

VoIP Operating System (VOS) for EdgeMarc

User Manual

Version 3.0



U.S. Headquarters:

2895 Northwestern Parkway
Santa Clara, California 95051

Phone: 408.351.7200

Fax: 408.727.6430

edgewaternetworks.com

© 2010 Edgewater Networks, Inc.

Edgewater Confidential, All Rights Reserved.

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.

EdgeMarc is a trademark of Edgewater Networks, Inc. in the United States and other countries. Any other trademarks appearing in this manual are owned by their respective companies.

Export Notice

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or re-export may be required by the U.S. Department of Commerce.

Regulatory Compliance

This product was tested to comply with FCC standards for home and office use.

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.

Release Date:

9/2/10

Contents

About this Guide	xi
Typographic Conventions	xii
1 Introduction	
The VoIP Operating System for EdgeMarc	1
Features	1
User Interface Components	2
Accessing the User Interface	2
2 Network Connectivity	
Configuration Overview	3
Configuration for IP Centrex Applications	4
Configuration for Station Side IP PBX Applications	6
System Configuration	8
Configuring WAN Settings	8
Configuring LAN Settings	8
Configuring VLANs	9
Configuring Ethernet Interface Link Settings	10
Configuring Subinterfaces	11
Configuring T1 Settings	12
3 DHCP Services	
DHCP Relay	17
DHCP Server	18
DHCP Leases	19
Configuring DHCP Server	19
4 Firewall	
Overview	21
Configuring the Standard Firewall	22
Configuring Advanced Firewall Settings	22
Custom Rules	23
Remote Management	24
Configuring Static Forwarding	24
5 NAT	
Overview	27
Dynamic and Static NAT	27

	NAT and Firewall Options	28
	Configuring NAT for the Standard Firewall.	28
	Configuring NAT for the Advanced Firewall.	29
	Configuring Static NAT	29
6	Advanced Data Capabilities	
	Configuring Certificates	31
	Configuring Dynamic DNS	31
	Configuring a DMZ Using Proxy ARP and Routed Subnets	32
	Proxy ARP.	32
	Configuring RADIUS.	33
	Configuring TACACS	34
	EdgeMarc Support for TACACS+ Authentication	34
	TACACS+ Authentication Modes	34
	EdgeMarc Support for TACACS+ Accounting	35
	TACACS+ and RADIUS	36
	Configuring TACACS+ Settings.	36
	Static Routes	37
7	Management	
	Trusted Management Addresses	39
	System Time	40
	Network Information	40
	Remote Management	41
	SNMP	41
	System message logging (syslog)	44
	System Information.	45
	Read-only Users	45
	User Commands	46
	Message of the Day.	46
8	VPNs	
	Overview and Examples	49
	Non-VLAN switches, one WAN subnet	49
	Single LAN Ethernet and Separate PC and Phone Subnets	50
	Single LAN Ethernet and Same PC and Phone Subnet.	50
	Non-VLAN Edgewater Appliance, Non-VLAN Switches, One WAN Subnet	51
	VLAN or Non-VLAN Edgewater Appliance, Non-VLAN Switches, Two WAN Switches	51
	Non-VLAN EdgeMarc Appliance.	52

VLAN-capable Ethernet switch, VLAN or Non-VLAN Edgewater Appliance	52
Non-VLAN EdgeMarc Appliance	52
Third Party Firewall in front of Edgewater Appliance	53
Dynamic WAN IP Address Assignment	53
Configuring VPN Settings	54
9 Voice Over IP	
Traffic Management	57
Traffic Shaping	58
Advanced Traffic Shaping	58
ToS Byte Setting	59
Traffic Marking	59
Call Admission Control	60
Traffic Management in the EdgeMarc Device	61
Priority IP Addresses	63
VoIP ALG	63
SIP Settings	64
SIP Trunking	64
H.323 Configuration	67
H.323 Activity	67
H.323 Alias Manipulation	68
H.323 Neighboring	68
Regular Expressions	69
MGCP Settings	70
VoIP Subnet Routing	70
10 Configuring FXS and FXO Ports	
Overview	73
Survivability	74
Session Initiation Protocol (SIP) Trunking	74
Two-Stage Dialing for Inbound IP and PSTN Calls	74
Transmit/Receive Gain	75
Priority Calling Support	75
FXS Hunt Group	76
Ad-Hoc Conferencing	76
Example Configurations	77
IP Centrex Configuration	77
SIP Trunking of Analog Ports Configuration	79
SIP Trunking of IP PBX Configuration	79
Configuring FXO Ports	80
Configuring T38 and G.711 Fax	82

Configuring FXS Ports	82
Gain Settings	83
Configuring SIP Trunking	83
SIP Trunking Devices	84
Rules	84
Priority Redirection	85
Configuring SIP Trunking Enhancements	85
Distinctive Rings	86
Configuring FXS Hunt Group	88
Calling Features for Analog Phones on the FXS port	90
11 Wireless	
Overview	93
Security	93
Service Set Identifiers	94
Channels and Power Levels	94
Wireless Status	95
Configuring Wireless Settings	95
Configuring VLAN Settings to Support Wireless Traffic	96
12 Survivability	
Overview	97
Configure Survivability	99
SIP Server Redundancy	99
SIP Server Availability	100
MGCP Survivability Configuration	101
Survivability in Transparent Mode	102
Survivability	106
Assigning SIP Modes	107
Survivability Voice Mail	108
Voice Mail Process	109
Configuring Survivability Voice Mail Settings	110
Using the IVR System	112
13 Stateful Failover	
Overview	117
Configuring Stateful Failover	117
Configure the LAN and WAN IP addresses	118
Configure Virtual IP addresses for the redundant pair	118
Configure the Management Interface	119
Configure the Stateful Failover page	119

14	WAN Link Redundancy	
	Overview	121
	Data and Voice Interface Switchover	122
	Manual Switchover	122
	Supported Interfaces	123
	Configuring WAN Link Redundancy	123
15	System Diagnostics	
	Viewing Version, Hardware Platform and LAN MAC Address	125
	Viewing the ALG Registration Code	125
	Entering the Registration Code	125
	Viewing Networking Information	126
	Routing Information	126
	Link Status	127
	Interface Information	127
	Viewing Advanced System Information	127
	Passive Voice Call Monitoring	127
	Using Troubleshooting Tools	128
	Verifying Registered Voice Devices	128
	Ping and Traceroute Tests	129
	Networking Restart	130
	Rebooting the System	130
	Using T1 Diagnostics	131
	Verifying Connectivity with the Test UA	132
16	Device Configuration Management	
	Overview	135
	own Command	135
	Logging off listed users	137
	Downloading Files	138
	Using the Internal TFTP Server	138
17	Edgemarc BGP and Routing Configuration and Troubleshooting	
	BGP enablement and configuration	141
	Troubleshooting using BGP and routing daemons	143
18	System Upgrades	
	Release Information	145
	Upgrade Procedure for Software Revision 1.3.11 or Later	146

Upgrade Procedure for Software Version 1.3.9 or Earlier	146
19 Primary Rate Interface(PRI)	
Overview	149
Configuring T1 for PRI	149
Configuring Client Side ISDN PRI (PRI/GW)	150
Configuring Network Side ISDN PRI (PRI/UA)	152
Configuring SIP Trunking for PRI	153
A Syslog Messages	
B Configuration Parameters	
Network Page	169
Subinterfaces Page	171
DHCP Relay Page	172
DHCP Server Page	173
DHCP Leases Page	176
Standard Firewall Page	176
Advanced Firewall Page	179
Custom Rules Page	183
Current Advanced Firewall Rules (Show Rules)	185
Forwarding Rules Page	186
Message of the Day Page	188
NAT Pages	189
Traffic Shaper Page	193
Advanced Traffic Shaper Page	196
VoIP ALG Page	200
H.323 Settings Page	204
H.323 Activity Page	208
H.323 Alias Manipulation Page	209
H.323 Neighboring Page	211
MGCP Settings Page	213
SIP Settings Page	216
SIP Trunking Page	218
Survivability Page	221
FXS/Phone Port Settings - Basic (SIP UA) Page	228
FXS/Phone Port Settings - Advanced Page	229
FXS/Phone Port FAX Settings Page	234
Distinctive Ring Page	237

SIP FXO/Line Port Configuration (SIP GW) Page	238
VPN Page	243
VPN Subnet Page	244
VPN Tunnel Settings Page	245
System Page	247
Certificate Page	249
Clients List Page	251
Dynamic DNS Page	253
File Download Page	255
File Server Page	256
Network Information	258
Network Restart Page	259
Network Test Tools Page	260
Proxy ARP Page	262
RADIUS Settings Page	264
Reboot System Page	265
Remote Management	266
Route Page	267
Services Configuration	267
Set Link Page	271
Stateful Failover	272
System Information	274
System Time Page	276
Test UA Settings page	277
T1 Configuration Page	278
T1 Configuration Page - MLPPPoFR	282
T1 Diagnostics Page	283
TACACS Settings Page	286
Upgrade Firmware Page	288
User Commands Page	289
VoIP Subnet Routing Page	290
VLAN Configuration Page	291
Wireless Configuration Page	293
Client Side ISDN PRI (PRI/GW) Configuration Page	295
Client Side ISDN CAS (CAS/GW) Configuration Page	298
Network Side ISDN PRI (PRI/UA) Configuration Page	301
Network Side ISDN CAS (CAS/UA) Configuration Page	304
WAN Link Redundancy Configuration Page	307
Secondary Interface Settings Configuration Page	309

WAN Link Parameters Configuration Page312

C License Information

EdgeMarc Software License Agreement.315
Asterisk Copyright.318
Data Encryption Standard Copyright318
XML 1.0 Parser Library License.319
Open LDAP Copyright319
Open LDAP License320
Open H.323 Copying Permission321
Henry Spencer Regex License.322
Berkeley Source Distribution License.322
Sleepycat Software License.323
Perl Compatible Regular Expressions License324
Vovida Software License.325
Blowfish License326
Open SSL License327
Open SSL Toolkit License329
Net SNMP License330
Point-to-Point Protocol Daemon License334
SSH License336
Shadow Utilities License.341
GNU General Public License Version 2342
GNU General Public License Version 2.1.349

D Product Warranties

Hardware Warranty359
Software Warranty.359

Preface

Thank you for your purchase of the EdgeMarc Converged Network Appliance. This guide describes the EdgeMarc VoIP Operation System (VOS), and is intended for network installers, network operators, and security officers.

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

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

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

<http://www.edgewaternetworks.com/kb>

About this Guide

The following table briefly describes each chapter and appendix in this guide.

<small>Chapter</small> Chapter or Appendix	Description
Chapter 1, Introduction	Lists the features of VOS for EdgeMarc and briefly describes the VOS user interface.
Chapter 2, Network Connectivity	Describes how to configure The EdgeMarc appliance to support network services
Chapter 3, DHCP Services	Describes how to configure DHCP services with and without VLANs.
Chapter 4, Firewall	Describes how to configure firewall features on the EdgeMarc appliance.
Chapter 5, NAT	Describes how to configure Network Address Translation (NAT) on the EdgeMarc appliance.
Chapter 6, Advanced Data Capabilities	Describes how to configure advanced data capabilities on the EdgeMarc appliance.
Chapter 7, Management	Describes how to configure management capabilities on the EdgeMarc appliance.
Chapter 8, VPNs	Describes how to configure virtual private networks (VPNs) on the EdgeMarc appliance.
Chapter 9, Voice Over IP	Describes how to configure Voice over IP (VoIP) features on the EdgeMarc appliance.
Chapter 10, Configuring FXS and FXO Ports	Describes how to use the FXS and FXO ports available on the EdgeMarc appliance.
Chapter 11, Wireless	Describes how to configure the EdgeMarc appliance as a wireless access point.

