proceed to Configuring the Audit Endpoint.

Configuring the Audit Endpoint

Audit Endpoint specifies whether MGCP clients should be automatically audited by sending a message to each client and waiting for a response.

1. Choose **VoIP** > **MGCP** (Figure 6-21).
2. Select the **Automatic MGCP Audit** checkbox (Figure 6-23).

Figure 6-23 Automatic MGCP Audit



3. In the **Audit Cycle Interval (m)** field, enter the number of minutes to specify how often these messages are sent to the clients. All endpoints are audited every cycle, so the sent message rate is dependent upon the number of clients currently registered. Default is 15 minutes.
4. Enter a value in minutes in the **Stale Time (m)** field to mark a client stale or unavailable. Default is 1440 minutes.
5. Select the **Prevent stale re-registration** checkbox to disable the automatic MGCP re-registration feature for stale clients.
6. Select the **Automatic Client Deletion** checkbox to delete clients that have been unavailable for a given period of time.

7. In the **Deletion Time (m)** field, enter a number of minutes to specify when to delete clients that have been unavailable. A stale client displays a warning icon in the client list.
8. Click **Submit**.

   A message indicates that service will be temporarily interrupted.
9. Click **OK** to confirm.

Configuring SIP Settings

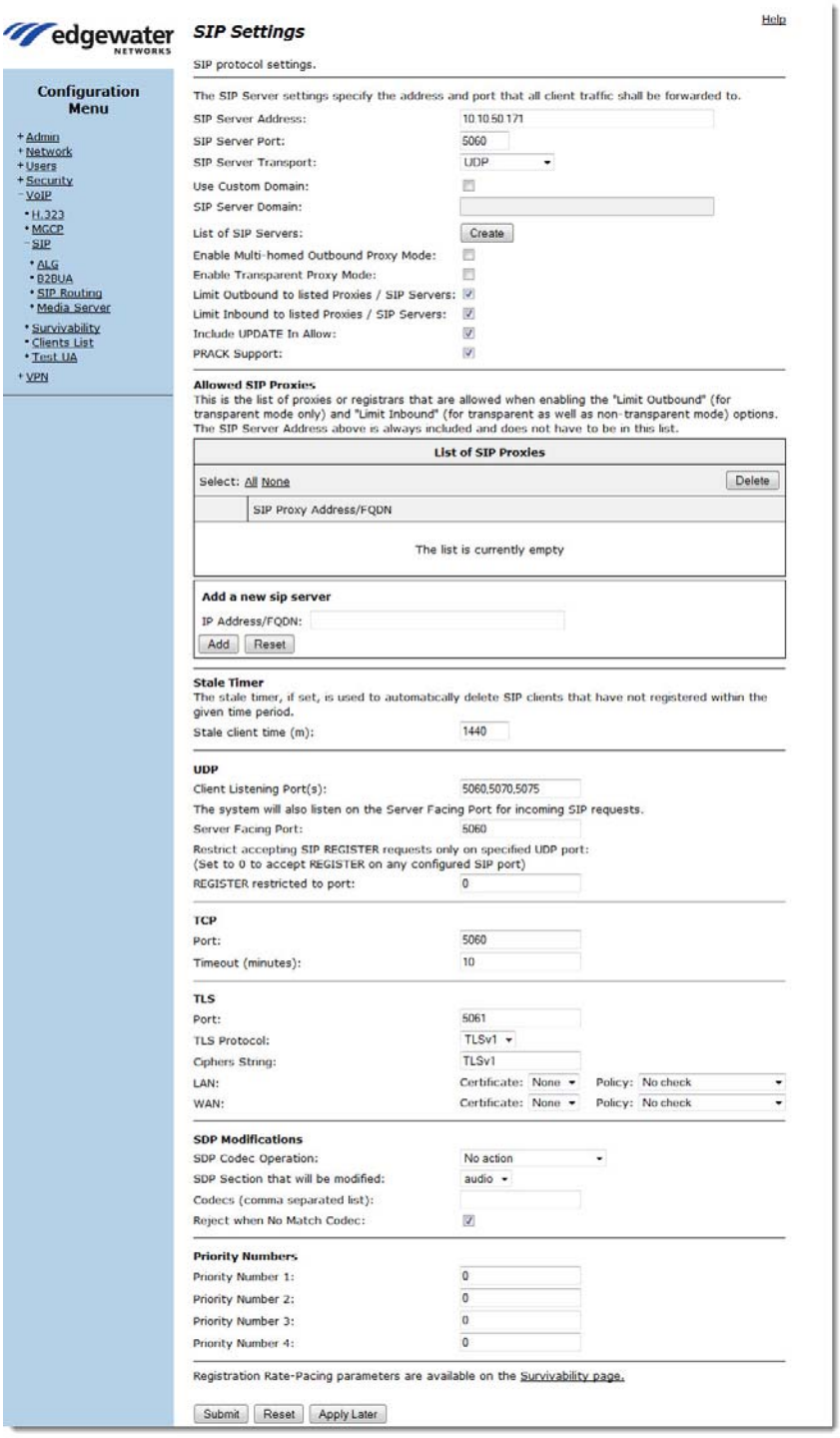
Use the SIP Settings page to configure SIP for the VoIP ALG.

- Using the SIP Settings Page
- Configuring SIP Protocol Settings
- Configuring Allowed SIP Proxies
- Managing the List of SIP Servers
- Configuring the SIP Stale Timer

Using the SIP Settings Page

1. Choose **VoIP** > **SIP** (Figure 6-24).

Figure 6-24 SIP Settings Page



2. Configure settings using the information in Table 6-19 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 6-19 SIP Settings Parameters

Item	Description
SIP Protocol Settings	
Configures SIP ALG settings. See Configuring SIP Protocol Settings.	
SIP Server Address	Specifies the SIP server IP address or URL.
SIP Server Port	Specifies the SIP server port number.
SIP Server Transport	Specifies SIP server transport: ■ Pass Through ■ UDP ■ TCP ■ TLS If the Client/Phone transport is different from the Server transport, the system does the transport conversion. The system cannot convert from UDP to TCP or TLS while in ALG mode.
Use Custom Domain	Configures a custom domain name other than the default SIP domain, which is the same as the SIP Sever address.
SIP Server Domain	Specifies the domain name of the SIP server that accepts forwarded client traffic.
List of SIP Servers	
The system supports auto failover to secondary SIP servers, if it is provided with a list of SIP servers. There are two methods to obtain the list of SIP servers: ■ DNS SRV Lookup on SIP Server URL—Default; done automatically if the address of the SIP Server is a URL. ■ Manually enter the list—The **Create** button opens the List of SIP Servers window. See Managing the List of SIP Servers.	
Add a new proxy	
Specifies the IP address and port of the SIP Server or Session Border Controller (SBC).	
Enable Multi-homed Outbound Proxy Mode	Allows phones behind the same system to use the default softswitch or a specified softswitch.

Table 6-19 SIP Settings Parameters (continued)

Item	Description
Enable Transparent Proxy Mode	Allows the system to intercept SIP messages from a LAN-side phone regardless of the Outbound Proxy and SIP Proxy values configured in the phone.
Limit Outbound to listed Proxies / SIP Servers	Restricts the number of permitted proxies that are specified in the Allowed SIP Proxies window. Limit Outbound is the default in Transparent Proxy Mode. The system only process outbound messages intended for a pre-configured list of proxies and SIP servers. un-checking this box allows the system to process all outbound messages for any SIP proxy/server.
Limit Inbound to listed Proxies / SIP Servers	Allows the system to process only inbound messages from a pre-configured list of proxies and SIP servers. un-checking the box allows the system to process all inbound messages from any SIP proxy/server.

Allowed SIP Proxies

Lists the 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 is always included and does not have to be in this list.

See Configuring Allowed SIP Proxies.

List of SIP Proxies

Lists the IP addresses of outbound proxies or registrars that are allowed in transparent proxy mode.

Add a new proxy

Configures a list of proxies and SIP servers.

Stale Timer

See Configuring the SIP Stale Timer.

Stale Timer	Automatically deletes SIP clients that have not registered within the given time period. If no REGISTER requests have been received from the client during this time, the client will be automatically deleted. Default is 1440 minutes. It is recommended that this time be much longer than the normal re-registration period in order to avoid clients being accidentally deleted.
Disable NAT traversal	Disables NAT traversal logic even when NAT traversal sessions are licensed.

Table 6-19 SIP Settings Parameters (continued)

Item	Description
Round robin SIP requests	Forwards requests from endpoints to IP addresses configured in the Round Robin SIP proxies list in a round robin manner.
UDP Settings	
See Configuring UDP Settings.	
Client Listening Port(s)	Specifies the ports on which the system listens for SIP over UDP messages from SIP clients. To specify multiple UDP ports, separate each port with a comma. Default is “5060,5070,5075.”
Server Facing Port	Specifies the source port to use when sending SIP over UDP messages to the SIP Server. The system also listens for SIP messages on this port, similar to the Client Listening Ports.
REGISTER restricted to port	Specifies that REGISTER requests will only be processed on the specified port if set to a non-zero port number that matches one of the specified UDP Inbound ports. REGISTER messages sent to other SIP ports are logged and discarded without further processing. When set to zero, REGISTER requests are processed normally on all configured SIP ports and connections. Default is 0.
TCP Settings	
See Configuring TCP Settings.	
Port	Specifies the port on which this device will listen for SIP over TCP connection requests. Enter any valid TCP port.
Timeout (minutes)	Sets the amount of inactive time. The system monitors all TCP connections and if there is no activity on any connection for a specified amount of time, that connection is closed. Minimum value is 4 minutes.
TLS Settings	
See Configuring TLS Settings.	
Port	Specifies the port on which this device will listen for SIP over TLS connection requests. Enter any valid TCP port. The TLS port cannot be the same as the TCP port.

Table 6-19 SIP Settings Parameters (continued)

Item	Description
TLS Protocol	Specifies TLSv1—Allows TLS version 1.0 protocol only (RFC 2246)
Ciphers String	Adds or restricts the cipher suites offered by this device during a TLS handshake. Enter the following string in the **Ciphers String** field: **TLSv1+HIGH:!eNULL:!aNULL**
LAN and WAN	Selects the LAN and WAN interface policies. The following options are available: ■ Certificate—The X.509 certificate for the interface in PEM format. The certificates are loaded using the **Security** > **Certificates** page. Make sure that the common name (CN) in the certificate matches the domain name or IP of the interface. ■ Policy—Peer certificate verification policy: ■ No check—The peer certificate is not verified. ■ Verify if provided—Send a client certificate request to clients but continue handshake if the client does not return a certificate. Fail if certificate is returned and the verification fails. ■ Require and Verify—Send a client certificate request to clients and continue only if the client sends a certificate and the certificate verification succeeds. ■ Require and Verify Once—Same as Require and Verify except that client certificate requests are not sent during renegotiation.
SDP Modifications	
Modifies codecs in the SDP. See Configuring SDP Modifications Settings.	
SDP Codec Operation	Selects the type of operation to be performed on codec payloads in the SDP. The following options are available: ■ No Action ■ Delete given codecs—The list of codecs given in the codecs list will be deleted from the SDP. ■ Only Allow given codecs—If the SDP has any codecs not listed in the list of codecs then it will be removed from the SDP. ■ Change Codec Order—If the codecs given in the codecs list occur in the SDP, the system ensures that the list is ordered entered.

Table 6-19 SIP Settings Parameters (continued)

Item	Description
SDP Section that will be modified	Selects the media section for searching the codecs: ■ Audio—Search for audio codecs. ■ Video—Search for video codecs.
Codecs	Specifies a comma separated list of codecs to search for. The codecs should be referred by their names such as PCMU, PCMA, G723, G729, H261, and so on. Refer to Real-Time Transport Protocol (RTP) Parameters at the following link for standardized codec names: http://www.iana.org/assignments/rtp-parameters/rtp-parameters.xml
Reject when No Match Codec	Select the checkbox to allow the EdgeMarc to reject the incoming INVITE with a 488 SIP response code when no remaining codec is left in the SDP after codec operation. When the box is un-checked, the EdgeMarc continues forwarding the SDP after codec operation to the remote side. This option is only available for SIP B2BUA mode.

Priority Numbers

The EdgeMarc allows you to set up to 4 priority numbers for calls that will take precedence over non-priority numbers. These priority numbers are treated for high priority call completion. For example, a company might have priority numbers for special applications assigned to speed-dial number keys that have been programmed into phone for emergency or security. These priority numbers are configured in the EdgeMarc through the following interface.

When a priority number is called and the call limit has been reached (via the license key limit or CAC), the EdgeMarc will drop the non-priority calls and complete the call that has been assigned the priority number. Calls with priority numbers cannot be dropped if all active calls are assigned priority numbers and additional call attempts are also made with a priority number.

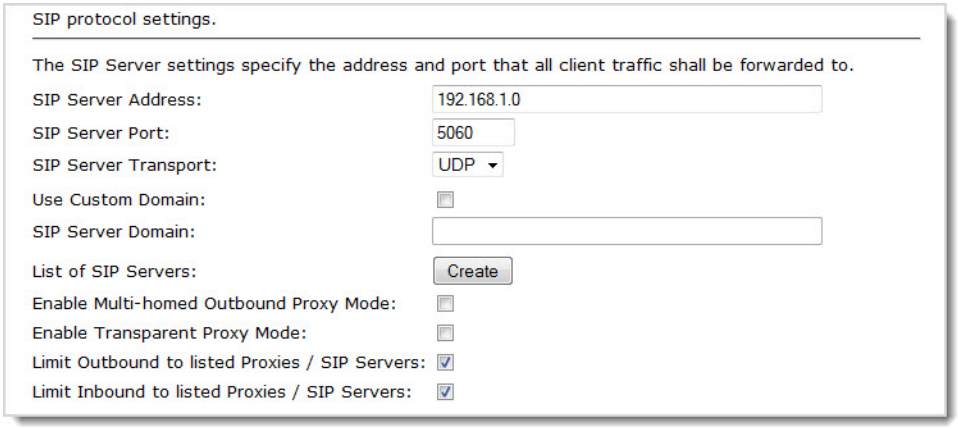
Priority Number 1-4	Enter a number in the Priority Number field, for example, “777.”

Registration Rate-Pacing parameters are available on the Survivability page. Click the **Survivability page** link at the bottom of the SIP Settings page, or choose **VoIP** > **Survivability** and refer to Configuring Survivability.

Configuring SIP Protocol Settings

1. Choose **VoIP** > **SIP** (Figure 6-25).

Figure 6-25 SIP Protocol Settings



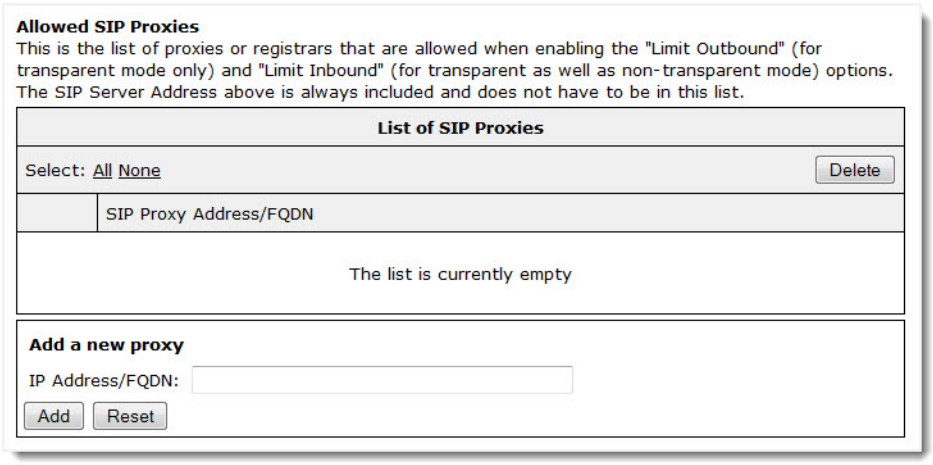
2. In the **SIP Server Address** field, enter an IP address or URL.
3. In the **SIP Server Port** field, enter the port number.
4. (Optional) If you want to configure a custom domain name other than the default SIP Server address, select the **Use Custom Domain** checkbox. The SIP Server Domain field becomes active.
5. Enter a custom domain in the **SIP Server Domain** field if you selected the **Use Custom Domain** checkbox.
6. Create a list of secondary SIP servers for automatic failover in **List of SIP Servers**. See Managing the List of SIP Servers.
7. Select the **Enable Multi-homed Outbound Proxy Mode** checkbox to allow phones behind the same system to use the default SIP Server or a specified server.
8. Select the **Enable Transparent Proxy Mode** checkbox to intercept SIP messages from a LAN-side phone regardless of the Outbound Proxy and SIP Proxy values configured on the phone.
9. Select the **Limit Outbound to listed Proxies / SIP Servers** checkbox to process only outbound messages intended for a pre-configured list of proxies and SIP servers.
10. Select the **Limit Inbound to listed Proxies / SIP Servers** checkbox to process inbound messages from a pre-configured list of proxies and SIP servers.
11. Proceed to Configuring Allowed SIP Proxies.

Configuring Allowed SIP Proxies

This is the list of proxies or registrars that are allowed when enabling the Limit Outbound and Limit Inbound options.

1. Choose **VoIP ALG** > **SIP** (Figure 6-24).
2. Scroll to **Allowed SIP Proxies**.

Figure 6-26 Allowed SIP Proxies



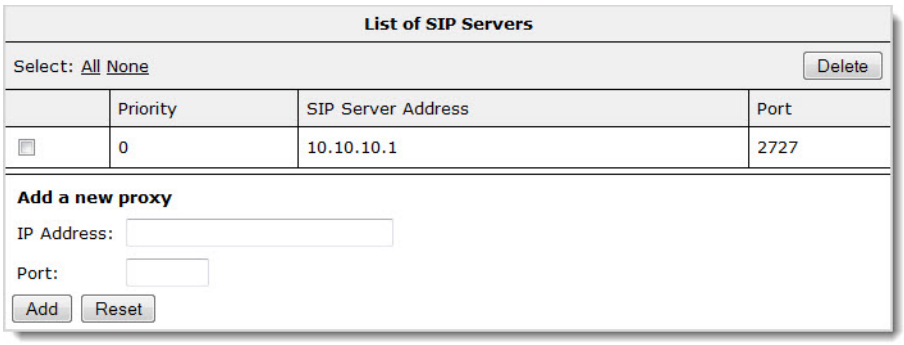
3. Manage SIP proxies in the **List of SIP Proxies** table:
   a. Select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
   b. Click **Delete** to remove an entry.
   c. Click **OK** to confirm.
4. Add a new proxy in the **Add a new proxy** window:
   a. Enter the IP address of the SIP Server or SBC. URLs are not allowed in this field.
   b. Click **Add**. The new proxy is added to the List of SIP Proxies table.

Managing the List of SIP Servers

Create and manage the list of secondary SIP servers for automatic failover.

1. Choose **VoIP** > **SIP** (Figure 6-24).
2. Click **Create** to open the List of SIP Servers window (Figure 6-27).

Figure 6-27 List of SIP Servers



3. Manage SIP servers In the **List of SIP Servers** table:
   a. Select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
   b. Click **Delete** to remove an entry.
   c. Click **OK** to confirm
4. Add a new proxy in the **Add a new proxy** window:
   a. In the **IP Address** field, enter a new IP address. URLs are not allowed in this field.
   b. In the **Port** field, enter SIP Server or SBC port.
   c. If all the SIP servers belong to the same domain, enter a SIP domain in the field provided, otherwise leave this field empty.
   d. To revert back to the single SIP Server entry field, delete all rows in the table by clicking the garbage can in each row.
5. Click **Add**. The new SIP Server Address is added to the List of SIP Servers table.
6. Proceed to Configuring the SIP Stale Timer.

Configuring the SIP Stale Timer

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

1. Choose **VoIP** > **SIP** (Figure 6-24).
2. Scroll to **Stale Timer** (Figure 6-28).

Figure 6-28 SIP Stale Timer



3. Enter a number of minutes in the **Stale client time (m)** field. If no REGISTER requests have been received from the client during this time, the client will be automatically deleted. Default is 1440 minutes. It is recommended that this time be much longer than the normal

re-registration period in order to avoid clients being accidentally deleted.

4. Click **Submit**.

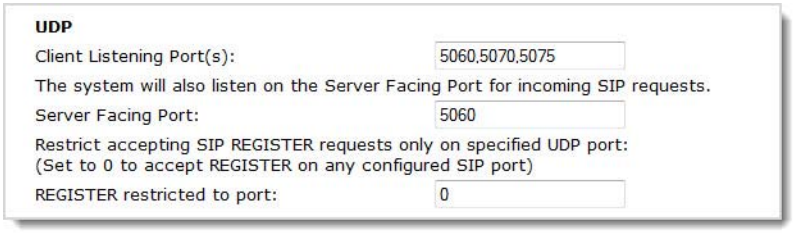
   A message indicates that service will be temporarily interrupted.

5. Click **OK** to confirm.

Configuring UDP Settings

1. Choose **VoIP** > **SIP** (Figure 6-24).
2. Scroll to **UDP** (Figure 6-29).

Figure 6-29 SIP Settings - Configuring UDP



3. In the **Client Listening Port(s)** field, enter the port(s) on which the system listens for SIP over UDP messages from SIP clients. To specify multiple UDP ports, separate each port with a comma. The default value is “5060,5070,5075.”
4. In the **Server Facing Port** field, enter a source port to use when sending SIP over UDP messages to the SIP Server. The system also listens for SIP messages on this port similar to the Client Listening Port(s).
5. In the **REGISTER restricted to port** field, enter 0 to accept REGISTER on any configured SIP port. Or enter any UDP port number to restrict REGISTER requests to the specified port.

Configuring TCP Settings

1. Choose **VoIP** > **SIP** (Figure 6-24).
2. Scroll to **TCP** (Figure 6-30).

Figure 6-30 SIP Settings - Configuring TCP



3. In the **Port** field, enter the port on which this device will listen for SIP over TCP connection requests. Enter any valid TCP port.
4. In the **Timeout (minutes)** field, enter a length of time in minutes for this device to monitor all TCP connections. If there is no activity on any

of them for a specified amount of time, the connection is closed. Minimum value is 4 minutes.

Configuring TLS Settings

1. Choose **VoIP** > **SIP** (Figure 6-24).
2. Scroll to **TLS** (Figure 6-31).

Figure 6-31 SIP Settings - Configuring TLS

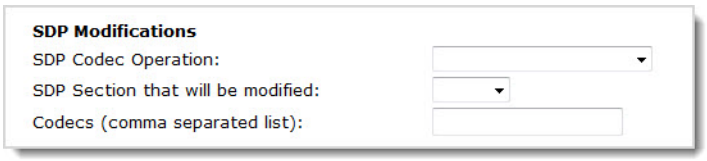


3. In the **Port** field, enter the port on which this device will listen for SIP over TLS connection requests. Enter any valid TCP port. The TLS port cannot be the same as the TCP port.
4. Select a protocol from the TLS Protocol drop-down list:
   - TLSv1—Allow TLS version 1.0 protocol only (RFC 2246)
5. In the **Ciphers String** field, enter a string to add or restrict the cipher suites offered by this device during a TLS handshake.
6. Select **LAN** and **WAN** interface policies from the following drop-down lists:
   - **Certificate**—The X.509 certificate for the interface in PEM format. The certificates are loaded using the Security > Certificate Store page. Make sure that the common name (CN) in the certificate matches the domain name or IP of the interface.
   - **Policy**—Peer certificate verification policy:
     - No check—The peer certificate is not verified
     - Verify if provided—Send a client certificate request to clients but continue handshake if the client does not return a certificate. Fail if certificate is returned and the verification fails.
     - Require and Verify—Send a client certificate request to clients and continue only if the client sends a certificate and the certificate verification succeeds.
     - Require and Verify Once—Same as “Require and Verify” except that client certificate requests are not sent during renegotiation

Configuring SDP Modifications Settings

1. Choose **VoIP** > **SIP** (Figure 6-24).
2. Scroll to **SDP Modifications** (Figure 6-31).

Figure 6-32 SIP Settings - SDP Modifications



3. Choose a type of operation to be performed on codec payloads in the SDP from the SDP Codec Operation drop-down list:
   - Delete given codecs—The list of codecs in the codecs list will be deleted from the SDP.
   - Only Allow given codecs—If the SDP has any codecs not listed in the list of codecs they will be removed from the SDP.
   - Change Codec Order—If the codecs given in the codecs list occur in the SDP, the system automatically orders the list.
4. Choose the media type to be searched in the **SDP Section that will be modified** drop-down list:
   - Audio—Search for audio codecs.
   - Video—Search for video codecs.
5. In the **Codecs** field, enter the list of codecs to search for separated by commas. Use names such as PCMU, PCMA, G723, G729, H261, and so on. Refer to Real-Time Transport Protocol (RTP) Parameters at the following link for standardized codec names:

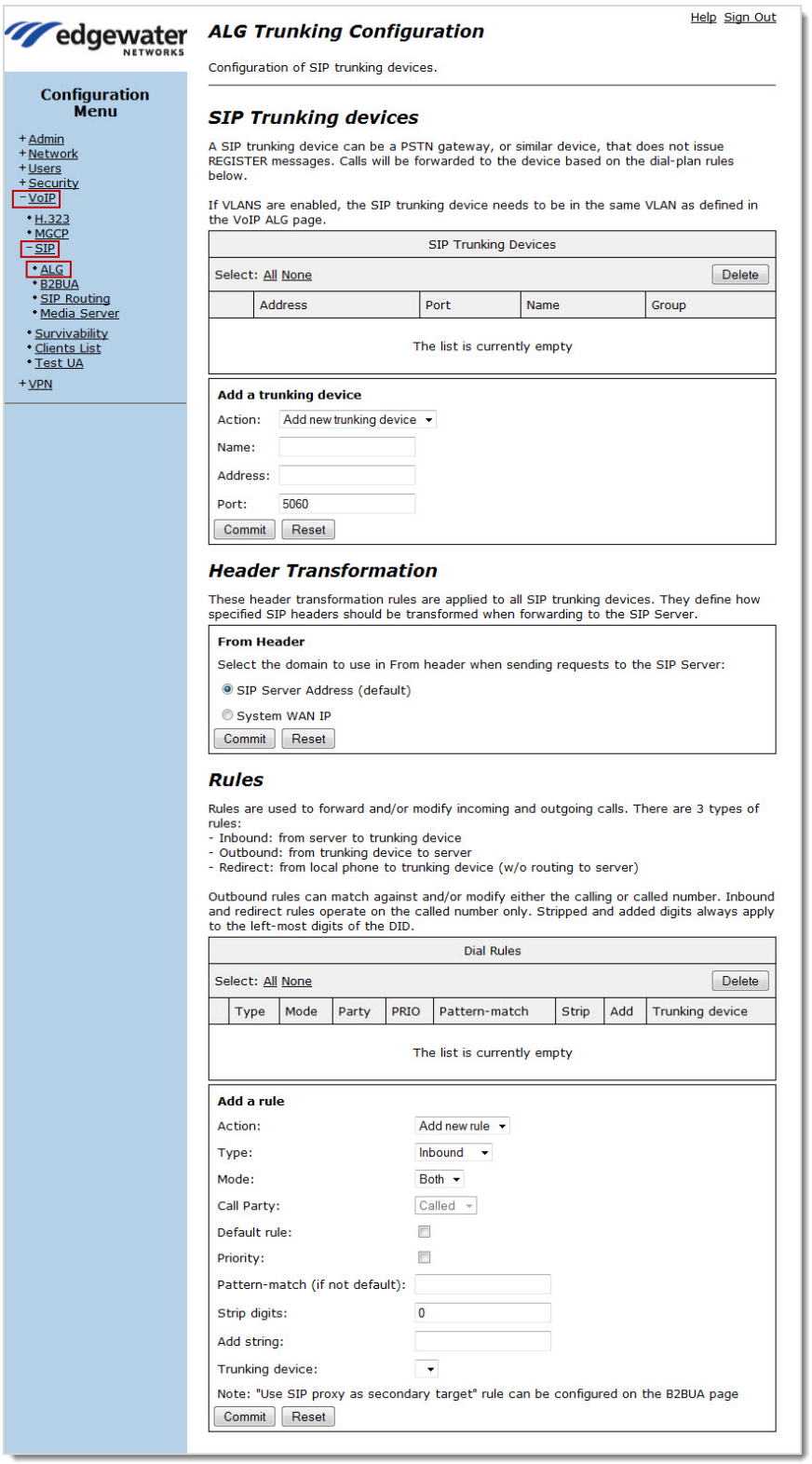
   http://www.iana.org/assignments/rtp-parameters/rtp-parameters.xml
6. Click **Submit** to save all settings on the page.

Configuring SIP ALG Trunking

SIP trunking is used to configure dial plans or rules to route calls to and from the softswitch/IP-PBX to client devices that do not register. A number of trunking devices are configured and rules are set up to route calls from the softswitch/IP-PBX to these devices (Inbound rules), manipulate dial strings in calls from these devices to a softswitch/IP-PBX (Outbound rules), or redirect calls from other local devices to these trunking devices without routing the call to the softswitch/IP-PBX first (Redirect rules).

1. Choose **VoIP** > **SIP** > **ALG** (Figure 6-33).

Figure 6-33 VoIP ALG Trunking Configuration Page



2. Configure settings on the ALG Trunking Configuration page:

- Configuring SIP Trunking Devices
- Configuring Header Transformation
- Configuring Dial Rules

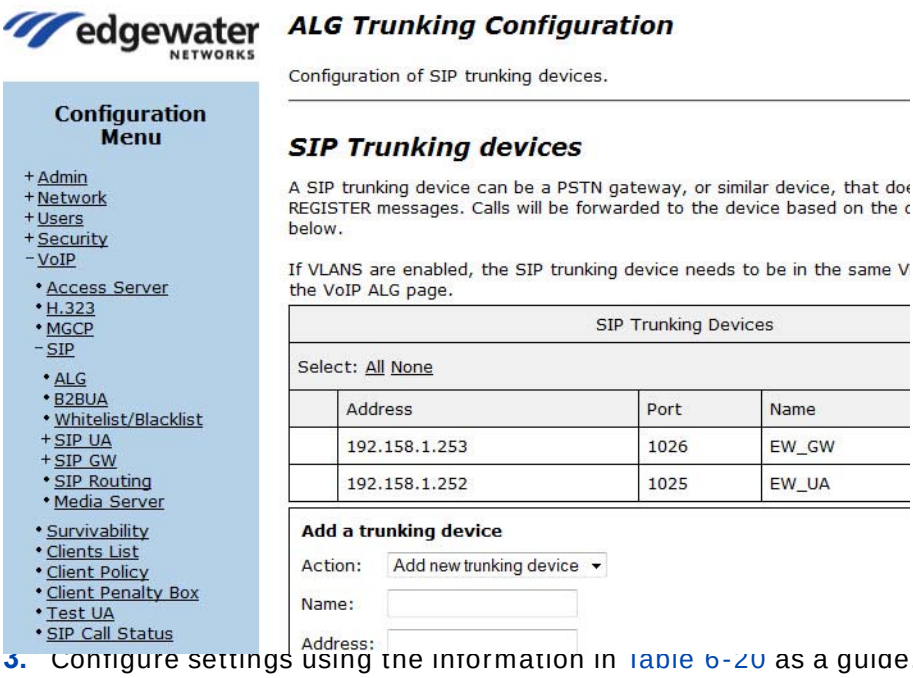
Configuring SIP Trunking Devices

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

Tip
If VLANS are enabled, the SIP trunking device must have the same VLAN as defined on the **VoIP ALG** home page. See Configuring VoIP ALG Settings. If internal FXO ports are available (on appropriate platforms) and enabled, they act as a default device unless configured otherwise.

1. Choose **VoIP** > **SIP** > **ALG** (Figure 6-33).
2. Scroll to **SIP Trunking Devices** (Figure 6-34).

Figure 6-34 SIP Trunking Devices



3. Configure settings using the information in Table 6-20 as a guide. When you have finished configuring settings, click **Commit** to make your changes take effect.

Table 6-20 SIP Trunking Devices Configuration Parameters

Item	Description
SIP Trunking Devices	
Adds and manages available SIP trunking devices in a list. **Note:** Do not connect to the network until all registered trunking devices are completely configured on the ALG Trunking page. Otherwise the registrations will create separate client entries in the system database and will not be recognized as trunking device lines. If this happens, go to the SIP Clients List page and delete these entries. Choose **VoIP** > **Clients List** and refer to Configuring the Clients List.	
Action	Add or edit a SIP trunking device in the **Add a trunking device** window.
Name	(Optional) Enter a name to make it easier to remember which device the entry refers to. This name is only used for user feedback.
Address	Enter the SIP trunking IP address.
Port	Enter the SIP trunking port number. If internal FXO ports are available (on appropriate platforms) and enabled, they will act as a default device unless configured otherwise.

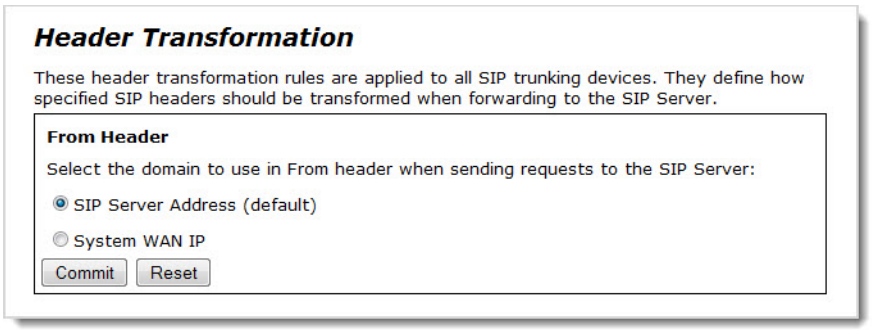
4. Click **Commit** to save your settings.
5. To delete SIP trunking devices In the SIP Trunking Devices table:
   a. Select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
   b. Click **Delete** to remove an entry.
   c. Click **OK** to confirm
6. Proceed to Configuring Header Transformation.

Configuring Header Transformation

When forwarding SIP messages from a trunking device to the SIP Server, certain headers may need to be transformed differently for proper interoperation. Define how specified SIP headers should be transformed when forwarding to the SIP Server. These settings are applied to all SIP trunking devices.