Chapter or Appendix	Description
Chapter 12, Survivability	Describes how to manage survivability on the EdgeMarc appliance.
Chapter 13, Stateful Failover	Describes how to configure two EdgeMarc devices to act as a redundant pair.
Chapter 14, WAN Link Redundancy	Describes how to configure the EdgeMarc appliance to support the WAN Link Redundancy (WLR) feature.
Chapter 15, System Diagnostics	Describes how to use the diagnostic information, troubleshooting tools, and system maintenance utilities on the EdgeMarc appliance.
Chapter 16, Device Configuration Management	Describes the tools available to manage the EdgeMarc appliance configuration
Chapter 17, System Upgrades	Describes how to upgrade the EdgeMarc device to the latest software release available from Edgewater Networks.
Chapter 18, Primary Rate Interface(PRI)	Describes how to configure the ISDN Primary Rate Interface (PRI) on the EdgeMarc appliance
Appendix A, Syslog Messages	Lists syslog messages for the EdgeMarc appliance.
Appendix B, Configuration Parameters	Describes all the parameters available on the EdgeMarc device configuration pages

Typographic Conventions

User input is displayed in **boldface** type and can represent either keyboard input or mouse selections in a browser window depending on the context.

Names of web GUI menus and input areas are in *italics*.



Note

This format highlights information that is important or that has special interest.



Warning

This format highlights information that will help you prevent system damage or loss of data.

Contact and Support Information

Edgewater Networks, Inc.
2730 San Tomas Expressway, Suite 200
Santa Clara, California 95051
www.edgewaternetworks.com
Phone: 408.351.7200

General: info@edgewaternetworks.com

Sales: sales@edgewaternetworks.com

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

Introduction

This chapter introduces the features and user interface of the EdgeMarc appliance. It contains the following sections:

- The VoIP Operating System for EdgeMarc
- Features
- User Interface Components

The VoIP Operating System for EdgeMarc

The VoIP Operating System (VOS) for EdgeMarc is a new generation of operating system providing the demarcation point for real-time, interactive IP services. It is the ideal solution for connecting enterprise PCs and IP Phones to a private or public IP network. It replaces multiple standalone systems by integrating voice-over-IP (VoIP), network security, traffic management and voice call quality monitoring into a low-cost, easily managed device.

Use VOS to ensure high quality voice calls, maximize WAN link utilization for data traffic and protect the enterprise LAN from network based attacks.

VOS supports all EdgeMarc converged network appliance models from Edgewater Networks. For a current list of available models, go to the Edgewater Networks web site at www.edgewaternetworks.com.

Features

The VOS for EdgeMarc provides the following features:

- Resolves NAT/firewall traversal problems for VoIP by providing a VoIP Application Layer Gateway (ALG) that supports SIP, MGCP and H.323
- Supports 2 to 30 concurrent VoIP calls
- Protects the enterprise LAN using a stateful packet inspection (SPI) firewall for both voice and data traffic
- Provides NAT and PAT for voice and data
- Performs static IP routing
- Performs traffic management including prioritization, classification, queuing, TOS bit setting and call admission control for voice

- Provides voice call quality monitoring and testing
- Provides integrated test tools to facilitate problem isolation
- Provides a DHCP server for enterprise PCs and IP phones
- Performs TFTP relay for IP phone images
- Uses a simple web-based GUI for configuration and management
- Supports logging to external syslog servers and interfaces to network management systems using SNMP

User Interface Components

The VOS interface consists of a navigation pane at the left of the window and a larger content pane at the right. The navigation pane contains the Configuration Menu, which lists the available configuration screens arranged in a hierarchical list or tree. When you make a selection in the Configuration Menu, the corresponding configuration page is displayed in the content pane. If a configuration function has more than one associated page, clicking on that function in the configuration menu expands the list to show the list of screens associated with that function.

Configuration pages contain the following types of information:

- Configurable fields
- Selection buttons
- Check boxes
- Read-only information

Accessing the User Interface

Reset administrator password

1. Choose **System** from the Configuration Menu.
2. Click **Changed** in the Change Administrator Password area.
3. Enter and confirm the new password.
4. Click **Submit**.

Network Connectivity

You can configure the EdgeMarc appliance to support a wide range of network services and enable or disable specific services based on the requirements of your network.

This chapter describes how to configure The EdgeMarc appliance to support network services. It contains the following sections:

- Configuration Overview
- System Configuration
 - Configuring WAN Settings
 - Configuring LAN Settings
 - Configuring VLANs
 - Configuring Ethernet Interface Link Settings
 - Configuring Subinterfaces
 - Configuring T1 Settings

Configuration Overview

The EdgeMarc device is a flexible, easy-to-use converged network appliance that provides many critical networking functions for IP-based voice and data. It can be installed in several different VoIP topologies:

- At the customer premises for IP Centrex applications
- At the station side of enterprise IP PBXs

Most users will follow the steps in “[System Configuration](#)” on page 8 to initially connect the EdgeMarc device into the IP network. The remainder of the configuration can be different based on the application, VoIP topology, and presence of other networking equipment such as firewalls or DHCP servers. In general, however, the steps used to configure the EdgeMarc device are:

Step	Task
1	System configuration
2	VoIP configuration
3	Data networking configuration
4	Firewall configuration

5 Traffic management configuration

Some of the steps are optional depending on your particular application. We have provided configuration guidelines below for each of the application types supported by the EdgeMarc device.

Configuration for IP Centrex Applications

A typical EdgeMarc device installation for an IP Centrex application uses an external router, xDSL, or cable modem to terminate the WAN link from the service provider. The EdgeMarc device is then connected directly to the WAN termination device and the LAN port of the EdgeMarc device is connected to the enterprise Ethernet local area network (typically a layer 2 switch). VoIP signaling is performed in the service provider network via a softswitch and the EdgeMarc device acts as a proxy for the voice devices installed in the enterprise LAN. In this configuration a single public IP address is used to proxy for all of the IP phones and to route to multiple PCs installed on the LAN. This particular example also uses static NAT entries to route to the publicly addressable servers. The EdgeMarc device performs the following functions in this application:

- WAN/LAN IP routing.
- Traffic shaping and priority queuing to guarantee high quality voice traffic. These mechanisms protect voice and data traffic from contending for the same network resources to guarantee low latency and the highest call quality possible for VoIP traffic. At the same time they ensure the best utilization of WAN bandwidth by enabling data traffic to burst up to full line rate in the absence of voice calls. Precedence is given to traffic for the range of addresses reserved for the IP phones.
- NAT/PAT translation for IP phones and PCs. This allows a single public IP address to be used on the WAN link to represent all of the private IP addresses assigned to the LAN IP phones and PCs.
- Static NAT entries. This enables the customer to use a WAN public IP address for data servers (for example web, mail, or FTP) connected behind the EdgeMarc device. These servers can then be configured with private IP addresses for additional security.
- A VoIP-aware firewall. A full layer 7 gateway for voice traffic and a stateful packet inspection firewall for data traffic.
- 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.
- DHCP server and TFTP relay. These features are used to simplify and expedite the IP configuration of phones and PCs. This also includes VoIP signaling gateway information (MGCP, SIP and H.323).

- Call quality monitoring and test tools.

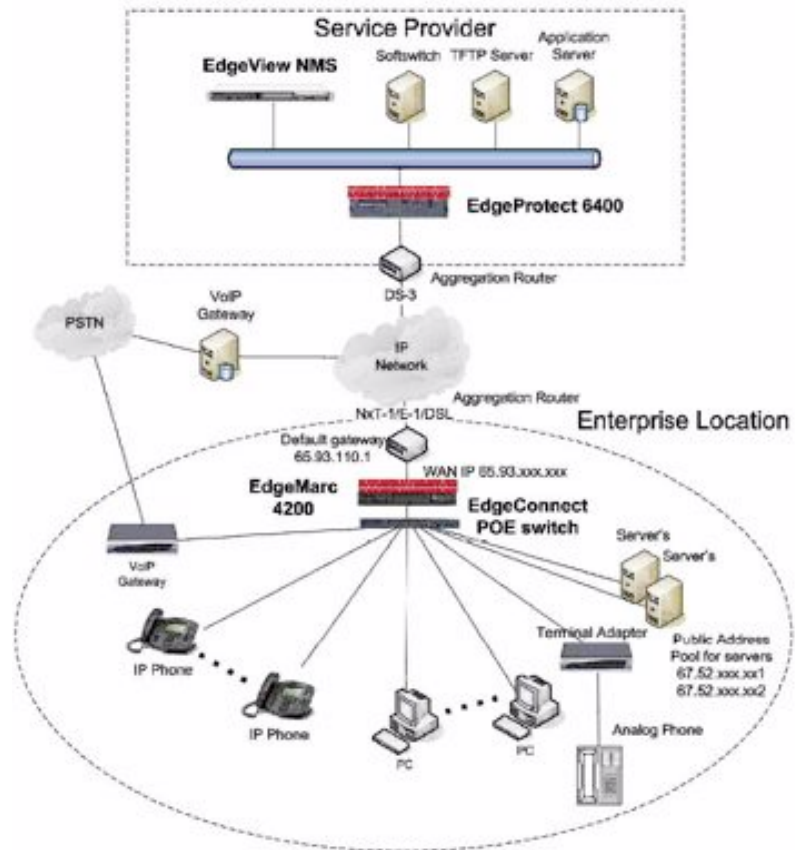


Table 1 Configuration Outline

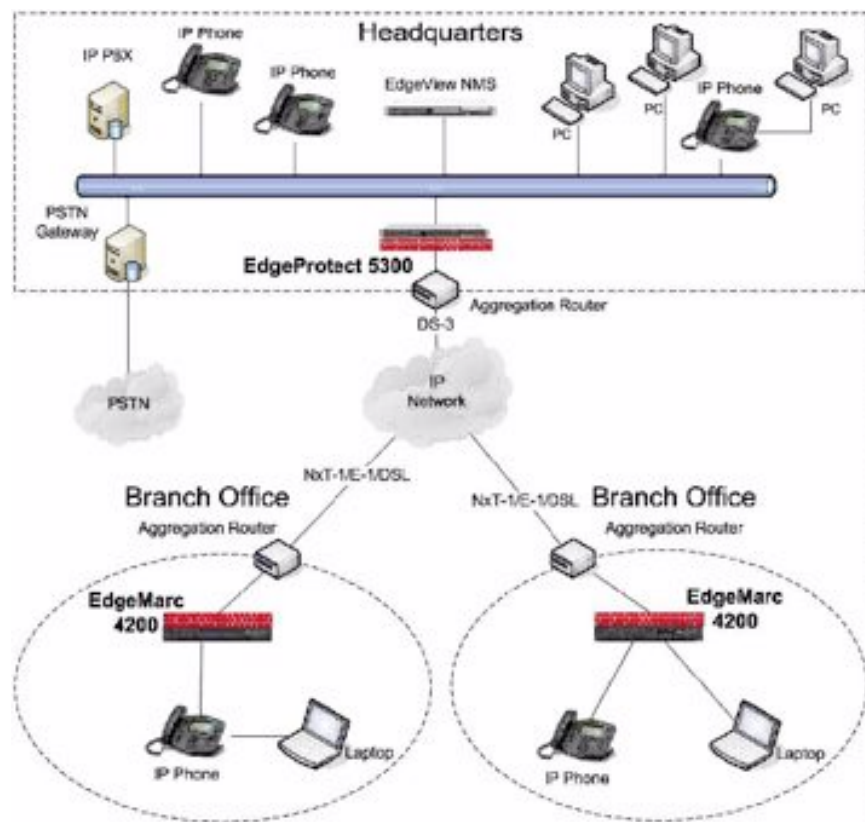
Task	Subtask	Configure For IP Centrex Application?
System Configuration	Configure LAN/WAN interface.	Yes
	Set Ethernet link rate.	Optional
	Enable the DHCP server.	Optional but recommended
	Configure SNMP.	Optional
VoIP Configuration	Enable the VoIP ALG.	Yes
	Configure a VoIP subnet route.	Optional
Data Networking Configuration	Configure dynamic NAT.	Optional but recommended
	Configure static NAT.	Optional
	Configure static IP routing.	Optional
Firewall Configuration	Enable the data firewall.	Yes
	Configure basic settings.	Optional
	Configure advanced settings.	Optional

Table 1 Configuration Outline

Traffic Management Configuration	Enable traffic shaping.	Yes
	Enable Call Admission Control.	Yes

Configuration for Station Side IP PBX Applications

Most private enterprise VoIP networks use an IP PBX at the corporate headquarters location to provide voice switching among headquarters, branch offices, and the PSTN. The EdgeMarc device is used in these environments to securely connect branch office employees to the IP PBX installed in the corporate headquarters location.