1. Choose **VoIP** > **SIP** > **ALG** (Figure 6-34).
2. Scroll to **Header Transformation** (Figure 6-35).

Figure 6-35 Header Transformation



3. Configure settings using the information in Table 6-21 as a guide.

Table 6-21 Header Transformation Configuration Parameters

Item	Description
Header Transformation	Defines how specified SIP headers should be transformed when forwarding to the SIP Server. These settings are applied to all SIP trunking devices.
From Header	Select the domain to use in From header when sending requests to the SIP Server: ■ SIP Server address (default)—SIP endpoints that register typically use the SIP Server address. ■ System WAN IP address—Endpoints that do not register (most trunking devices) set the domain to the systems IP address. SIP endpoints that register typically set the domain in the From header to the SIP Server address. Endpoints that do not register (most trunking devices) set the domain to the system IP address. Check your SIP server configuration on the SIP Settings page to determine which setting is correct. **Choose** > **SIP** and refer to Configuring SIP Settings.

4. Click **Commit** to save your settings.
5. Proceed to Configuring Dial Rules.

Configuring Dial Rules

Dial rules match incoming calls to a specific device. A rule is written with a number of explicit digits and/or patterns.

Understanding Dial Rules

A rule is written with a number of explicit digits and/or patterns. The patterns may match a range of digits. Each rule can have a number of digits to strip, and a string of digits to add, associated with it. If a rule has a number of digits to strip, this number of digits will be removed from the called number when there is a match. Likewise, a string of digits to add will be added to the dialed number when the rule matches.

Rules are used to forward and/or modify incoming and outgoing calls. There are 3 types of rules:

- Inbound—From the server to the trunking device.
- Outbound—From the trunking device to the server.
- Redirect—From the local phone to the trunking device (without routing to the server).

Outbound rules can match against and/or modify either the calling or called number. Inbound and redirect rules operate on the called number only. Stripped and added digits always apply to the left-most digits of the DID.

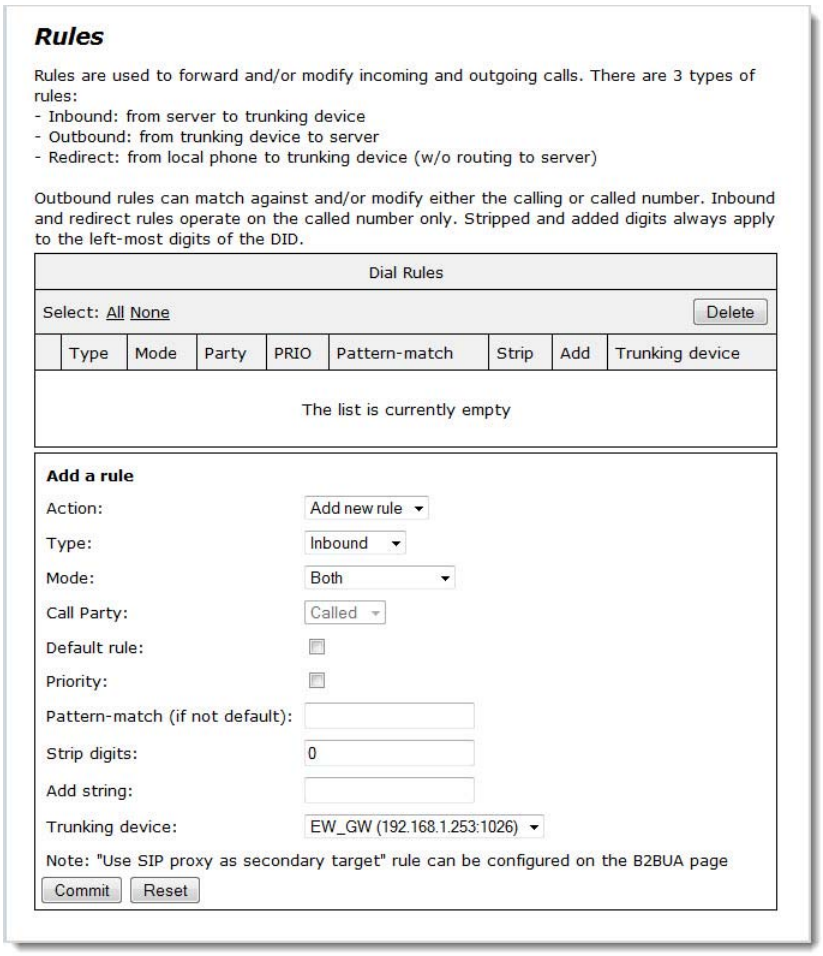
When entering an Outbound rule on the Trunking Device page, the drop-down list offers an option “Any.” When this option is selected the rule is matched based on pattern only.

An inbound or redirect rule can be given priority. Any non-priority rule is preempted in favor of a priority call. A default rule cannot have a dial string for matching. There can be only one default rule. A default rule can only be inbound.

Configure Rules

1. Choose **VoIP** > **SIP** > **ALG** (Figure 6-34).
2. Scroll to **Rules** (Figure 6-36).

Figure 6-36 Rules Settings



3. Configure settings using the information in Table 6-22 as a guide. When you have finished configuring settings, click **Commit** to make your changes take effect.

Table 6-22 Rules Parameters

Item	Description
Rules	Configure rules for forwarding and/or modifying incoming and outgoing calls.
Add a New Rule	Add a new rule in the **Add a rule** window:
Action	Choose **Add a new rule** from the **Action** drop-down list.

Table 6-22 Rules Parameters (continued)

Item	Description
Type	Choose a rule type from the drop-down list: ■ Inbound—From the softswitch via the voice system to the trunking device. Used to determine which trunking device to use for an inbound call. ■ Outbound—From the trunking device via the voice system to the softswitch. Used to determine a dial string modification rule to use for calls from a specified trunking device. ■ Redirect—From a local device directly to the trunking device. Used to directly connect a local device to a trunking device without sending the signaling to the softswitch first. An inbound or redirect rule can be given priority; non-priority rules are preempted in order to connect a priority call. A default rule cannot have a dial string for matching and there can be only one default rule, which can only be inbound. Each rule can have a number of digits to strip, and a string of digits to add. If a rule has a number of digits to strip, this number of digits is removed from the called number in case of a match. Likewise, a string of digits to add is added to the dialed number in case the rule matches.

Table 6-22 Rules Parameters (continued)

Item	Description
Mode	Choose a mode from the Mode drop-down list: ■ **Both**—Default when Survivability is on and the only option if Survivability is turned off. When a rule is configured in Both mode, and all other criteria match then this rule will be selected whether the EdgeMarc is in local or remote mode. ■ **Local Mode On**—Allows you to configure a separate set of voice routing rules when the unit is operating in local mode. The rule for the EdgeMarc can be in Local Mode or Both mode. ■ **Local Mode Off**—The rule for the EdgeMarc can be in Remote Mode or Both mode. **Note:** If multiple rules are configured in Both and Local Mode Off, the first matching rule will be selected when Survivability is turned on and the EdgeMarc is in Remote Mode. Similarly, if multiple rules are configured in Both and Local Mode On, the first matching rule will be selected when Survivability is turned on and The EdgeMarc is in Local Mode.
Call Party	Specifies either **Called** or **Calling** if the type is Outbound.
Default	Select the **Default rule** checkbox to specify the default match for any inbound call that was not able to find a destination. **Note:** A default rule cannot have a dial string for matching. There can be only one default rule. A default rule can only be inbound.
Pattern match	Enter a pattern to match a pattern to a call party. See SIP Trunking Patterns for supported trunking patterns and pattern examples.
Strip digits	Enter the number of digits to strip from the beginning of the number.
Add string	Enter a dial string to prepend to the beginning of the number.
Trunking device	Choose a configured trunking device from the SIP Trunking Devices drop-down list. **Tip:** See Configuring SIP Trunking Devices to create a list of devices.

4. Click **Commit** to save your settings.

5. Edit a rule in the **Add a rule** window:
   a. Choose **Edit new rule** from the **Action** drop-down list.
   b. Edit settings in the fields provided.
   c. Click **Commit** to save your settings.
6. To delete rules in the **Dial Rules** table:
   a. Select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
   b. Click **Delete**.
   c. Click **OK** to confirm.



Tip
To use the default SIP proxy as a secondary target rule, go to the B2BUA Trunking Configuration page under Credentials and Registration. Choose **VoIP** > **SIP** > **B2BUA** and refer to Managing B2BUA Credentials and Registration.

SIP Trunking Patterns

Table 6-23 Trunking Patterns

Symbol	Description
Patterns	
.	Matches one or more digits.
[x-y]	Matches any single digit between x and y (inclusive).
X	Matches any digit between 0 and 9, equivalent to [0-9].
Z	Matches digit between 1 and 9, equivalent to [1-9].
N	Matches any digit between 2 and 9, equivalent to [2-9].
Pattern Examples	
■ **1XXX** Matches any four-digit number starting with 1, e.gS. 1000, 1200, 1234	
■ **9NXXXXXX** Local calls preceded by a 9, e.g. 95551234	
■ **91NXXNXXXXXX** Long distance calls preceded by a 9, e.g. 914085551234	

Configuring VoIP SIP B2BUA Trunking

Back-to-Back User Agent (B2BUA) enables the EdgeMarc to control all aspects of a call that are defined in a SIP INVITE request or in subsequent SIP methods that inherit the header contents of a SIP INVITE request. B2BUA provides the system administrator with the ability to finely tune the rules by which SIP traffic is distributed between a SIP Server and a PBX on your network.

SIP B2BUA Request Methods

Table 6-24 SIP B2BUA Request Method Support

Item	Description
PRACK and UPDATE	■ PRACK—Enabling or disabling this option provides SIP PRACK interoperability support. SIP PRACK interoperability provides B2BUA support to allow an endpoint that does not support PRACK to interoperate with an endpoint that requires PRACK support. When enabled, the system will add Supported: 100rel in the SIP INVITE or add Required: 100rel in the 18X response messages the systems B2BUA sends out. Disabling this option will revert the systems B2BUA to PRACK pass-through support. Default value: Enabled. ■ UPDATE—Modifies the state of a session without changing the state of the dialog. B2BUA can mediate PRACK and UPDATE signaling between endpoints that require PRACK and UPDATE and endpoints that do not support PRACK and UPDATE. For example, if B2BUA receives an INVITE that requires reliable provisional responses, but the call destination does not support reliable provisional responses, B2BUA will generate reliable provisional responses and will also handle the retransmission of reliable provisional responses. Similarly B2BUA will always indicate support for reliable provisional responses even if the calling party does not indicate it. This way the recipient can choose to the send provisional responses reliably or unreliably
INFO	Sends mid-session information that does not modify the session state.
MESSAGE	Transports instant messages using SIP.

Table 6-24 SIP B2BUA Request Method Support

Item	Description
NOTIFY	Notifies the subscriber of a new Event.
OPTIONS	Queries the capabilities of servers.
PING	Confirms that the endpoints are alive and verifies that a signaling path is still valid.
PUBLISH	Publishes an event to the server.
SUBSCRIBE	Subscribes for an Event of Notification from the Notifier.

Configure B2BUA Trunking

The B2BUA Trunking Configuration page is divided into sections. Each section may have an **Update** button at the end. Clicking this button applies the changes to the local cache; it does not affect the EdgeMarc. To send configuration changes to the EdgeMarc, click **Submit** at the end of the page.

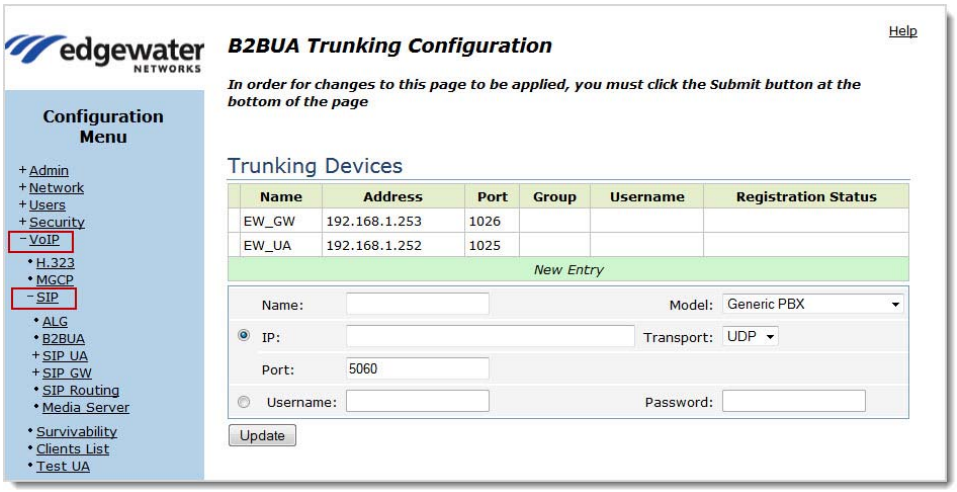
1. Choose **VoIP** > **SIP** > **B2BUA** to open the B2BUA Trunking Configuration page.
2. Configure the following settings on the B2BUA Trunking Configuration page:

- Creating a New Trunking Device
- Managing B2BUA Credentials and Registration
- Managing B2BUA Actions
- Managing B2BUA Pattern and Digit Matching
- Managing Header Manipulation Language

Creating a New Trunking Device

1. Choose **VoIP** > **SIP** > **B2BUA** to open the B2BUA Trunking Configuration page. The first configuration window on the page is Trunking Devices (Figure 6-37).

Figure 6-37 B2BUA Trunking Devices Configuration



2. Configure settings using the information in Table 6-25 as a guide. When you have finished configuring settings, click **Update** to make your changes take effect.

Table 6-25 B2BUA Trunking Configuration Parameters

Item	Description

Trunking Devices	Displays a list of configured trunking devices and their registration status on the system:
	■ Name—Identifies the trunking device.
	■ Address—PBX IP address for the trunking device.
	■ Port—Port number of the trunking device.
	■ Group—Group that the trunking device has been assigned to.
	■ Username—Authenticates the trunking device.
	■ Registration Status—Registration status for the trunking device:
	  ■ Registered
	  ■ Not Registered

New Entry	Creates a new trunking device on the system and adds it to the Trunking Devices table. When the trunking device has registered with the system the Registration Status column displays “Registered” and the Address and Port columns update with the address information from the Contact header of the Register request. Create a new trunking device in the Trunking Devices window (Figure 6-37). If necessary, click **New Entry** to open the new trunking device entry window.
Name	Enter the name for identifying the trunking device.
Model	Choose the PBX model for the trunking device from the **Model** drop-down list. Required for dynamically configured trunking devices.
IP	Click the **IP** radio button and enter an IP address in the field provided. Enter the PBX IP address for the trunking device: ■ Statically configured—You must also enter a port. ■ Dynamically configured—The trunking device registers with the system and requires a username and password.
Transport	Choose a transport method from the **Transport** drop-down list. ■ UDP ■ TCP ■ TLS
Port	Enter the port number for the trunking device. Required for statically configured trunking devices.

Table 6-25 B2BUA Trunking Configuration Parameters (continued)

Item	Description
Username	Enter the user name for authentication with dynamically configured trunking devices.
Password	Enter the password for authentication with dynamically configured trunking devices.
Note: Click **Update** to save your settings in the Trunking Devices window. Your changes are applied to the local cache. To save your configuration changes to the EdgeMarc, click **Submit**.	

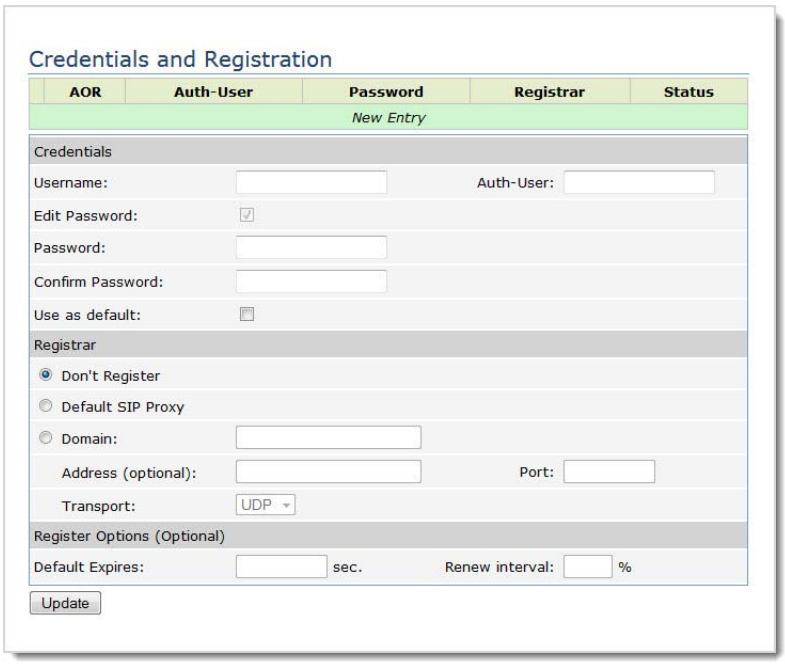
3. To add another trunking device, click **New Row** to add a new row to the Trunking Devices table.
4. To edit a device:
   a. Click once on the device in the Trunking Devices table. The row is highlighted and the information from the selected line is displayed in the details box below the table.
   b. Edit trunking device details and click **Update**. Your changes are applied to the local cache. To save your configuration changes to the EdgeMarc, click **Submit**.
5. To delete a device, click the red X next to the selected device. The device is immediately removed from the Trunking Devices table. You do not have to click **Submit** when deleting a device.
6. Click **Update** to save your settings in the Trunking Devices window.
7. Proceed to Managing B2BUA Credentials and Registration.

Managing B2BUA Credentials and Registration

The Credentials and Registration window configures authentication credentials and specifications for registering Address of Records (AORs).

1. Choose **VoIP** > **SIP** > **B2BUA**.
2. Scroll to the **Credentials and Registration** window (Figure 6-38). If necessary, click **New Entry** to open the new credentials and registrar entry window.

Figure 6-38 B2BUA Credentials and Registration Configuration



3. Configure settings using the information in Table 6-26 as a guide. When you have finished configuring settings, click **Update** to make your changes take effect.

Table 6-26 B2BUA Credentials and Registration Configuration Parameters

Item	Description
Credentials and Registration	Displays a list of registered AORs. See Managing B2BUA Credentials and Registration.
AOR	Displays the Address of Record or Username. The values in this column can one of the following: ■ Username—If the entry is an Authentication credential or the registrar is the default proxy, this column displays the Username, for example 2408881028. ■ SIP URI—If the entry is for registering an AOR to non-default proxy, full SIP URI is displayed. For example, sip:1234567890@sipdomain.com. Where “sipdomain.com” is the domain name of the registrar. ■ Default—For default or wild card credentials.

Table 6-26 B2BUA Credentials and Registration Configuration Parameters (continued)

Item	Description
Auth-User	Displays the authentication user. If the field is blank, the authentication user is the same as the Username. The AOR Auth-User field supports up to 50 characters. A warning message is displayed on the B2BUA Trunking Configuration page if more than 50 characters are entered.
Password	Specifies the shared secret for SIP digest authentication.
Registrar	Displays registrar information: ■ If an address was given for a non-default registrar, this is shown in the format IP-ADDRESS:PORT. ■ If no address was given for a non-default registrar, this field is blank, because the address is determined through a DNS A lookup. ■ The field displays “Default” for default SIP Registrar.
Status	Displays registration status: ■ Trying—Register request has been sent but no response yet. ■ OK—A 200 response was received. The registration is successful. ■ Error message—The error code and the error phrase are displayed. For example, the registration failed for 403 Forbidden.

Credentials - New Entry

Creates new credentials and registration information.

Username	Enter a valid SIP Username. This becomes part of the user portion of the AOR. If you want to enter a default credential, leave this field blank.
Auth-User	Enter required default credentials. Otherwise leave this field blank; B2BUA uses the Username as Auth-user.
Password	Enter the required shared secret for SIP digest authentication. This field cannot be blank if you entered credentials in the Auth-User field.
Use as default	Select the **Use as Default** checkbox to use this SIP Authentication credential by default (recommended).

Table 6-26 B2BUA Credentials and Registration Configuration Parameters (continued)

Item	Description
Registrar - New Entry Select a registration type radio button: ■ **Don't Register**—Default. The Username will not be registered. ■ **Default SIP Proxy**—B2BUA uses the default SIP proxy as configured on the SIP Settings page. Choose **VoIP** > **SIP** and refer to Configuring SIP Protocol Settings to register the AOR. ■ **Custom**—Specifies custom Registrar settings.	
Domain	Enter the Registrar domain. This should be entered as **sip:proxydomain.com** or **sip:1.2.3.4**
Address	(Optional) Enter the Registrar IP Address. If the IP address is provided, B2BUA does not do a DNS A lookup on the domain name and uses this address instead.
Port	Enter the Registrar port.
Transport	Select the Registrar port from the Transport drop-down list: ■ UDP ■ TCP ■ TLS
Register Options (Optional) Sets registration options when you set Default SIP Proxy or Domain as the Registrar: ■ **Default Expires**—Enter the number of seconds until expiration for the initial Register request. Defaults to 3600 seconds if left blank. ■ **Renew Interval**—Enter the percentage of registration interval after which the B2BUA will renew the registration. Defaults to 80% if left blank.	

4. To edit a credentials entry:
   a. Click once on the entry in the Credentials and Registration table. The row is highlighted and the information from the selected line is displayed in the details box below the table.
   b. Edit details and click **Update**. Your changes are applied to the local cache. To save your configuration changes to the EdgeMarc, click **Submit**.

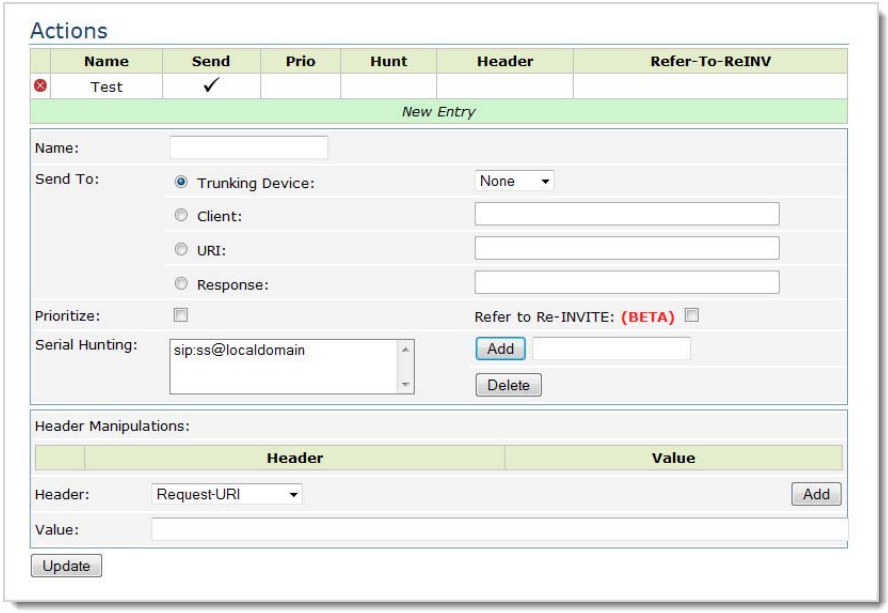
5. To delete a credentials entry, click the red X next to the selected entry. The entry is immediately removed from the Credentials and Registration table. You do not have to click **Submit** when deleting an entry.
6. Click **Update** to save your settings in the Credentials and Registration window.
7. Proceed to Managing B2BUA Actions.

Managing B2BUA Actions

Define the actions you would like the EdgeMarc to take when an INVITE is selected.

1. Choose **VoIP** > **SIP** > **B2BUA**.
2. Scroll to the **Actions** window (Figure 6-39). If necessary, click **New Row** to create a new Actions entry.

Figure 6-39 B2BUA Actions



3. Configure settings using the information in Table 6-27 as a guide. When you have finished configuring settings, click **Update** to make your changes take effect.

Table 6-27 B2BUA Actions Configuration Parameters

Item	Description
Actions and Pattern Matching	First define the Actions you would like the system to take when an INVITE is selected and then define a Matching criterion for the INVITE. Refer to the following: ■ Regular Expressions and Expression Examples ■ SIP Trunking Patterns
Actions	Displays a list of configured actions on the system: ■ Name—Enter the name that identifies the action. ■ Send—Indicates whether the call is redirected to the specified Trunking device. ■ Prio—Indicates that this is a priority call being sent to the FXO port (PSTN line). ■ Hunt—Lists configured INVITE serial hunting contact headers. ■ Header—Displays the Header type. ■ Refer to Re-INVITE—Indicates whether this call supports REFER Re-INVITE requests.
New Entry	Defines the actions you would like the system to take when an INVITE is selected. Once you have set the Actions, you can define a matching criterion for the INVITE in Match.
Name	Enter a unique name to identify the action. This name is used in the drop-down list in the Match section.

Table 6-27 B2BUA Actions Configuration Parameters (continued)

Item	Description
Send To	Select one of the following radio buttons: ■ **Send To**—Redirects the call to the specified location: ■ **Trunking Device**—Choose a device from the drop-down list: ■ **None**—The call is sent to the default target softswitch for outbound calls and the client found by called number lookup for inbound calls. ■ Trunking device configured on the system ■ **Client**—Manually specified client. ■ **URI**—If you choose a SIP response, it must be a response code between 300 and 699 inclusive. Any Header Manipulation Rules (HMR) rules added to the action are applied to the response. ■ **Response**—Returns a manually specified SIP response.
Prioritize	Select the **Prioritize** checkbox to identify this call as a priority call that will be sent to an FXO port (PSTN line).
Refer to Re-INVITE	Select the **Refer to Re-INVITE** checkbox to specify that REFER requests received for this call shall be converted into a series of Re-INVITE requests.
Serial Hunting	In the **Serial Hunting** field, add a list of contact headers. Click **Add** to add your entries to Serial Hunting list. A special SIP URI “sip:ss@localdomain” can be used in this field to refer to the current softswitch. To delete an entry, click once on the entry in the Serial Hunting field to highlight the entry and click **Delete**.
Header Manipulations	

Table 6-27 B2BUA Actions Configuration Parameters (continued)

Item	Description
Header	Add custom headers to the SIP message in the **Header Manipulations** fields: ■ Select a header name from the **Header** drop-down list. ■ If the name is not listed, select **Other** from the drop-down list and enter the name of the header in the field provided.
Value	Enter the header value using EdgeMarc Header Manipulation language using the information in Managing B2BUA Pattern and Digit Matching as a guide. The text should follow the format required of the SIP header. For example, if the selected header from the drop-down list is “P-Asserted-Identity,” the value should be “sip:123456@example.com. When you are finished, click **Add**. See the following support information: ■ Regular Expressions and Expression Examples ■ SIP Trunking Patterns

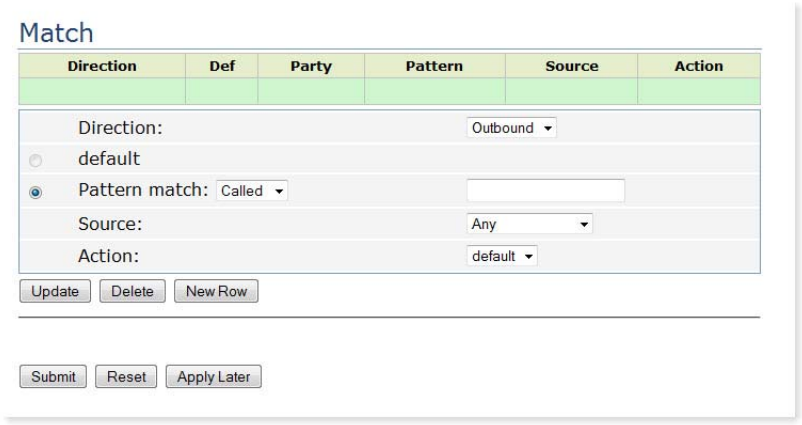
4. To edit an entry:
   a. Click once on the entry in the Actions table. The row is highlighted and the information from the selected line is displayed in the details box below the table.
   b. Edit details and click **Update**. Your changes are applied to the local cache. To save your configuration changes to the EdgeMarc, click **Submit**.
5. To delete an entry, click the red X next to the selected entry. The entry is immediately removed from the Actions table. You do not have to click **Submit** when deleting an entry.
6. Click **Update** to apply the changes to the local cache. To send configuration changes to the EdgeMarc, click **Submit** at the bottom of the B2BUA Trunking Configuration page.
7. Proceed to Managing B2BUA Pattern and Digit Matching.

Managing B2BUA Pattern and Digit Matching

Define a matching criterion for the INVITE:

1. Choose **VoIP** > **SIP** > **B2BUA**.
2. Scroll to the **Match** window (Figure 6-40). If necessary, click **New Row** to create a new Match entry.

Figure 6-40 B2BUA Match Configuration



3. Configure settings using the information in Table 6-28 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 6-28 B2BUA Match Configuration Parameters

Item	Description
Match	
Displays matching criterion for the INVITE:	
Direction	Displays the inbound softswitch and outbound trunking device or client traffic direction: ■ Inbound ■ Outbound ■ REFER-Initiated
Def	Displays the default match for any inbound call that was not able to find a destination. **Note:** Default is only available for inbound calls.
Party	Displays whether the party is Called or Caller.
Match	Displays whether the pattern matches or does not match.
Pattern	Displays the pattern match.
Source	Displays the originating trunking device for the calls to which the match should apply. If the source is Any, all calls are checked for a match.
Action	Displays whether the inbound call or the outbound call is the default.

Table 6-28 B2BUA Match Configuration Parameters (continued)

Item	Description
New Entry First define the actions you would like the system to take when an INVITE is selected. See Managing B2BUA Actions. Next, define a matching criterion for the INVITE:	
Direction	Choose the client traffic direction from the drop-down list: ■ **Inbound**—From the softswitch. ■ **Outbound**—From the trunking device or client ■ **REFER-Initiated**—Used with the REFER-to-ReINVITE feature in cases where a new INVITE is initiated from a received REFER.
Mode	Choose a mode from the Mode drop-down list: ■ **Both**—Default when Survivability is on and the only option if Survivability is turned off. When a rule is configured in Both mode, and all other criteria match then this rule will be selected whether EdgeMarc is in local or remote mode. ■ **Local Mode On**—The rule for the EdgeMarc can be in Local Mode or Both mode. ■ **Local Mode Off**—The rule for the EdgeMarc can be in Remote Mode or Both mode. **Note:** If multiple rules are configured in Both and Local Mode Off, the first matching rule will be selected when Survivability is turned on and the EdgeMarc is in Remote Mode. Similarly, if multiple rules are configured in Both and Local Mode On, the first matching rule will be selected when Survivability is turned on and The EdgeMarc is in Local Mode.
Default	If you choose Inbound as the Direction, the Default radio button becomes active: ■ Click the **Default** radio button to match any inbound call for which the EdgeMarc was not able to find a destination. Or ■ Select the **Pattern** radio button and choose either **Called** or **Caller** from the drop-down list. **Note:** Default is only available for inbound calls.

Table 6-28 B2BUA Match Configuration Parameters (continued)

Item	Description
Pattern	Select the **Pattern** radio button and choose the following criteria from the drop-down list: ■ **Called** or **Calling**—Selects whether the pattern applies to Calling or Called numbers. ■ **Match**—Selects whether the pattern matches or does not match. Or you can enter the pattern manually in the field provided. See the following support information: ■ Regular Expressions and Expression Examples ■ SIP Trunking Patterns
Source	Select the originating device of the call from the drop-down list. If the source is **Any**, all calls will be checked for a match.
Action	Selects the action from the drop-down list. The drop-down list contains all previously defined actions from the Actions window. It also lists a default action: ■ When direction is outbound—Sends the call to the configured SIP Proxy. ■ When direction is inbound—Drops the call. See Managing B2BUA Actions.

Click **Update** to save your settings in the Match window.
Click **Submit** to save all settings on the page.

Managing Header Manipulation Language

Table 6-29 EdgeMarc Header Manipulation Language

Item or Header Name	Value or Variable	Description
HMR Syntax		
Enter the header value as a concatenation of segments using the "+" sign. Example: **segment + segment + segment + ...**		
Literal		
A string literal that needs to be copied verbatim into the resulting header value. The string literal should be enclosed in single quotes. Example: **'sip:'**		

Table 6-29 EdgeMarc Header Manipulation Language (continued)

Item or Header Name	Value or Variable	Description
Variable		
One of the pre-defined variables. Variables extract a value from the received SIP message or the environment and place it into the value. Variables are preceded with a "$" sign. Example: **$from.uri.user**		
Function		
Functions operate on the variables and insert the result into the value. Example: **replace ($diversion, '88', '408')**		
Headers	**Value or Variable**	**Description**
Includes the following Headers: ■ From ■ To ■ Contact ■ Route ■ Value of From parameter 'tag' ■ P-Asserted-Identity (PAI) ■ P-Preferred-Identity (PPF)	$from.dispname	Display name
	$from.uri.user	User name portion of the URI
	$from.uri.host	Host portion of the URI
	$from.uri.port	Port from the URI
	$from.uri.parameter[user]	Value of URI Parameter 'user'
	$from.uri.header[h1]	Value of URI header 'h1'
	$from.parameter	Value of From parameter 'tag'
Via	$via.ip.host	Value of sent-by
	$via.ip.port	Value of sent-by port
	$via.parameter[branch]	Value of parameter 'branch'
Request URI	$request.method	SIP method
	$request.uri.user	Request-URI user
	$request.uri.host	Request-URI host
	$request.uri.port	Request-URI port
Other headers	$diversion.text	Extract the entire diversion header from the received message
nth header	<header-name>#<number>.<sub-field>.<sub-field>	$via.ip.host returns the sent-by value of the top most Via header. This is the same as $via#0.ip.host. To refer to a second Via header, the syntax is $via#1.ip.host. A third Via header is $via#2.ip.host, and so on.
Environmental Variables		
Variable Name	Value	

Table 6-29 EdgeMarc Header Manipulation Language (continued)

Item or Header Name	Value or Variable	Description
$env.in_intf_host	IP Address of the interface on which the message was received	
$env.in_intf_port	TCP/IP Port on which the message was received	
$env.out_intf_host	IP Address of the interface from which the message will leave EM	
$env.out_intf_port	Source port that is used for sending the message	
$env.target_host	IP Address of the destination of the message	
$env.target.port	Destination port of the message	
$env.target_domain	Domain name of the destination of the message	
Functions		
Name		**Description**
substr (src_string, start_index, len)		The substr() function extracts a sub-string of length “len” from the src_string starting at index “start_index.” The index is zero-based. For example, the first character is index “0”, and the second character is index “1.” If the start_index is negative, counting starts from the end of the string. For example “-1” would be the last character, and “-2” would be the second to last character. This can be useful when stripping characters from the left side of “src_string.”
replace (src_string, 'search_string', 'replace_value')		replace() function searches the “src_string” for all occurrences of “search_string” and replaces them with “replace_value.”