The installation of an EdgeMarc device on the station side of an enterprise IP PBX is very similar to the IP Centrex application previously described. The branch office is connected to the corporate network using VPNs or private T1 links terminated by a WAN router. The EdgeMarc device is then connected directly to the WAN router and the LAN port of the EdgeMarc device is connected to the enterprise Ethernet local area network (typically a layer 2 switch). The IP PBX in the corporate headquarters location performs VoIP signaling, and the EdgeMarc device acts as a proxy for the

voice devices installed at the branch office. The EdgeMarc device can perform the following functions in this application:

- WAN/LAN IP routing.
- Traffic shaping and priority queuing to guarantee high quality voice traffic. These mechanisms protect voice and data traffic from contending for the same network resources to guarantee low latency and the highest call quality possible for VoIP traffic. At the same time they ensure the best utilization of WAN bandwidth by enabling data traffic to burst up to full line rate in the absence of voice calls. Precedence is given to traffic for the range of addresses reserved for the IP phones.
- NAT/PAT translation for IP phones and PCs. This allows a single IP address to be used on the WAN link to represent all of the private IP addresses assigned to the LAN IP phones and PCs.
- A VoIP-aware firewall. A full layer 7 gateway for voice traffic and a stateful packet inspection firewall for data traffic.
- 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.
- DHCP server and TFTP relay. These features are used to simplify and expedite the IP configuration of phones and PCs. This also includes VoIP signaling gateway information (MGCP, SIP, H.323).
- Call quality monitoring and test tools.

Table 2 Configuration Outline

Task	Subtask	Configure For Station Side IP PBX Application?
System Configuration	Configure LAN/WAN interface.	Yes
	Set Ethernet link rate.	Optional
	Enable the DHCP server.	Optional but recommended
	Configure SNMP.	Optional
VoIP Configuration	Enable the VoIP ALG.	Yes
	Configure a VoIP subnet route.	Optional
Data Networking Configuration	Configure dynamic NAT.	Optional but recommended
	Configure static NAT.	Optional
	Configure static IP routing.	Optional
Firewall Configuration	Enable the data firewall.	Yes
	Configure basic settings.	Optional
	Configure advanced settings.	Optional
Traffic Management Configuration	Enable traffic shaping.	Yes
	Enable Call Admission Control.	Optional

System Configuration

This section explains how to configure the EdgeMarc device to function in your IP network. You will configure the Ethernet interfaces, network addresses, DNS settings, default gateway, and SNMP settings, and change the administrative password.

Configuring WAN Settings

This section describes how to set up WAN network parameters.



Note

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

Configure WAN settings

1. Choose **Network** from the Configuration Menu.
2. Select the method to use to obtain an Internet connection.

When you select a connection method, the page displays the appropriate settings in the WAN Interface Settings area.

- ADSL-PPPoE—Enter the user name and password assigned by the network provider, and indicate whether to monitor the connection using keepalive ping messages.
- DHCP—No additional configuration required.
- Static IP Address—Enter the IP address and subnet mask.
- EVDO—Enter the user name and password assigned by the EVDO service provider if required.



Note

For a list of specific EVDO cards that are supported by the EdgeMarc, visit <http://portal.knowledgebase.net/article.asp?article=291396&p=4739>.

- T1—Enter the IP address and subnet mask. Click the underlined T1 link to open the T1 Configuration page and set additional T1 parameters. See “Configuring T1 Settings” on page 12.
3. Click **Submit**.
A message indicates that service will be temporarily interrupted.
 4. Click **OK** to confirm.

Configuring LAN 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.

**Note**

The EdgeMarc appliance is shipped with LAN IP address 192.168.1.1 and subnet mask 255.255.255.0.

Configure LAN network settings without VLANs

1. Choose **Network** from the Configuration Menu.

The LAN Interface Settings area of the Network page shows the LAN IP address (192.168.1.1) and subnet mask (255.255.255.0).

2. Clear the Enable VLANs checkbox.
3. Click **Submit**.

A message indicates that service will be interrupted while the new interface is added.

4. Click **OK** to confirm.

Configure LAN network settings with VLANs

1. Choose **Network** from the Configuration Menu.
2. Select **Enable VLANs**.
3. Click **Submit**.

A message indicates that service will be interrupted while the new interface is added.

4. Click **OK** to confirm.
5. Click **VLAN Settings** to open the VLAN page.
6. Configure settings as appropriate for your EdgeMarc model. See “Set up VLANs on the 4200 and 4300T” on page 10 and “Set up VLANs on the 5300 and 6400” on page 10.

Configuring VLANs

The EdgeMarc appliance 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.

All EdgeMarc appliances (4200, 4300T, 5300, and 6400) provide support for multiple tagged VLANs. The 5300 and 6400 each support a single untagged VLAN; while the 4200 and 4300 each support up to four untagged VLANs.

All EdgeMarc appliances support up to 16 VLANs.

**Note**

All voice devices should be placed in the same VLAN.

Set up VLANs on the 4200 and 4300T

1. Choose **System > VLAN Configuration** from the Configuration Menu.
2. Choose 802.1 or 802.1q from the LAN Port Membership pull-down list. Click **Modify**. If 802.1 is selected, radio buttons are presented to permit selection of a single VLAN. If 802.1q is selected, checkboxes are presented to permit selection of multiple tagged VLANs.
3. To add and configure a new VLAN, enter the new VLAN ID, IP address, and network mask. Press **Add**. A new VLAN entry is added to the VLAN configuration. The mode of the physical port determines the rules for VLAN assignment:
 - 802.1 mode: Assign the port to a single VLAN.
 - 802.1q mode: Assign the port to multiple VLANs
4. Repeat steps 3 and 4 for each VLAN you wish to create.



Note

For detailed field descriptions, see “[VLAN Configuration Page](#)” on page 291.

Set up VLANs on the 5300 and 6400

1. Choose **System > VLAN Configuration**.

The screen displays the IP address and subnet mask of the default untagged VLAN. Each Ethernet port on the 5300 and 6400 can have both an untagged and multiple tagged VLANs. Each new VLAN that you add must be tagged.
2. To add a tagged VLAN, enter the VLAN ID, IP address, and network mask, and click **Submit**.

A message indicates that service will be interrupted while the new interface is added.
3. Click **OK** to confirm.
4. Repeat steps 2 and 3 for each VLAN you want to create.

Delete a VLAN

1. Choose **System > VLAN Configuration** from the Configuration Menu.
2. Click the trash can icon to the right of the VLAN entry. It is not necessary to press Submit after deleting a VLAN.

Configuring Ethernet Interface Link Settings

You can modify the Ethernet interface link settings for the appliance, if needed to establish a reliable connection, and adjust the MTU size of the WAN interface to reduce the effects of large data packet on media data.

**Note**

Take care when adjusting the Ethernet link rate. The device may become unreachable if an incompatible rate is set.

Configure Ethernet interface link settings

1. Choose **System > Set Link**.
2. Select a rate for each Ethernet link, or choose Autonegotiate. For details, see “[Set Link Page](#)” on page 271.
3. Click **Add**.
A message indicates that service will be interrupted while the new interface is added.
4. Click **OK** to confirm.

Configuring Subinterfaces

The Subinterfaces page allows you to assign additional IP addresses to a system interface. After creating a LAN subinterface, it is often necessary to configure a firewall forwarding rule to permit IP packets through the system. To configure forwarding, see “[Configuring Static Forwarding](#)” on page 24.

Configure network subinterfaces

1. Choose **Network > Subinterfaces** from the Configuration Menu.
2. Enter IP address and interface information. For details, see “[Subinterfaces Page](#)” on page 171.
3. Click **Add**.
A message indicates that service will be interrupted while the new interface is added.
4. Click **OK** to confirm.
5. Enter additional subinterfaces as needed.

Delete a subinterface

1. Choose **Network > Subinterfaces** from the Configuration Menu.
2. Select checkboxes for the entries that you want to delete. Click **Select: All** to choose all the entries or **Select: None** to clear your selections.
3. Click **Delete**.
4. Click **OK** to confirm.

Configuring T1 Settings

Use the T1 Configuration page to configure and test the T1 interface on the appliance. This section describes the features that apply to the T1 interface:

- [MLPPP](#)
- [Framing Mode and Line Encoding](#)
- [T1 Interface Configuration](#)
- [Multiple DLCIs and Fractional T1 Links](#)

MLPPP

Multilink Point-to-Point Protocol (MLPPP) is a line aggregation protocol that enables multiple physical connections between two network devices to appear as one virtual connection.

By aggregating or bundling multiple links (such as multiple T1 lines) into a single virtual connection, MLPPP expands the bandwidth available between devices while remaining transparent to users. For example, MLPPP can be used to combine two channels into a single virtual channel, thereby doubling the available bandwidth from 1.5Mbps to 3Mbps.

MLPPP also provides redundancy. If more than one physical line is in a bundle (single virtual line), then losing a physical line may not bring down the entire virtual line.

To operate, MLPPP must be implemented at both ends of the network connection. At the transmitting end, MLPPP controls the process of disassembling datagrams, recombining them according to the protocol design, and sending them in logical sequence across the multiple connections. At the receiving end, an MLPPP-equipped device disassembles the datagrams and reconstitutes them as needed for delivery to the appropriate destinations.

MLPPP is an extension of Point-to-Point Protocol (PPP), which is a standard method of preparing data packets for transmission over a single channel WAN connection.

The EdgeMarc appliance can be configured to use MLPPP for communication with an aggregating router. MLPPP creates a virtual interface to handle all voice and data traffic, and then the traffic is distributed over individual T1 lines. With MLPPP running on both the EdgeMarc appliance and aggregating router, the two devices automatically identify and activate the transport parameters that control which T1 lines are responsible for transporting each packet of information. The EdgeMarc appliance supports these protocols: HDLC, ANSI, and CCITT.



Note

MLPPP is licensed according to the number of available T1 lines. Before configuring MLPPP, verify that the feature is included with your license.

Configure MLPPP

1. Choose **System > T1 Configuration**.
2. To use MLPPP, select the Enable MLPPP checkbox and click **Submit**.



Note

When you enable or disable MLPPP, you must submit the changes before completing the rest of the configuration.

When MLPPP is enabled, any combination of the licensed T1 lines can join the virtual link. When MLPPP is disabled, only the first T1 port is available for use.