Configuring SIP UA

This section describes how to use SIP UA to configure analog phones at each EdgeMarc Foreign eXchange Subscriber (FXS) port to make IP or PSTN calls:

- Overview
- Configuring Basic SIP UA FXS Settings
- Configuring Basic FXS/Phone Port Level Settings
- Configuring Advanced SIP UA FXS Settings
- Configuring Advanced FXS/Phone Global Settings
- Configuring Advanced FXS/Phone Port Level Settings
- Managing Extended Hunt Group Members
- Configuring Fax

- Configuring Distinctive Ring
- Configuring Network Side ISDN PRI (PRI/UA)
- Configuring Network Side (CAS/UA)

Overview

A SIP user agent (UA) is a logical network endpoint used to create or receive SIP messages and thereby manage a SIP session. A SIP UA can perform the role of a User Agent Client (UAC), which sends SIP requests, and the User Agent Server (UAS), which receives the requests and returns a SIP response. These roles of UAC and UAS only last for the duration of a SIP transaction.

A SIP phone is a SIP user agent that provides the traditional call functions of a telephone, such as dial, answer, reject, hold/unhold, and call transfer. SIP phones may be implemented as a hardware device or as a softphone. As vendors increasingly implement SIP as a standard telephony platform, often driven by 4G efforts, the distinction between hardware-based and software-based SIP phones is being blurred and SIP elements are implemented in the basic firmware functions of many IP-capable devices. Examples are devices from Nokia and Research in Motion.

In SIP, as in HTTP, the user agent may identify itself using a message header field 'User-Agent', containing a text description of the software/hardware/product involved. The User-Agent field is sent in request messages, which means that the receiving SIP server can see this information. SIP network elements sometimes store this information, and it can be useful in diagnosing SIP compatibility problems.

FXS and FXO Ports

FXS and Foreign eXchange Office (FXO) are standard analog telephony interfaces that are used in Public Switched Telephone Network (PSTN) networks. The FXS interface is the modular wall plug that connects the telephone to the central office (CO) of the PSTN. The CO delivers power, dial tone, and ringing capabilities by way of the FXS interface.

The FXO interface is the companion interface that receives analog phone service from the CO. Phones and other analog phone system devices each have an FXO port that receives on-hook and off-hook signals from the CO.

For more information about FXO ports, see Configuring SIP Gateway FXO Ports.

Transmit/Receive Gain

You can configure the transmit and receive gain setting for each FXS port on the EdgeMarc. Most devices operate with the default 0dB Rx gain setting, but you can adjust the setting to interoperate with user endpoints such as phones, fax, or key systems.

When an endpoint device is hooked to the FXS port, it may be necessary to adjust the receive gain settings if the port is unable to detect the digits

sent from the device. Adjust the gain in steps of -4dB using the FXS port Tx/Rx gain settings until the digits are detected.

FXS Hunt Group

The FXS Hunt Group feature enables the EdgeMarc to group all FXS ports into a pool for answering incoming calls from the IP network. If a port is busy, the next port is picked until the call is answered by an idle port. If no FXS port is free to receive a call, a busy signal is returned to the calling party. The following characteristics apply to the Hunt Group feature:

- The EdgeMarc can have only one hunt group consisting of all FXS ports.
- The Hunt group is identified by a unique DID.
- The DID and authentication credentials are replicated for all ports.
- The EdgeMarc supports sequential hunting only

Dialed-in Prefix

Dial-in prefix is used in PBX deployments to provide a way to manipulate the incoming dial pattern for 4-digit dialing. If the dial-in prefix matches the beginning of the incoming dial string, the prefix is stripped from the incoming dial string before that dial-pattern is forwarded to the PBX. For example, if the dial-in prefix is 408555 and the dial-in string is 4085551234, the dial pattern given to the PBX is 1234 after stripping. If the dial-in prefix field is not specified, the dial pattern sent to the PBX contains all 10 digits (10-digit dialing), for example 4085551234.

Ad Hoc Conferencing

The EdgeMarc supports ad hoc SIP conferencing using conference Uniform Resource Identifier (URI). The conference URI identifies a resource in the SIP/IP network that can handle conferencing and media mixing. When the EdgeMarc is configured for ad hoc conferencing, the FXS port uses this configured network for third party conferencing. If the EdgeMarc is not configured for ad hoc conferencing, the FXS port mixes the local media. Your ISP identifies the resources for ad hoc conferencing.

Analog Phone Calling Features on the FXS Port

All EdgeMarc platforms support the following features for analog phones connected to the FXS port:

- Call Hold
- Call Transfer – Unattended
- Call Transfer – Attended
- Call Waiting
- 3-Way Calling

Configuring Basic SIP UA FXS Settings

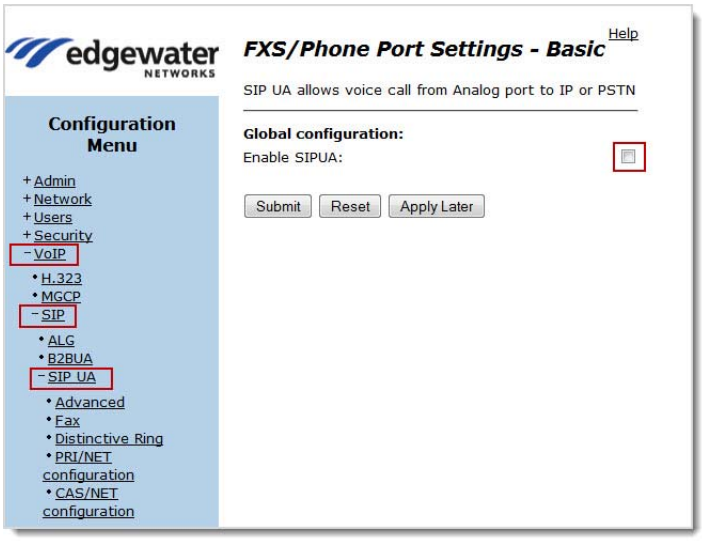
SIP UA enables analog phones at each FXS port to make IP or PSTN calls. Each FXS port represents an instance of a SIP user agent. Once configured,

each FXS port registers to the configured domain using outbound proxy. If registration is successful, the phone at the FXS port will have a dial tone.

Note
You must enable SIP UA service to configure SIP UA ports.

1. Choose **VoIP** > **SIP** > **SIPUA** (Figure 6-41).

Figure 6-41 Enable SIP B2BUA

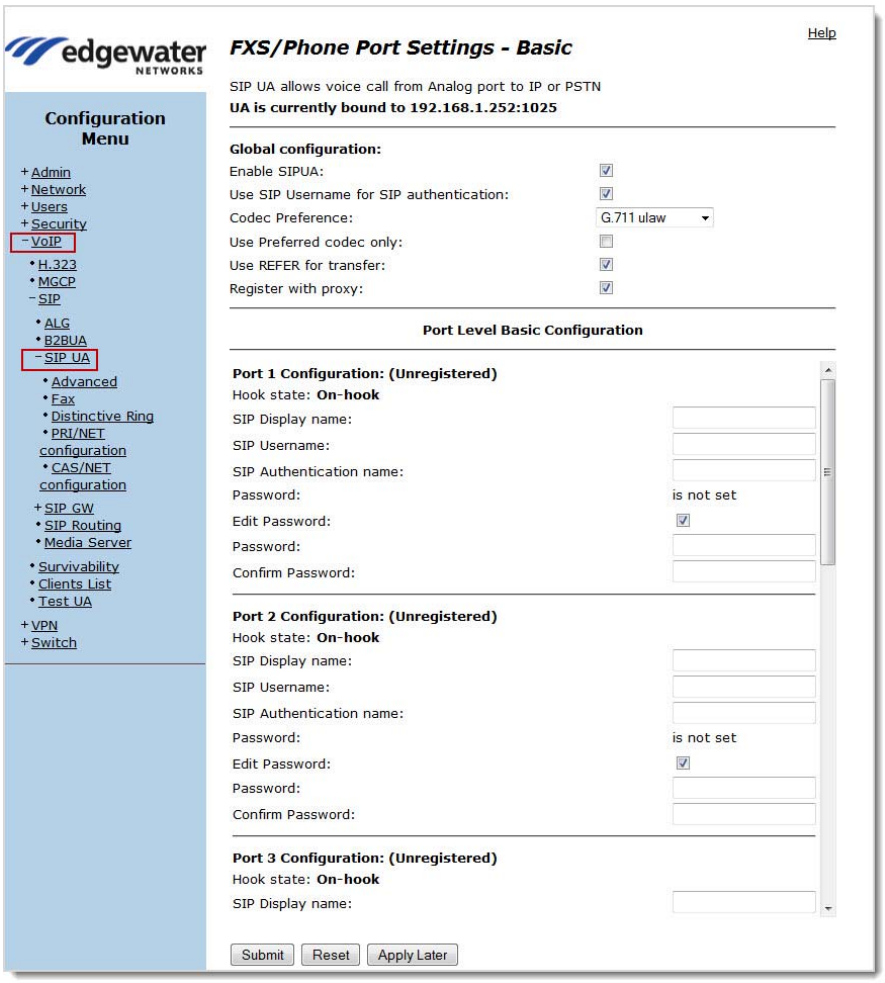


2. Select the **Enable SIPUA** checkbox and click **Submit**.

   A message indicates that service will be temporarily interrupted.

3. Click **OK** to confirm. Fields on the FXS/Phone Port Settings - Basic page become active (Figure 6-42).

Figure 6-42 SIP UA FXS/Phone Port Settings - Basic



4. Configure settings using the information in Table 6-30 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 6-30 FXS/Phone Port Settings - Basic

Item	Description
Global Configuration Settings apply to all ports.	
Enable SIPUA	Select the **Enable SIPUA** checkbox if it is not already checked.
Use SIP Username for SIP authentication	Select the **Use SIP Username for SIP authentication** checkbox to enable SIP authentication when authenticating an FXS port.

Table 6-30 FXS/Phone Port Settings - Basic (continued)

Item	Description
Codec Preference	Choose a codec type from the **Codec Preference** drop-down list. This selects the codec that is used by all FXS ports for encoding analog data. The codec must be part of the negotiated codec list: G.711 ulawG.711 alawG.729G.728G.726,16 Kbps G.726, 24 Kbps G.726, 32 Kbps G.726, 40 Kbps
Use preferred codec only	Select the **Use Preferred codec only** checkbox to specify that the system use only the preferred codec type. This specifies that only the preferred codec is used when the FXS places a call.
Use REFER for transfer	Select the **Use REFER for transfer** checkbox if your VoIP switch supports REFER requests as outlined in RFC3515 to perform call transfer.
Register with proxy	Select the **Register with proxy** checkbox to instruct each configured FXS port to send a REGISTER request to the configured domain through a configured outbound proxy. If this checkbox is not checked, FXS ports will not register. **Note:** Some VoIP deployments use static registration for the FXS ports and do not require port registration.
Enable Dry-Closure (FXO-FXS)	EdgeMarc 250 only: Specifies FXS port 4 to connect to the FXO port (known as “dry closure”) during a power failure. For systems licensed with less than four ports, user phones are connected to FXS ports 1-3 and can be completely disconnected from the FXO port to allow dry closure. To connect the FXO port to one of the FXS phones during a power failure, swap the port 1 license to port 4.
Port Level Basic Configuration This section includes a set of parameters for each port. Use the scroll bar on the right to access all eight port configuration windows.	
Hook state	Displays dynamic status of a given FXS port: ■ On-Hook ■ Off-Hook ■ In-Call
SIP Display Name	Specifies the SIP display name.

Table 6-30 FXS/Phone Port Settings - Basic (continued)

Item	Description
SIP Username	Identifies the analog phone connected to the FXS port. This value can be either a name or a number that callers use to reach the analog phone.
SIP Authentication name	Specifies the name used by the FXS port to authentication itself if the **Use SIP Username for SIP authentication** box is *NOT* checked in Configuring Basic SIP UA FXS Settings.
Password	Specifies the passwords to authenticate the SIP UA against the softswitch or outbound proxy.

5. Click **Submit**.

   Your ports are now registered on the FXS/Phone Port Settings - Basic page. You can now make and receive calls on the phones that are connected to the configured FXS ports.

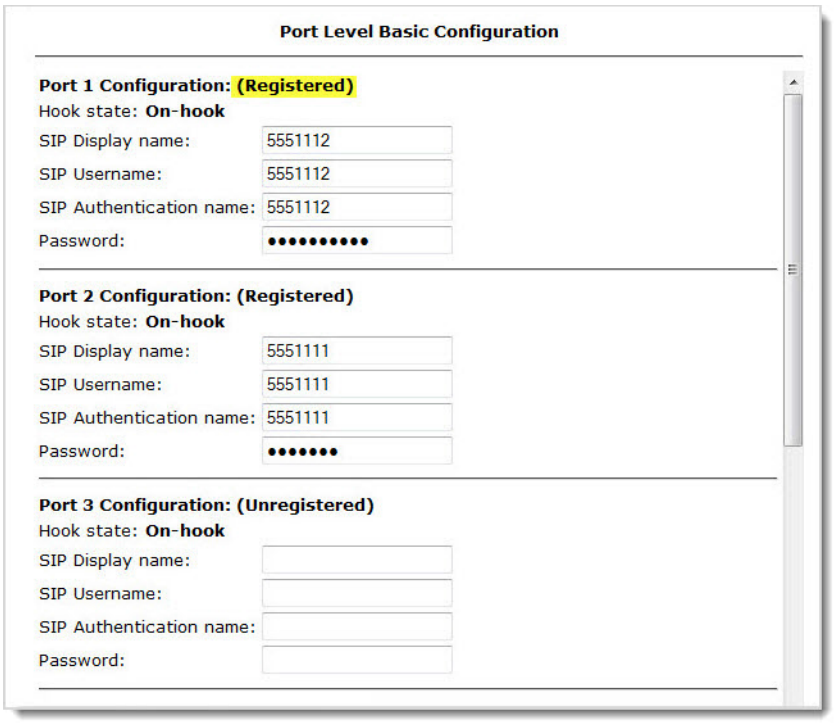
6. Choose **VoIP** > **SIP** > **SIP UA** from the Configuration Menu to open the FXS/Phone Port Settings page (Figure 6-43).



Tip

If your changes are not visible on the page, click **SIP UA** again from the Configuration Menu to refresh the page. The Port Configuration state should change from Unregistered to Registered. If the state is still unregistered, check with your VoIP provider to confirm that the Authentication Name and Password is valid.

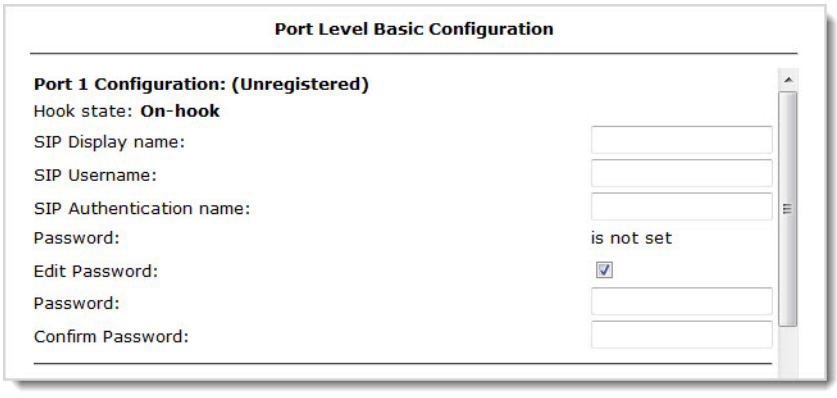
Figure 6-43 Registered FXS Ports



Configuring Basic FXS/Phone Port Level Settings

1. Choose **VoIP** > **SIP** > **SIP UA** from the Configuration Menu (Figure 6-42).
2. Scroll to **Port Level Basic Configuration** (Figure 6-44).

Figure 6-44 Port Level Basic Configuration - Unregistered



3. Configure ports as needed:
   a. Enter a name in the **SIP Display name** field.
   b. Enter a username in the **SIP Username** field to identify the analog phone connected to the FXS port.

c. In the **SIP Authentication name** field, enter the name that is used by the FXS port to authentication itself.

Note
Enter information only if the **Use SIP Username for SIP authentication** box is *NOT* checked in Configuring Basic SIP UA FXS Settings.

d. In the **Password** field, enter a password to authenticate the SIP UA against the softswitch or outbound proxy.

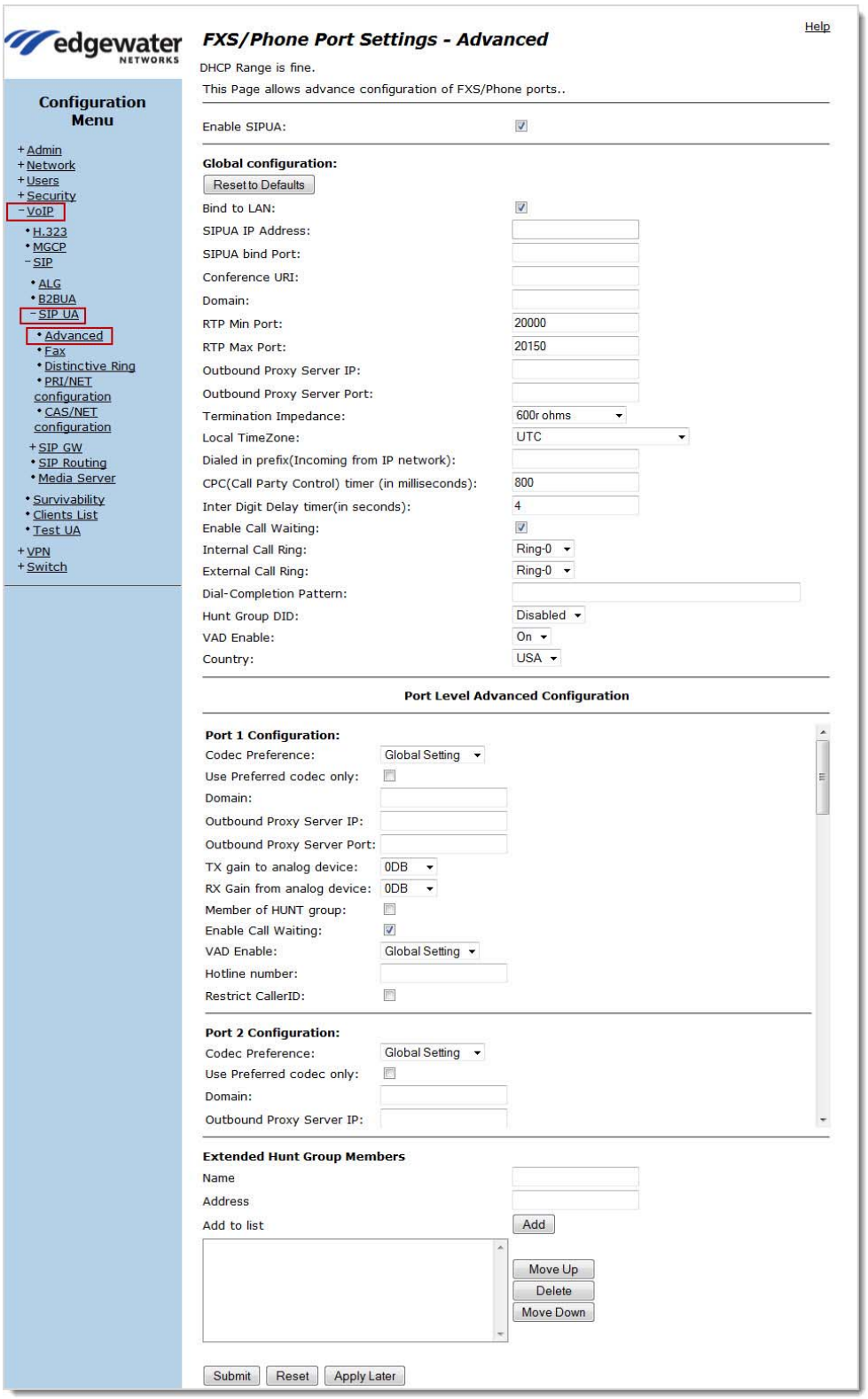
4. Click **Submit**.

Configuring Advanced SIP UA FXS Settings

The Advanced configuration page for SIP UA allows you to fine tune your configuration globally and at the port level.

1. Choose **VoIP** > **SIP** > **SIP UA** > **Advanced** (Figure 6-45).

Figure 6-45 FXS/Phone Port Settings - Advanced Page

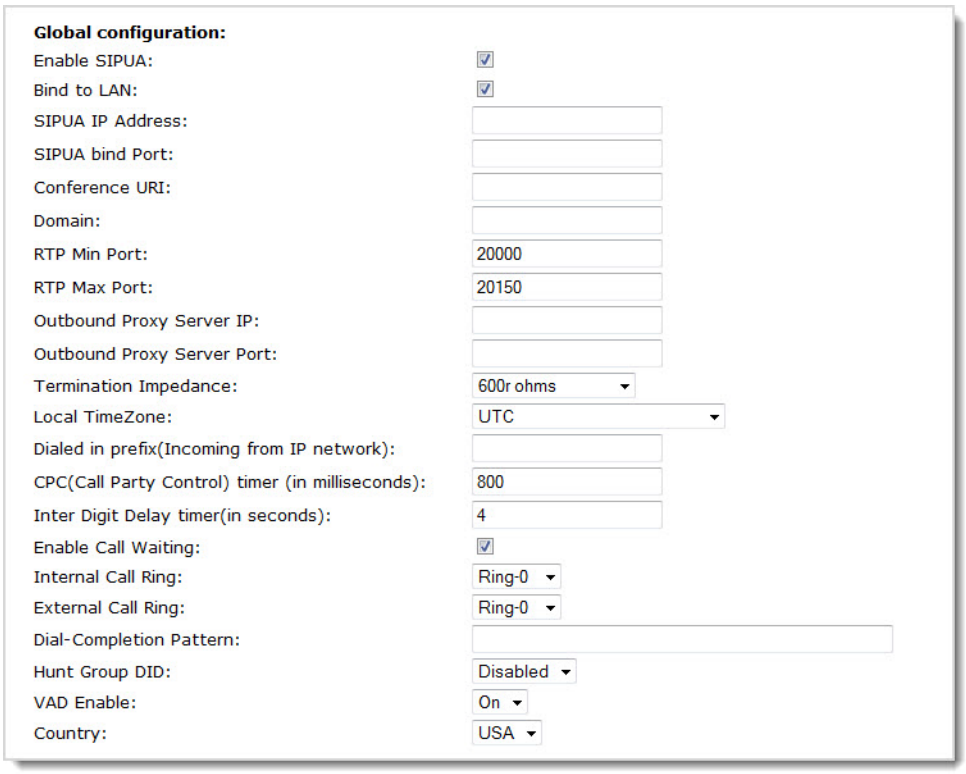


2. Configure settings in the following sections:
   - Configuring Advanced FXS/Phone Global Settings
   - Configuring Advanced FXS/Phone Port Level Settings

Configuring Advanced FXS/Phone Global Settings

1. Choose **VoIP** > **SIP** >**SIP UA** > **Advanced** (Figure 6-46).

Figure 6-46 SIP UA Advanced Settings - Global Configuration



2. Configure settings using the information in Table 6-31 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 6-31 FXS/Phone Port Advanced - Global Configuration Parameters

Item	Description
Global Configuration	
Settings apply to all ports.	
Note: Values set for individual FXS/Phone ports on advanced page override the global settings on the FXS/Phone Port Settings - Basic page.	
Enable SIPUA	Select the **Enable SIPUA** checkbox.

Table 6-31 FXS/Phone Port Advanced - Global Configuration Parameters

Item	Description
Bind to LAN	Select the **Bind to LAN** checkbox to bind the UA to the LAN IP of the EdgeMarc by default, processing all signaling through the EdgeMarc ALG. If not selected, the UA internally binds to the WAN IP, bypassing the EdgeMarc ALG; used only in special circumstances.
SIPUA IP Address	Enter the LAN side IP address with which the SIP UA binds. When this field is blank, the IP address is set to the class C subnet of the VoIP ALG LAN plus 252. For example, if the ALG LAN is 192.168.1.0/24, the default IP address of the SIP UA is 192.168.1.252. If the default IP address conflicts with another host on the VoIP ALG LAN, you can define the SIP UA IP address in this field. In most of the cases, the default configuration is sufficient.
SIPUA bind Port	Enter a port number to which SIP UA binds and listens for SIP messages. If left empty, SIP UA binds to internal port 1025 by default. **Note:** If you use IAD mode or bind-to-WAN, you can use port 5060. In all other cases port 5060 cannot be used here.
Conference URI	Enter the Conference URI if your softswitch supports creating a conference using ad hoc SIP methods as outlined in RFC 4579, section 5.4. Format in the same manner as a SIP endpoint (user@host).
Domain	Enter the softswitch domain where each of the FXS ports will be provisioned. The domain is also the authentication domain for each FXS port. By default, when left blank, all FXS ports use the system ALG LAN IP address as the domain unless the value is overridden at port level. Factory default is to leave the field blank.
RTP Min Port RTP Max Port	Enter the range of RTP ports that SIP UA uses for media.
Outbound Proxy Server IP	Enter the IP address of the outboard proxy server. Use when the “Bind to LAN” box is un-checked.

Table 6-31 FXS/Phone Port Advanced - Global Configuration Parameters

Item	Description
Outbound Proxy Server Port	Enter the outbound proxy server port that SIP UA uses to register each FXS port and make outbound calls. Use when the “Bind to LAN” box is un-checked. The UA binds to the WAN IP of the EdgeMarc and directly sends packets to the Outbound Proxy Server IP and Port. These values, when left blank, default to the address of EdgeMarc ALG IP address and port. Factory default is to leave this field blank.
Termination Impedance	Choose the impedance on the outboard port based on the analog devices being connected and length of cable hooking up the device. Default is 600r for connections less than 5000 meters in length.
Local Time Zone	Choose the local time zone for FXS ports. The local time zone is used when sending date/time information in CallerID to an analog device connected to the FXS port.
Dialed in prefix (Incoming from IP network)	Enter a dial pattern for the incoming IP network. Applicable only when Hunt mode is enabled. When a dial pattern is defined, the system looks for that pattern in the dialed in number (the “TO” field of the SIP message). If the found pattern is identified as a prefix, that prefix is stripped out and the remaining digits are given to the PBX as the dial pattern.
CPC (Call Party Control) timer (in milliseconds)	Enter the CPC timer value in milliseconds. Range is 250 to 1500ms. CPC is a signal sent from electronic COs to indicate that the Calling Party has hung up. CPC is also referred to as Open Loop Disconnect when programming telephone equipment. CPC is normally sent as an open (0 volts DC), ranging from 250 to 500 milliseconds. When FXS is in call and the remote party hangs up, FXS sends the CPC disconnect signal to the PBX/Key-system that is connected to the FXS.
Inter Digit Delay timer (in seconds)	Enter the maximum delay between two dialed digits. If a key is not pressed within the defined delay, dialing is auto-completed and the collected digits are dialed out. Default is 4 seconds.

Table 6-31 FXS/Phone Port Advanced - Global Configuration Parameters

Item	Description
Enable Call Waiting	Select the **Enable Call Waiting** checkbox to enable call waiting globally on all FXS ports. This box is checked by default and call waiting is enabled on all ports. To control call waiting at port level, disable the global setting and select the settings a port level.
Internal Call Ring	Choose the ring index to use for ringing the called phone. Range is Ring-0 to Ring-4. If the Alert-Internal header is missing, a ringing pattern is used based on the distinct ring rules configured on the FXS/Phone Port Distinctive Ring configuration page. The header must look like this: Alert-Info:info=alert-internal See Configuring Distinctive Ring to configure the ring type and the rules defining an internal call.
External Call Ring	Choose the ring index to use for ringing the called phone. Range is Ring-0 to Ring-4. If the Alert-External header is missing, a ringing pattern is used based on the distinct ring rules configured on the FXS/Phone Port Distinctive Ring configuration page. The header must look like this: Alert-Info:info=alert-external See Configuring Distinctive Ring to configure the ring type and the rules defining an external call.
Dial-Completion Pattern	Enter a value in the **Dial-Completion Pattern** field using the information in Table 6-32 as a guide. Enter the dial-completion pattern that is used to auto-complete the dialed string on the FXS port. Each pattern can be defined in a list separated by the pipe character (“ | ”).
Hunt Group DID	Choose whether the Hunt Group Direct Inward Dialing (DID) is enabled or disabled (default) at the global level. At individual port setting this value takes effect if port level settings are set to Global Setting. When DIDs are mapped to the Hunt Group, all destinations configured under this group ring in order one after another with a timeout configured per destination. When the EdgeMarc receives the call from the IP network, it uses the Dial Rules to match the DID and forward the calls to the Hunt Group. Once the destination is answered, the call is connected and call hunting is stopped.

Table 6-31 FXS/Phone Port Advanced - Global Configuration Parameters

Item	Description
VAD Enable	Choose whether to globally enable voice activity detection. VAD is turned on by default.
Caller ID Time offset	Define the offset value in hours and minutes (positive or negative) that would be necessary to reflect the hours and minutes in the local time zone, as compared to the time zone where the EdgeMarc is located.
Country	Choose the country where the EdgeMarc is located.

Click **Submit** at the bottom of the page to save your changes or click **Reset to Defaults** at the top of the page.

Dial Completion Patterns

Table 6-32 Dial Completion Pattern Formatting

Symbol	Description
.	Matches one or more digits.
[x-y]	Matches any single digit between x and y. For example, [1-3] matches 1, 2, or 3.
X	Matches any digit between 0 and 9, equivalent to [0-9].
Z	Matches any digit between 1 and 9, equivalent to [1-9].
N	Matches any digit between 2 and 9, equivalent to [2-9].

Dial Completion Pattern Example

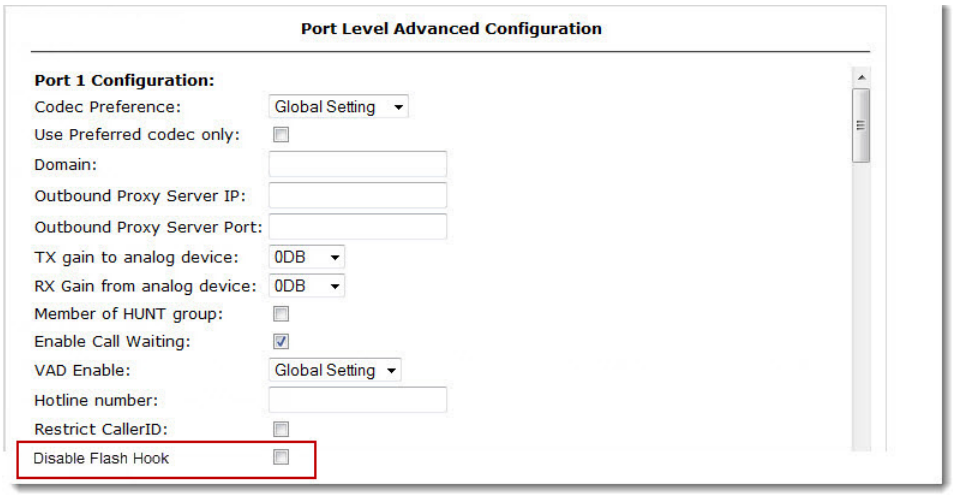
911|XXXX|XXXXXXX

If the dialed pattern matched 911 or any 4 or 7 digit number, dial operation is complete and the call is placed.

Configuring Advanced FXS/Phone Port Level Settings

1. Choose **VoIP** > **SIP** >**SIP UA** > **Advanced** (Figure 6-45).
2. Scroll to **Port Level Advanced Configuration** (Figure 6-47).

Figure 6-47 Port Level Advanced Configuration



3. Configure settings using the information in Table 6-33 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 6-33 FXS/Phone Port Settings - Advanced

Item	Description
Port Level Advanced Configuration	
Configures parameters for each port.	
Port 1 Configuration	
Codec Preference	Choose the codec that is given preference when making or receiving a call. When making or receiving a call, if that codec is part of the negotiated codec list, then that codec is used to encode and send voice packets. Select the Global setting to use the Global codec preference at port level (default).
Use preferred codec only	Select the **Use preferred codec only** checkbox to specify that only the preferred codec is used when the FXS places a call. If an incoming call does not have the preferred codec, the call is rejected. This setting does not apply if the preferred codec is set to Global Setting.
Domain	Enter the domain of the given FXS port. This field is blank by default to use global configuration.

Table 6-33 FXS/Phone Port Settings - Advanced (continued)

Item	Description
Outbound Proxy Server IP	Enter the IP address of the outboard proxy server. Each FXS port can use a different outgoing proxy and domain for SIP signaling. This field is blank by default to use global configuration.
Outbound Proxy Server Port	Enter the outbound proxy server port that SIP UA uses to register each FXS port and make outbound calls. Each FXS port can use different outgoing proxy and domain for SIP signaling. This field is blank by default to use global configuration. If VoIP-ALG is enabled, the outbound proxy must point to the VOIP ALG LAN interface.
TX gain to analog device	Choose the analog transmit gain for the FXS port. The default setting of 0dB is appropriate for most installations; however, you can adjust the setting to interoperate with user endpoints such as phones, fax, or key systems. Range is -16dB to 16dB, default is 0dB.
RX gain from analog device	Choose the analog receive gain for the FXS port. The default setting of 0dB is appropriate for most installations; however, you can adjust the setting to interoperate with user endpoints such as phones, fax, or key systems. Range is -16dB to 16dB, default is 0dB.
Member of Hunt Group	Select the **Member of Hunt Group** checkbox to enable the associated FXS port to answer incoming calls that are placed to the hunt group from an IP network. If the port is busy or the call has comes to a hunt group DID, ports in the group are picked up in a round-robin scheme from first port in the group to port N in the group. When no FXS port is free in the pool to receive the call, a “486 Busy” is sent.
Enable Call Waiting	Select the **Enable Call Waiting** checkbox to enable call waiting at the port level. If call waiting is enabled globally, it is enabled at port level as well. Call waiting can be disabled globally and enabled at port level.
VAD Enable	Choose voice activity detection for the FXS port: ■ On ■ Off ■ **Global Setting**—Allows global VAD settings to be applied at the port level.
Hotline Number	Enter the number that a port calls automatically when it goes off-hook. If the field is empty, the feature is disabled.