3. Choose the T1 ports to include in the MLPPP group.
4. Choose the T1 protocol to use. The following protocol options are supported.

Protocol	Single T1	MLPPP
HDLC	Y	Y
cHDLC	Y	-
PPP	Y	-
ANSI	Y	Y
CCITT	Y	Y

5. Select a checkbox for each physical T1 line that you want to enable.
6. Click **Submit**.
7. Choose **System > T1 Network** to open the Network page.
8. Select **T1**.
9. Enter the default gateway information.
10. Click **Submit**.

MLPPP is now configured.



Note

For detailed field descriptions, see [“Network Page”](#) on page 169 and [“Test UA Settings page”](#) on page 277.

Framing Mode and Line Encoding

Framing mode defines the T1/E1 framing mode. This typically defines the number of frames that are grouped together. Currently only ESF (F24) and D3/D4 (F12) are supported. ESF has 24 frames. D3/D4 has 12 frames.

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.

Protocol: Display and set the T1 layer 2 protocol.

MLPPP Disabled: The protocols supported are HDLC, Cisco HDLC, PPP, Frame Relay ANSI and CCITT. The default setting is HDLC.

MLPPP Enabled: The protocols supported are HLDC, Frame Relay ANSI and CCITT.

The protocol must match the protocol sent by the network provider.

Configure framing mode

1. Choose **System > T1 Configuration**.
2. Select a framing mode from the pull-down list.
3. Click **Submit**.

A message indicates that service will be interrupted while the new interface is added.

4. Click **OK** to confirm.

T1 Interface Configuration

You can assign a name to each T1 interface, choose the protocol for the interface, choose a timing option, and use the LBO parameter to assign power and attenuation characteristics of the transmit signal from the EdgeMarc T1 interfaces.

The LBO setting is used to configure the power and attenuation characteristics of the transmit signal from EdgMarc T1 interfaces.

DS1 level settings are used when connecting an EdgeMarc T1 to a smartjack or telephone company provided T1. 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.

The DSX-1 level settings are used when connecting an EdgeMarc T1 to a private line or a co-resident PBX without a CSU/DSU. The DSX-1 settings can be changed based on the distance between the EdgeMarc and the terminating device.

Configure LBO

1. Choose **System > T1 Configuration**.
2. Select an LBO option from the pull-down list.
3. Click **Submit**.

A message indicates that service will be interrupted while the new interface is added.

4. Click **OK** to confirm.

Multiple DLCIs and Fractional T1 Links

When the protocol is a frame relay value, additional configuration values are needed. The mode value sets the equipment type, either DTE or DCE. Generally, this value will be 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. Values 0-15 and 1023 are reserved and should not be used.

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, you define a 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 a 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.

The next procedure describes how to configure multiple DLCIs and fractional T1 links.

Configure DLCIs and fractional T1

1. Choose **System > T1 Configuration** to open the T1 Configuration page.
2. Assign frame relay settings for multiple DLCIs and fractional T1 as described in “[Test UA Settings page](#)” on page 277.
3. Click **Submit**.



Note

For detailed field descriptions, see “[Test UA Settings page](#)” on page 277.

Configuring IP Phones, IADs or Softphones

After configuring the EdgeMarc device VoIP ALG the voice devices must be configured to point to the LAN interface of the EdgeMarc device as their signaling gateway and optionally as their TFTP server (if they use the TFTP protocol to retrieve their software images). The steps required to set up these devices differ from vendor to vendor. Using the DHCP server included in the EdgeMarc device will significantly simplify the setup of these devices if they are able to obtain their IP configuration via DHCP. Consult the applicable user's guide of each device for detailed instructions. For your convenience we have provided the configuration steps for a number of these devices in the support section of our website at: www.edgewaternetworks.com

DHCP Services

This chapter describes how to configure DHCP services with and without VLANs. You can relay DHCP requests to an external DHCP server or use the DHCP server included in the EdgeMarc appliance.

It contains the following sections:

- DHCP Relay
- DHCP Server
- DHCP Leases
- Configuring DHCP Server
- Configuring DHCP With VLANs This section describes using the DHCP Server capability on the EdgeMarc appliance with configured VLANs. The EdgeMarc appliances supports a maximum of 16 VLANs, all of which could be associated with the DHCP Server. The following are default VLAN IDs used on the EdgeMarc appliance:

DHCP Relay

When you enable DHCP relay and point to a valid DHCP server, you determine that all DHCP requests will be forwarded to that server.

Local DHCP and DHCP Relay are mutually exclusive. That is, 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.

Configure DHCP relay

1. Choose **DHCP Relay** from the Configuration Menu.
2. Configure parameters as described in “DHCP Relay Page” on page 172.
3. Click **Submit**.

A message indicates that service will be temporarily interrupted.

4. Click **OK** to confirm.

DHCP Server

DHCP is a protocol that enables PCs and workstations to get temporary or permanent IP addresses (out of a pool) from centrally administered servers. The EdgeMarc appliance can act as a DHCP server, granting IP addresses to devices in the network. You can configure blocks of IP addresses, default gateway, DNS servers, and other parameters that can be served to requesting devices. Table 1 lists the DHCP options supported by the DHCP Server.

Table 1 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	Allows the user to enter 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	Allows the user to enter 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.

DHCP on your system does not have to be enabled if a DHCP server exists elsewhere in your company network. It can be disabled. 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 using the Enable DHCP Server box without having to change other settings.

The DHCP IP Address Ranges table shows the dynamic addresses to use for the LAN devices. Enter individual DHCP IP addresses or a range. Assign static IP addresses for any common-access devices, such as printers or fax machines.

DHCP Leases

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

View DHCP lease information

- Choose **DHCP Server > DHCP Leases**.

Configuring DHCP Server

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

Configure DHCP

1. Choose **DHCP Server** to open the DHCP Server page.
2. Configure parameters as described in “[DHCP Server Page](#)” on page 173.
3. Click **Submit**.

A message indicates that service will be temporarily interrupted.

4. Click **OK** to confirm.

Configuring DHCP With VLANs This section describes using the DHCP Server capability on the EdgeMarc appliance with configured VLANs. The EdgeMarc appliances supports a maximum of 16 VLANs, all of which could be associated with the DHCP Server. The following are default VLAN IDs used on the EdgeMarc appliance:

- VLAN ID 1 (formerly 2730)-- used for management interface
- VLAN ID 500 -- used for voice
- VLAN ID 600 -- used for data



Note

To use DHCP with VLANs, the VLAN capability must be enabled and VLANs configured. To enable VLAN capability, refer to “[Configuring VLANs](#)” on page 9 or “[Network Page](#)” on page 169.

Once VLAN capability is enabled and VLANs configured, use the following procedure.

1. Select the VLAN to be used from the drop down list
2. Check **Enable DHCP Server**.
3. Add DHCP IP Address Ranges (Scope). In the DHCP IP Address Range table input the starting and ending IP address, then click **Add**.



Note

Click **Save** if you delete a VLAN, the DHCP Server must be re-enabled for the remaining VLANs.

Firewall

This chapter describes how to configure firewall features on the EdgeMarc appliance. It contains the following sections:

- Overview
- Configuring the Standard Firewall
- Configuring Advanced Firewall Settings
- Configuring Static Forwarding

Overview

The EdgeMarc appliance 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.

Users can define policies to filter traffics that traverse the device or administration traffics destined to the device.

Voice and video firewalls are implemented by VoIP Proxy. For more information on VoIP Proxy functions and configuration, see “[VoIP ALG](#)” on page 63.

The EdgeMarc supports two firewall versions:

- Standard Firewall—the standard (default) version of the firewall.
- Advanced Firewall—the advanced version of the firewall, which includes options for pre-defined policies and logging.

You can switch between the standard and advanced firewall by following the link provided at the bottom of each firewall page.

Configuring the Standard Firewall

Use the Standard Firewall page to configure settings for the default firewall.

Configure the standard firewall

1. Open the Standard Firewall page:
 - If the standard firewall is currently enabled (default), choose **Standard Firewall** from the Configuration Menu.
 - If the advanced firewall has been enabled, choose **Advanced Firewall** from the Configuration Menu, and then click the link at the bottom of the page to open the Standard Firewall page.
2. Enable the firewall by selecting the Enable Firewall checkbox.
3. Click **Submit**.
4. Select protocol and port options for the WAN firewall. To restrict the configuration to a specified set of addresses, enter the addresses in the Trusted Management Addresses area. Enter the forwarding rules that will apply to packets being forwarded to systems that run behind the firewall. For detailed field descriptions, see “Standard Firewall Page” on page 176.
5. Click **Submit**.

A message indicates that service will be interrupted while the new interface is added.
6. Click **OK** to confirm.

Configuring Advanced Firewall Settings

The Advanced Firewall page allows you to configure options for firewall policies, session control, and remote management. You can choose from a set of pre-defined policies and desired logging options.

Configure the advanced firewall

1. Open the Advanced Firewall page:
 - If the advanced firewall has already been enabled, choose **Advanced Firewall** from the Configuration Menu.
 - If the advanced firewall has not yet been enabled, choose **Standard Firewall** from the Configuration Menu, and then click the link at the bottom of the page to open the Advanced Firewall page.
2. Select **Enable** from the pull-down list to activate the firewall functionality.
3. Select logging options to apply when the firewall is enabled:
 - Log Denied Packet enables logging of packets that are blocked by the firewall.

- Log Allowed Packet enables logging of packets that are blocked by the firewall.
4. Select one of the Log Interface options:
 - WAN Only generates system log messages for traffic handling to and from the network/WAN interface.
 - LAN Only generates system log messages for traffic handling to and from the LAN interface (more resource-intensive).

**Warning**

Logging LAN traffic creates a large number of system log messages and affects the system's performance.

- WAN and LAN generates system log messages for traffic handling to and from the LAN and WAN interfaces. This option generates the maximum number of firewall rules, is very CPU-intensive, and should be avoided.
5. For Inbound Connection Rate Limit, select a rate in connections per second for inbound connections. This rate is used for automatic detection of denial of service (DoS) attacks from the public network. Packet requests to establish new sessions from the WAN to LAN that exceed this rate are temporarily denied. If this parameter is not defined, the default limit of 20 new sessions is used.
 6. For Outbound Connection Rate Limit, select a rate in connections per second for new outbound connections. This rate is used for automatic detection of denial of service (DoS) attacks from behind the firewall to the public network. Packet requests to establish new sessions from the LAN to WAN that exceed this rate are temporarily denied. If this parameter is not defined, the default limit of 20 new sessions is used.
 7. Select allowed outbound protocols.
 - For each checked protocol under Outbound protocols to be allowed, the firewall will allow sessions of that type to be created by LAN clients and will pass the inbound and associated outbound traffic through the firewall.
 - To enable any protocol not specifically mentioned, select **ALL OTHERS**.
 8. Click **Submit**.

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

Custom Rules

The Custom Rules page allows you to define additional rules for the advanced firewall that are not included in the NAT or port forwarding configuration. When configured, the custom rules are automatically loaded by the advanced firewall.

Configure custom firewall rules

1. Enable the advanced firewall, if it is not already enabled, and choose **Advanced Firewall > Custom Rules** from the Configuration Menu. See “[Configuring Advanced Firewall Settings](#)” on page 22.
2. Enter the custom rules, with each rule specified on a new line.
3. Click **Submit**.
A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

For sample rules, see “[Custom Rules Page](#)” on page 183.

Display custom firewall rules

1. Enable the advanced firewall, if it is not already enabled, and choose **Advanced Firewall > Show Rules** from the Configuration Menu. See “[Configuring Advanced Firewall Settings](#)” on page 22.
2. View the current rules.