Table 6-33 FXS/Phone Port Settings - Advanced (continued)

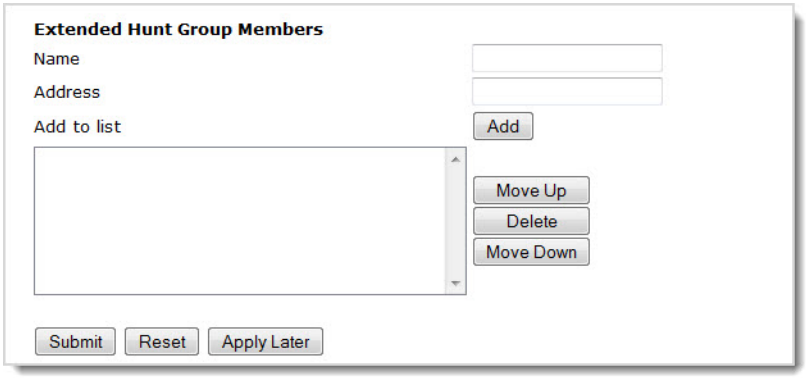
Item	Description
Restrict CallerID	Select the **Restrict CallerID** checkbox to enable endpoint call privacy - user provisioned on the port - in a trusted SIP network (RFC 3325). Caller Identity in From SIP header is restricted and is instead carried in P-Preferred-Identity SIP header. If the endpoint does not trust the proxy that it sends request to, leave the box un-checked.
Disable Flash Hook	Select the **Disable Flash Hook** checkbox and click **Submit** to disable Flash Hook on SIPUA FXS Ports.

Click **Submit** at the bottom of the page to save your changes or click **Reset to Defaults** at the top of the page.

Managing Extended Hunt Group Members

1. Choose **VoIP** > **SIP** > **SIP UA** > **Advanced** (Figure 6-45).
2. Scroll to **Extended Hunt Group Members** (Figure 6-48).

Figure 6-48 Extended Hunt Group Members



3. Add a new member:
   a. In the **Name** field, enter the member name.
   b. In the **Address** field, enter the member IP address.
   c. Click **Add** in the **Add to list** field. The member name is added to the list box.
   d. Click **Submit** to add the new member or click **Delete** to clear the entry.
4. Manage extended hunt group members in the list by clicking the **Move Up**, **Delete**, and **Move Down** buttons.
5. Click **Submit** to save your changes.

Configuring Fax

FXS phone ports can be used to hook up a Group 3 fax equipment (G3FE) terminal for T.38 fax transmission over UDP to an IP network. If support for T.38 is disabled, G711uLaw is used for sending and receiving fax.

Table 6-34 describes specific EdgeMarc platform support.

Table 6-34 FXS/Phone Port FAX Platform Support

Platform	Support
EdgeMarc 250 Series	
E200 series H/W platform, Fax detection is supported on all FXS/Phone ports, however T.38 fax is only supported on FXS/Phone port 1. Port 2 performs fax pass-through using G711ulaw.	
250 Series	Fax detection and T.38 is supported on all FXS/Phone ports.
EdgeMarc 4500 Series	
EdgeMarc 4500 series H/W platforms support fax detection on all FXS/Phone ports, however T.38 fax is only supported on FXS/Phone ports 1 and 2. Ports other than 1 and 2 perform fax pass-through using G711ulaw.	
4570,4571, 4572, 4574, 4575, and 4576	T.38 fax is supported on all FXS/Phone ports.

Before You Begin

SIP UA must be enabled to configure FXS ports for fax services:

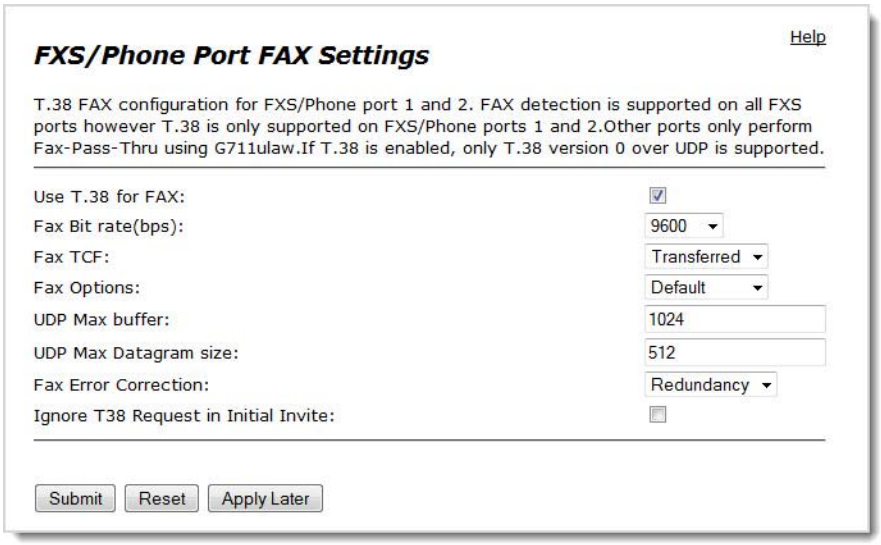
1. Choose **SIP UA** from the Configuration Menu.
2. Select the **Enable SIPUA** checkbox.
3. Click **Submit**.

Refer to Configuring Basic SIP UA FXS Settings.

Configure T.38 Fax Settings

1. Choose **VoIP** > **SIP** > **SIP UA** > **Fax** (Figure 6-49).

Figure 6-49 FXS/Phone Port FAX Settings Page



2. Configure settings using the information in Table 6-35 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 6-35 FXS/Phone Port FAX Settings

Item	Description
Use T38 for FAX	Select the **Use T.38 for FAX** checkbox to enable T.38 fax capability. If this checkbox is not selected, G711ulaw is used to send and receives faxes.
Fax Bit rate (bps)	Choose a rate from the **Fax Bit rate (bps)** drop-down list: ■ 2400 ■ 4800 ■ 7200 ■ 9600 ■ 14400 Specifies the data rate that the fax machine support. Maximum rate is 14400 bps.

Table 6-35 FXS/Phone Port FAX Settings (continued)

Item	Description
Fax TCF	Choose the data rate management method for the Training Check Function (TCF) signal. Data rate management is carried out by the emitting gateway, which takes the T30 data and encodes it into T38 packets, port 1 or 2, based on training results from local and remote FAX terminals. This method is used for TCP connections and is optional for UDP. ■ **Local**—Requires that the TCF training signal is generated locally by the receiving gateway, which receives the T38 data and translates it into T30 data, port 1 or 2. ■ **Transferred**—Requires that the TCF signal is transferred from the emitting gateway to the receiving gateway. In this case, the speed selection is carried out by the G3FEs in the same way as a PSTN connection. This method is mandatory for UDP.
Fax Options	Choose special settings for the fax machine: ■ Default—No option is set. ■ BitRemoval—Fill bits can be inserted or removed in the Message Transmission Phase C, non-ECM data to reduce bandwidth in the packet network. ■ TransMMR—Conversion between Modified Modified READ (MMR) T.6 and the line format to increase data compression and reduce bandwidth in the packet network. ■ JBIGTranscoding—Joint Bi-level Image Experts Group (JBIG) T.30 provides the ability to convert to/from JBIG to reduce bandwidth.
UDP Max buffer	Enter the maximum number of octets that can be stored on the remote device before an overflow condition occurs. Maximum value is 4096.
UDP Max Datagram size	Enter the maximum size of a UDP Transport Layer (UDPTL) packet or the maximum size of the payload within an RTP packet that can be accepted by the remote side. Maximum is 512.
Fax Error Correction	Choose the error correction method used by the fax machine: ■ Transparent ■ FEC—Forward error correction (FEC)

Table 6-35 FXS/Phone Port FAX Settings (continued)

Item	Description
Ignore T38 Request in Initial Invite	(Optional) Select the checkbox to specify that an initial T38 request be ignored and to establish an audio call instead. On calls terminating onto a FXS port, in rare cases a T38 request can arrive in the initial INVITE message. Unless this option is specifically needed, the box should be left un-checked.

Click **Submit** to save all settings on the page.

Configuring Distinctive Ring

The EdgeMarc is shipped with five distinctive ring patterns (Ring-0 through Ring-4) that are available for use when ringing an analog phone on the FXS/phone port. The EdgeMarc automatically selects a ring pattern based on the number that is being called or the number that originated the call.

Distinctive Ring Pattern Rules

By default, the appliance is configured to use Ring-0 for all calls. You can assign different ring patterns based the types of rules listed in Table 6-36.

Table 6-36 Ring Pattern Rules

Ring Pattern Rule	Description
Caller-Pattern-match	Uses the ring pattern if the caller's phone number matches the pattern.
Called-Pattern-match	Uses the ring pattern if the called phone number matches the pattern.
Caller-Pattern-match and Called-Pattern-match	Uses the ring pattern if the caller's phone number matches the pattern AND the called phone number also matches the pattern.

Caller and Called Number Patterns

Table 6-37 Caller and Called Number Patterns

Symbol	Description
.	Matches one or more digits.
[x-y]	Matches any single digit between x and y. For example, [1-3] matches 1, 2, or 3.
X	Matches any digit between 0 and 9, equivalent to [0-9].

Table 6-37 Caller and Called Number Patterns

Symbol	Description
Z	Matches any digit between 1 and 9, equivalent to [1-9].
N	Matches any digit between 2 and 9, equivalent to [2-9].

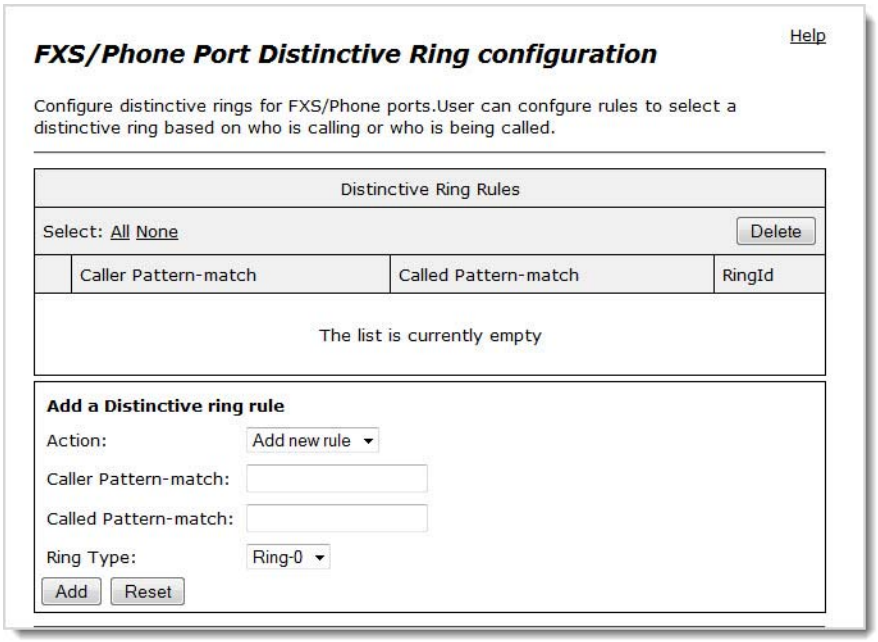
Example Call Pattern Rules

Caller Pattern-match	Called Pattern-match	Ring Id	Description
.	408.	1	For any caller, if call is going to an FXS/Port extension starting with 408, ring the phone with ring pattern ID=1.
408.	.	2	If a call is from caller with number starting with 408 and call is going to any FXS/Port extension, ring the phone with the ring pattern ID=3.
.	91NXXNXXXXXX	3	If a call is a long distance call (for example, the called pattern is 914085551222), terminating on analog FXS/Phone port, ring the phone with the ring pattern ID=4.

Adding a Distinctive Ring Pattern Rule

1. Choose **VoIP** > **SIP** > **SIP UA** > **Distinctive Ring** (Figure 6-50).

Figure 6-50 FXS/Phone Port Distinctive Ring Configuration Page



2. Configure settings using the information in Table 6-38 as a guide. When you have finished configuring settings, click **Add** to make your changes take effect.

Table 6-38 FXS/Phone Port Distinctive Ring Configuration Parameters

Item	Description
Distinctive Ring Rules	Manages the distinctive ring list.
Add a Distinctive Ring Rule	Configures distinctive rings for FXS/Phone ports. Distinctive ring rules are applied in the order in which they are defined. If a rule matches, the ring pattern defined for the rule is used to ring analog phones on the FXS/phone port. **Note:** You cannot change the order in which rules are applied. If the order is not as desired, you must delete or redefine the existing rules. **Tip:** Rules can include a mix of the digits and patterns listed in the following sections: ■ Distinctive Ring Pattern Rules ■ Caller and Called Number Patterns

Table 6-38 FXS/Phone Port Distinctive Ring Configuration Parameters

Item	Description
Action	Adds or edits a rule. To add a new rule, choose **Add new rule** from the **Action** drop-down list.
Caller Pattern Match	Enter a caller pattern that triggers the distinctive ring.
Called Pattern Match	Enter a pattern in the one or both of the following fields: ■ Caller Pattern-match ■ Called Pattern-match
Ring Type	Choose a ring type from the Ring Type drop-down list: ■ Ring-0 (default) ■ Ring-1 ■ Ring-2 ■ Ring-3 ■ Ring-4
	Click **Add**. The new entry is added to the Distinctive Ring Rules table. Click **Submit All** to save your settings to the EdgeMarc. A message indicates that service will be temporarily interrupted. Click **OK** to confirm.

Editing or Deleting a Distinctive Ring

1. Choose **Edit rule** from the **Action** drop-down list and select the rule you want to edit.
2. Edit settings in the fields provided and click **Add**.
3. To delete an entry from the Distinctive Rules table:
   a. Select the checkbox of the Rule that you want to delete and click **Delete**.

      A message asks whether you are you want to delete the selected entry and that service will be temporarily interrupted.

   b. Click **OK** to confirm.
4. Click **Submit All** to save your settings to the EdgeMarc.

   A message indicates that service will be temporarily interrupted.
5. Click **OK** to confirm.

Configuring Network Side ISDN PRI (PRI/UA)

1. Choose **VoIP** > **SIP** > **SIP UA** > **PRI/NET Configuration**.
2. Refer to Configuring Network Side ISDN PRI (PRI/UA) in Chapter 3, *Network Deployment* to configure Network Side ISDN PRI (PRI/UA).

Configuring Network Side (CAS/UA)

1. Choose **VoIP** > **SIP** > **SIP UA** > **CAS/NET Configuration**.
2. Refer to Configuring Network Side CAS/UA in Chapter 3, *Network Deployment* to configure Network Side CAS/UA.

Configuring the SIP Gateway

The SIP FXO/Line port page configures SIP gateway FXO/Line ports to support voice calls from IP networks to the PSTN. Once FXO ports are configured and Survivability is enabled, FXO ports can act as a LAN side gateway if the softswitch becomes unreachable.

- Overview
- Using the SIP GW Page
- Configuring Global SIP Gateway FXO/Line Port Settings
- Registering with the SIP Server
- Configuring SIP Gateway FXO Ports
- Configuring Network Side ISDN PRI (PRI/UA)
- Configuring Network Side (CAS/UA)

Before You Begin

Before configuring the FXO ports, verify that Survivability is included with your license:

1. Choose **Network** from the Configuration Menu.
2. Scroll to **Registration Status**.
3. Click **View License Key**.

To configure Survivability, choose **VoIP** > **Survivability** and refer to Configuring Survivability.



Note
The EdgeMarc 250W requires that a phone be connected to PSTN FXS port 4.

Overview

The EdgeMarc supports PSTN connections through its FXO ports and connections to analog phones through its FXS ports. It provides a low-cost long distance connectivity solution for enterprises that have PBXs in geographically separated locations. It also provides Survivability capabilities. A softswitch can also use the EdgeMarc FXO ports as an enterprise gateway to route calls.

A Private Branch eXchange (PBX) can be connected to the EdgeMarc for Session Initiation Protocol (SIP) trunking applications. A PBX is a private telephone switch that provides local phone service for an office or building. A PBX typically contains both FXS and FXO ports.

For more information about FXS ports, choose **VoIP** > **SIP** > **SIP UA** and refer to Configuring SIP UA.

Two-Stage Dialing for Inbound IP and PSTN Calls

You can enable two-stage dialing for inbound calls from the IP network and the PSTN:

- Inbound IP network calls—For calls that come into FXO/line ports on the EdgeMarc from the IP network, dial tone is provided to the caller to enable the caller to dial a number and connect through the PSTN.
- Inbound PSTN calls—For calls that come in from the PSTN, the SIP/FXO line port provides dial tone when the PSTN call is answered. This enables the caller to dial an extension to complete the call or hang up.

Priority Calling Support

Priority calling services route priority calls as defined in the VoIP ALG SIP trunking plan. Calls made to a priority calling number from any FXS port are routed and connected on a priority basis.

The following rules determine the treatment of an incoming priority call:

- If a free FXO port is available, the priority call is routed and connected.
- If all FXO ports are busy, a non-priority call on one of the ports is dropped to allow the priority call to be routed and connected. The PSTN live connection to the FXO port must support 3-way calling.
- If all FXO ports are busy with priority calls, the incoming priority call is not accepted.

To configure priority calling, enable the feature on the SIP FXO/Line Port Configuration Page and then define priority rules on the ALG Trunking Configuration page. Choose **VoIP** > **SIP** > **ALG** and refer to Configuring Bandwidth Settings for H.323.



Note
Priority calling services cannot be configured when WAN Link Redundancy is enabled.

Transmit/Receive Gain

FXO port TX/RX gain settings are adjusted at the WAN interface. TX adjusts the gain from the FXO port to the IP WAN. RX adjusts the gain from the IP WAN to the FXO port.

Using the SIP GW Page

The SIP FXO/Line port configuration page configures the system to allow voice calls from IP networks to the PSTN.

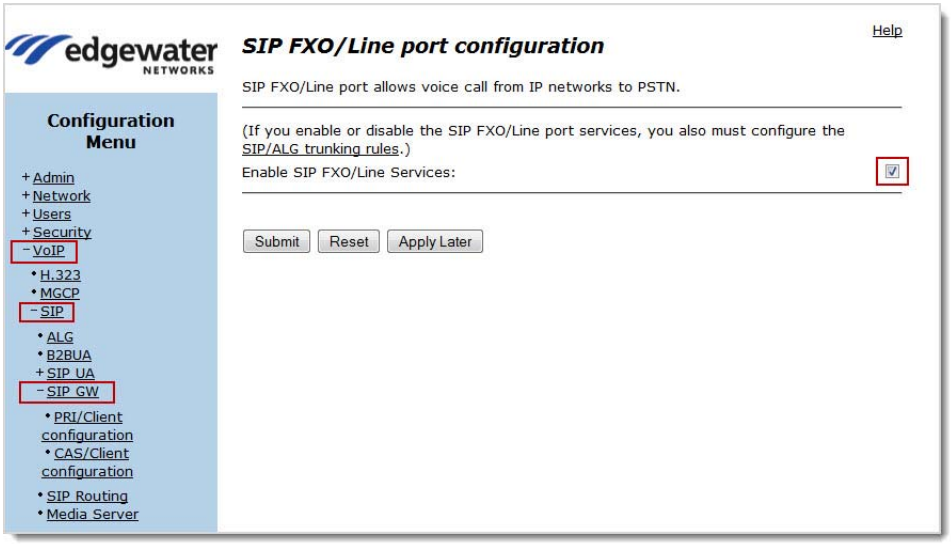
Before You Begin

If you enable or disable the SIP FXO/Line port services, you also must configure SIP/ALG trunking rules. Choose **VoIP** > **SIP** > **ALG** and refer to Configuring Bandwidth Settings for H.323.

Configure SIP FXO Line Ports

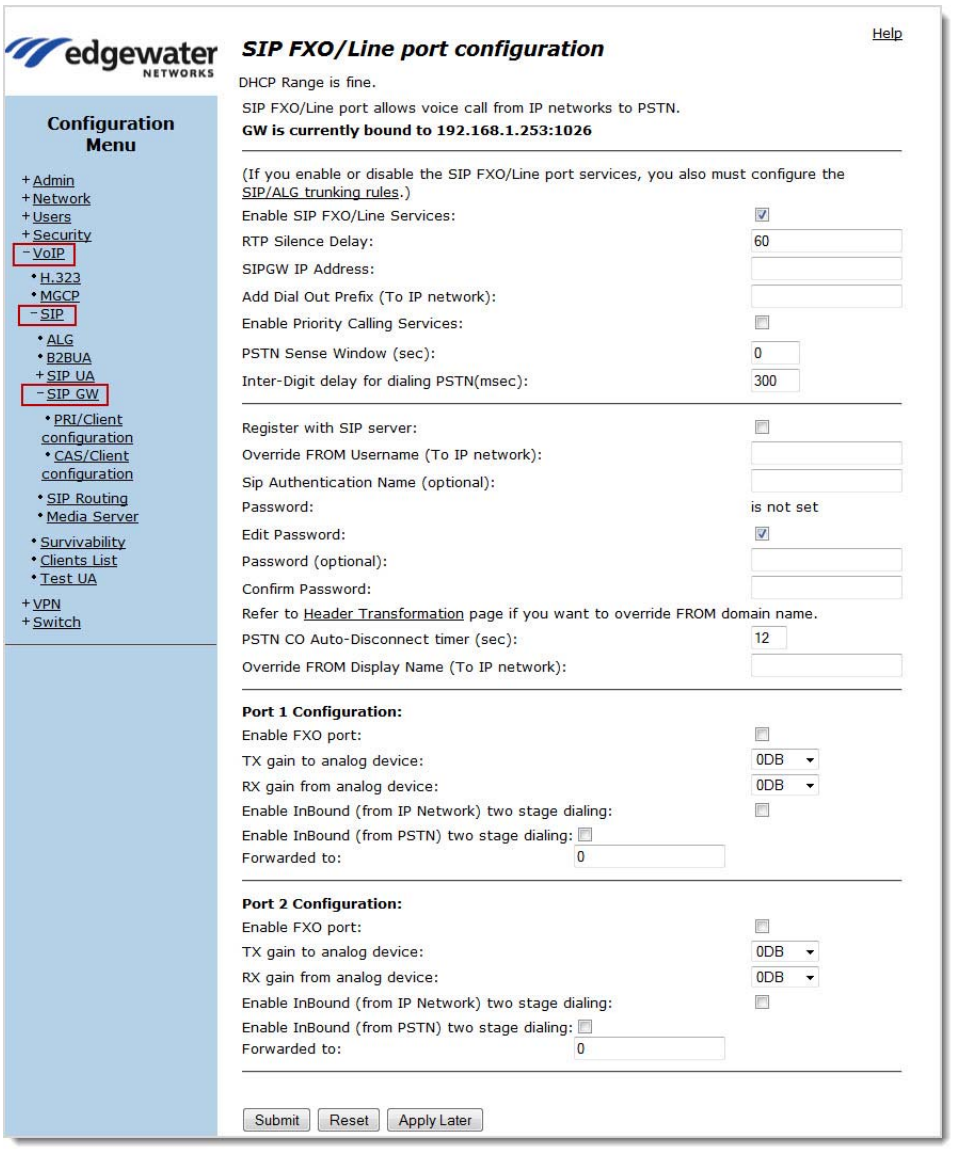
1. Choose **VoIP** > **SIP** > **SIP GW** (Figure 6-51).

Figure 6-51 Enable SIP FXO/Line Services



2. Select the **Enable SIP FXO/Line Services** checkbox and click **Submit** to activate configuration fields on the SIP FXO/Line port configuration page (Figure 6-52).

Figure 6-52 SIP FXO/Line Port Configuration Page



3. Configure the following settings on the SIP FXO/Line Port Configuration page:

- Configuring Global SIP Gateway FXO/Line Port Settings
- Registering with the SIP Server

Configuring Global SIP Gateway FXO/Line Port Settings

1. Choose **VoIP** > **SIP** > **SIP GW** (Figure 6-51).
2. Configure settings using the information in Table 6-39 as a guide.

Table 6-39 SIP FXO/Line Port Global Configuration Fields

Item	Description
Global Configuration Settings	
See Configuring Global SIP Gateway FXO/Line Port Settings.	
Enable SIP FXO/Line Port Services	Select the **Enable SIP FXO/Line Port Services** checkbox.
RTP Silence Delay	Enter the RTP silence delay when in call. If there is a continuous RTP silence from the PSTN side, the FXO/Line port terminates the call. Default is 120 seconds.
SIPGW IP Address	Enter the LAN side IP address to which the SIP gateway binds. By default, it is set to the class C subnet of the ALG LAN plus 253 (recommended). For example, if the ALG LAN is 192.168.1.0/24, the default IP address of the SIP gateway is 192.168.1.253. If the default IP address conflicts with another host on the ALG LAN, you can modify the SIP gateway IP address in this field.
Add Dial Out Prefix (To IP network)	Enter a value to prepend to the caller-id received from PSTN to create the FROM field when trunking a call from the PSTN to the IP network. Use digits [0-9].
Enable Priority Calling services	Select the checkbox to enable priority calling services for FXO ports. When priority call services are enabled, any call placed to a priority calling number from any FXS port or LAN-side SIP phone is routed on priority basis to the FXO port and connected. **Note:** Enabling Priority Calling Services overrides (or hides) the following settings for individual ports: ■ Enable InBound (from PSTN) two-stage dialing ■ Forwarded To settings **Note:** Priority calling services cannot be configured when WAN Link Redundancy (WLR) is enabled. **Tip:** Once priority calling service is enabled, make sure VoIP ALG has a dial plan set for priority calls in SIP trunking rules. Verify your dial plan settings by clicking the **SIP/ALG trunking rules** link or choose **VoIP** > **SIP** > **ALG** and refer to Configuring Bandwidth Settings for H.323.

Table 6-39 SIP FXO/Line Port Global Configuration Fields (continued)

Item	Description
Default Callback Extension	Enter a default callback number to receive callbacks from priority calling service operators after the Priority Call Window has lapsed. A callback may occur when a user (FXS or IP phone) dials the priority calling number and then hangs up. Ensure that this setting is set to an extension that is always up. This extension must be an FXS port or an extension on the LAN side, preferably the administrator desk extension. This field is required when Priority Calling Services are enabled. **Note:** When priority calling is enabled, the Callback Extension overrides any forwarding number configured for FXO ports.
Priority Call Window (sec)	Enter the amount of time in seconds during which an inbound call from PSTN is forwarded to the last IP caller that made an outbound priority call through that FXO port. The window starts when an outbound priority call is completed. If the window has lapsed and an inbound call from the PSTN is made, the call is forwarded to the Default Callback Extension instead. This field is only visible when Priority Calling Services are enabled. You must also configure **Priority calling SIP/B2BUA trunking rules**. Click the link provided or choose **VoIP** > **SIP** > **B2BUA** and refer to Configuring VoIP SIP B2BUA Trunking.
PSTN Sense Window (sec)	Enter the amount of time that the gateway senses the port to check if the PSTN line is connected to the FXO port and the line is alive. If there is no analog signal during this sensing period, the call is rejected with a “486” error. If value is set to 0 seconds, this feature is disabled.
Inter-Digit delay for dialing PSTN (msec)	Enter the delay in milliseconds between dialed digits to the PSTN.

3. Proceed to Registering with the SIP Server.

Registering with the SIP Server

1. Choose **VoIP** > **SIP** > **SIP GW** (Figure 6-52).
2. Scroll to **Register with SIP Server**.
3. Configure settings using the information in Table 6-40 as a guide.

Table 6-40 SIP FXO/Line Port SIP Server Configuration Fields

Item	Description
SIP Server Settings	
Register with SIP server	Select the **Register with SIP server** checkbox to register the FXO/GW with the SIP server using Override SIP FROM as SIP user name.
Override FROM Username (To IP Network)	Enter a message to override the system default SIP message FROM field. The FXO/GW registers with this name. **Note:** When the Override FROM field is specified with the SIP username, it replaces Dial Out Prefix and CallerID.
Sip Authentication Name	Enter a name and password in the **SIP Authentication Name** and **Password** fields only if the SIP FXO/Line port needs to be authenticated. **Tip:** Override the FROM domain name on the ALG Trunking Configuration page under Header Transformation. Choose **VoIP** > **SIP** > **ALG** and refer to Configuring Bandwidth Settings for H.323.
Password	(Optional) Enter the password to authenticate the SIP FXO/Line port against the SIP softswitch or outbound proxy. This field is only needed if SIP FXO/Line port must be authenticated
PSTN CO Auto-Disconnect timer (sec)	Enter the time in seconds for the PSTN CO to terminate the connection. This specifies the time after the SIP caller has hung up for the PSTN CO line to terminate the connection when the call originated from the PSTN through the FXO port. The time is usually 12-13 seconds. During this defined time value, the FXO port is not be available for making any outbound calls to the PSTN.
Override FROM Display Name (To IP network)	Enter a display name to override the default “anonymous” display name. If an override display name is not configured, the system uses information received from the PSTN as part of the CallerID by default. If CallerID feature is not present on the PSTN line, the default is “anonymous.”

4. Proceed to Configuring SIP Gateway FXO Ports.

Configuring SIP Gateway FXO Ports

1. Choose **VoIP** > **SIP** > **SIP GW** (Figure 6-52).
2. Scroll to **Port 1 Configuration**.
3. Configure settings using the information in Table 6-41 as a guide.

Table 6-41 SIP FXO/Line Port Configuration Fields

Item	Description
Port Configuration Settings	
Sets parameters for Port 1 and Port 2.	
Enable FXO Port	Select the **Enable FXO port** checkbox to enable the FXO/Line port for incoming and outgoing calls. When this field is not checked, the FXO/Line port is disabled.
TX gain to analog device	Choose the Analog Transmit gain. Adjusts the gain to optimize echo cancellation in a call. Default is 0db. **Note:** In cases where the default value does not optimize echo cancellation, adjust the gain with -6DB in steps to -10DB until echo is gone.
RX gain from analog device	Choose the Analog Receive gain. Adjusts the gain to optimize DTMF detection coming from the PSTN. Based on the line conditions, sometimes level of DTMF signal needs to be boosted to make DTMF detection more reliable. Default is 0DB.
Enable InBound (from IP Network) two stage dialing	Select the **Enable InBound (from IP network) two stage dialing** checkbox to allow two-stage dialing for incoming calls from the IP network.
Enable InBound (from PSTN) two stage dialing	Select **Enable InBound (from PSTN) two stage dialing** to allow two-stage dialing for incoming calls from the PSTN. Provides dial tone when a call is answered. The caller can then dial an extension to further complete the call or hang up.
Forwarded to	If the Enable InBound (from PSTN) two stage dialing checkbox is not selected, enter a name or number in the **Forward to** field to automatically forward incoming calls from the PSTN to this name or number.
Click **Submit** to save all settings on the SIP FXO/Line Port Configuration page.	

Configuring Network Side ISDN PRI (PRI/UA)

1. Choose **VoIP** > **SIP** > **SIP UA** > **PRI/NET Configuration**.
2. Refer to Configuring Network Side ISDN PRI (PRI/UA) in Chapter 3, *Network Deployment* to configure Network Side ISDN PRI (PRI/UA).

Configuring Network Side (CAS/UA)

1. Choose **VoIP** > **SIP** > **SIP UA** > **CAS/NET Configuration**.
2. Refer to Configuring Network Side CAS/UA in Chapter 3, *Network Deployment* to configure Network Side CAS/UA.

Configuring SIP Routing

Routing groups are groups of redundant LAN side SIP endpoints that act as a single routing point.

Before You Begin

LAN side trunking devices are configured on the ALG or B2BUA page. Once the devices have been configured, they can be grouped together on the SIP Routing page to create routing groups.

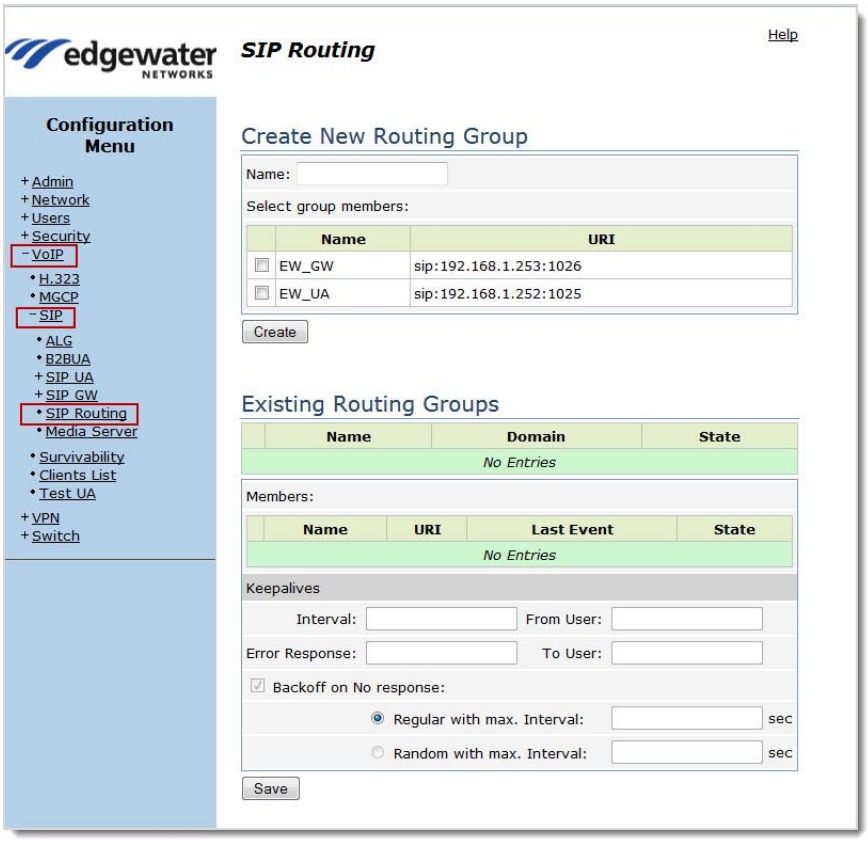
Configure LAN side trunking devices:

- Choose **VoIP** > **SIP** > **ALG** and configure settings on the ALG Trunking Configuration page. Refer to Configuring SIP ALG Trunking.
- Choose **VoIP** > **SIP** > **B2BUA** and configure settings on the B2BUA Trunking Configuration page. Refer to Configuring VoIP SIP B2BUA Trunking.

Creating and Managing Routing Groups and Keepalives

1. Choose **VoIP** > **SIP** > **SIP Routing** (Figure 6-53).

Figure 6-53 SIP Routing Configuration Page



2. Configure settings using the information in Table 6-42 as a guide. When you have finished configuring settings, click **Submit All** to make your changes take effect.

Table 6-42 SIP Routing Configuration Parameters

Item	Description
Create New Routing Group	
Name	In the **Name** field, enter a name for the routing group. For example, “Group1.”

Table 6-42 SIP Routing Configuration Parameters (continued)

Item	Description
Select group members	Choose routing group members by selecting the checkbox next to the names in the list. If this list is empty, go the ALG or B2BUA page and configure the trunking devices. Refer to the following: ■ Choose **VoIP** > **SIP** > **ALG** and configure settings on the ALG Trunking Configuration page. Refer to Configuring SIP ALG Trunking. ■ Choose **VoIP** > **SIP** > **B2BUA** and configure settings on the B2BUA Trunking Configuration page. Refer to Configuring VoIP SIP B2BUA Trunking. Click **Create**. The chosen entries are moved from the Create a New Routing Group table to the Existing Routing Group table.