Remote Management

The Remote Management Page allows you to specify the protocols that are permitted for management traffic and to restrict management access to defined subnets. You can access the Remote Management page from the System menu or by clicking the link in the Remote Management area of the Advanced Firewall page.

Configure remote management

1. Choose **System > Remote Management** from the Configuration Menu.
2. Configure parameters as described in “[Remote Management](#)” on page 266.
3. Click **Submit**.
A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

Configuring Static Forwarding

Forwarding rules define how the firewall forwards data traffic for a subnet from one interface to another. When forwarding a subnet, an IP address must be assigned to the system to serve as the default router for the subnet.

When forwarding, one address from the forwarded range of addresses must be assigned to the rule's output interface. The EdgeMarc appliance uses this address to

act as a gateway router for the subnet. The address may be assigned using the Subinterfaces page.



Note

The subnet and forwarded addresses are not protected by the firewall.

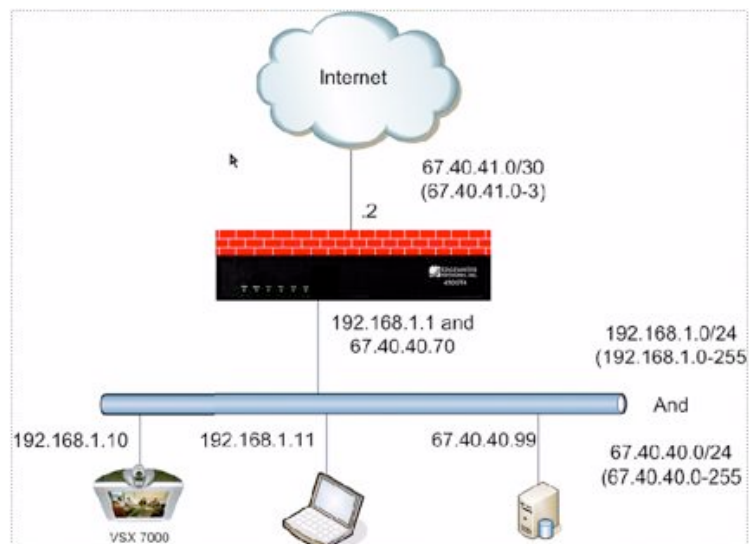
A similar method for forwarding traffic is provided by Proxy ARP. Proxy ARP is used to “bridge” addresses within a single subnet range from one interface to another. Often this is used to bridge and forward a public address to the protected side of the system without having to subnet the public address 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 forwarded data.

The following example shows how the feature is used.

- The ISP has supplied two separate subnets to the customer:
 - A small one (2 hosts) for the WAN link
 - A large one (254 hosts) for a bank of servers
- 67.40.41.2 is the WAN IP address for the EdgeMarc appliance.
- NAT is a private IP range of 192.168.1.xxx using the WAN address for PCs and Phones
- On the LAN side of the EdgeMarc appliance are the following:
 - Private IP subnet (192.168.1.xxx)
 - Public IP subnet (67.40.40.xxx)

This is shown in [Figure 1](#).

Figure 1 Static Forwarding



Note

The subnet and forwarded addresses are not protected by the firewall

Configure static forwarding

1. Choose **Standard Firewall > Forwarding Rules** or **Advanced Firewall > Forwarding Rules** from the Configuration Menu.
2. The Forwarding Rules page contains a Forwarding Rules table, which shows the list of defined forwarding rules. To select a single table entry, click the entry. To select all entries, click **Select: All**. To deselect all selected entries, click **Select: None**.
3. To delete one or more entries from the table, select the entry or entries and click the **Delete** button.

To add an entry to the table, configure parameters as described in [Forwarding Rules Page on page 186](#) and click **Add**.

This chapter describes how to configure Network Address Translation (NAT) on the EdgeMarc appliance. It contains the following sections:

- Overview
- Configuring NAT for the Standard Firewall
- Configuring Static NAT

Overview

Network Address Translation (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.

After traffic shaping, the packets undergo the NAT process, which maps the single public IP address of 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. This is a problem for IP phone devices that need to accept calls from the public network. To handle this issue, the system implements a call-agent proxy to map the common public address to unique private addresses.

For VoIP, the system restricts the UDP port range on the public side to the minimum required for the number of simultaneous calls desired. This is typically four times the number of sessions: an RTP port and RTCP port in both directions. This is done to minimize the UDP port range that must be opened when using an external firewall.

Additional security is provided by dynamically creating port mappings when a communication session is initiated and destroying them when a session is terminated. In addition to VoIP devices, the NAT function can be used for standard data applications and devices.

Dynamic and Static NAT

The EdgeMarc device supports dynamic NAT and static NAT. Dynamic NAT rewrites outbound packets' source addresses and ports to the device's WAN IP address and

dynamically allocated ports. Static NAT rewrites inbound packets' destination addresses and ports to addresses and ports of hosts behind the device.

Because NAT reuses public IP addresses and maps public address to private address and vice versa, users can access hosts with private address from the public network, or access public networks from hosts with private addresses. NAT also hides the internal network and protects the internal network from being exposed to the public networks.



Note

NAT can be used to translate the LAN IP addresses to the public routable IP address that is assigned to the WAN port.

NAT and Firewall Options

The available NAT options depend upon whether the standard firewall or advanced firewall is used.

- Standard firewall—Enable NAT on the LAN and configure static NAT client entries.
- Advanced firewall—Enable dynamic NAT and add any static NAT entries.

Configuring NAT for the Standard Firewall

The next procedure describes how to configure NAT for the standard firewall.

Configure NAT

1. Choose **Standard Firewall > NAT** from the Configuration Menu. For information on configuring the standard firewall, see “[Configuring the Standard Firewall](#)” on page 22.
2. Select the checkbox to enable NAT.
3. Enter the information in the format described in “[NAT Pages](#)” on page 189.
A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

Delete a NAT entry

1. Choose **Standard Firewall > NAT** from the Configuration Menu.
2. Delete the text for the NAT rule.
3. Click **Submit**.
A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

Configuring NAT for the Advanced Firewall

The next procedure describes how to configure settings to support dynamic NAT.

Configure dynamic NAT

1. Enable the advanced firewall, if it is not already enabled, and choose **Advanced Firewall > NAT** from the Configuration Menu. See “[Configuring Advanced Firewall Settings](#)” on page 22.
2. Select the Dynamic NAT checkbox, and click **Submit**.
A message indicates that service will be temporarily interrupted.
3. Click **OK** to confirm.

Configuring Static NAT

The next procedure describes how to configure settings to support static NAT.

Configure static NAT

1. If the standard firewall is used, choose **Firewall > NAT** from the Configuration Menu. If the advanced firewall is used, choose **Advanced Firewall > NAT** from the Configuration Menu.
2. Enter address and port information, as described in “[NAT Pages](#)” on page 189.
3. Click **Submit**.
A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

Delete a static NAT entry

1. Choose **Firewall > NAT** from the Configuration Menu.
2. Highlight the entry, and click **Delete**.
A message indicates that service will be temporarily interrupted.
3. Click **OK** to confirm.

Advanced Data Capabilities

This chapter describes how to configure advanced data capabilities on the EdgeMarc appliance. It contains the following sections:

- Configuring Certificates
- Configuring Dynamic DNS
- Configuring a DMZ Using Proxy ARP and Routed Subnets
- Configuring RADIUS
- Configuring TACACS
- Static Routes

Configuring Certificates

The Certificate page allows you to configure the device certificate used by HTTPS for secure remote management. To access the device via the WAN, HTTPS access must be granted through the firewall.

Configure certificate

To access the Certificate page, select **System > Certificate** from the Configuration Menu. This page includes the following fields:

1. Choose **System > Certificate**.
2. Configure parameters as described in [Certificate Page on page 249](#).
3. Click **Add**.

A message indicates that service will be interrupted while the new interface is added.

4. Click **OK** to confirm.

Configuring Dynamic DNS

Dynamic DNS allows a system administrator to associate a name with the public address of the system. When a change occurs to the public interface of the system, the Dynamic DNS service is notified of the change. Common uses for Dynamic DNS are

systems with a frequently changing public address (DHCP or PPPoE). Even systems with static addresses can use dynamic DNS to assign a name to a system.

Configure dynamic DNS

1. Choose **System > Dynamic DNS**.
2. Configure parameters as described in [Dynamic DNS Page on page 253](#).
3. Click **Add**.

A message indicates that service will be interrupted while the new interface is added.

4. Click **OK** to confirm.

Configuring a DMZ Using Proxy ARP and Routed Subnets

This section describes how to set up a DMZ using proxy ARP and routed subnets.

Proxy ARP

Proxy ARP is used 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. Proxy 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.



Warning

If an address is proxied, the system using the address should have a firewall or it should not be on the public network. In addition to proxying individual addresses, a range of addresses can be proxied by specifying a network netmask rather than a host netmask.

Configure proxy ARP

1. Choose **System > Proxy ARP**.
2. Configure parameters as described in [“Proxy ARP Page” on page 262](#).
3. Click **Submit**.

A message indicates that service will be temporarily interrupted.

4. Click **OK** to confirm.

Delete a proxy ARP entry

1. Select checkboxes for the entries that you want to delete. Click **Select: All** to choose all the entries or **Select: None** to clear your selections.
2. Click **Delete**.
A message indicates that service will be temporarily interrupted.
3. Click **OK** to confirm.

Configuring RADIUS

Remote Authentication Dial In User Service (RADIUS) is an authentication, authorization and accounting protocol that is used for management sessions with the EdgeMarc series appliances. If RADIUS authentication is configured, the EdgeMarc appliance 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.

The following screen shows RADIUS server configuration for the RADIUS server with IP address 192.168.12.2, using three server retries and the CHAP authorization mode.

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, as in the following example:

Sessions authenticated locally on the EdgeMarc appliance are identified with the string “System” in the login prompt. A sample http login using local authentication is shown in the following example:

Configure RADIUS

1. Choose **System > RADIUS Settings**.
2. Configure parameters as described in “[RADIUS Settings Page](#)” on page 264.
3. Click **Submit**.
A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

Configuring TACACS

Terminal Access Controller Access Control System (TACACS) is an authentication and accounting protocol designed for use with UNIX platforms. In TACACS authentication, a remote server supplies user login and password information to an authentication server. In TACACS accounting, detailed accounting information is sent to a remote server.

TACACS+ is a newer generation replacement for TACACS, which 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.

EdgeMarc Support for TACACS+ Authentication

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

- HTTP/HTTPS
- Console Login
- SSH
- Telnet

If TACACS+ is enabled, then the system prompts for user name and password whenever a user attempts to login in using the above-mentioned protocols. Upon receiving the user name and password, the EdgeMarc appliance 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 appliance.

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

- 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 Modes

The EdgeMarc appliance 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).

EdgeMarc Support for TACACS+ Accounting

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

Logging of GUI Interactions

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=attributevalue

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.

and so on.

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

TACACS+ and RADIUS

The EdgeMarc appliance supports use of TACACS+ or Remote Authentication Dial In User Service (RADIUS), but not both. 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.

Configuring TACACS+ Settings

This section describes how to configure TACACS+ on the TACACS+ Configuration Page. The page contains these checkboxes:

- a. Enable TACACS+ Authentication—Enables the TACACS+ authentication feature.
- b. Enable TACACS+ Logging—Enables the TACACS+ accounting feature.

Select the checkboxes for the TACACS+ features that you want to use.:

- a and b—Enable both authentication and logging
- a only—Enable authentication only
- b only—Enable logging only
- No selection—Disable both logging and authentication



Note

All of the other fields on the TACACS+ Configuration page apply to authentication and accounting, except TACACS+ Authentication Mode, which applies only to authentication.