Existing Routing Groups

Lists and monitors all the currently configured routing groups.

- Name—Name of the routing group. Group name should consist of alphabet,numbers, and '-' or '_' symbols.
- Domain—Domain Name to which all group members (trunking devices) are registered.
- State—Displays the status of the routing group. The status can have the following values:
  - Unavailable—None of the members in the group are reachable.
  - Available—At least one of the members is reachable
  - Unknown—Members are either unavailable or not monitored

Table 6-42 SIP Routing Configuration Parameters (continued)

Item	Description
Members	Lists all the members of the selected routing group. The last column of the table gives the current state of the SIP device: ■ Name—Name of the trunking device which is configured on the ALG or B2BUA page. ■ URI—SIP URI is consists of 'sip:' word followed by IP address of trunking device and port no. e.g. sip:192.168.5.11:5060. ■ Last Event—Date and time of last event from group member (trunking device). ■ State—Displays the current state of the SIP device, which can be one of the following three: ■ Available—Reachability test passed. ■ Unavailable—Reachability test failed. ■ Not monitored—No reachability test configured for this device.
Keepalives	
Manages configuration options for the keepalive messages used by the system to monitor each trunking device. The system monitors the routing group members by sending them periodic SIP OPTIONS Keepalive messages:	
Interval	Enter the interval in seconds between each keepalive message.
From User	Enter the From username in the SIP OPTIONS message generated by the system.
To User	Enter the To username in the SIP OPTIONS message generated by the system.
Error Response	Enter a response code to treats the trunking device as unreachable. Only one response code may be entered: ■ Backoff on No response—Manages the behavior of Keepalives when no response is received. ■ Regular with max. Interval—Successively doubles the interval until it reaches the maximum interval. ■ Random with max. Interval—Sends the next keepalive after a randomly selected interval between three seconds and the maximum interval.

Table 6-42 SIP Routing Configuration Parameters (continued)

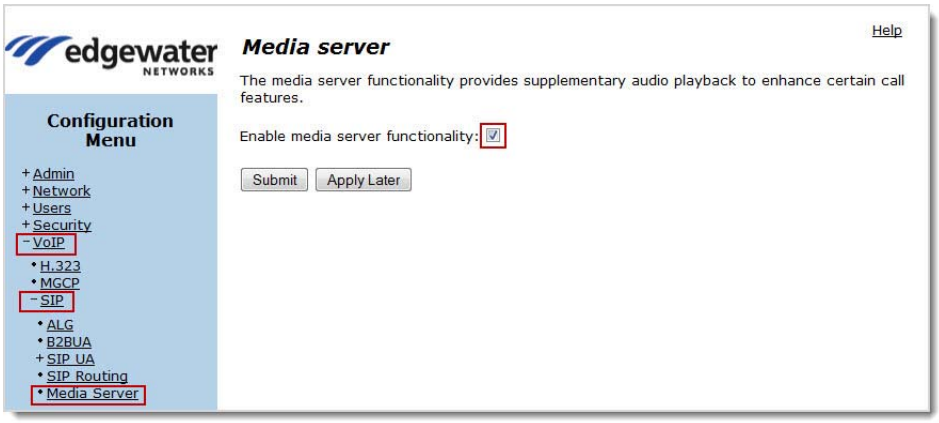
Item	Description
	Click **Save**. Click **Submit All** to save all changes on the page. To delete any entry in the Existing Routing Group table, click the red x next to entry that you want to delete from the routing group. The entry is removed from the Existing Routing Group table and appears in the Create a New Routing Group table.

Configuring the SIP Media Server

Enable media server functionality to configure supplementary audio playback to enhance certain call features, such as simulated ring tone during an unattended transfer.

1. Choose **VoIP** > **SIP** > **Media Server** (Figure 6-54).

Figure 6-54 Media Server Configuration Page



2. Select the **Enable media server functionality** checkbox and click **Submit**.

Configuring Survivability

Manage Survivability to extend VoIP service availability on the EdgeMarc.

- Overview
- Viewing Current Survivability Status
- Configuring Survivability Common Settings
- Configuring SIP Server Reachability
- Configuring SIP Server Redundancy
- Configuring Local Call Control

- Configuring SIP Registration Control

Overview

Survivability is a collection of features that enables the system to extend VoIP service availability. These features include support for redundant SIP soft switches and local call control in the event of WAN link failure, softswitch failure, or during periods of network congestion that result in loss of connectivity.

Dynamic WAN links (DHCP and PPPoE, for example) can renegotiate their public IP address at any time, interrupting VoIP services. All system services must be restarted when the WAN connection is restarted, because the WAN IP address may have changed. Because Survivability must communicate with the softswitch/IP PBX, Survivability is restarted when WAN link renegotiation occurs, interrupting any local calls that are in progress.



Note
Survivability is not recommended for systems that use dynamic WAN links.

Survivability allows users connected to an EdgeMarc to make and receive calls when the softswitch or the link to the softswitch is down. Survivability provides the following capabilities:

- Availability—Detects when the softswitch is unreachable.
- Redundancy—Switches to a redundant softswitch:
  - Makes and receives station-to-station calls while the softswitch is unreachable
  - Makes and receives PSTN calls while the softswitch is unreachable.

To switch to Survivability mode, the EdgeMarc must be able to detect when the softswitch is unreachable. The softswitch may be unreachable for the following reasons:

- The softswitch is down.
- A router on the path to the softswitch is malfunctioning.
- The network is physically disconnected.

The most reliable way to ensure that the softswitch is reachable and available is to make a request at the application layer. If the request receives a response, the softswitch is reachable at the IP layer and is servicing requests.

How Survivability Works

SIP requests sent to and received from the softswitch are monitored for softswitch availability. If requests are sent to the softswitch but no responses are received in a configured time interval, the softswitch is considered unreachable and a backup server (if available) is selected as the current server. The default time interval is configured so that failover

occurs before the phone has finished re-sending its request. This enables the call to be connected with only a slight delay.

A configuration option also allows the active softswitch to be monitored with keepalive messages. The messages are sent at a configurable intervals with time allowed for a response to be received. If too many messages are unanswered, the softswitch is considered unreachable.

When a softswitch is marked as unreachable, the EdgeMarc uses a different keepalive mechanism to determine when it becomes available again. The EdgeMarc sends keepalive messages to failed servers using a backoff algorithm that progressively increases the interval, until a maximum is reached. By default, the maximum interval is longer than the one used when no other backup server is available.

An upstream EdgeMarc or EdgeProtect device can send a specially marked keepalive response to inform the downstream EdgeMarc about loss of connectivity to the softswitch. This causes an immediate fallback to the backup server or Survivability mode in the downstream EdgeMarc without a time delay.

The EdgeMarc can choose the active softswitch from a list of multiple redundant softswitches based on priority and availability. It can obtain the list of redundant softswitches dynamically by doing a DNS SRV lookup on the SIP Server domain name or from a list entered in the appliance user interface. When multiple IP addresses are configured, the highest priority one is used. If this server becomes unreachable, the next reachable server in the order of priority is used. If a previously unreachable server becomes available and it has a higher priority than the currently used server, the higher priority server is used again.

If no softswitch is available, the EdgeMarc enters Survivability mode and handles call signaling itself. Because the EdgeMarc forwards all messages between the phones and the softswitch, it knows the address of all phones and can direct calls to the phones itself.

A SIP PSTN gateway can be installed on the LAN side of the EdgeMarc and used for inbound and outbound calling during Survivability. (Normally, the gateway functionality is provided by the softswitch.) The gateway can be configured to send any incoming calls to the EdgeMarc, and the EdgeMarc can be configured to use the gateway as the default destination for calls not directed to another local phone.

When connectivity to the softswitch is restored, the EdgeMarc automatically returns control of all subsequent call requests to the softswitch. Calls in progress that were established while the EdgeMarc was in fallback mode are not disrupted.

Survivability in Transparent Mode

The EdgeMarc now supports Survivability when the transparent option is selected for the Session Initiation Protocol (SIP) mode.

An EdgeMarc is typically deployed with two separate IP addresses:

- Public IP address used for interactions with the WAN
- Private IP address used for communications with locally-installed phones and other devices

The devices attached to the EdgeMarc communicate with the appliance using the private IP address, and the EdgeMarc communicates with the WAN using the public IP address. The network softswitch that provides feature services knows the public IP address but has no knowledge of the private address. The treatment of traffic sent between phones and the network depends on the choice of SIP mode.

In *normal* (default) mode, a phone connected to the EdgeMarc is configured with a private IP address and views the appliance as if the appliance is a softswitch. The Layer 3 signaling between the phone and the EdgeMarc is terminated at the appliance, and a separate Layer 3 signaling link is established between the EdgeMarc and the softswitch on the network. The phone device cannot see all the way to the network softswitch, and the softswitch cannot see all the way to the phone.

In *multi-homed outbound proxy* mode, the EdgeMarc functions as a proxy server. Each phone connected to the appliance is configured with the IP address of the network softswitch. An outbound proxy address is also configured, which the EdgeMarc is able to translate. Because the phone includes the softswitch address in its SIP message, the EdgeMarc is able to forward the SIP message to the softswitch. The proxy mode is multi-homed, because it is possible for phones connected to a single EdgeMarc to be served by different softswitches. In addition to performing translation, the EdgeMarc is able to forward the signaling to the correct softswitch for each phone.

In *transparent* mode, the phone is configured with the IP address of the softswitch, and Layer 3 packets are sent all the way from the phone to the softswitch without being terminated. The EdgeMarc picks up the signals as they are forwarded through the appliance and translates, but does not terminate them. Because the EdgeMarc hides the local topology from the WAN, the softswitch does not know the private IP addresses of the phones attached to the appliance; however, the phones know the identity of the softswitch. For this reason, it is also possible for different phones connected to the EdgeMarc to be served by different softswitches.

Survivability Mode

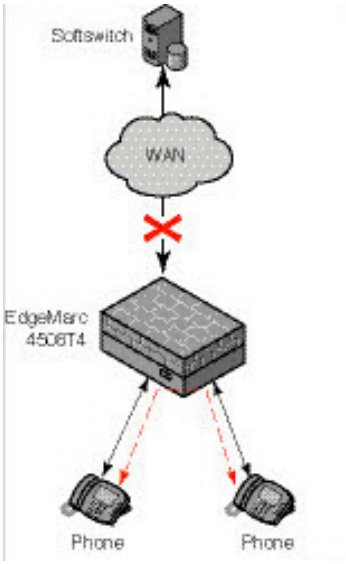
Survivability capabilities are triggered if the EdgeMarc loses its connection to the WAN or if the network softswitch is not accessible. When this occurs, the EdgeMarc uses the information that was obtained from the terminated

or forwarded phone signals to direct local calls between phones attached to the appliance.

For example, assume that phones A and B are connected to the EdgeMarc and that A attempts to call B. The Survivability process works as follows:

1. Phone A sends a request to the EdgeMarc.
2. The EdgeMarc attempts to forward the call to the softswitch IP address that is configured in the appliance. The number of attempts is dictated by the Survivability settings.
3. If the attempt to contact the softswitch fails, the EdgeMarc takes over and performs the softswitch function, connecting phone A to phone B (Figure 6-55).

Figure 6-55 Survivability



Note
The EdgeMarc always attempts to connect to the softswitch configured in the appliance. In transparent mode, this could be different from the softswitch configured in the phones. If the softswitches are different, the EdgeMarc is unable to perform the Survivability function.

Viewing Current Survivability Status

1. Choose **VoIP** > **Survivability** (Figure 6-56).

Figure 6-56 Survivability - Current Status

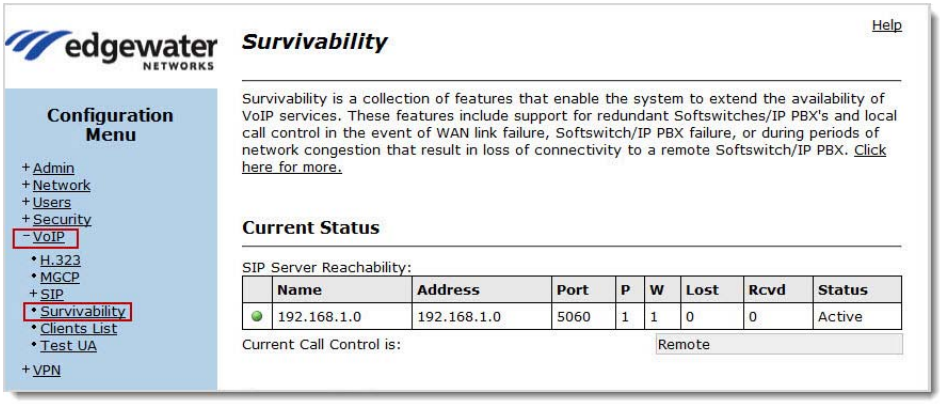


Table 6-43 describes SIP Server Reachability status.

Table 6-43 Current Status - SIP Server Reachability Fields

Item	Description
Status Indicator	
Green Button	The server is reachable and currently in use.
Red Button	The server is unreachable and is currently being monitored with OPTIONS messages.
Empty Button	The status of the server is not known.
SIP Server Redundancy	
Name	Name of the server as returned by the DNS server.
Address	IP address of the server.
Port	Port for the SIP protocol.
P	Priority of the server.
W	Weight of the server.
Lost	Number of consecutive OPTION messages lost.
Rcvd	Number of consecutive OPTIONS messages received.
Status	

Table 6-43 Current Status - SIP Server Reachability Fields (continued)

Item	Description
Active	The server is in use right now. If keepalives for the active server are enabled, the Rcvd column shows how many consecutive replies have been received so far.
Unreachable	The server is not reachable and is currently being monitored with OPTIONS messages.
Idle	The server is not being monitored and its status is unknown.
Current Call Control	Shows whether the system is in remote or local mode.
Registration Status	Shows the SIP registration status for the OPTIONS user name. Visible when **Register user with softswitch** is enabled and a User name has been provided in the Authentication section.

Configuring Survivability Common Settings

1. Choose **VoIP** > **Survivability**.
2. Scroll to **Common Settings** (Figure 6-57).

Figure 6-57 Common Settings



3. Configure settings using the information in Table 6-44 as a guide.

Table 6-44 Survivability Common Settings Parameters

Item	Description
Common Settings	
Survivability	Choose an option from the **Survivability** drop-down list: ■ **Disabled** (default)—The system does not provide local call switching in the event of a loss of connectivity to the Softswitch/IP PBX. ■ **Enabled** (auto)—The system automatically performs local call switching when the Softswitch/IP PBX becomes unavailable. ■ **Always Local**—The system always provides local call switching even when the Softswitch/IP PBX is available to process calls. **Tip:** When all softswitches are unreachable, the system can act as a proxy for the locally attached phones.
Time between DNS lookups	Enter the number of seconds between the DNS SRV lookup on the SIP server URL that was entered on the **VOIP** > **SIP** page. See Configuring Survivability Common Settings.

Click **Submit** to save your settings.

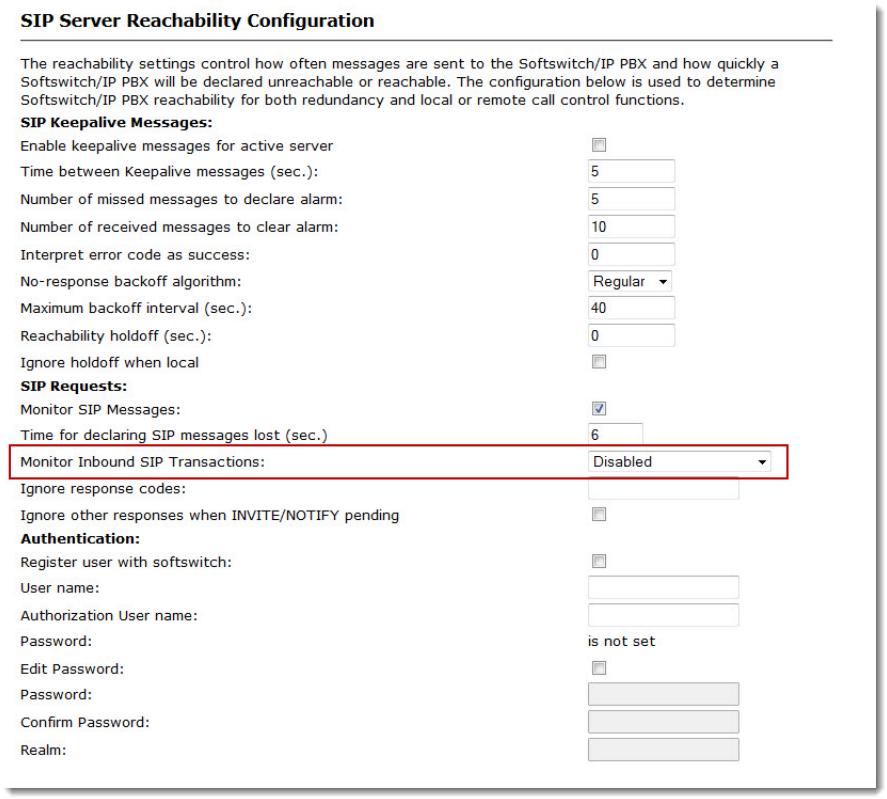
Proceed to Configuring SIP Server Reachability.

Configuring SIP Server Reachability

Reachability settings control how often messages are sent to the softswitch/IP PBX and how quickly a softswitch/IP PBX is declared unreachable or reachable. Configure softswitch/IP PBX reachability for both redundancy and local or remote call control functions.

1. Choose **VoIP** > **Survivability**.
2. Scroll to **SIP Server Reachability Configuration** (Figure 6-58).

Figure 6-58 SIP Server Reachability Configuration



3. Configure settings using the information in Table 6-45 as a guide.

Table 6-45 SIP Server Reachability Configuration Parameters

Item	Description
SIP Server Reachability Configuration	Controls how often messages are sent to the Softswitch/IP PBX and how quickly a Softswitch/IP PBX is declared unreachable or reachable. Determines Softswitch/IP PBX reachability for redundancy and local or remote call control functions.
SIP Keepalive Messages	Configure SIP keepalive messages:

Table 6-45 SIP Server Reachability Configuration Parameters (continued)

Item	Description
Enable keepalive messages for active server	Select the checkbox to enable keepalive messages for active server. The Survivability module sends SIP OPTIONS messages to the Active softswitch at regular intervals and monitors the replies to establish availability of the softswitch.
Time Between Keepalive Messages	Enter the number of seconds between consecutive keepalive messages sent to the softswitch to determine connectivity. **Note:** This field only controls the time between keepalives sent to the active server. When the server is marked unavailable, a backoff algorithm is used for the time interval between keepalives to this server.
Number of Missed Messages To Declare Alarm	Enter the number of missed messages after which a loss of connectivity to the remote switch is declared. The interval used for these keepalives is the defined initial interval of the regular backoff algorithm, described below. This is 5 seconds by default.
Number of received messages to clear alarm	Enter the number of consecutively received keepalive messages required for the system to declare successful connectivity to the remote softswitch.
Interpret error code as success	Enter the error code to be treated as a successful response (range 300-699). A response with a successful return code (range 200-299) is always accepted.

Table 6-45 SIP Server Reachability Configuration Parameters (continued)

Item	Description
No-response backoff algorithm	Choose the behavior of keepalive messages when a SIP server becomes unavailable. The following options control the behavior of these keepalive messages when no response is received. Once a response is received, the system resets the interval to the default initial value (5 seconds). ■ **Regular**—Keepalive messages to the failed server are started immediately after unavailability is detected. If the system does not receive any response to the keepalive messages, it doubles the interval for the next message until it reaches a maximum. The maximum interval is 40 seconds when in local mode and 160 seconds when in remote mode. ■ **Random**—Keepalive messages are not immediately started. The system waits for a random period between 3 seconds and the maximum configured value, Tmax, before starting the OPTIONS pings. If the system does not receive any response to the keepalive messages, it continues to wait for a randomly selected period between 3 seconds and Tmax seconds before sending the next OPTIONS message.
Maximum backoff interval	Enter the maximum back off interval when you choose the Random option for the No-response back off algorithm.
Reachability holdoff	Enter the minimum number of seconds to wait after the reachability algorithm detects that a higher priority server has become reachable before marking the server active. This is used to help prevent flip-flopping of the available server when an SBC responds to keepalives but the actual SIP server is not ready to handle registrations. Most installations use a default value of 0 seconds.
Ignore holdoff when local	Select the checkbox to instruct the system not to apply the Reachability Holdoff delay when the system is running in local mode. This prevents unnecessary delay when switching from local mode to remote SIP servers.
SIP Requests	

Table 6-45 SIP Server Reachability Configuration Parameters (continued)

Item	Description
Monitor SIP Messages	Select the checkbox to monitor SIP requests sent to the active server. When this option is selected, the system monitors the SIP requests sent to the active server (excluding keepalive messages generated by the system). If no response is received within the specified time, that server is marked as unavailable.
Time for declaring SIP messages lost (seconds)	Enter the number of seconds to wait for a reply to a SIP request. If no request is received within this time interval, the softswitch is declared unreachable.
Monitor Inbound SIP Transactions	Monitors SIP requests from the active SIP server trigger cancellation of the “Monitor SIP Messages” timer. Disabled—The cancellation of the SIP messages timer on request received from active SIP server is disabled. All SIP Requests—Monitor all SIP requests to cancel the SIP messages timer. All except SIP OPTIONS—Monitor all SIP requests except OPTIONS to cancel the SIP messages timer.
Ignore response codes	Enter response codes that ignore SIP request timeout messages once the Session Border Controller (SBC) has received 100 Trying responses. Enter a comma separated list of response codes. For example, if the list is “100,404,” Survivability ignores a 100 Trying response and 404 Not Found response when determining whether a SIP message has been responded to.

Table 6-45 SIP Server Reachability Configuration Parameters (continued)

Item	Description
Ignore other responses when INVITE/NOTIFY pending	Select the checkbox to ignore SIP request timeout messages that have an INVITE pending. The Ignore options are useful in environments that have an SBC in the network that responds directly to certain SIP messages. In particular, REGISTER messages are handled by the SBC. Other messages, INVITES in particular, are handled by the SS. In this configuration, the Survivability algorithm might not detect a failure, if the Softswitch went down, but the SBC kept running. It would see responses from the REGISTER messages, but no responses from INVITES. Depending on how they were intermixed, it would at least delay entry into Survivability, and potentially not go into Survivability at all. With the Ignore options set, the Survivability algorithm ignores any response traffic except for non-100 INVITE responses.
Authentication	
Register user with softswitch	Select the **Register user with softswitch** checkbox to enable the SBC to recognize OPTIONS sent to the softswitch by registering the “From” username of the OPTIONS message.
User name	Enter the user name that is used in the SIP Keepalive messages. If the “Register user with softswitch” box is checked, this username is also registered with the softswitch.
Authorization User name	Enter the username to be used in authorization response.
Password	Enter the authentication password.
Realm	Enter the realm string for the server where the above credentials are to be used. The realm string can be set to any base64 value to identify the secure area and may used by HTTP clients to manage passwords. For example: “aHR0cHdhdGNoOmY=” If this field is left blank, the credentials are used for all realms. If a realm string value is provided, the password is not saved in clear text in the configuration file.

Click **Submit** to save your settings.

Proceed to Configuring SIP Server Redundancy.

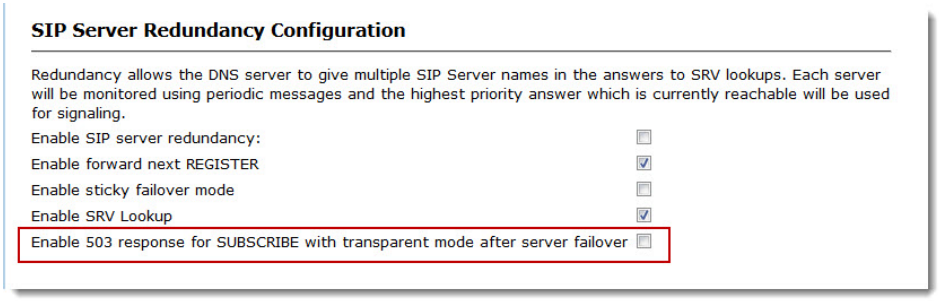
Configuring SIP Server Redundancy

Redundancy allows the DNS server to give multiple SIP Server names in the answers to SRV lookups. Each server is monitored using periodic messages; the highest priority answer that can be reached is used for signaling.

To configure SIP server redundancy:

1. Choose **VoIP** > **Survivability**.
2. Scroll to **SIP Server Redundancy Configuration** (Figure 6-59).

Figure 6-59 SIP Server Redundancy



3. Configure settings using the information in Table 6-46 as a guide.

Table 6-46 SIP Server Redundancy Parameters

Item	Description
Authorization User name	Specifies the username to be used in authorization response.
Password	Specifies the authentication password.

SIP Server Redundancy Configuration

Allows the DNS server to give multiple SIP server names in the answers to SRV lookups. Each server is monitored using periodic messages. The highest priority server that is currently reachable is used for signaling. See Configuring SIP Server Redundancy.

Enable SIP server redundancy	Select the checkbox to enable monitoring of multiple SIP servers. A lower priority SIP server can be used if connectivity to the main SIP server is lost.
Enable forward next REGISTER	Select the checkbox to forward the first REGISTER message from each SIP client to the softswitch after it becomes available. After the first REGISTER has been sent, normal REGISTER rate-pacing begins.
Enable sticky failover mode	Select the checkbox to allow the Survivability module to stick to the failover server and discourage switch back to the failed higher priority softswitch.

Table 6-46 SIP Server Redundancy Parameters (continued)

Item	Description
Enable SRV Lookup	Checkbox is selected by default. Allows service record (SRV) lookup for the SIP server FQDN. If SRV Lookup is disabled (checkbox is un-checked), the system uses A-Lookup only.
Enable 503 response	Select the checkbox to enable 503 response for SUBSCRIBE with transparent mode after server failover. With SIP server redundancy enabled, if there is a loss of connectivity to the SBC detected (Options or SIP message counter), existing active subscriptions do not terminate until expiration, which can cause a service outage for phones using SCA/BLF.

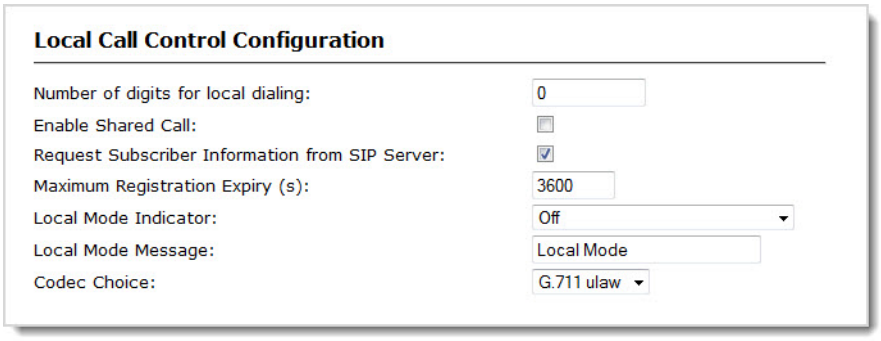
Click **Submit** to save your settings.

Proceed to Configuring Local Call Control.

Configuring Local Call Control

1. Choose **VoIP** > **Survivability**.
2. Scroll to **Local Call Control Configuration** (Figure 6-60).

Figure 6-60 Local Call Control



3. Configure settings using the information in Table 6-47 as a guide.

Table 6-47 Local Call Control Parameters

Item	Description
Local Call Control Configuration	
Number of digits for local dialing	Enter the number of digits that the system uses to process local calls during local call switching. For example, if you enter the number 4, the last four digits are used as the phone extension. If you enter 0, the whole phone number is used.

Table 6-47 Local Call Control Parameters (continued)

Item	Description
Enable Local-Mode Indicator	Select the checkbox to instruct the system to ignore Register messages from the phone. The phone displays a different Icon or Line-Appearance symbol while in Local mode.
Enable Shared Call	Select the checkbox to route all SIP calls to the phone primary line appearance while in Local mode. Use this option when the phone is configured to have multiple shared/bridged call appearances. Without this option, calls made to any of the appearances other than the first appearance are ignored by the EdgeMarc while it is in Local mode. SIP only.
Request Subscriber Information from SIP Server	Select the checkbox to request subscriber information as a part of the phone registration procedure. The Softswitch/IP PBX then returns additional information about the phone, such as additional extensions, that can be used in survivable mode.
Maximum Registration Expiry	Enter the maximum registration expiry interval, in seconds, that the local call control server accepts from SIP endpoints. Use this field to match the registration expiry interval of the local call control server with the remote server. If the local expiry interval is longer than that of the remote server, the endpoints lose their registration with the remote softswitch when they come out of local mode.
Local Mode Indicator	Choose an option for handling Register messages when in local mode: ■ **Off** —No local mode indicator is used. ■ **Suppress Register Response**—The system ignores Register messages from the phone to cause the phone to display a different Icon or Line-Appearance symbol while in Local mode. ■ **Send Response Information**—The system sends information back to the phone in the register response, which the phone then displays to the user.
Local Mode Message	Enter a local mode message that will be shown on the user's phone (for phones that support this feature) when the system is in local mode. SIP only.

Table 6-47 Local Call Control Parameters (continued)

Item	Description
Codec Choice	Choose a codec to signal when in Survivability mode from the **Codec Choice** drop-down list: ■ G.711 ulaw ■ G.711 alaw ■ G.729

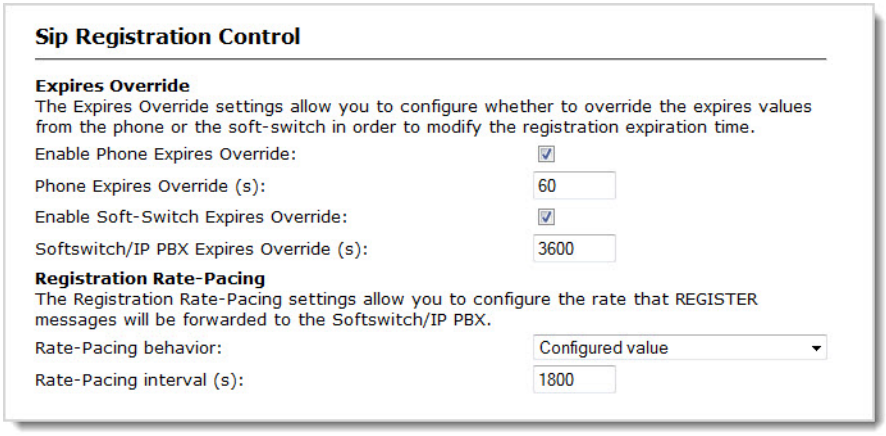
Click **Submit** to save your settings.

Proceed to Configuring SIP Registration Control.

Configuring SIP Registration Control

1. Choose **VoIP** > **Survivability**.
2. Scroll to **SIP Registration Control** (Figure 6-61).

Figure 6-61 SIP Registration Control



3. Configure settings using the information in Table 6-48 as a guide.

Table 6-48 SIP Registration Control Parameters

Item	Description
SIP Registration Control	
Expires Override	Allows the device to alter the “expires” values in the REGISTER message and the response to this message. If these fields are disabled, the expires values are not altered.

Table 6-48 SIP Registration Control Parameters (continued)

Item	Description
Enable Phone Expires Override	Select the checkbox to override the Registration expiry interval sent to the phone with the value given in the next field.
Phone Expires Override	Enter the number of seconds that a phone considers a registration valid. This value replaces the value given by the SIP server in the response to the REGISTER message. The phone sends the next registration before this time has passed, therefore speeding up the rate at which the phone sends registrations.
Enable Softswitch Expires Override	Select the checkbox to enable softswitch expires override checkbox.
Softswitch/IP PBX Expires Override	Specifies the number of seconds that the SIP server considers a registration valid: ■ **Phone Expires Override**—Specifies the number of seconds that a phone should consider a registration valid. This value replaces the value given by the SIP server in the response to the REGISTER message. The phone sends the next registration before this time has passed. Use to speed up the rate at which the phone sends registrations. ■ **Softswitch Expires Override**—Specifies the number of seconds that the SIP server should consider a registration valid. This value replaces the value given by the phone in the REGISTER message. This value should be higher than the rate-pacing value so that the SIP server does not consider the phone registration to have expired.
Registration Rate-Pacing Specifies the rate at which registration messages are forwarded to the Softswitch/IP PBX.	

Table 6-48 SIP Registration Control Parameters (continued)

Item	Description
Rate-Pacing behavior	Choose a mode from the **Rate-Pacing behavior** drop-down list: ■ **None**—No rate pacing is applied. ■ **SoftSwitch / IP PBX provided value**—Rate of pace is calculated from the value provided by the SIP server. ■ **Configured value**—Rate of pace is configured. For example, if you choose the SoftSwitch/IP PBX provided value: Pace Time = SIP server provided value - 2 * Phone Expires Override This ensures that the system allows registration to the SIP server before the registration has expired.
Rate-Pacing interval	Enter the number of seconds to wait before forwarding a register message from one phone to the SIP server. If the Phone Expires Override field is set to a low value, the number of registration messages may overload the SIP server. To avoid this, set this field to the number of seconds to wait before forwarding a register message from one phone to the SIP server. Any register messages received before this time is answered locally by the system. For example, you may set the Phone Expires Override value to 60 and the Registration Rate-Pacing value to 1800 to have the phone register to the system every minute, but only let a register message through to the SIP server every 30 minutes.
Click **Submit** to save all settings on the Survivability configuration page.	

Configuring the Clients List

Use this page to configure the entries for devices that have registered with the EdgeMarc. When you select a protocol on the page, the page refreshes to show information for the selected protocol: SIP, MGCP, or H.323. Clients can be added and deleted without restarting the system.