Configure TACACS+

1. Choose **System > TACACS Settings**.
2. If want to use the authentication features, select **Enable TACACS+ Authentication**.



Note

An error message is presented if you attempt to enable TACACS+ while RADIUS is enabled. To disable RADIUS, choose **System > RADIUS Settings** from the Configuration Menu, clear the Enable checkbox, and click **Submit**.

3. Configure parameters as described in “**TACACS Settings Page**” on page 286.
4. Click **Submit**.
A message indicates that service will be temporarily interrupted.
5. Click **OK** to confirm.

Disable TACACS+ authentication

1. Choose **System > TACACS Settings**.
2. Clear the **Enable TACACS+ Authentication** checkbox.
3. Click **Submit**.
A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

Disable TACACS+ accounting

1. Choose **System > TACACS Settings**.
2. Clear the **Enable TACACS+ Logging** checkbox.
3. Click **Submit**.
A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

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

Use care when configuring static routes! Static routes may prevent the other networking features in the system from functioning properly.



Note

To configure routing to support the transfer of VoIP data for more than one subnet, see **“VoIP Subnet Routing”** on page 70.

Configure static routes

1. Choose **System > Route** to open the Static Routes page.
2. Select the Apply Route checkbox.
3. Enter address information, as described in **“Route Page”** on page 267.
4. Click **Submit**.
A message indicates that service will be temporarily interrupted.
5. Click **OK** to confirm.

Management

This chapter describes how to configure management capabilities on the EdgeMarc appliance. It contains the following sections:

- Trusted Management Addresses
- System Time
- Network Information
- Remote Management
- SNMP
- System message logging (syslog)
- System Information
- User Commands
- Message of the Day

Trusted Management Addresses

This section describes Trusted Management Addresses and discusses how to configure the capability in the firewall. Trusted Management Addresses define a list of trusted management host addresses or network/masks. All other addresses are blocked from accessing the device.

To configure Trusted Management Addresses use the following procedure.

Configuring Trusted Management Addresses

1. On the Configuration Menu, select **Firewall**.
2. Within the Trusted Management Addresses, enter a list of trusted management host addresses or network/masks.

The basic firewall rules will be applied only to the listed addresses. All other addresses will be blocked from accessing the device. If you do not include your management station, or a station to which you have access, you lose access to the appliance. You can only reinstate access by connecting to the serial console interface.

3. Press Submit.



Note

For more information on configuring the firewall, refer to “[Configuring the Standard Firewall](#)” on page 22 or “[Standard Firewall Page](#)” on page 176.

System Time

Use the System Time page to set the system's time or configure it to synchronize with a network time source via Simple Network Time Protocol (SNTP).

Set the system time

1. Choose **System > System Time**.
2. Choose one of the following methods to set the time:
 - To use SNTP, select the Enable SNTP checkbox, and enter the domain name or IP address of the SNTP server.
 - Enter the time manually.
3. Click **Submit**.

A message indicates that service will be interrupted while the new interface is added.
4. Click **OK** to confirm.



Note

For detailed field descriptions, see “[System Time Page](#)” on page 276.

Network Information

The read-only page Network Information page displays the low-level network configuration of the system. The display areas include Routing Information, Link Status, and Interface Information.

The system routing table contains the static routes for hosts and networks that are configured on the system. When the LAN and WAN settings have been fully configured, four routing lines are displayed. The order of the lines may vary depending on the subnet masks, but they include:

- The private subnet associated with the LAN interface
- A similar line for the WAN interface
- A line for the loopback interface
- The network default gateway forwarding to the WAN interface

Additional lines may be present, depending on the contents of the Route and VoIP Subnet Routing pages. Each entry on one of these pages causes an additional entry in the routing table.

View network information

1. Choose **System > Network Information** from the Configuration Menu.
2. View the settings as described in “[Network Information](#)” on page 258.

Remote Management

Remote Management allows you to specify the protocols that are permitted for management traffic and to restrict management access to defined subnets.



Note

At any time, you can logoff a listed remote or local user who has management access to the device. For more information, see [Enter the number of the assigned user that you wish logoff. A message is displayed confirming that the assigned user has been logged off. on page 138.](#)

Configure remote management

1. Choose **System > Remote Management** from the Configuration Menu.
2. Configure the settings as described in “[Remote Management](#)” on page 266.
3. Click **Submit**.
A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

SNMP

EdgeMarc appliances can be managed remotely by an SNMP network management system such as HP Openview. The EdgeMarc appliances support SNMPv1, v2, and v3 and the following MIBS:

- 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)

All MIB variables are read only. The SNMPv2-MIB variables sysContact, sysLocation and sysName can be set through the web GUI.

VOS 6.1 supports the configuration of multiple SNMP v1 and SNMP v2 trap destinations. The traps are sent to each of the configured destination using the appropriate protocol version and community string. SNMPv3 supports only one trap destination.

The EdgeMarc appliances send the following traps:

- coldStart
- authenticationFailure
- linkup
- linkDown

Configure SNMP

1. Choose **System > Services Configuration**.
2. To use SNMPv1, select the Enable SNMPv3 checkbox. By default, the agent-address field in SNMPv1 traps is set to the address of the interface that is used to send the trap. You can assign a custom IP address by entering a value in the SNMPv1 Trap Agent IP Address field.
3. To use SNMPv3, check the Enable SNMPv3 checkbox. Enter the user name, passphrase, security method, trap context, and destination trap IP address. The following security methods are supported:
 - None: No authentication and no Privacy
 - Auth(MD5): Authentication using MD5
 - AuthPriv(MD5/DES): Authentication using MD5 and Privacy using DES protocol
4. Configure other parameter on the page as described in “Services Configuration” on page 267.
5. Click **Submit**.

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

The figure below displays the EdgeMarc configuration for the SNMP Network setup shown in the figure y:

Services Configuration

[Help](#)

Customize the configuration of the services accessible on the System.

Enable SNMPv1:

SNMPv1 Read-Only Community:

SNMPv1 Trap Agent IP Address:

Trap Destinations:

IP Address	Version	Community	Delete
192.168.1.20	2	public	<input type="button" value="Delete"/>
192.168.1.30	1	public	<input type="button" value="Delete"/>
192.168.1.40	1	local	<input type="button" value="Delete"/>

Enable SNMPv3:

SNMPv3 User Name:

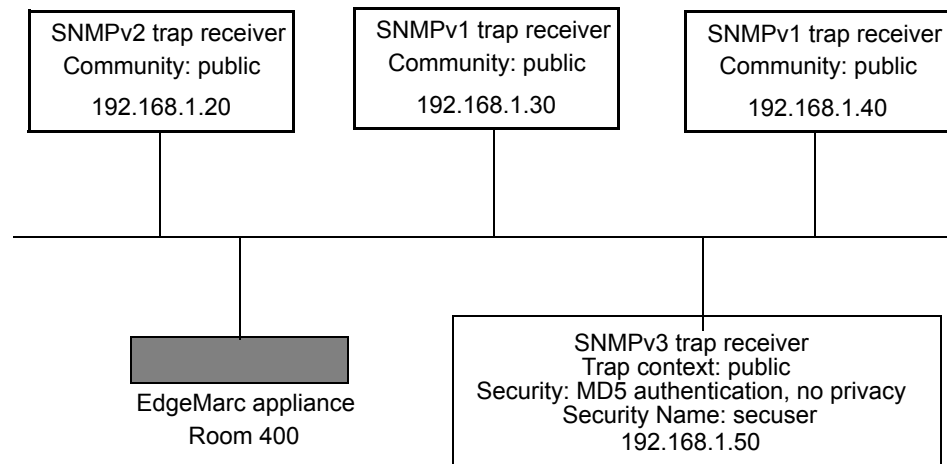
SNMPv3 Passphrase:

SNMPv3 Security:

SNMPv3 Trap Context:

SNMPv3 Trap Destination IP Address:

Figure 2 SNMP Configuration Example



Disable SNMP

1. Choose **System > Services Configuration**.
2. Clear the Enable SNMPv1 or Enable SNMPv3 checkbox.
A message indicates that service will be temporarily interrupted.
3. Click **OK** to confirm.

Delete an SNMP trap

1. Choose **System > Services Configuration**.
2. Click the wastebasket icon for the trap.
3. Click **Delete**.

System message logging (syslog)

You can configure remote systems to receive syslog messages from the EdgeMarc appliance.

Configure systems to receive syslog messages

1. Choose **System > Services Configuration**.
2. Check **Enable Remote System Logging**.
3. Enter the hostnames or IP addresses of the remote hosts (space-separated) and select the filter level, as described in “[Services Configuration](#)” on page 267.
4. Click **Submit**.

A message indicates that service will be temporarily interrupted.

5. Click **OK** to confirm.

The next figure shows how to assign the system with IP address 10.10.20.159 and the system with host name “remhost” as remote syslog hosts.

The screenshot displays the configuration interface for Syslog. It includes the following fields and controls:

- Enable Remote System Logging:** A checked checkbox.
- Remote Syslog Hosts:** A text input field containing "10.10.20.159". Below it is a note: "[Syslog Hosts are Space delimited]".
- Syslog filter:** A dropdown menu set to "Debug".
- Current Hostname:** A text input field containing "remhost".
- Set Hostname:** A text input field containing "remhost".
- Admin Inactivity Timeout (seconds):** A text input field containing "0".
- Enable MOS Scoring:** A checked checkbox.
- Current MOS Threshold:** A text input field containing "2.5".
- Set MOS Threshold:** A text input field containing "2.5".

At the bottom of the form are two buttons: **Submit** and **Reset**.

System Information

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

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.

The password for administrator web access is set on the Reset 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.

Configure network subinterfaces

1. Choose **System** from the Configuration Menu.
2. View the settings as described in “[Stateful Failover](#)” on page 272.

Read-only Users

You can configure a user with the user name *rouser* to have read-only access to the system. All information is displayed in a non-changeable form. Information changed in entry boxes cannot be submitted. In fact, most Submit and OK buttons are not visible when the read-only user logs in.



Note

You must have administrator privileges and log in as an administrator to change read-only user.

Enable a read-only user

1. Choose **System** from the Configuration Menu.
2. In the Read-Only Password area, click **changed**.



Note

All open web browsers must be closed when you change between administrative user “root” and read-only rouser.

3. Enter and confirm the password, which must be a minimum of six characters long.
4. Click **Submit**.
A message indicates that service will be temporarily interrupted.
5. Click **OK** to confirm.

When the system using the user name rouser and the configured password, all fields are read-only.

User Commands

The User Commands page allows you to enter specialized commands or enable features that are not available through other GUI pages. User commands are stored in the file `/etc/config/user_defs.conf`, as described in a number of Edgewater Knowledgebase articles. They are automatically executed whenever the box starts or a Network Restart is performed. User commands are commonly used to create user specific firewall and routing rules.

User Commands should only be entered when following instructions in an Edgewater Knowledgebase article or by request of the Edgewater TAC.

User commands:

```
ifconfig eth0:20 192.168.20.10 netmask 255.255.255.0
iptables -I POSTROUTING -t nat -s 192.168.20.10 -j ACCEPT
```



Caution

Take care when adding user commands. If an incorrect command is entered, the system may become unreachable.

Access the user commands page

1. Choose **System > User commands**.
2. Enter commands in the User Commands area. Enter each command on a new line.
3. Click **Submit**.
A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

It is recommended that you perform a network restart if you change other GUI pages after issuing performing user commands.

Message of the Day

The EdgeMarc appliance supports configuration of custom messages of the day (MOTD) for administrators who log in to the system console.