Add a client to the specified Clients List:

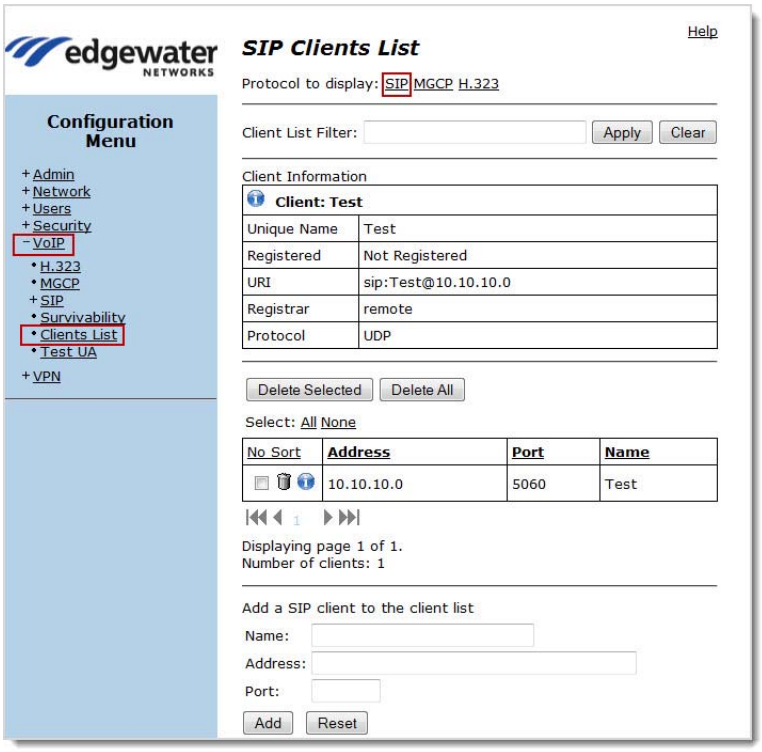
- SIP Clients List

- MGCP Clients List
- H.323 Clients List

SIP Clients List

1. Choose **Voip** > **Clients List** (Figure 6-62). The SIP Clients List opens by default.
2. (Optional) Enter text in the Client List Filter field to narrow your clients list search and click **Apply**. To remove the filter to return to a general search, click **Clear**.

Figure 6-62 SIP Client List Configuration Page



3. Configure settings using the information in Table 6-49 as a guide. When you have finished configuring settings, click **Add** to make your changes take effect.

Table 6-49 SIP Clients List Parameters

Item	Description
Protocol to Display	Click **SIP** to display the SIP clients list.
Client List Filter	Narrows a client search for a subset of clients based on text entered into the field. The **Apply** button applies the currently typed string, and the **Clear** button removes the specific search filter.

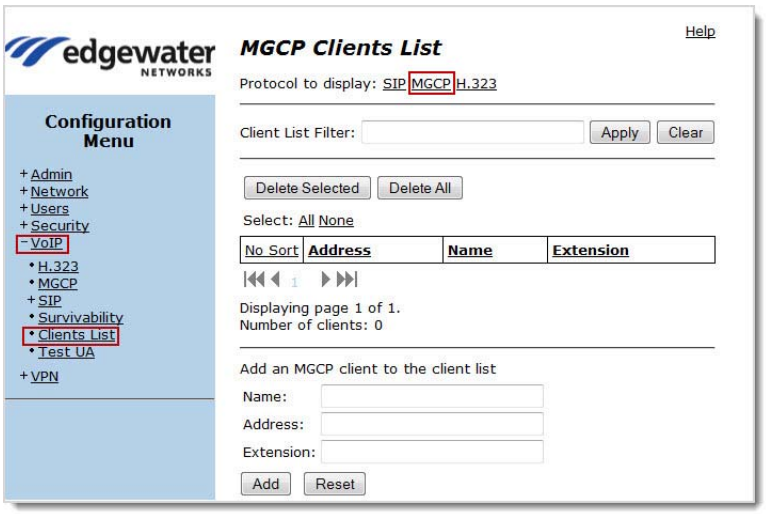
Table 6-49 SIP Clients List Parameters (continued)

Item	Description
Clients List	
	Icons in the first column of the Clients List allow you to manage list entries depending on the protocol: ■ Trash can—Deletes the entry. ■ Info—Displays additional information about the client. ■ Warning—Client has not responded to audits for the given amount of time.
Add a SIP Client to the Clients List	
Name	Enter the name of the SIP client.
Address	Enter the IP address of the SIP client.
Port	Enter the port used by the SIP client.
	Click **Add** to add the specified SIP client to the Clients List. Manage clients in the Clients List table by clicking the accompanying icons. Delete a client by selecting the checkbox next to the client entry and clicking **Delete** or by clicking the trash can icon.

MGCP Clients List

1. Choose **Voip** > **Clients List** (Figure 6-62). The SIP Clients List opens by default.
2. In the Protocol to Display field, click **MGCP**.
3. (Optional) Enter text in the Client List Filter field to narrow your clients list search and click **Apply**. To remove the filter to return to a general search, click **Clear**.

Figure 6-63 MGCP Client List Page



4. Configure settings using the information in Table 6-50 as a guide. When you have finished configuring settings, click **Add** to make your changes take effect.

Table 6-50 MGCP Clients List Parameters

Item	Description
Protocol to Display	Click **MGCP** to display the MGCP clients list.
Client List Filter	Narrows a client search for a subset of clients based on text entered into the field. The **Apply** button applies the currently typed string, and the **Clear** button removes the specific search filter.
WAN Gatekeeper status	MGCP only. Displays gatekeeper mode information.

Clients List

Icons in the first column of the Clients List allow you to manage list entries depending on the protocol:

- Trash can—Deletes the entry.
- Info—Displays additional information about the client.
- Warning—Client has not responded to audits for the given amount of time.
- MGCP star—Modifies the extension number of the client. The client extension number is required only if the MGCP Survivability feature is enabled. Otherwise, it can be left blank.

Add an MCGCP Client to the Clients List

Table 6-50 MGCP Clients List Parameters (continued)

Item	Description
Name	Enter the name of the MGCP client.
Address	Enter the IP address of the MGCP client.
Extension	Enter the MGCP client's phone extension.

Click **Add** to add the specified MGCP client to the Clients List.

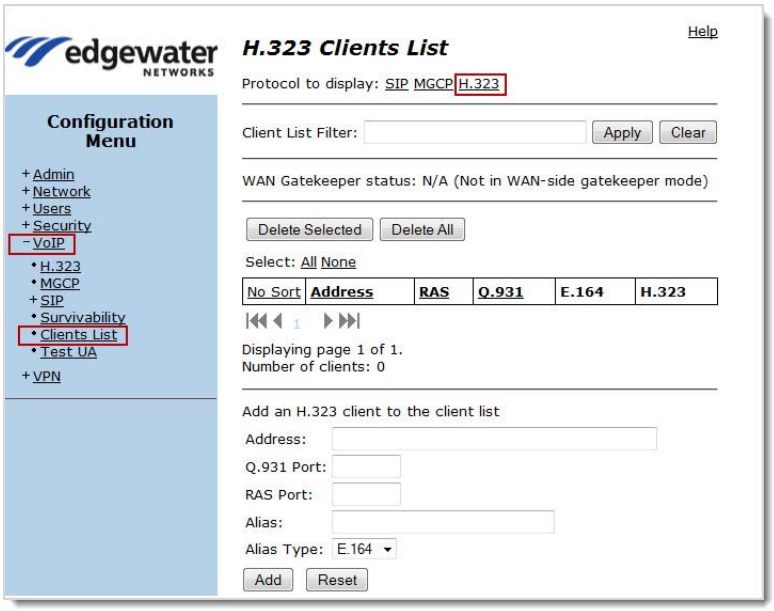
Manage clients in the Clients List table by clicking the accompanying icons.

Delete a client by selecting the checkbox next to the client entry and clicking **Delete** or by clicking the trash can icon.

H.323 Clients List

1. Choose **Voip** > **Clients List** (Figure 6-62). The SIP Clients List opens by default.
2. In the Protocol to Display field, click **H.323**.
3. (Optional) Enter text in the Client List Filter field to narrow your clients list search and click **Apply**. To remove the filter to return to a general search, click **Clear**.

Figure 6-64 H.323 Client List Page



4. Configure settings using the information in Table 6-51 as a guide. When you have finished configuring settings, click **Add** to make your changes take effect.

Table 6-51 H.323 Clients List Parameters

Item	Description
Protocol to Display	Click **H.323** to display the H.323 clients list.
Client List Filter	Narrows a client search for a subset of clients based on text entered into the field. The **Apply** button applies the currently typed string, and the **Clear** button removes the specific search filter.

Clients List

Icons in the first column of the Clients List allow you to manage list entries depending on the protocol:

- Trash can—Deletes the entry.
- Info—Displays additional information about the client.
- Warning—Client has not responded to audits for the given amount of time.
- H.323 lock—Locks or unlocks the endpoint. A locked endpoint is not automatically deleted by the system (if that feature is enabled).

Add an H.323 Client to the Clients List

Address	Enter the static IP address of the H.323 client.
Q.931 Port	Enter the Q.931 call signaling port on which the endpoint sends call setup information. Port 1720 is generally used.
RAS Port	Enter the Registration, Admission and Status (RAS) port. Port 1719 is generally used.
Alias	Enter the H.323 or E.164 alias for the static client that you are adding.
Alias Type	Choose the type of alias entered in the Alias field: ■ E.164 ■ H.323

Click **Add** to add the specified H.323 client to the Clients List.

Manage clients in the Clients List table by clicking the accompanying icons.

Delete a client by selecting the checkbox next to the client entry and clicking **Delete** or by clicking the trash can icon.

Managing Test UA

Use the Test UA page to make calls to and from the EdgeMarc to verify VoIP connectivity and conduct audio quality audits.

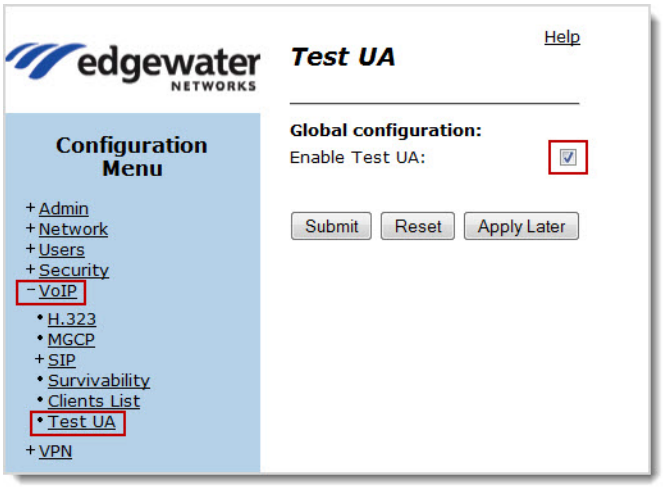
- Using the Test UA Settings Page
- Verifying Connectivity with Test UA

Using the Test UA Settings Page

Test UA settings are only available on some EdgeMarc models.

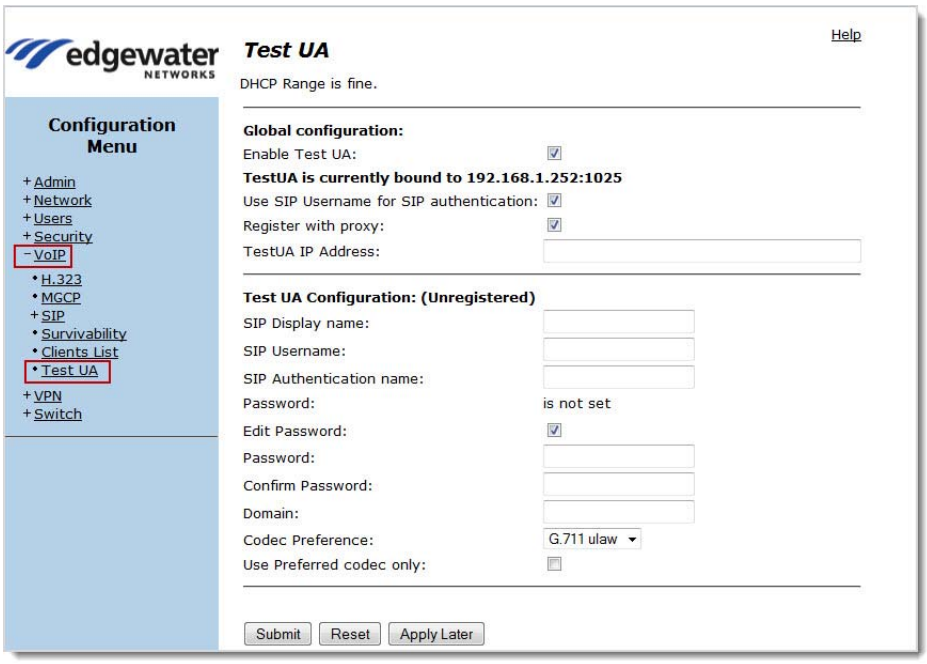
1. Choose **VoIP** > **Test UA** (Figure 6-65).

Figure 6-65 Test UA Page



2. Select the **Enable Test UA** checkbox and click **Submit**. Test UA settings fields become active (Figure 6-66).

Figure 6-66 Test UA Settings Configuration Page



3. Configure settings using the information in Table 6-52 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 6-52 Test UA Page Parameters

Item	Description
Global Configuration	
Enable Test UA	Select the checkbox to enable the Test UA function on the EdgeMarc. **Note**: un-checking this box does not delete any pre-existing Test UA configuration.
Use SIP Username for SIP authentication	Enter the SIP username for SIP authentication.
Register with proxy	Select the checkbox to register Test UA with a configured domain using a configured outbound proxy. If the box is not checked, the Test UA does not register.

Table 6-52 Test UA Page Parameters (continued)

Item	Description
Test UA IP Address	Enter the LAN IP address assigned to the user agent. When left blank, the IP address is set to the class C subnet of the VoIP ALG LAN plus 252 by default. For example, if the ALG LAN is 192.111.1.0/24, the default IP address of the SIP UA is 192.111.1.252. If the default IP address conflicts with another host on the VoIP ALG LAN, you can define the Test UA IP address in this field. The default configuration is sufficient in most cases.
Test UA Configuration	
SIP Display name	Enter a display name.
SIP Username	Enter a SIP User name to define the identity of the Test UA. This can be either a name or a number that is used to reach the Test UA.
SIP Authentication Name	Enter the SIP authentication name if the **Use SIP Username for SIP authentication** box is NOT checked in Global Configuration. This name is used by the Test UA to authenticate itself and can be the same as the SIP Username.
Password Edit Password	Select the **Edit Password** checkbox and enter a password in the field provided to set authorization credentials for the softswitch or outbound proxy. See Password Restrictions in Chapter 2, *System Administration* for help with setting passwords.
Domain	Enter the softswitch domain where each Test UA is provisioned and authenticated. If the field is left blank, the Test UA uses the EdgeMarc ALG LAN IP address by default.
Codec Preference	Enter the preferred codec to use to decode and play voice packets when making or receiving a call.
Use Preferred codec only	Select the checkbox to specify that only the preferred codec is used when Test UA is placing and receiving a call.

Click **Submit** to save your settings.

Proceed to Verifying Connectivity with Test UA.

Verifying Connectivity with Test UA

Use Test UA to verify VoIP connectivity by placing a call to the EdgeMarc itself. Confirm that the call was successfully placed and received and monitor the quality of service (QOS) for the call in the System Logging Messages.



Tip
A telephone number must be assigned to the Test UA on the softswitch assigned to the EdgeMarc.

1. Choose **VoIP** > **Test UA** (Figure 6-66).
2. Complete the steps in the following sections:
   - Using the Test UA Settings Page



Tip
Use the telephone number assigned to the Test UA and the IP address for the softswitch on which the telephone number is registered.

3. Place a call to the telephone number. A successfully placed call to the EdgeMarc results in a series of beeps.
4. Verify test results on the system:
   a. Choose **Network** > **Network Information**.
   b. Scroll to **System Logging Messages**. This section provides a message for every logged call.

      A successfully placed call appears in the syslog:

```
Call ID [ID] [IP Start Address]->[IP End Address]: Call
complete.  Remaining active calls=0.  Minimum MOS=[MOS
Score] Average MOS=[MOS Score]
```

Configuring IP Phones, IADs, or Softphones

After configuring the EdgeMarc VoIP ALG, the voice devices must be configured to point to the LAN interface of the EdgeMarc as the signaling gateway and optionally as the TFTP server. The steps required to set up these devices differ from vendor to vendor. Using the DHCP server included in the EdgeMarc significantly simplifies device setup. Consult the user guide for your device for detailed instructions. For your convenience, configuration steps are provided for a number of these devices by logging into **Edgewater Networks** > **Support** at: www.edgewaternetworks.com

7

Configuring VPN Settings

The following sections describe how to configure IPsec virtual private networks (VPNs) on the EdgeMarc to protect data communication using the **VPN** tab in the Configuration Menu.

- Configuring VPNs
- Managing VPN Subnets
- Configuring the PPTP Server



Note
Not all EdgeMarc models support VPN.

Configuring VPNs

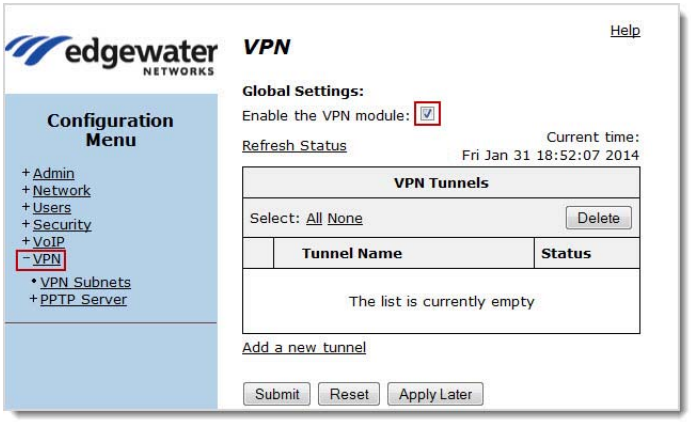
The VPN Configuration page allows you to create, configure, edit, and delete VPN tunnels:

- Using the VPN Configuration Page
- Adding a VPN Tunnel
- Modifying a VPN Tunnel
- Disabling a VPN Connection
- Deleting a VPN Tunnel

Using the VPN Configuration Page

1. Choose **VPN** from the Configuration Menu (Figure 7-1).

Figure 7-1 VPN Configuration Enable



2. To enable the VPN module globally, select the **Enable the VPN module** checkbox and click **Submit**.

   If the box is not checked, no tunnels are available, even if the tunnels themselves are enabled. You can still save settings on this page for future use. A disabled tunnel is counted towards the maximum number of allowed tunnels.

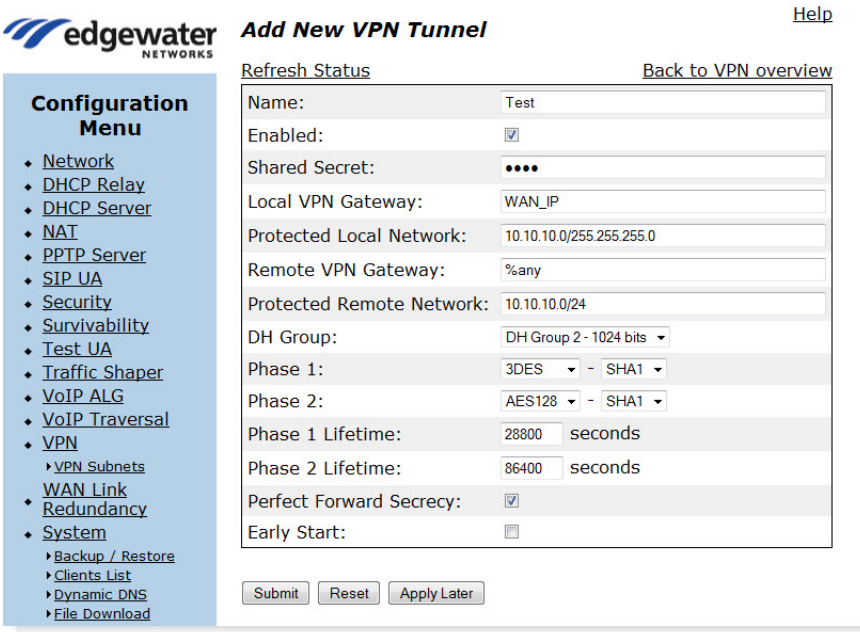
3. To refresh the status of all tunnels, click **Refresh Status**. If more information is available, an information icon is displayed to indicate the time the status event occurred, the IP address of the remote party, or detailed Help text, for example.

4. The VPN Tunnels table allows you to manage tunnels on the system:
   - Adding a VPN Tunnel
   - Modifying a VPN Tunnel
   - Disabling a VPN Connection
   - Deleting a VPN Tunnel

Adding a VPN Tunnel

1. Choose **VPN** from the Configuration Menu (Figure 7-1).
2. Click **Add a New Tunnel** to open the Add New VPN Tunnel configuration page (Figure 7-2).

Figure 7-2 Add a New VPN Tunnel Configuration Page



3. Configure settings using the information in Table 7-1 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 7-1 Add New VPN Tunnel Settings

Item	Description
Name	Enter the name of the VPN tunnel. The name must be unique per device, with a maximum length of 32 characters. The tunnel name must start with an alphabetical character and can consist of characters (A-Z, a-z), digits (0-9), hyphen (-), period (.), and underscore (_).
Enabled	Select the **Enabled** checkbox to use the tunnel on the system now or leave the box un-checked to save the tunnel configuration for later. A disabled tunnel is counted towards the maximum number of allowed tunnels. However, this allows you to save the tunnel configuration if the tunnel is needed at a later stage. A disabled tunnel is counted towards the maximum number of allowed tunnels.

Table 7-1 Add New VPN Tunnel Settings

Item	Description
Shared Secret	Enter the shared secret key for Phase 1 Internet Key Exchange (IKE) authentication. This key must not be longer than 32 characters. **Note:** If you allow your browser to remember the password for this page, it may automatically supply the saved shared secret when you submit the page even if you typed a new shared secret. To ensure that the correct shared secret is used, never allow the browser to remember the password on this page.
Local VPN Gateway	Enter the WAN IP address for the device in the **Local VPN Gateway** field. Or Enter the **WAN_IP** token. This allows the tunnel to use the correct WAN IP address even if features such as DHCP or PPP are used where the IP address may change dynamically.
Protected Local Network	Enter the address of the local subnet that is protected by this tunnel in network/mask or network/bits format. Example: 10.10.10.0/255.255.255.0 or 10.10.10.0/24. When VLANs are configured on the system, the appropriate VLAN network designation should be configured as the protected local network. Note that only traffic originating from that local VLAN will be allowed to traverse the VPN tunnel. All other traffic from Local VLANs are blocked from entering the tunnel, and will use the appropriate system routes (default or discrete network or host routes). Similarly, only traffic bound to that VLAN through the tunnel i routed to the destination IP address. All other traffic arriving from the remote protected network will not be routed.

Table 7-1 Add New VPN Tunnel Settings

Item	Description
Remote VPN Gateway	Enter the remote VPN gateway IP address. Use a static IP address, the DNS host name of the remote peer, or the token **%any**. If you use **%any**, any remote site is allowed to connect (given that it has the correct credentials and settings). **Note:** You cannot use Early Start if you specified **%any** in the Remote VPN Gateway field; you must specify an IP address in the Remote VPN Gateway field to use Early Start. Because the remote address is not known, the tunnel cannot be established until the remote gateway sets up the tunnel. In addition, all tunnels using **%any** share the same Shared Secret. If the Shared Secret is changed for one tunnel using the token **%any**, it will automatically be changed for all tunnels using the token **%any**. **Note:** A new VPN tunnel configuration requires that you select the Early Start checkbox in order to initialize the tunnel.
Protected Remote Network	Enter the IP address of the remote subnet protected by the tunnel, in network/mask or network/bits format. Example: 10.10.10.0/255.255.255.0. or 10.10.10.0/24. **Note:** The Remote Protected Network can be a supernet of the Local networks (LAN, VLAN, and subinterface networks), but it cannot be the same as, or a subnet of, the Local networks.
DH Group	Choose the Diffie-Hellman (DH) group to use for Phase 1 and Phase 2. Supported values: ■ DH Group 2 (1024-bit key) ■ DH Group 5” (1536-bit key) To manage DH settings, choose **Network** > **Firewall Traversal** and refer to Configuring Diffie-Hellman Parameters in Chapter 3, *Network Deployment*.
Phase 1	Choose the cipher and hash algorithms to use for Phase 1 (IKE) encryption. Supported settings: ■ 3DES or AES for cipher ■ MD5 or SHA1 for hash

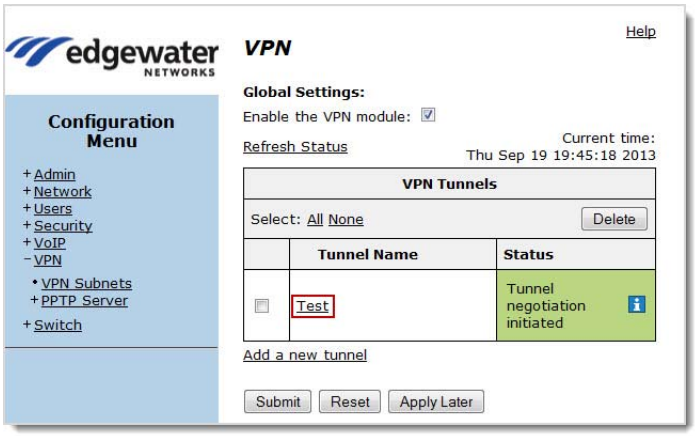
Table 7-1 Add New VPN Tunnel Settings

Item	Description
Phase 2	Choose the cipher and hash algorithms to use for Phase 2 Encapsulating Security Payload (ESP) encryption. Supported settings: ■ 3DES or AES for cipher ■ MD5 or SHA1 for hash
Phase 1 lifetime	Enter the time that the keying channel (ISAKMP SA) should last before being renegotiated. Valid range for the Phase 1 Lifetime is 600-28800 seconds.
Phase 2 lifetime	Enter the time that the connection (IPsec SA) should last before being renegotiated. Valid range for the Phase 2 Lifetime is 600-86400 seconds.
Perfect Forward Secrecy	Select the **Perfect Forward Secrecy** checkbox to ensure proper IKE negotiation. PFS is a cryptographic concept where each new key is unrelated to any previous key. In IPsec negotiations, Phase 2 keys are based on Phase 1 keys unless you specify Perfect Forward Secrecy. IKE, also called ISAKMP, is the negotiation protocol that lets two hosts agree on how to build an IPsec security association. To configure the adaptive security appliance for virtual private networks, you set global IKE parameters that apply system wide, and you also create IKE policies that the peers negotiate to establish a VPN connection. PFS must be enabled on both sides of the tunnel; if you enable one side, the other side must also have it enabled.
Early Start	Select the **Early Start** checkbox to initiate VPN gateway key negotiation when you click **Apply** or when the gateway reboots. If Early Start is not selected, the local gateway defers the key negotiation until the remote VPN gateway starts key negotiation or a packet from the protected local network attempts to pass through the tunnel. **Note:** You cannot use Early Start if you specified **%any** in the Remote VPN Gateway field; you must specify an IP address in the Remote VPN Gateway field to use Early Start. A new VPN tunnel configuration requires that you select the Early Start checkbox in order to initialize the tunnel.

Modifying a VPN Tunnel

1. Choose **VPN** from the Configuration Menu (Figure 7-1).
2. In the **VPN Tunnels** table, click the VPN tunnel that you want to modify (Figure 7-3).

Figure 7-3 Modify a VPN Tunnel

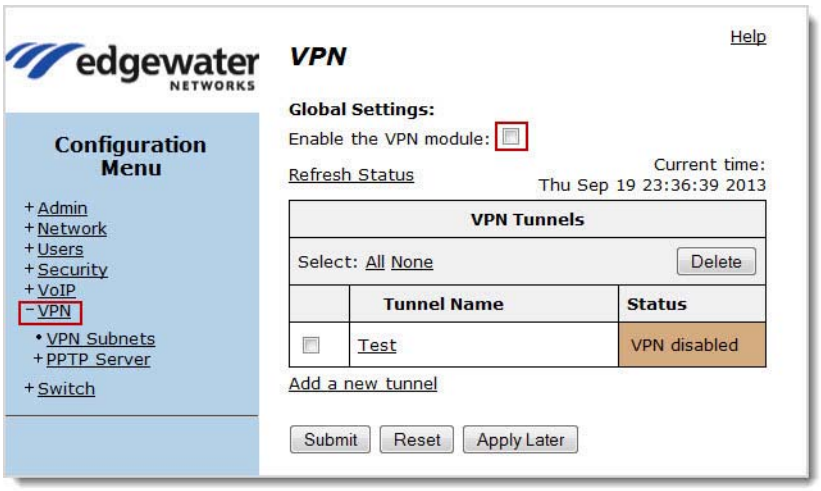


3. The VPN Tunnel Settings page opens to display the configuration of the selected tunnel (Figure 7-2).
4. Edit settings using the information in Table 7-1 as a guide.
5. Click **Submit** to save your settings.
6. Click **Back to VPN overview** to return to the VPN Configuration page.

Disabling a VPN Connection

1. Choose **VPN** from the Configuration Menu (Figure 7-1).
2. Un-check the **Enable the VPN module** checkbox and click **Submit**. VPN is disabled (Figure 7-4).

Figure 7-4 VPN Disabled



Deleting a VPN Tunnel

1. Choose **VPN** from the Configuration Menu (Figure 7-1).
2. In the **VPN Tunnel**s table, select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
3. Click **Delete**.
4. Click **OK** to confirm

Managing VPN Subnets

Additional VPN subnets can be added to route traffic through existing VPN tunnels.

Note
The VPN Subnets feature only works with EdgeMarc devices or other Linux-based / Open Swan VPN implementations. Interoperability with other vendor IPsec implementations has not been verified.

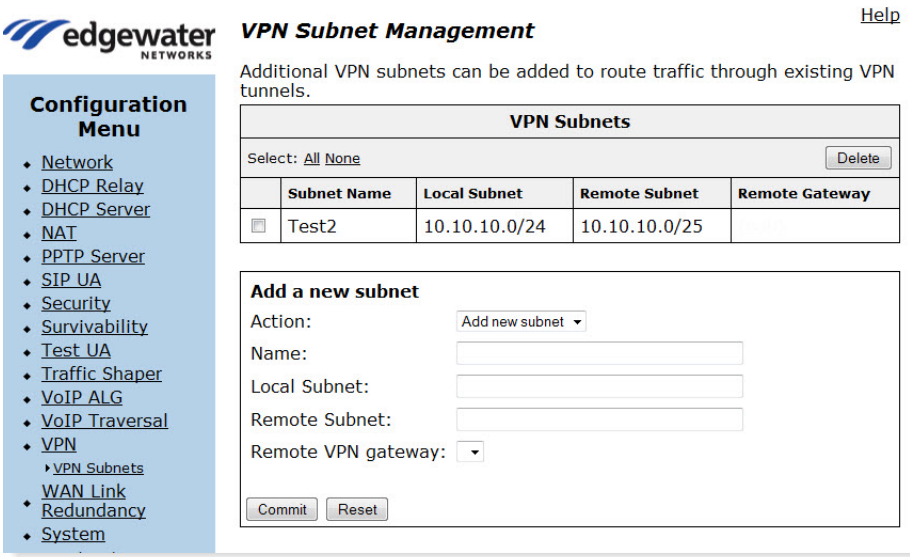
Proceed to the following sections:

- Adding or Editing a VPN Subnet
- Deleting a VPN Subnet

Adding or Editing a VPN Subnet

1. Choose **VPN** > **VPN Subnets** (Figure 7-5).

Figure 7-5 VPN Subnet Management Page



2. Configure settings using the information in Table 7-2 as a guide. When you have finished configuring settings, click **Commit** and click **Submit All** to make your changes take effect.

Table 7-2 VPN Subnet Management Parameters

Item	Description
VPN Subnets	
	Lists currently configured VPN subnets. You can select and delete subnets from this list by using the checkboxes and clicking **Delete**.
Add or Edit a Subnet	
Action	Choose an action from the **Action** drop-down list: ■ Add new subnet ■ Edit
Name	Enter a unique name for the subnet.
Local Subnet	Enter a new local subnet or edit an existing one. Use the network/mask or network/bits format. For example, 10.10.10.0/24 or 10.10.10.0/255.255.255.0.

Item	Description
Remote Subnet	Enter a new remote subnet or edit an existing one. Use the network/mask or network/bits format. For example, 10.10.10.0/24 or 10.10.10.0/255.255.255.0.
Remote VPN gateway	Enter a new remote VPN gateway or edit an existing one. The remote VPN gateway processes packets matching the given local and remote subnet.

Deleting a VPN Subnet

1. Choose **VPN** > **VPN Subnets** (Figure 7-5).
2. In the **VPN Subnets** table, select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
3. Click **Delete**.
4. Click **OK** to confirm.
5. Click **Submit All** to save all settings on the VPN Subnet Management page.

Configuring the PPTP Server

The PPTP Server page configures the Point-to-Point Tunneling Protocol (PPTP) on the EdgeMarc to enable secure data transfer from a remote client to a private enterprise server.

- Overview
- Enabling PPTP
- Configuring PPTP Usernames
- Displaying PPTP Active Users
- Displaying PPTP Log Messages

Overview

PPTP is a network protocol that enables secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks. PPTP encapsulates PPP packets into IP datagrams for transmission over the Internet or other public TCP/IP-based networks.

The PPTP Server allows remote users secure access to the LAN. Remote users are connected to the system's LAN via an encrypted VPN, allowing access to information and services on the local network.

Enabling PPTP

1. Choose **VPN** > **PPTP Server** (Figure 7-6).

Figure 7-6 PPTP Server Page



2. Configure settings using the information in Table 7-3 as a guide. When you have finished configuring settings, click **Submit** to make your changes take effect.

Table 7-3 PPTP Server Parameters

Item	Description
Enable PPTP Server	Select the **Enable PPTP Server** checkbox.
IP Range	Enter the available IP addresses that are assigned to the peer PPP interface for the incoming PPTP client session. IP range format is “10.0.0.2-100.”
WINS1 WINS2	(Optional) Enter a value in the **WINS1** and **WINS2** fields to allow network computer name resolution. Windows Internet Naming Service. Determines the IP address associated with a particular network computer. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. WINS uses a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one.
PPTP Authentication Mode	Choose a PPTP authentication mode from the **PPTP Authentication Mode** drop-down list: ■ MSCHAPV2+MPPE—Uses Microsoft Point to Point Encryption (MPPE) ■ MSCHAPV2—(MS-CHAP v2) stronger security for remote access connections ■ MSCHAP—(MS-CHAP v1) authenticates remote Windows workstations

Configuring PPTP Usernames

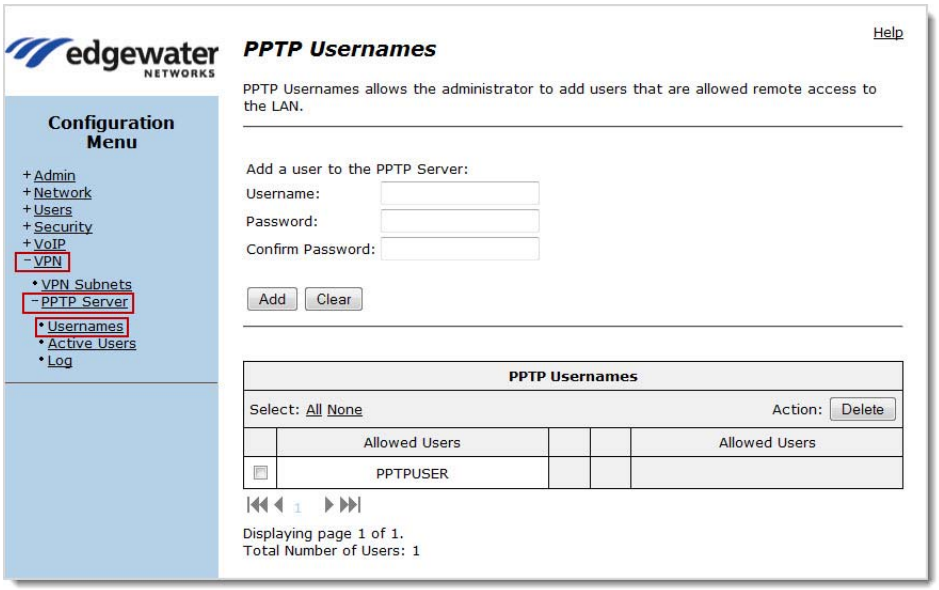
PPTP Usernames allows the administrator to manage users that are allowed remote access to the LAN.

- Adding a User to the PPTP Server
- Deleting PPTP Users

Adding a User to the PPTP Server

1. Choose **VPN** > **PPTP Server** > **Usernames** (Figure 7-7).

Figure 7-7 PPTP Usernames Configuration Page



2. In the **Username** field, enter a user name to add to the PPTP database. The maximum entry is 64 characters.
3. In the **Password** field, enter the user password. The maximum entry is 20 characters.
4. Verify your password entry in the **Confirm Password** field.
5. Click **Add**.

   A message indicates that service will be interrupted.
6. Click **OK** to confirm.

Deleting PPTP Users

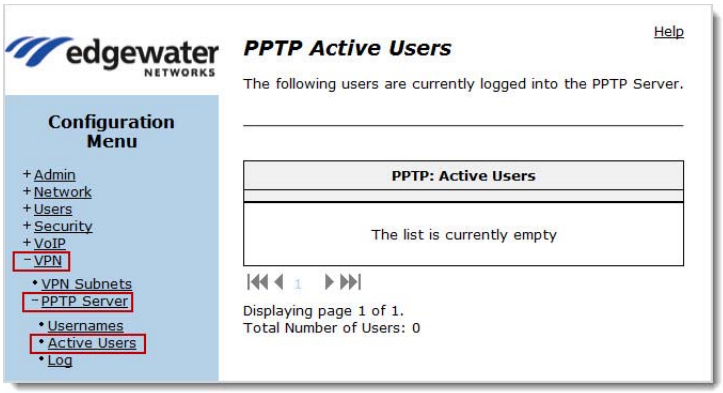
1. Choose **PPTP Server** > **Usernames** (Figure 7-7).
2. In the **PPTP Usernames** list, select checkboxes for the entries that you want to delete. Click **All** to choose all the entries or **None** to clear your selections.
3. Click **Delete**.
4. Click **OK** to confirm.
5. Navigate to additional pages using the arrows provided at the bottom of the PPTP Usernames page.

Displaying PPTP Active Users

The PPTP Active Users list shows users who are currently logged into the PPTP Server.

1. Choose **VPN** > **PPTP** > **Active Users** (Figure 7-8).

Figure 7-8 PPTP Active Users Page



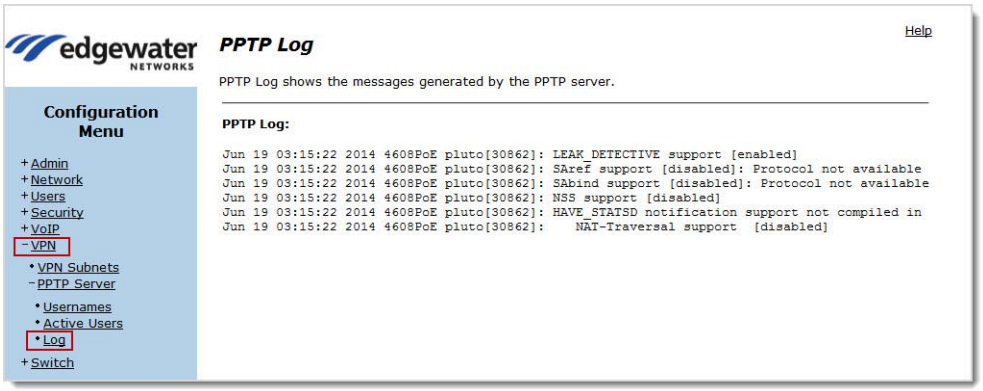
2. Navigate to additional pages using the arrows provided at the bottom of the PPTP Active Users page.

Displaying PPTP Log Messages

PPTP Log shows the messages generated by the PPTP server.

1. Choose **VPN** > **PPTP Server** > **Log** (Figure 7-9).

Figure 7-9 PPTP Log Page



8

Configuring Switch Settings

The following sections describe how to configure management IP LAN switch settings using the **Switch** tab in the Configuration Menu.



Tip
Switch settings are only available on the EdgeMarc 4600 PoE Series; the **Switch** tab does not appear in the Configuration Menu of other EdgeMarc models.

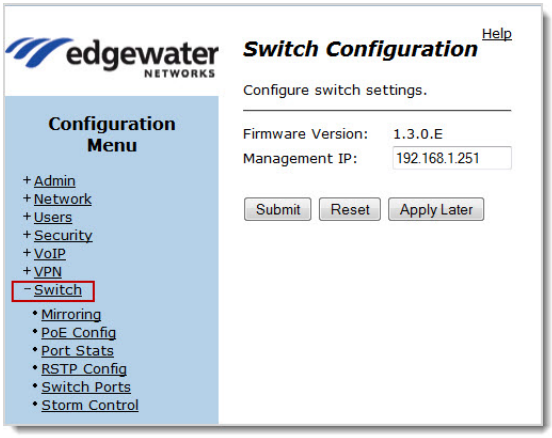
- Configuring the Management LAN IP
- Managing Mirror Monitoring
- Configuring PoE (Power over Ethernet)
- Managing Port Statistics
- Configuring RSTP
- Configuring Switch Ports
- Configuring Storm Control

Configuring the Management LAN IP

The switch requires a valid management IP address to enable certain switch features such as firmware upgrade. This IP must be in the subnet of the system LAN network. By default, the management IP is the LAN Network with the last octet being 251. For example, if the LAN Network is 192.168.1.0, the switch management IP would be 192.168.1.251.

1. Choose **Switch** from the Configuration Menu (Figure 8-1).

Figure 8-1 Switch Configuration Page



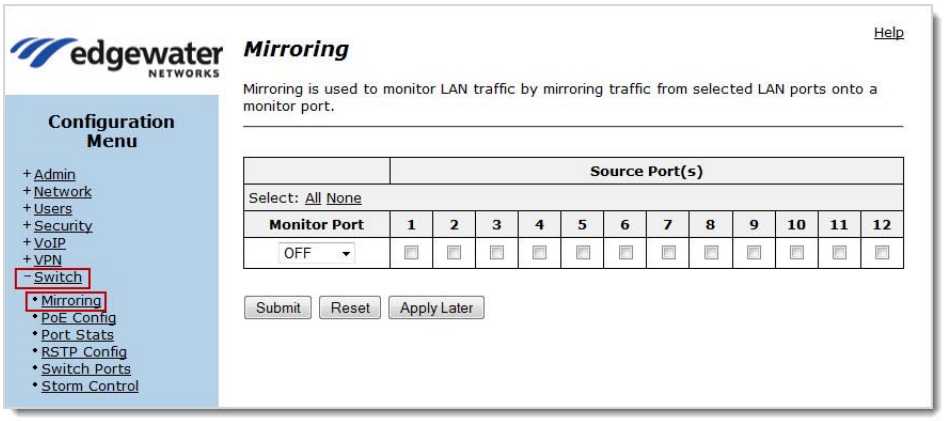
2. View the current firmware version.
3. In the **Management IP** field, view the current LAN IP address or enter a new IP address. For example, 192.168.1.251.
4. Click **Submit** to save your settings.

Managing Mirror Monitoring

Mirroring is used to monitor LAN traffic by mirroring traffic from selected LAN ports onto a monitor port.

1. Choose **Switch** > **Mirroring** (Figure 8-2).

Figure 8-2 Mirroring Configuration Page



2. Configure settings using the information in Table 8-1 as a guide.

Table 8-1 Switch Mirroring Settings

Item	Description
Source Port(s)	
Monitor Port	Selects a LAN port be the monitor port. All traffic from source ports are mirrored onto this port: ■ None—No ports are selected. ■ System—Monitors traffic on the system LAN port. ■ Port_1 through Port_24
Source Port	Selects the LAN ports to be mirrored onto the monitor port. All traffic from these ports are mirrored onto the monitor port: Port_1 through Port_24.

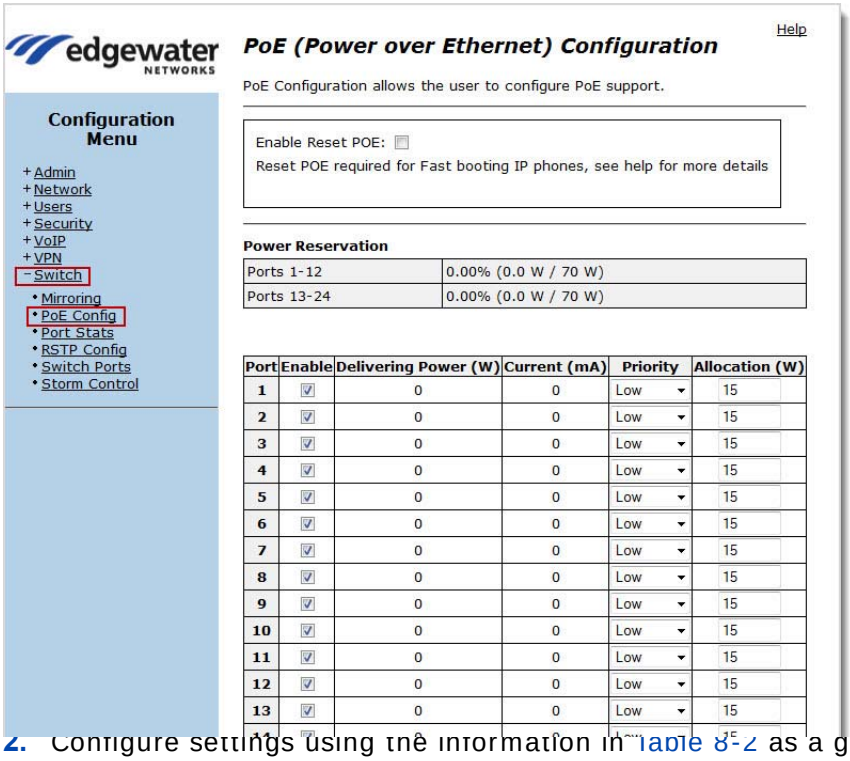
3. In the Source Port table, choose a setting from the **Monitor Port** drop-down list:
   - None—No ports are selected.
   - System—Monitors traffic on the system LAN port.
   - Port_1 through Port_24
4. In the Source Port table, select checkboxes for each source port for traffic that you want to mirror to the Monitor Port: Port_1 through Port_24. To select all ports, click **All** or click **None** to deselect all ports.
5. Click **Submit** to save your settings.

Configuring PoE (Power over Ethernet)

PoE is used to transmit power along with data over standard twisted-pair cable. This is useful for powering IP telephones, wireless LAN access points, and other devices that would be inconvenient to supply power separately. There are global and port settings that can be configured in this page along with port PoE status information.

1. Choose **Switch** > **PoE Config** (Figure 8-3).

Figure 8-3 PoE (Power over Ethernet) Configuration Page



2. Configure settings using the information in Table 8-2 as a guide.

Table 8-2 PoE Configuration Parameters

Item	Description
Power Management Mode	Configures the method for distributing power to the PoE ports. ■ Priority based mode—Distributes power based on priority from high to low. ■ Allocation based mode—Distributes power based on the allocated power configured per port.
Enable Reset POE	Allows you to reset PoE quickly before starting LLDP to give the system time to register before the IP phones boot.

Table 8-2 PoE Configuration Parameters (continued)

Item	Description
Power Reservation	
Sets the percentage of total power reserved.	
Ports 1-12	0.00% (0.0 W / 70 W)
Ports 13-24	0.00% (0.0 W / 70 W)
Port	Lists all ports on the system.
Enable	Enables or disables PoE on a port.
Delivering Power (W)	Displays the power currently being delivered to a port in watts.
Current (mA)	Displays the current being drawn from a port in milliamps.
Priority	Sets port power priority for each port: ■ High ■ Medium ■ Low
Allocation (W)	Sets the power allocation in watts for each port. The sum of power for all ports cannot exceed the system's total power.

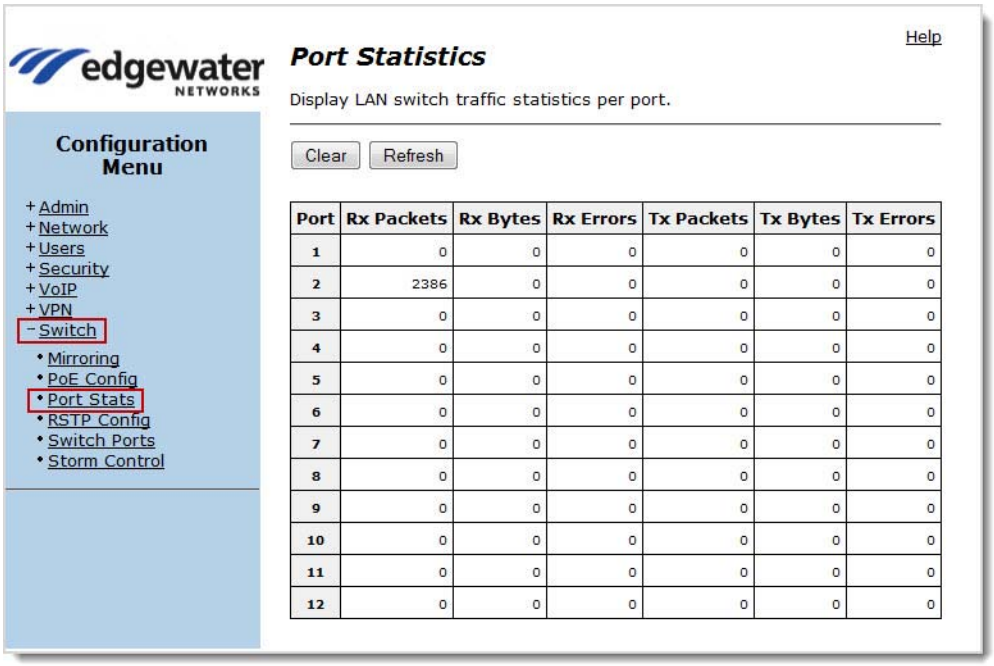
3. Select the **Enable Reset PoE** checkbox to allow the IP phones to register in sync with system network configuration.
4. Observe current power levels in the **Power Reservation** table.
5. Allocate power to individual ports:
   a. Select the checkbox for each port that you want to manage.
   b. Choose a power priority for the chosen port from the **Priority** drop-down list:
      - High
      - Medium
      - Low
   c. In the **Allocation (W)** field for the chosen port, enter the power allocation in watts.
6. Click **Submit** to save your settings.

Managing Port Statistics

The Port Statistics page displays LAN switch traffic statistics per port.

1. Choose **Switch** > **Port Stats** (Figure 8-4).

Figure 8-4 Port Statistics Page



2. View LAN switch port statistics such as receive and transmit packet count, number of bytes, and number of errors.
3. Click **Clear** to clear statistics counters for all ports.
4. Click **Refresh** to refresh the statistics counters for all ports.

Configuring RSTP

The RSTP Configuration page configures Rapid Spanning Tree Protocol (RSTP) settings.

- Overview
- Configuring RSTP Settings

Overview

The Spanning Tree Protocol ensures a loop-free topology for a bridged LAN. It allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails without the danger of bridge loops flooding the network or the need for manual enabling/disabling of these backup links.

RSTP significantly reduces the convergence time after a topology change occurs in the network. While STP can take 30 to 50 seconds to transit from a blocking state to a forwarding state, RSTP is typically able to respond less than 10 seconds of a physical link failure.

RSTP works by adding an alternative port and a backup port compared to STP. These ports are allowed to immediately enter the forwarding state rather than passively wait for the network to converge.

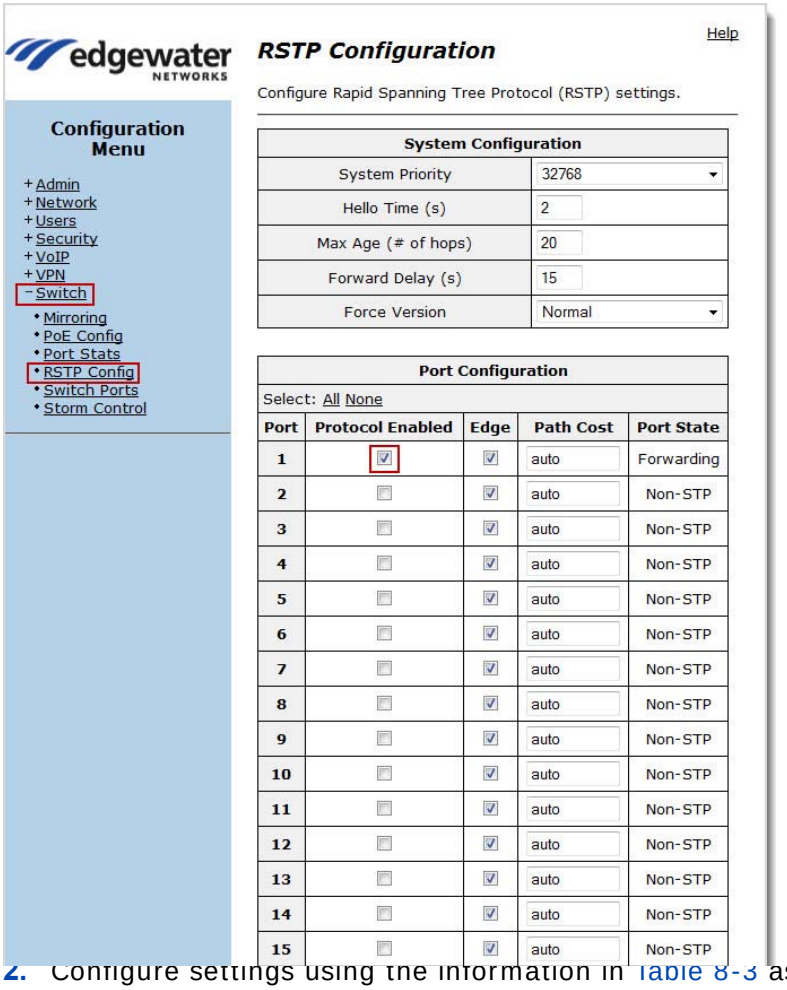
RSTP bridge port roles:

- Root port—A forwarding port that is the closest to the root bridge in terms of path cost
- Designated port—A forwarding port for every LAN segment
- Alternate port—A best alternate path to the root bridge. This path is different than using the root port. The alternative port moves to the forwarding state if there is a failure on the designated port for the segment.
- Backup port— A backup/redundant path to a segment where another bridge port already connects. The backup port applies only when a single switch has two links to the same segment (collision domain). To have two links to the same collision domain, the switch must be attached to a hub.
- Disabled port—Not strictly part of STP, a network administrator can manually disable a port.

Configuring RSTP Settings

1. Choose **Switch** > **RSTP Config** (Figure 8-5).

Figure 8-5 RSTP Configuration Page



2. Configure settings using the information in Table 8-3 as a guide.

Table 8-3 RSTP Configuration Parameters

Item	Description
System Configuration	
System Priority	Designates a priority number between 0 and 61440 in increments of 4096 (default is 32768). The lower the system priority the more likely the switch is to become root in Spanning tree.
Hello Time (s)	Specifies the number of seconds between periodic configuration Bridge Protocol Data Units (BPDUs). Default is two seconds.

Table 8-3 RSTP Configuration Parameters (continued)

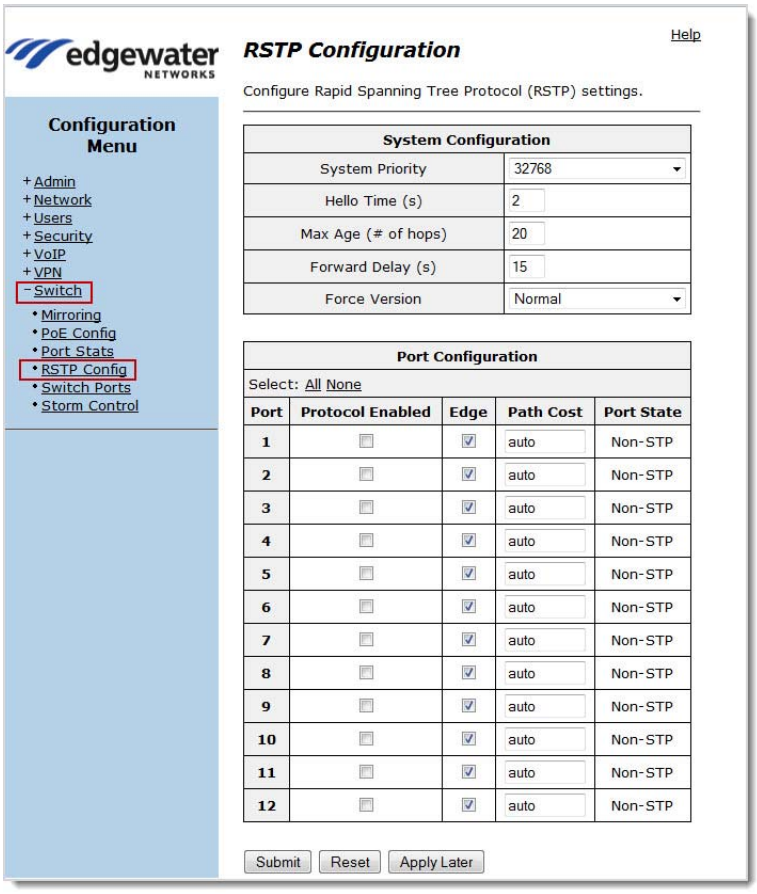
Item	Description
Max Age (# of hops)	Sets the maximum time that a BPDU is saved Default is 20.
Forward Delay (s)	Sets the time spent in the Listening and Learning states. Default is 15 seconds.
Force Version	Selects the RSTP protocol version to use: ■ Normal—Use RSTP (default) ■ Compatible—Compatible with old STP
Port Configuration	
Protocol Enabled	Enables or disables RSTP for this port. Default is disabled.
Edge	Configures the port as an edge port if a port has no other bridge attached to it. The checkbox is selected by default.
Path Cost	Sets the path cost of the link connected to this port leading to the root bridge. This is dependent on the speed of the link. Designated ports are selected based on the lowest path cost to the root bridge for a segment. Default is auto.
Port State	Displays the current state of the port: ■ Blocking—A port that would cause a switching loop. No user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determined the port may transition to the forwarding state. BPDU data is still received in blocking state. ■ Listening—The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state. ■ Learning—While the port does not yet forward frames (packets) it does learn source addresses from frames received and adds them to the filtering database (switching database). ■ Forwarding—A port receiving and sending data in normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop. ■ Disabled—Not strictly part of STP, the administrator can manually disable the port. ■ Non-STP—RSTP is not enabled on this port.

3. Configure settings in Managing RSTP System Configuration.

Managing RSTP System Configuration

1. Choose **Switch** > **RSTP Config** (Figure 8-5).
2. In System Configuration (Figure 8-6), choose a priority number between 0 and 61440 from the **System Priority** drop-down list. The lower the system priority the more likely the switch is to become root in Spanning tree.

Figure 8-6 RSTP System Configuration



3. In the **Hello Time** field, enter the number of seconds between periodic configuration BPDUs. Default is two seconds.
4. In the **Max Age (# of hops)** field, enter the maximum amount of time that a BPDU is saved. Default is 20.
5. In the **Forward Delay** field, enter the time spent in the Listening and Learning states. Default is 15 seconds.
6. Choose a RSTP protocol version type from the Force Version drop-down list:
   - Normal—Use RSTP (default)

- Compatible—Compatible with old STP

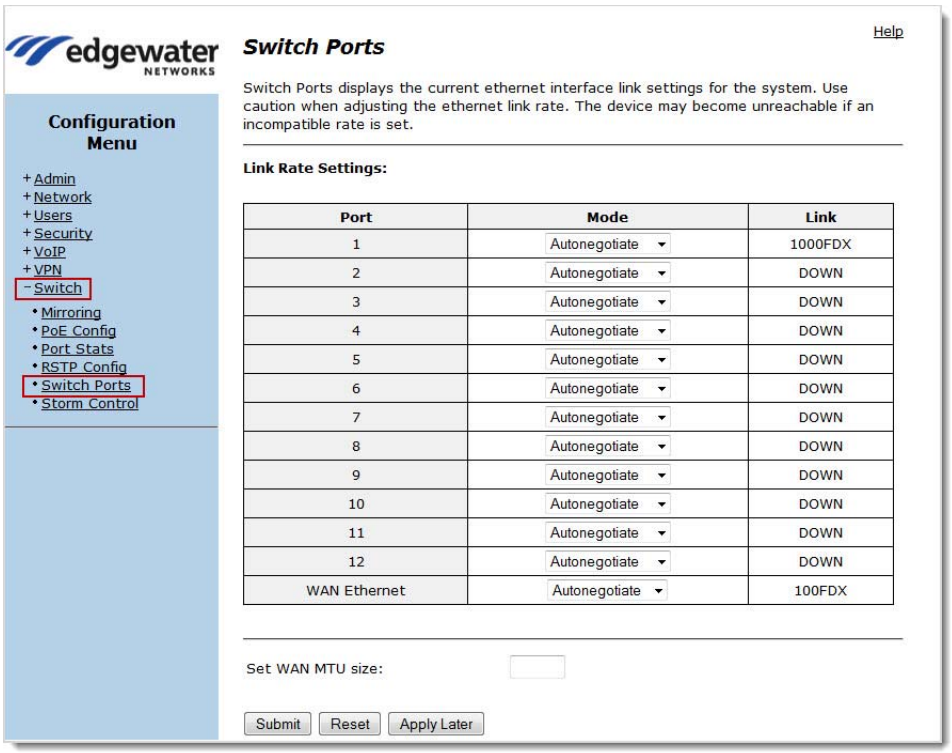
7. Scroll to **Port Configuration**.
8. Select a port to manage. To select all ports, click **All** or click **None** to deselect all ports
9. Select the **Protocol Enabled** checkbox to enable RSTP for this port.
10. Select the **Edge** checkbox if a port has no other bridge attached to it. The box is checked by default.
11. In the **Path Cost** field, enter the path cost of the link connected to this port leading to the Root Bridge. Default is auto.
12. View the current state of a port in the Port State field:
    - Blocking
    - Listening
    - Learning
    - Forwarding
    - Disabled
    - Non-STP
13. Click **Submit** to save all settings on the page.

Configuring Switch Ports

Switch Ports displays the current Ethernet interface link settings for the system. If needed, the rate for each interface can be set manually to establish a reliable connection. The MTU size of the WAN interface can be adjusted to reduce the effects of large data packet on media data.

1. Choose **Switch** > **Switch Ports** (Figure 8-7).

Figure 8-7 Switch Ports Configuration Page



2. Configure settings using the information in Table 8-4 as a guide.

Table 8-4 Switch Ports Configuration Parameters

Item	Description
Link Rate Settings	
Displays the current Port and Mode settings for the LAN and WAN interfaces.	
Port	Lists ports on the system and WAN Ethernet information.

Table 8-4 Switch Ports Configuration Parameters (continued)

Item	Description
Mode	Sets the link rate of an interface: ■ Autonegotiate (default) ■ 10Base T-HD ■ 10Base T-FD ■ 100Base T-HD ■ 100Base T-FD ■ 1000Base T-FD The default setting is autonegotiate. When connecting a device to the system that cannot be hard coded, leave these ports set to autonegotiate. **Note:** The link rate of an interface can be set to static values, and it is recommended to statically set the values on both the system and devices connecting to any port when applicable. Inconsistent rates may cause “flutter,” leading to intermittent voice outages.
Link Lists detailed Link Rate Information. If the negotiated rates change intermittently or the link is reported as no link or down, the link rate may need to be set manually. Both sides of the link must be set to the same rate. Inconsistent rates may cause “flutter,” leading to intermittent voice outages. **Note:** When the link rate is set manually, ensure that the device at the far end of the connection can communicate at the desired rate. Incompatible rates can cause a loss of communication with the system.	
Set WAN MTU Size Sets the WAN MTU size on some EdgeMarc platforms to reduce the latency that is introduced when large data packets are sent over a slow link. The default setting is 1500 bytes for static IP addresses. PPPoE links negotiate the value automatically although the value can be overridden using this field. If the WAN Upstream Bandwidth is less than 256 Kbps, the MTU size is automatically reduced to 800 bytes. The WAN interface must have an IPv4 address assigned. **Note:** When the link rate is set manually, ensure that the device at the far end of the connection can communicate at the desired rate. Incompatible rates can cause a loss of communication with the system.	

3. In the **Mode** column, choose from the following rates for each Ethernet link, or choose **Autonegotiate**:
   - 10Base T-HD
   - 10Base T-FD
   - 100Base T-HD

- 100Base T-FD
- 1000Base T-FD

4. In the Set WAN MTU size field, adjust the WAN MTU size to reduce latency when large data packets are sent over a slow link. Default is 1500 bytes for static IP addresses.
5. Click **Submit**.

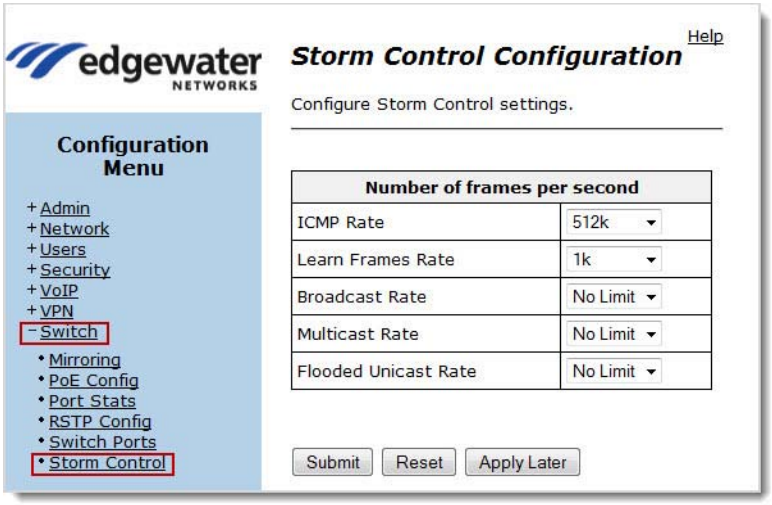
Configuring Storm Control

A traffic storm occurs when packets flood the LAN creating excessive traffic, degrading network performance. The storm control feature can limit the rate of flooding and forwarding of various types of traffic:

- ICMP Frames
- MAC Address Learn Frames
- Broadcast Forwarding
- Multicast Flooding
- Unicast Flooding

1. Choose **Switch** > **Storm Control** (Figure 8-8).

Figure 8-8 Storm Control Configuration Page



2. Configure settings using the information in Table 8-5 as a guide.

Table 8-5 Storm Control Configuration Parameters

Item	Description
Number of Frames Per Second	Sets the FPS for the selected traffic type. The configurable frame rates are exponential and range from 0 to 32 megaframes per second. Possible configurations are, for example, 1, 2, 4, or 8 kiloframes per second, and so on. **Note:** The storm controller is centralized, so the configured rate specifies the maximum total number of frames per second for the entire switch (and not per port).
ICMP Rate	Sets the Internet Control Message Protocol (ICMP) frame rate: ■ 1K to 512K ■ No Limit
Learn Frames Rate	Sets the MAC address learn frame rate. Switches learn MAC addresses only from the source MAC addresses of incoming frames: ■ 1K to 512K ■ No Limit
Broadcast Rate	Sets the broadcast forwarding frame rate. Broadcast packets are duplicated and copies sent on multiple links to devices within a broadcast domain. ■ 1K to 512K ■ No Limit
Multicast Rate	Multicast traffic is flooded to a switch port because a MAC address has timed out or has not been learned by the switch. ■ 1K to 512K ■ No Limit
Flooded Unicast Rate	Unicast traffic is flooded to a switch port because a MAC address has timed out or has not been learned by the switch. ■ 1K to 512K ■ No Limit

3. Choose a frame rate for the following traffic types:
   - ICMP Frames
   - MAC Address Learn Frames
   - Broadcast Forwarding
   - Multicast Flooding
   - Unicast Flooding
4. Click **Submit**.

9

Troubleshooting Tips

Use the information in this chapter to troubleshoot your system and provide information requested by technical support.

- Contacting Edgewater Networks Support
- Locating Information About Your EdgeMarc
- EdgeMarc System Call Messages

Contacting Edgewater Networks Support

When you call EWN support, make sure you have the following information ready:

- EdgeMarc MAC address
- Description of the issue, for example:
  - Hosted PBX issue
  - SIP trunking issue
- EdgeMarc IP address, public and private
- EdgeMarc firmware release
- System log information from the following sources as necessary:
  - sys_report output (from CLI)
  - tcpdump (if needed)
  - mandcall log (if an active call is involved)

How to Contact Edgewater Support

Enter a support ticket at the following link:

www.edgewaternetworks.com/support

Send an email:

support@edgewaternetworks.com

By phone:

(408) 351-7255

Locating Information About Your EdgeMarc

Table 9-1 describes how to find information about your system from the EdgeMarc Configuration Menu.