The following message types are supported:

- System Authorization Message of the Day—This message is presented to users before they log into the system. A typical message would warn users that access

is private and requires permission. Unauthorized users can be prompted to terminate the login session before attempting to log in.

- **System Greeting Message of the Day**—This message is displayed following successful login. A typical message would include a system greeting along with notification about important events or changes to the system.

Several methods are supported for system login to the EdgeMarc appliance. The choice of login method determines which of the configured messages are displayed:

- **Command line access through serial console connection**—The System Authorization and System Greeting messages are displayed.
- **Telnet or SSH access**—The System Greeting message is displayed, but not the System Authorization message.
- **HTTP/HTTPS**—Neither the System Authorization nor System Greeting message is displayed.

Configure message of the day

1. Choose **System > MOTD** from the Configuration Menu.
2. Enter text messages as described in [Message of the Day Page on page 188](#)
3. Click **Submit**.

A message indicates that service will be temporarily interrupted.

4. Click **OK** to confirm.



Note

For detailed field descriptions, see [Message of the Day Page on page 188](#).

This chapter describes how to configure virtual private networks (VPNs) on the EdgeMarc appliance. It contains the following sections:

- Overview and Examples
- Configuring VPN Settings

Overview and Examples

Multiple options are available to configure VPN and firewall for use with the EdgeMarc appliance. The available options described in this section depend upon the EdgeMarc device, VLAN configuration, and IP configuration.

- Non-VLAN switches, one WAN subnet
- Single LAN Ethernet and Separate PC and Phone Subnets
- Single LAN Ethernet and Same PC and Phone Subnet
- Non-VLAN Edgewater Appliance, Non-VLAN Switches, One WAN Subnet
- VLAN or Non-VLAN Edgewater Appliance, Non-VLAN Switches, Two WAN Switches
- Non-VLAN EdgeMarc Appliance
- VLAN-capable Ethernet switch, VLAN or Non-VLAN Edgewater Appliance
- Non-VLAN EdgeMarc Appliance
- Third Party Firewall in front of Edgewater Appliance

Non-VLAN switches, one WAN subnet

Use these configurations with non-VLAN switches and one WAN subnet are supported on the Edgewater appliances that VLAN. The following characteristics apply to these configurations.

- The EdgeMarc device provides NAT, Firewall and DHCP Plug ‘n Dial to phones.
- A third-party firewall provides NAT, Firewall and DHCP to PCs.
- The WAN interface has one free IP address. The EdgeMarc is assigned an IP address from the WAN subnet, while Other addresses, including the one already being used by the third-party Firewall/VPN device, are bridged through the EdgeMarc to its LAN interface.
- EdgeMarc LAN interface uses two VLANs:

- VLAN #2730 is used for the private subnet for phones (associated with EM LAN port 4). This LAN uses standard 802.1 frames.
- VLAN #2 with a public subnet for the 3rd-party VPN / Firewall device (associated with EdgeMarc LAN port 3). This LAN uses standard 802.1 frames.

These configuration options have the following limitations:

- Two two drops per cube or office are required.
- Because DHCP is used separately for PCs and phones, two broadcast domains (and two LANs) are required.

Single LAN Ethernet and Separate PC and Phone Subnets

These configurations are possible only on Edgewater appliances that provide VLAN support, such as the 4300 series appliances. The following characteristics apply to these configurations.

- The EdgeMarc device provides NAT and firewall capabilities to phones.
- A third party firewall provides NAT, Firewall and DHCP to PCs.
- The WAN interface has one free IP address. The EdgeMarc is assigned an IP address from the WAN subnet, while Other addresses, including the one already being used by the third-party Firewall/VPN device, are bridged through the EdgeMarc to its LAN interface.
- EdgeMarc LAN interface uses two VLANs:
 - VLAN #2730 is used for the private subnet for phones (associated with EdgeMarc LAN port 4). This LAN uses standard 802.1 frames.
 - VLAN #2 with a public subnet for the 3rd-party VPN / Firewall device (associated with EdgeMarc LAN port 3). This LAN uses standard 802.1 frames.

These configuration options have the following limitations:

- DHCP and Plug 'n Dial not available for phones
- Phones must be manually configured with IP addresses in the 10.10.10.0 subnet and a SIP Proxy or MGCP Control Server address of the EdgeMarc.
- This configuration is only possible on Edgewater appliances that provide VLAN support, such as the 4300 Series appliance.

Single LAN Ethernet and Same PC and Phone Subnet

These configurations are possible only on Edgewater appliances that provide VLAN support, such as the 4300 series appliances. The following characteristics apply to these configurations.

- EdgeMarc provides ALG functionality to phones.
- A third party firewall provides NAT, Firewall and DHCP to PCs and phones.
- Phones receive IP addresses from the same pool as PCs.
- The default router for PC and phones is the third party firewall.
- The EdgeMarc device is the SIP Proxy or MGCP control server to phones.
- The WAN interface has one free IP address:

- The EdgeMarc is assigned one IP address from the WAN subnet.
- Other address(es), including the one already being used by the 3rd-party Firewall/VPN device, are bridged through the EdgeMarc to its LAN interface.
- The EdgeMarc LAN interface uses two VLANs:
 - VLAN #2730 with private subnet for phones, and shared by PCs (associated with EM LAN port 4). This LAN uses standard 802.1 frames.
 - VLAN #2 with a public subnet for the 3rd-party VPN / Firewall device (associated with EM LAN port 3). This LAN uses standard 802.1 frames.

These configuration options have the following limitation:

- This configuration is only possible on Edgewater appliances that provide VLAN support, such as the 4300 Series appliance.

Non-VLAN Edgewater Appliance, Non-VLAN Switches, One WAN Subnet

The following characteristics apply to these configurations:

- EdgeMarc provides NAT, Firewall and DHCP Plug 'n Dial to phones
- A third-party firewall provides NAT, Firewall and DHCP to PCs
- The WAN interface has one free IP address:
 - The EdgeMarc is assigned one IP address from the WAN subnet
 - Other address(es), including the one already being used by the 3rd-party Firewall/VPN device, are bridged through the EdgeMarc to its LAN interface.

These configuration options have the following limitation:

- This configuration requires two drops per cube or office. DHCP is used separately for PCs and Phones, requiring two broadcast domains. Two broadcast domains means two LANs.

VLAN or Non-VLAN Edgewater Appliance, Non-VLAN Switches, Two WAN Switches

The following characteristics apply to these configurations:

- You must create two LAN-side VLANs:
 - One VLAN with a public subnet for the 3rd-party VPN / Firewall device (associated with EM LAN port 3).
 - One VLAN with private subnet for phones (associated with EM LAN port 1).
- VPN / Firewall device provides DHCP, Firewall and NAT to PCs and servers.
 - The VPN creates a third subnet (192.168.3.0, above), but it is ignored by the EdgeMarc and only used by the VPN and associated PCs.
- EdgeMarc provides Firewall and NAT to phones.

These configuration options have the following limitations:

- Plug ‘n Dial is not available for phones. Phones must be manually configured with SIP Proxy or MGCP Control Server address.
- This configuration is only possible on Edgewater appliances that provide VLAN support, such as the 4300 Series appliance.

Non-VLAN EdgeMarc Appliance

The following characteristics apply to these configurations:

- EdgeMarc provides DHCP, Firewall and NAT to phones
- VPN / Firewall provides DHCP, Firewall and NAT to PCs and servers

These configuration options have the following limitations:

- This configuration requires two Ethernet drops to each desk

VLAN-capable Ethernet switch, VLAN or Non-VLAN Edgewater Appliance

The following characteristics apply to these configurations:

- EdgeMarc provides NAT, Firewall and DHCP Plug ‘n Dial to phones.
- A third party firewall provides NAT, Firewall and DHCP to PCs:
- The WAN interface has at least one free IP address:
 - The EdgeMarc is assigned one IP address from the WAN subnet
 - Other address(es), including the one already being used by the 3rd-party Firewall/VPN device, are bridged through the EdgeMarc to its LAN interface.
- EdgeMarc LAN interface uses two VLANs:
 - VLAN #200 with private subnet for phones (associated with EM LAN port 2). This LAN uses 802.1q frames.
 - VLAN #2 with a public subnet for the 3rd-party VPN / Firewall device (associated with EM LAN port 3). This LAN uses standard 802.1 frames.

These configuration options have the following limitation:

- Requires VLAN-capable and CDP-capable Ethernet switch and phones.

Non-VLAN EdgeMarc Appliance

The following characteristics apply to these configurations:

- EdgeMarc provides NAT, Firewall and DHCP Plug ‘n Dial to phones
- A third-party firewall provides NAT, Firewall and DHCP to PCs
- The WAN interface has at least one free IP address:
 - The EdgeMarc is assigned one IP address from the WAN subnet
 - Other address(es), including the one already being used by the 3rd-party Firewall/VPN device, are bridged through the EdgeMarc to its LAN interface.
- EdgeMarc LAN interface uses two Subnets (over one LAN segment)

- Subnet 10.10.10.0/24 for phones (VLAN #200 within switch)
- Proxy ARP subnet 67.40.40.2/32 for the 3rd-party VPN / Firewall device (VLAN #2 within switch).

These configuration options have the following limitation:

- Requires VLAN-capable and CDP-capable Ethernet switch and phones.
- VLANs #2 and #200 share Ethernet segment at EdgeMarc

Third Party Firewall in front of Edgewater Appliance

The following characteristics apply to these configurations:

- External device provides port firewalling
- EdgeMarc provides Traffic Shaping (by having the servers, PCs and phones behind the EdgeMarc)
- EdgeMarc provides DHCP and NAT to PCs and phones
- EdgeMarc provides IP address passthrough from firewall to servers

These configuration options have the following limitation:

- This scenario is more complex than the above in that it requires the firewall to open ports necessary for VoIP protocol.

Dynamic WAN IP Address Assignment

In some network environments, it is necessary for the EdgeMarc device to use a dynamically assigned WAN IP address rather than a static address assigned by way of the EdgeMarc GUI.

Examples:

- WAN DHCP—The EdgeMarc device is connected via Ethernet behind a router that includes a DHCP server. This is common in small office/home office (SOHO) environments. The DHCP server assigns the IP address.
- PPPoE—The EdgeMarc device is connected via Ethernet behind a DSL router, and a Point to Point Protocol (PPP) session is terminated in the carrier network using a digital subscriber line access multiplexer (DSLAM). The DSLAM assigns the IP address to the EdgeMarc device.
- T1 PPPoFR, MLPoFR — The EdgeMarc device is connected using single or Multiple T1 interfaces running over frame relay. The dynamic WAN IP address is negotiated using the PPP protocol.

To support these environments, IPSec VPNs on the EdgeMarc device are now compatible with dynamic WAN IPs. Support includes the case in which the IP address changes on both ends of an IPSec tunnel.

The EdgeMarc device also supports dynamic WAN IPs if IPSec is not configured.

Example:

- An installation has a key system on the LAN side of a central EdgeMarc device, and IP phones or soft clients connect over the Internet through a remote EdgeMarc device without using VPN. When the WAN IP address on the remote

EdgeMarc device changes, the device can continue to send traffic using the new address. The ALG is not used and the voice traffic is treated as data. The IP phone re-registers using the new IP address so that the central-site key system can learn the new address of the remote device.

Support for dynamic IP addresses extends to NAT operations. Static NAT statements permit mapping between public IP:ports and private IP:ports. In the dynamic WAN IP environment, any change of WAN IP address now results in the updating of NAT table entries.