Table 9-1 Troubleshooting Tips

Troubleshoot	Where to Go
License key information ALG registration	Choose **Admin** from the Configuration Menu, scroll to **Registration Status** and click **View License Key**. **Note:** The ALG registration code is available on a sticker on the bottom of the device or from your service provider. See Managing the License Key in Chapter 2, *System Administration*.
Backup or restore a configuration	Choose **Admin** > **Backup / Restore**. See Configuring Backup and Restore in Chapter 2, *System Administration*.
Call logs and system logging messages	Choose **Admin** > **System Information**. See Viewing System Information in Chapter 2, *System Administration*.
Download new firmware	VOS firmware is available on the Edgewater Networks FTP site: ftp.edgewaternetworks.com Contact Edgewater TAC/support to obtain the name of the file to look for on the FTP site: support@edgewaternetworks.com Choose **Admin** > **Upgrade Firmware** or **Admin** > **Upgrade SOC2** and refer to the following sections in Chapter 2, *System Administration*: ■ Upgrading Firmware ■ Upgrading SOC2 Firmware
Software version Hardware platform LAN MAC address	Common system configuration information. Choose **Admin** from the Configuration Menu and refer to Chapter 2, *System Administration*.
Change administrative passwords	Choose **Admin** from the Configuration Menu and scroll to **Change Administrative Password**. See Changing the Administrative Password in Chapter 2, *System Administration*.
Network configuration and EdgeMarc status	Choose **Network** > **Network Information**. See Viewing Network Information in Chapter 3, *Network Deployment*.

Table 9-1 Troubleshooting Tips (continued)

Troubleshoot	Where to Go
Ping and traceroute tests	A ping test is the most common test used to verify basic connectivity to a networking device. Choose **Network** > **Network Test Tools**. See Using Network Test Tools in Chapter 3, *Network Deployment*.
Restart or reboot the device	Choose **Network** > **Network Restart**. Choose **Network** > **Reboot System**. As an alternative to rebooting, you can perform a reset locally by temporarily disconnecting the power cable from the EdgeMarc then plugging it back in. See Initiating Network Restart in Chapter 3, *Network Deployment*.
Verify and update registered voice devices	Choose **VoIP** > **Clients List**. Update the clients list by deleting any duplicate or stale entries. See Configuring the Clients List in Chapter 6, *Configuring VoIP Settings*.

EdgeMarc System Call Messages

Refer to Chapter 6, *Configuring VoIP Settings* for messages that may appear on your system during a call:

- H.323 Call Status Messages
- H.323 Call Termination Messages

License and Warranty Information

License information related to the operation of EdgeMarc™ hardware and software is located on the EdgeMarc Software License Information page:

http://edgewaternetworks.com/support/licenses/

EdgeMarc Warranty

Hardware Warranty

For a period of one (1) year after shipment of the Product, Edgewater Network warrants that such Hardware will substantially conform to Edgewater Networks' published specifications for such Hardware on the date of order if properly used in accordance with procedures described in the documentation supplied by Edgewater Networks. End-user shall notify Edgewater of any nonconformance during the warranty period, obtain a return authorization for the nonconforming Hardware from Edgewater, and return the nonconforming Hardware to Edgewater's designated repair facility, freight prepaid, with a statement describing the nonconformity. Edgewater Networks' exclusive obligations with respect to nonconforming Hardware shall be, at Edgewater Networks' option, repair such Hardware, replace such Hardware, or to refund to End-user the purchase price paid for the Product if it is determined to be defective.

See more at:
http://edgewaternetworks.com/warranties-hardware-and-software/

Software Warranty

Edgewater Networks warrants that the Software on the Product will substantially conform with Edgewater Networks published specifications for such Software on the date of the order for such Product for a period of one (1) year after the shipment of the Product, if properly used in accordance with the procedures described in the documentation supplied by Edgewater Networks. Edgewater Networks exclusive obligation with respect to nonconforming Software shall be, at Edgewater Networks option, to: (a) replace that copy of the Software with one that conforms to the specifications; (b) use diligent efforts to provide a correction of the defect, or (c) refund the purchase price paid for the Edgewater Networks Product on which the Software is installed. Defects in the Software must be reported during the warranty period and be reported to Edgewater Networks in a form and with supporting information reasonably requested by Edgewater Networks to enable it to verify, diagnose and correct the defect.

© 2014 Edgewater Networks. All Rights Reserved.

© 2013 Edgewater Networks. All Rights Reserved.

What's New

This section describes new features in the VOS GUI per release.

- New GUI Features in the VOS 14.7 Releases
- New GUI Features in the VOS 14.6 Releases

New GUI Features in the VOS 14.7 Releases

Table 11-1 features are new in the EdgeMarc configuration GUI in VOS Release 14.7.

Table 11-1 New Features in the VOS 14.7 Releases

Feature	Description	Action
ALG Multi-VLAN Support	Support is added for ALG supporting Multiple VLANs with certificate for VLANs. The **VoIP** > **ALG** configuration page displays EdgeMarc configured VLANs with checkboxes to select which ones the ALG will process.	• Choose **VoIP** from the Configuration Menu. • Select the **Enable ALG Multi-VLAN support** checkbox. See Chapter 6, *Configuring VoIP Settings*.
Editing VLANs in the EdgeMarc GUI	Existing VLANs can be edited and deleted from the **Network** > **VLAN** page via the Action drop-down menu.	• Choose **Network** > **VLAN**. • Select **Edit VLAN *x*** from the Create a new VLAN **Action** drop-down menu. • Edit information for the selected VLAN in the **Edit an existing VLAN** fields and click **Edit** to save your changes. See Chapter 3, *Network Deployment*.
EdgeView Groups Support	An **EV Group Name** field is added to the **Admin** > **Services** configuration page. This setting allows users to input the EdgeView Service Control Center (EdgeView SCC) group name within which the EdgeMarc will reside.	• Choose **Admin** > **Services**. • Scroll to the **EV Group Name** field. • Enter an EdgeView group name and click Submit. See Configuring Services in Chapter 2, *System Administration*.

Table 11-1 New Features in the VOS 14.7 Releases (continued)

Feature	Description	Action
Limit the Number of SSH Attempts	The Intrusion Prevention page allows a user to set a number of unsuccessful login attempts a remote host may have during a period of time before that remote host is locked out from being able to attempt to login.	• Choose **Security** > **Intrusion Prevention** from the Configuration Menu • Select the **Enable Intrusion Prevention** checkbox and click **Submit**. Additional fields become active • Enter a value in the **Failed Login Attempts (2-10)** field. • Enter a value in the **Host** Lockout Duration (1-480 mins) field. See Limiting the Number of SSH Attempts in Chapter 5, *Configuring System Security*.

New GUI Features in the VOS 14.6 Releases

Table 11-2 features are new in the EdgeMarc configuration GUI in VOS Release 14.6.

Table 11-2 New Features in the VOS 14.6 Releases

Feature	Description	Action
Disabling Flash Hook on SIPUA FXS Ports	Flash Hook functionality can now be disabled when configuring VLAN options.	• Choose **VoIP** > **SIP** > **SIP UA** > **Advanced**. • Scroll to **Port Level Advanced Configuration**. • Select the **Disable Flash Hook** checkbox and click **Submit**. See Configuring SIP Settings in Chapter 6, *Configuring VoIP Settings*.

Table 11-2 New Features in the VOS 14.6 Releases (continued)

Feature	Description	Action
SIP Analytics Collection	The system can now gather SIP, memory and CPU statistics on some EdgeMarc devices. Analytics is enabled by default.	• Choose **Admin** > **Services Configuration**. • Scroll to the bottom of the Services Configuration page and enter a value in the **Set Analytics Timeout** field. • Click **Submit**. See Configuring Services in Chapter 2, *System Administration*.
WAN Link Redundancy Enhancement	The WLR - Advanced page now supports three ping hosts, because a single host may fail even though the EdgeMarc still has full network access. The addition of multiple hosts avoids possible false positives if a ping host fails.	• Choose **Network** > **WAN Failover** > **Advanced**. • Scroll to **Ping Detection Settings**. • Enter DNS names or IP addresses into the additional Primary and Secondary ping host fields. See Configuring WAN Failover in Chapter 3, *Network Deployment*.

Edgewater Networks, Inc.
5225 Hellyer Ave. #100
San Jose, California 95138

Phone: 408.351.7200
Fax: 408.727.6430

edgewaternetworks.com



Glossary

A

802.1x Supplicant

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802 which is known as “EAP over LAN” or EAPOL, optional point to point encryption over the local LAN segment.

The supplicant is an entity at one end of a point-to-point LAN segment that seeks to be authenticated by an authenticator attached to the other end of that link. As used in the IEEE 802.1X standard, a supplicant can be either hardware or software. In practice, a supplicant is a software application installed on an end-user's computer. The user invokes the supplicant and submits credentials to connect the computer to a secure network. If the authentication is successful, the authenticator typically allows the computer to connect to the network.

An 802.1X authenticator is an entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link. In practice, the authenticator is usually a network switch or wireless access point that serves as the point of connection for computers joining the network. The authenticator receives connection requests from a supplicant on the connecting computer.

ACS

Auto Configuration Servers. Developed as part of the TR-069 protocol to automatically configure Internet access devices such as modems, routers, gateways, set-top boxes, and VoIP-phones for end-users. See TR-069.

B

Blacklist

Specifies a block of IP addresses that will be denied access to EdgeMarc. Blacklists allow you to block persistent hacking attempts by specifying a list of IP addresses that will be completely blocked from accessing EdgeMarc. Any input to EdgeMarc from these IP addresses is dropped.

If you have an EdgeMarc outside the firewall, the IP address of the EdgeMarc specified here must be managed inside the firewall. See also Whitelist.

C

CAC Call Admission Control. Prevents oversubscription of VoIP networks. It is used in the call set-up phase and applies to real-time media traffic as opposed to data traffic. CAC mechanisms complement and are distinct from the capabilities of Quality of Service tools to protect voice traffic from the negative effects of other voice traffic and to keep excess voice traffic off the network.

cipher SSL encryption algorithm that creates a special certificate, which is used as a key between two computers on the Internet. This certificate creates a secret encrypted connection between the two networked computers, which blocks unwanted snooping of shared data.

Conduit EdgeMarc uses conduits to communicate with the upstream softswitch for Plug and Dial. Using the conduit, EdgeMarc will inform the softswitch of a new phone and associate that phone with the requested user's profile. The EdgeMarc database includes an internal conduit. Additionally, EdgeMarc supports selected Broadsoft and Metaswitch conduits.

CSV Comma Separated Values. CSV is an exportable file that can be opened with XLS in a table format.

D

default gateway A router on a computer network that serves as an access point to another network.

Device EdgeMarc devices, IP phones, third-party nodes, SNMP-based nodes, EdgeConnects and (if licensed) Plug and Dial phones and Plug and Dial conduits.

Device Tree Shows hierarchical, collapsible lists of EdgeMarc devices, EdgeMarc Groups, EdgeConnects, Phones, Configuration Files and other nodes/devices managed by EdgeMarc. The entries in the device tree are associated with icons and are color-coded for quick identification of node/device type and service-affecting problems. You can use the controls at the top level of the Device Tree to expand and collapse the folders in the hierarchy, and also to search for EdgeMarc Groups and nodes/devices managed by EdgeMarc.

Device Tree Device Level The Device Level in the EdgeMarc device tree shows the individual nodes/devices being managed by EdgeMarc. Nodes/devices include EdgeMarc devices, phones, third-party nodes, SNMP-based nodes and EdgeConnects. If licensed, a node/device may also be Plug and Dial phones and Plug and Dial conduits.

Device Tree Group Level	The Group Level in the device tree lists all the nodes/devices in a selected EdgeMarc Group. There may also be sub groups shown at the Device Tree Group Level.
Device Tree Top Level	The Top Level in the Device Tree lists all EdgeMarc Groups and nodes/devices being managed by EdgeMarc. You can use the controls at the top level of the Device Tree to expand and collapse the folders in the hierarchy, and also to search for EdgeMarc Groups and nodes/devices managed by EdgeMarc.
DHCP	Dynamic Host Configuration Protocol is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual intervention.
DID and Short DID	Direct Inward Dial number usually called the “phone number”. Short DID is usually 3-5 digits for PBX-style dialing.
DN	Directory number.
DNS	Domain Name System. System used on the Internet for translating names of network nodes into addresses.
DSCP	Differentiated Services Code Point. Uses 6 bits of the TOS field in an IP packet header.

E

EAP	Extensible Authentication Protocol (EAP) authentication protocol. See FAST and PEAP.
EdgeMarc Configuration Template	An XML file that describes all the configuration files for a given EdgeMarc or group of EdgeMarc devices. An EdgeMarc template specifies the file names, variable names, types, constraints, and descriptions that can (but not necessarily must) be set for an EdgeMarc. The information and settings will vary depending on the EdgeMarc implementation.
EdgeMarc Configuration Template Manager	An application in EdgeMarc which provides a simple way to create, modify, and manage EdgeMarc templates. Using the Template Manager, you can generate, edit, copy, rename, delete, import and export template files. Once you've made your modifications, the template can be saved and used by the end user to push configuration values to the EdgeMarc.
EM	EdgeMarc

EdgeMarc Configuration Template Editor	The EdgeMarc Configuration template Editor (Editor) is accessible from the EdgeMarc Configuration Template Manager. Once you have generated an EdgeMarc configuration template, you use the Editor to modify configuration settings in the template.
EdgeMarc Group	A collection of EdgeMarc devices, IP phones, third-party nodes, SNMP-based nodes, EdgeConnects and (if licensed) Plug and Dial phones and Plug and Dial conduits that have been grouped together in EdgeMarc to make them easier to manage. By grouping nodes/devices, you can apply a single action to all nodes/devices in the EdgeMarc Group at once which saves you from having to configure each node/device individually. EdgeMarc Groups can also contain other EdgeMarc sub Groups. EdgeMarc Groups in the device tree are shown in blue.
EdgeMarc Product License	The EdgeMarc product license specifies the number of EdgeMarc devices (and similar nodes/devices), Tenants, endpoints and conduits that can be managed by your EdgeMarc. The EdgeMarc product license does not expire. You purchase an EdgeMarc product license based upon the number of nodes you need. You can add additional nodes; however if you do so, you will need to update the product license key in EdgeMarc.
EdgeMarc Support License	The EdgeMarc support license is set by the Edgewater Networks sales or support team at the time your product is shipped. It has a fixed expiration date. The support license key allows for upgrades and patches until the expiration date. When your EdgeMarc support license expires, EdgeMarc is still operational but you can no longer do patch upgrades or install new software on the EdgeMarc. A red alert displays at the top of the EdgeMarc License screen in the EdgeMarc GUI when the support license is about to expire.
Endpoint	An endpoint typically refers to a phone but it can be any device managed by EdgeMarc.

F

FAST

EAP-FAST (Flexible Authentication via Secure Tunneling) is a protocol proposal by Cisco Systems as a replacement for LEAP. The protocol was designed to address the weaknesses of LEAP while preserving the "lightweight" implementation. Use of server certificates is optional in EAP-FAST. EAP-FAST uses a Protected Access Credential (PAC) to establish a TLS tunnel in which client credentials are verified.

EAP-FAST has three phases, two of which are supported on the EdgeMarc:

Phase 1—Tunnel establishment. Authenticates using the PAC and establishes a tunnel key to provide confidentiality and integrity during the authentication process.

Phase 2—Authentication. Authenticates the peer with multiple tunneled, secure authentication mechanisms (credentials exchanged).

Feature Server

The upstream switch at the customer premises to which EdgeMarc communicates to get information about the phones. Also referred to as a "softswitch."

G

Generic Phone Configuration File

All phone manufacturers have a common or *generic* phone configuration file for each phone model. EdgeMarc Plug and Dial includes these files for each supported phone model. In a typical IP phone deployment (without Plug and Dial) system administrators must modify the generic phone configuration files with customer-specific network and phone settings. EdgeMarc Plug and Dial simplifies this process by automatically creating phone-specific configuration files based on input retrieved by the IVR when the user self-provisions their phone.

Generic Phone Template

A template file which is created from the phone manufacturer's generic phone configuration file. Generic phone templates are referred to as "Plug and Dial Templates" in EdgeMarc.

Group

An EdgeMarc Group. A collection of EdgeMarc devices, IP phones, third-party nodes, SNMP-based nodes, EdgeConnects and (if licensed) Plug and Dial phones and Plug and Dial conduits that have been grouped together in EdgeMarc to make them easier to manage. By grouping nodes/devices, you can apply a single action to all nodes/devices in the EdgeMarc Group at once which saves you from having to configure each node/device individually. EdgeMarc Groups can also contain other EdgeMarc Groups. EdgeMarc Groups in the device tree are shown in blue.

GUI

Graphical User Interface

H

HA High Availability. High Availability (HA) is designed to eliminate a single point of failure in a network configuration. High Availability uses the concept of a Primary and Secondary system with a heartbeat to define which system is active and which one is Idle and an automated data replication. If the Active system is failing, then the Idle system becomes active automatically.

I

IMIX Internet Mix or IMIX refers to typical Internet traffic passing some network equipment such as routers, switches or firewalls. When measuring equipment performance using an IMIX of packets, the performance is assumed to resemble what can be seen in “real world” conditions.

IP Address A device identifier on a TCP/IP network.

IP Address File List One of the three types of EdgeMarc configuration files. Contains only a list of IP addresses separated by new lines. Other EdgeMarc configuration file types are a Raw File and Variable/Value file.

IVR Interactive voice response (IVR) is a technology that allows users to interact with a company’s host system via a telephone keypad or by speech recognition, after which they can service their own inquiries by following the IVR dialogue. IVR systems can respond with prerecorded or dynamically generated audio to further direct users on how to proceed. IVR applications can be used to control almost any function where the interface can be broken down into a series of simple interactions. IVR systems deployed in the network are sized to handle large call volumes.

J

Jitter The variation in packet transit delay caused by queuing, contention, and serialization effects on the path through the network. In general, higher levels of jitter are more likely to occur on either slow or heavily congested links.

L

LAN Local Area Network. A LAN is a shared communications system to which many computers, switches, IP telephones, and IP telephone client adapters are attached. In addition to needing an Internet connection, the system must also be attached to your LAN to serve your voice, video and data needs.

Note: Your EdgeMarc is shipped with a LAN IP address of 192.168.1.1. This allows you to access the system using a PC to configure it. You can access the system using the preset IP address and the default subnet mask of 255.255.255.0. It is recommended that you change the default password using the System page once you configure your system.

LLC Logical Link Control (LLC) Encapsulation. Multiple protocols are multiplexed over a single ATM VC. The protocol of a carried protocol data unit (PDU) is identified by prefixing the PDU with an LLC header. See VC.

LLDP The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. Information gathered with LLDP is stored in the device as a management information database (MIB) and can be queried with the Simple Network Management Protocol (SNMP) as specified in RFC 2922. The topology of an LLDP-enabled network can be discovered by crawling the hosts and querying this database.

M

MAC address Media Access Control address. A hardware address that uniquely identifies each node of a network.

Menu Bar The EdgeMarc Status page menu bar on the Top Level, Group Level, and Device Level screens contains submenus for monitoring, provisioning, configuring and performing operations on EdgeMarc devices, EdgeMarc Groups, and other nodes/devices managed by EdgeMarc. The menu bar options change depending on which level you are at in the device tree.

MOS Mean Opinion Score. MOS is a test used in telephony networks to obtain the user's view of the quality of the network.

N

Node / Device EdgeMarc devices, phones, third-party nodes, SNMP-based nodes, EdgeConnects and (if licensed) Plug and Dial phones and Plug and Dial conduits.

O

Other Devices Third-party nodes and SNMP nodes.

P

Parent Group When there are subgroups under an EdgeMarc Group, the top level EdgeMarc Group is considered the Parent Group.

PEAP Protected Extensible Authentication Protocol (PEAP) is part of the Extensible Authentication Protocol (EAP) protocols.

PEAP uses Transport Layer Security (TLS) to create an encrypted channel between an authenticating PEAP client, such as a wireless computer, and a PEAP authenticator, such as a server running Network Policy Server (NPS) or other Remote Authentication Dial-In User Service (RADIUS) server.

Phone Template A configuration file used to provision a phone.

Phone-specific Configuration File A phone-specific configuration file which contains MAC address-specific configuration information such as the phone number (DID), phone extension, phone display name, and the AuthName/Pwd. The content of the phone-specific file overrides what is in the generic phone configuration file. Phone-specific files typically have the phone's MAC address embedded in the filename.

Phone-specific Template A template file which is created from a phone-specific configuration file. These files can also be used without Plug and Dial; you can manually set up a phone using these files without using the IVR. Phone-specific templates are referred to as "Phone Templates" in EdgeMarc.

Plug and Dial Refers to the workflow for automatically managing endpoints when a conduit is used. Sometimes referred to as "PnD", Plug-n-Dial, PND, and P&D.

PoE Power over Ethernet.

PPPoATM Point-to-Point Protocol Over Asynchronous Transfer Mode is a network protocol for encapsulating PPP frames in AAL5. It is used mainly with DOCSIS and DSL carriers.

PPPoE Point-to-Point Protocol over Ethernet. A network protocol for encapsulating PPP frames inside Ethernet frames. Used for the following:

PPPoE-speaking Internet DSL services where a PPPoE-speaking modem-router connects to the DSL service. Both the ISP and the modem-router need to speak PPPoE. PPPoE-over-DSL is referred to as PPPoEoA, or PPPoE over ATM.

PPPoE-speaking DSL modem is connected to a PPPoE-speaking Ethernet-only router using an Ethernet cable. For such two-box systems, DSL modem plus Ethernet-only router, PPPoE is now the preferred solution.

Proxy ARP Proxy using the Address Resolution Protocol to create a bridge between two interfaces on the system.

R

Raw File One of the three types of EdgeMarc configuration files. A Raw File may be any text file, especially those that do not meet the formats of the other two file types: Variable/Value File or IP Address File List.

RegEx Regular Expression.

revertive mode Revertive mode operation forces the configured primary WAN to return to active state after it recovers from a failure.

Rights Provides the system administrator with the ability to restrict users from using certain parts of EdgeMarc. Examples include Analyzing, Monitoring, Template Editing, Conduit Editing, Provisioning, VPN Editing, VPN Viewing, Device Configuration and System Administration.

S

SIP Session Initiation Protocol. Protocol designed to signal the setup of voice and multimedia calls over IP networks.

SIP Server The upstream SIP proxy server.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks as a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMP Read-Only Community String The SNMP password EdgeMarc uses so that outside Network Management Systems can access it.

Softswitch The upstream switch at the customer premises that EdgeMarc communicates with to retrieve information about the clients. Also referred to as the “feature server.”

SSH Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote shell services or command execution and other secure network.

State The UP/DOWN status of a node.

Strict Password Strict passwords require 6-8 characters, 2 or more character types and no dictionary words.

Substitution Variables Special variables that will, at deployment time, be replaced with actual useful values.

Survivability The Survivability feature enables an EdgeMarc to provide local calls (station to Station or station to PSTN if there is local PSTN connectivity) when the WAN link is failing.

Syslog System Logs (syslog). Debugging logs that are collected by EdgeMarc and used to diagnose and resolve issues. These messages are not ordinarily seen by the user.

T

TR-069 Technical Report 069. Defines an application layer protocol for remote management of end-user devices to provide the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). See ACS.

Tenant A Tenant has properties that are used for managing devices under the Tenant, such as whether an EdgeMarc can use Plug and Dial, how many nodes are supported by the Product License, default passwords, and ports. A Tenant is always tied to one EdgeMarc Group, but the EdgeMarc Group may have subgroups.

Trap A Simple Network Management Protocol trap is a message which is initiated by a network element and sent to the network management system.

U

Unassigned Group An EdgeMarc Group in the device tree which contains nodes/devices that have been discovered by EdgeMarc but have not been assigned to an EdgeMarc Group. When the EdgeMarc comes online or is rebooted, it sends a message through Syslog and EdgeMarc will then automatically add it to the “Unassigned” EdgeMarc Group in the device tree. The “Unassigned” EdgeMarc Group is automatically created if necessary.

V

Variable/Value File One of the three types of EdgeMarc configuration files. Contains variable/value pairs only of the format: variable=value. Other types of EdgeMarc configuration files are an IP Address File List and a Raw File List.

VC Virtual circuit (VC) based multiplexing. One PVC is defined per protocol. See LLC.

VPN A Virtual Private Network extends a private network and the resources contained in the network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if it were a private network with all the functionality, security and management policies of the private network

VPN Group A logical grouping of EdgeMarc devices for VPN configurations.

VPN Policy Defines the values of VPN properties.

W

WAN Wide Area Network.

Whitelist Specifies a block of IP addresses that are allowed to conduct management sessions with EdgeMarc. For EdgeMarc devices that are not behind a firewall (e.g., an EdgeMarc on the edge of the Internet), the Whitelist feature specifies a list of IP addresses that are allowed to conduct a management session with EdgeMarc. IP addresses that are not in the Whitelist are blocked from accessing EdgeMarc.

The Whitelist feature is similar in behavior to the “trusted management hosts” feature on the EdgeMarc. EdgeMarc administrators must use PCs/Workstations with the source IP addresses or networks listed in the Whitelist. See also Blacklist.

Numerics

802.1x supplicant
  configuring 3-128

A

accessing the GUI 1-5
administration configuration page 2-7
ADSL configuration page 3-97
ADSL modem settings
  WAN IPv4 settings 3-91
ADSL settings
  configuring 3-97
  line status 3-103
ALG registration 6-334, 9-520

B

B2BUA actions 6-415
B2BUA settings
  credentials and registration 6-411
  pattern and digit matching 6-418
B2BUA trunking 6-407
B2BUA trunking device
  creating 6-408
backing up your configuration 2-20
backup/restore configuration page 2-16

C

call control 6-474
call number patterns 6-444
call status messages 9-521
CAS/GW
  client configuration 3-170
CAS/UA
  network configuration 3-161
certificates 3-242
  adding local certificate 5-313
  managing 5-307
certificates and keys
  creating new 5-310
  downloading 5-312
CLI input options 2-59
clients list
  H.323 6-378
  H.323 clients 6-482
  MGCP clients 6-480
  SIP clients 6-479
  VoIP clients 6-478
configuration backup
  backup and restore 2-20

customer networks
  configuring 3-126

D

default gateway settings 3-95
DHCP configuration
  WAN IPv4 settings 3-93
DHCP configuration page 3-180
DHCP relay settings
  IPv4 settings 3-180
  IPv6 settings 3-181
DHCP server configuration page 3-182
DHCP server options 3-183
DHCP server settings
  IPv4 settings 3-184
  IPv6 settings 3-194
  vendor options 3-192
dial completion patterns 6-437
dial rules 6-402
Diffie-Hellman parameters 3-253
distinctive ring pattern
  adding a rule 6-446
distinctive ring pattern rules 6-444
DNS settings
  configuring 3-96
dual WAN ports, configuring 3-270
dynamic DNS configuration page 3-234

E

EdgeMarc device
  about 1-1
  changing your password 2-12
  deploying 1-2
  logging in 1-5
Edgewater Networks
  contacting support 1-iv
encryption key 2-18
encryption key, configuring 2-11

F

fax
  configuring 6-441
file download
  using FTP 2-60
file server
  managing 2-63

firewall traversal
certificates 3-242
external client mode 3-248
generating a static key 3-252
internal client mode 3-245
remote mode 3-254
firewall traversal page 3-242
firmware
download new 2-24
latest version 2-24
upgrading 2-23
upgrading SOC2 2-28
upgrading VOS 2-28
viewing current version 2-24
firmware upgrade
SOC2 settings 3-275
frame relay settings 3-143
FTP users configuration page 2-67
FXO line port settings 6-451
FXO settings
SIP gateway 6-448
FXS advanced settings 6-431
FXS ports 6-430

G

getting started 1-1
GRED/LLQ
about 3-203
configuring 3-216
GUI access
logging in 1-5

H

H.323 clients list 6-482
H.323 configuration page 6-336
H.323 settings
alias manipulation 6-361
B2B rules 6-375
bandwidth scheduling 6-369
call activity messages 6-358
clients list settings 6-378
managing 6-356
neighboring 6-365
registration rules 6-373
high availability configuration page 3-174
high availability settings 3-175
stateful failover 3-174
HTTPS settings 5-314
hunt groups
managing 6-440

L

LAN settings 3-82
LAN switch ports 8-508
license information, software 10-523
license key
  editing 2-10
licensing
  software features 2-10
link rate settings 3-229
log messages
  PPTP logs 7-502
logging
  remote system logging 2-44, 2-51

M

message header rules 6-421
message of the day (MOTD)
  setting 4-300
MGCP clients list 6-480
MGCP settings 6-380
  audit endpoint
    configuring 6-383
  endpoint re-registration 6-382
  softswitch protocol settings 6-382
MLPP settings 3-142
MOS filtering 2-51
MOS mean opinion score
  about 2-39
  configure settings 2-53
Multi LAN Ports 3-80

N

NAT configuration page 3-108
NAT settings
  configuring dynamic NAT 3-109
network configuration page 3-77
network default gateway settings 3-95
network information page 3-236
network restart 3-239
network settings
  configuring port forwarding 3-112
  configuring private networks 3-111
  LAN interface settings 3-82
  WAN interface settings 3-89
network test tools 3-240
NTP server, disable on LAN 2-58

P

pass-through rules
  configuring 3-219
passwords
  first time log on 2-12
  read-only user 2-14
peering-proxy mode settings 6-343
ping settings for WLR 3-264
ping test 9-521
  performing a ping test 3-241
PoE configuration page 8-506
PoE settings
  configuring switch ports 8-513
  managing port statistics 8-508
  storm control 8-516
  switch settings configuration 8-503
PPP settings 3-143
PPPoE configuration
  WAN IPv4 settings 3-92
PPTP configuration page 7-498
PPTP settings
  add a new user 7-500
  enabling PPTP 7-499
  log messages 7-502
  managing active users 7-502
prefix matching 6-322
PRI configuration page 3-153
PRI/GW
  client configuration 3-166
PRI/UA
  network configuration 3-156
proxy ARP configuration page 3-226
PSTN Sense Window 6-453

R

RADIUS settings
  configuring 2-29
reachability holdoff delay 6-470
rebooting the system 2-75
root user 3-126
round-trip-time, enabling 6-333
router advertisement
  IPv6 settings 3-276
RTSP configuration page 8-509

S

saving your configuration 2-20
secondary WAN, dual WAN ports 3-261
security certificates 3-242

security configuration page 5-303
security settings
  firewall traversal 3-242
  outbound protocol settings 5-316
  trusted hosts 5-316
  WAN firewall settings 5-304
server maintenance 2-67
services
  MOS filtering 2-51
  remote system logging 2-44, 2-51
  SNMP 2-37
  WAN settings 2-51
services configuration page 2-40
session management 4-281
  active users 4-296
  system audit 4-297
SIP ALG trunking 6-397
SIP clients list 6-479
SIP gateway settings 6-448
SIP GW settings
  FXO settings 6-451
SIP media server configuration page 6-460
SIP registration control 6-476
SIP routing configuration page 6-456
SIP server reachability 6-468
SIP server redundancy
  configuring 6-473
SIP servers 6-392
SIP settings
  configuring 6-391
  dial rules 6-402
  proxy settings 6-392
  SDP settings 6-395
  stale timer 6-393
  TCP settings 6-394
  TLS settings 6-395
  UDP settings 6-394
SIP settings page 6-384
SIP trunking
  message header transformation 6-400
SIP trunking devices
  configuring 6-399
  header rules 6-421
SIP trunking patterns 6-406
SIP UA configuration page 6-423
SIP UA hunt groups 6-440

SIP UA settings
  basic FXS settings 6-425
  dial patterns 6-437
  distinctive ring 6-444
    adding new 6-446
    pattern rules 6-444
  fax configuration settings 6-441
  FXS advanced settings 6-431
  FXS port settings 6-430
SNMP settings
  managing 2-37
SOC2 firmware
  upgrading 2-28
SOC2 firmware upgrade 3-275
software features
  licensing 2-10
stateful failover 3-174
static IP configuration
  WAN IPv4 settings 3-93
static routes configuration page 3-232
subinterfaces configuration page 3-223
survivability configuration page 6-460
survivability settings
  configuring common settings 6-466
  local call control 6-474
  SIP registration 6-476
  SIP server 6-468
  SIP server redundancy 6-473
switch ports configuration page
  link rate settings 3-229
switch settings
  managing the LAN IP 8-504
  mirror monitoring 8-505
system information
  system time and date 2-57
system information page 2-55
system reboot 2-75
system report, downloading 2-56

T

T1/E1 advanced diagnostics 3-152
T1/E1 configuration
  WAN IPv4 settings 3-95
T1/E1 configuration page 3-130
T1/E1 diagnostics 3-147

T1/E1 settings
  configuring ports 3-141
  fractional links 3-138
  frame relay settings 3-143
  link layer settings 3-140
  MLPP settings 3-142
  physical layer settings 3-137
  PPP LCP settings 3-143
TACACS settings
  configuring 2-31
test UA
  enabling 6-484
  verify connectivity 6-487
test UA management page 6-483
time and date settings 2-57
TR-069 settings
  configuring 2-72
traceroute test
  performing a traceroute test 3-242
Traffic Shaper
  IPv4/IPv6 mixed traffic 3-210
  IPv6 Class of Service 3-210
traffic shaper configuration page 3-197
traffic shaper settings
  basic traffic shaping 3-208
traffic shaping settings 3-204
  advanced traffic shaping 3-210
  GRED/LLQ 3-216
troubleshooting 9-519
  call status 6-358
  changing passwords 9-520
  configuration backup or restore 9-520
  contact support 9-519
  downloading and upgrading firmware 9-520
  hardware platform information 9-520
  license keys and registration 9-520
  registered voice devices
    clients list 9-521
  running a ping test 9-521
  system logging messages 9-520
  system messages 9-521
  system restart or reboot 9-521
  verifying device status 9-520
  verifying network status 9-520
  verifying software version 9-520
  verifying the MAC address 9-520

U

upgrading firmware
  ftp 2-25
  SCP 2-26

user accounts
managing 4-281
user command examples 2-60
user commands
CLI 2-59
user management
enabling 4-291
user/session management 4-281
users
managing 4-281

V

V.90 modem
configuring 2-74
vendor options 3-192
Virtual MAC, VMAC 3-176
VLAN configuration
WAN IPv4 settings 3-94
VLAN configuration page 3-116
VLAN settings
configuring 3-117
creating a new VLAN 3-119
port membership 3-122
port settings 3-123
VoIP bandwidth settings 6-334
VoIP clients list 6-478
VoIP configuration page 6-321
VoIP prefixing 6-322
VOS software
upgrading 2-28
VOS User Guide
organization 1-iii
VPN configuration page 7-489
VPN settings
enabling VPN 7-490
subnet settings 7-496
VPN tunnels
add new 7-490

W

WAN address 2-51
WAN bandwidth
calculating 3-201
WAN firewall
configuring 5-304
WAN hostname 2-51
WAN interface settings
IPv4 settings 3-91
IPv6 settings 3-89

WAN link redundancy
advanced settings 3-262
configuring WLR 3-257
secondary WAN settings 3-265
WAN public source IP 2-51
WAN settings 3-89
WAN VLAN settings
configuring 3-124
warranty, hardware 10-523