Example:

- A public IP:port 8080 is mapped to a private IP:port 80 webserver. If the WAN IP of the Edgemarc changes, the static NAT rules are automatically updated with the new WAN IP address.

When Dynamic DNS (DDNS) is used, the public IP of the EdgeMarc device is resolved using DNS. When the public IP changes, the DDNS client in the EdgeMarc device reports to the dynamic DNS server.



Note

If EdgeView is deployed, the EdgeMarc device updates EdgeView device by forwarding its MAC address, hostname and new IP address.

The following options are supported for configuration to support assignment of dynamic WAN IP addresses.

- WAN_IP only
- DNS only
- WAN_IP and DNS

where WAN_IP represents the WAN IP address of the EdgeMarc device, and DNS refers to the IP address of the remote VPN server.

Configuring VPN Settings

The VPN Configuration page allows you to create, configure, edit, and delete VPN tunnels.



Note

Only some EdgeMarc devices support VPN.

Add a VPN tunnel

1. Choose **VPN** from the Configuration Menu.
2. Click on the **Add Tunnel** button. The VPN Tunnel Settings page opens to display the configuration of the selected tunnel.
3. Configure settings as described in “[VPN Tunnel Settings Page](#)” on page 245.
4. Click **Apply**.

Modify a VPN tunnel

1. Choose **VPN** from the Configuration Menu.
2. Click on the tunnel name of the VPN tunnel that you want to modify. The VPN Tunnel Settings page opens to display the configuration of the selected tunnel.
3. Configure settings as described in “[VPN Tunnel Settings Page](#)” on page 245.
4. Click **Apply**.

Delete a VPN tunnel

1. Choose **VPN** from the Configuration Menu.
2. Select the tunnel and click the **Delete** button.

Voice Over IP

This chapter describes how to configure Voice over IP (VoIP) features on the EdgeMarc appliance. It contains the following sections:

- Traffic Management
- VoIP ALG
- VoIP Subnet Routing

Traffic Management

Traffic management is required to ensure high quality voice calls when both voice and data traffic share the same WAN link. Voice traffic must be prioritized for transmission over data traffic to meet the stringent jitter, latency, and packet loss requirements for toll-quality voice. By default, the EdgeMarc device:

- Automatically prioritizes voice traffic over data traffic to ensure toll-quality voice calls.
- Manages bandwidth using different upstream and downstream link speeds (for example ADSL).
- Maximizes WAN link utilization by allowing data traffic to burst up to full line rate in the absence of voice calls.
- Controls the data transfer rate of upstream TCP devices to limit WAN link congestion.
- Optimizes throughput for low-bandwidth WAN links (for example ADSL) by automatically adjusting the maximum transmission unit (MTU) and maximum segment size of IP datagrams during periods of WAN congestion.
- Supports network-based QoS applications by setting the TOS bits for all VoIP packets sent to the WAN and the LAN. TOS bits are used so that VoIP packets can be prioritized in the network by DiffServ enabled routers. The TOS bit value used by the EdgeMarc device is to “minimize delay and maximize throughput” or 8p hexadecimal. This value is set for all VoIP packets processed by the EdgeMarc device and overwrites any specific TOS bit configuration set by VoIP endpoints.
- Ensures that bandwidth allocated to new voice calls does not adversely affect the quality of existing active calls (call admission control or CAC).
- When deployed in an MPLS-based virtual private network, the EdgeMarc provides up to 8 priority queues that can accommodate multiple applications with different needs for bandwidth and priority.

To use traffic shaping, you must configure the incoming and outgoing physical link data rates for the bottleneck link in the network. The bottleneck most often occurs on the WAN link in the form of a T-1 or DSL line.

If Call Admission Control (CAC) will be enabled, you must first determine the number of calls that can be supported. 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. 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.

One example configuration would be a DSL line with physical data rates of 768/128 Kbytes. You would enter 768 in the WAN Downstream Bandwidth field and 128 in the WAN Upstream Bandwidth field. If CAC were enabled and the codec used was G.711, then the maximum number of calls supported would be one call. In this case, the upstream bandwidth is the limiting value.

Another example configuration would be a T1 line with physical data rates of 1544/1544 Kbytes. You would enter 1544 in the WAN Downstream Bandwidth field and 1544 in the WAN Upstream Bandwidth field. If CAC were enabled and the codec used was G.711, then the maximum number of calls supported would be 15 calls.

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.

Traffic shaping uses a combination of queues to both prioritize and smooth the media data. As packets pass through the system, they are marked as either high or low priority based. All packets are placed in a class-based queue. The two classes of data support by the queue are high and low. When data is available in the high priority queue, it is sent out at up to the configured upstream bandwidth. To smooth bursts from high speed data links (typically the LAN Ethernet), priority data is sent using a periodic queue that smooths the data and sends it at a rate that the slowest link can support. Non-priority data is sent when there is available bandwidth.

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 will be restricted to the bandwidth values assigned to them. In the case where multiple classes are exceeding the bandwidth values assigned to them but the WAN link is not yet saturated each class will be allocated the remaining unused bandwidth equally. This will continue until the WAN link becomes congested or saturated at which point the throughput for any class will fall back to its configured bandwidth.

If a class is not created for a DSCP value in use, all packets with that value will be sent to the class that has a DSCP value of Best Effort. Furthermore, 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

Since 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 auditable 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 4300T marks the ToS byte in the IP header as “High Priority,” and strips (set to 0) the ToS byte for all other traffic. Unchecking 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 it travels through the network.

For all real-time transport protocol (RTP) traffic (voice and video), the EdgeMarc 4300T marks the ToS byte in the IP header as High Priority, and strips (set to 0) the ToS byte for all other traffic. Unchecking 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

The EdgeMarc device 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 device by enabling CAC. When the EdgeMarc device 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 device. Check with your IT administrator to determine if this is the case.



Note

CAC is available in the EdgeMarc device 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 = (Maximum WAN upstream bandwidth * .85)/VoIP codec rate

where

Maximum WAN upstream bandwidth = value entered in the **WAN Upstream Bandwidth** field (in Kbps)

VoIP codec rate = 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 device 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.

Examples

The maximum number of G.711 voice calls supported by a T1 (1.544 Kbps) WAN is calculated as follows:

$$(1544 * .85) / 85.6 = 15.3 \text{ or } 15 \text{ total voice calls.}$$

The maximum number of G.711 voice calls supported by a 768Kbps SDSL WAN is calculated as follows:

$$(768 * .85) / 85.6 = 7.6 \text{ or } 7 \text{ total voice calls}$$

The maximum number of G.711 voice calls supported by an ADSL WAN with 768Kbps downstream WAN bandwidth and 256Kbps upstream WAN bandwidth is calculated as follows:

$$(256 * .85) / 85.6 = 2.5 \text{ or } 2 \text{ total voice calls}$$

The maximum number of G.729 voice calls supported by an ADSL WAN with 768Kbps downstream WAN bandwidth and 256Kbps upstream WAN bandwidth is calculated as follows:

$$(256 * .85) / 29.6 = 7.4 \text{ or } 7 \text{ total voice calls}$$

After determining the maximum number of voice calls, enable CAC as follows:

1. Click the **Enable Call Admission Control** checkbox.
2. Enter **Maximum number of calls allowed** as calculated above.
3. Click **Submit**.

Traffic Management in the EdgeMarc Device

The traffic management mechanisms provided by the EdgeMarc device 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 the case of 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 device VOS. As the EdgeMarc device processes packets they are marked as either high or low priority based on this configuration.

Upstream Traffic Management

The EdgeMarc device 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 device uses a buffer that clocks data out at a rate not exceeding the maximum amount for the slowest link. Any lasting burst condition will cause packets to be delayed and then dropped.

Downstream Traffic Management

In the upstream direction (LAN to WAN) it is easy to see how QoS mechanisms can be applied to traffic being sent by the EdgeMarc device to guarantee sufficient bandwidth for voice traffic. The EdgeMarc device has control over how packets are handed to the WAN interface. In the downstream direction (WAN to LAN) The EdgeMarc device 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. How then can we still guarantee the quality of voice traffic when it is entirely possible for an FTP session, for example, to consume the vast majority of downstream bandwidth?

Voice traffic quality can be guaranteed by shaping on both the egress LAN and egress WAN ports of the EdgeMarc device 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 device. Similarly, data traffic sent back to the EdgeMarc device 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.

For example, consider situation where no voice calls are being sent over an SDSL WAN link, and multiple FTP sessions are consuming all available bandwidth. In this situation:

- A new call request is received by the EdgeMarc device from the WAN.
- All signaling messages for the call are classified as voice traffic and prioritized for transmission over the LAN before servicing FTP data.
- RTP traffic is similarly classified as voice traffic and treated with priority.
- FTP data is buffered (or dropped) on the egress LAN port and ACKs are also delayed on the egress WAN port. This throttles the transmit rate of the FTP hosts to reduce overall WAN bandwidth consumption.

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

Priority IP Addresses

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 device.

Configure traffic shaping

1. Choose **Traffic Shaper** from the Configuration Menu.
2. Configure settings as described in “[Traffic Shaper Page](#)” on page 193.
3. Click **Submit**.
A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

VoIP ALG

An 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 must 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 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.

Configure ALG

1. Choose **VoIP ALG**.
2. Configure settings as described in [Advanced Traffic Shaper Page on page 196](#).
3. Click **Submit**.

A message indicates that service will be temporarily interrupted.

4. Click **OK** to confirm.

To configure a protocol for the VoIP ALG, select one of the following items under VoIP ALG on the Configuration Menu:

- [H.323 Configuration](#)
- [MGCP Settings](#)
- [SIP Settings](#)

SIP Settings

Use the SIP Settings page to configure SIP for the VoIP ALG.

Configure SIP settings

1. Choose **VoIP ALG > SIP** from the Configuration Menu.
2. Configure settings as described in [Advanced Traffic Shaper Page on page 196](#).
3. Click **Submit**.

A message indicates that service will be temporarily interrupted.

4. Click **OK** to confirm.

SIP Trunking

You can configure the following SIP trunking functions for the EdgeMarc appliance:

- [Dial String Manipulation](#)
- [Priority Redirection](#)

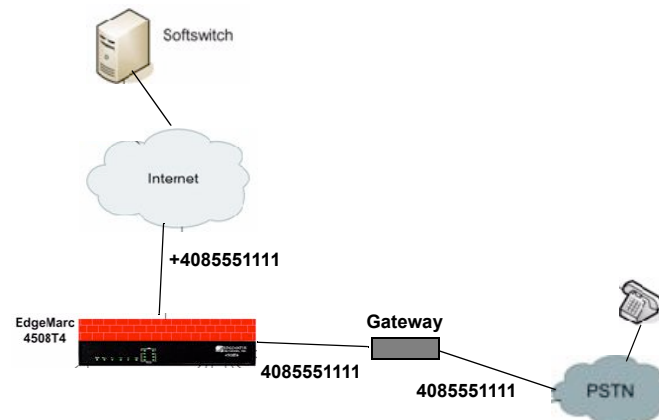
Dial String Manipulation

Outbound SIP trunking rules are now available to support dial string manipulation for outbound calls sent out to a network softswitch. Outbound rules allow a gateway to direct calls through the EdgeMarc appliance 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 3 shows how the SIP trunking rule works. A call comes in from the PSTN through a gateway to the EdgeMarc appliance. The gateway does not support + dialing, so the EdgeMarc appliance applies an outbound SIP trunking rule to prepend a + sign before forwarding the call to the Softswitch.

Figure 3 Outbound Dial String Manipulation



If you assign a particular gateway to multiple outbound SIP trunking rules. The EdgeMarc device 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 device 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 4. 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 appliance 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.



Note

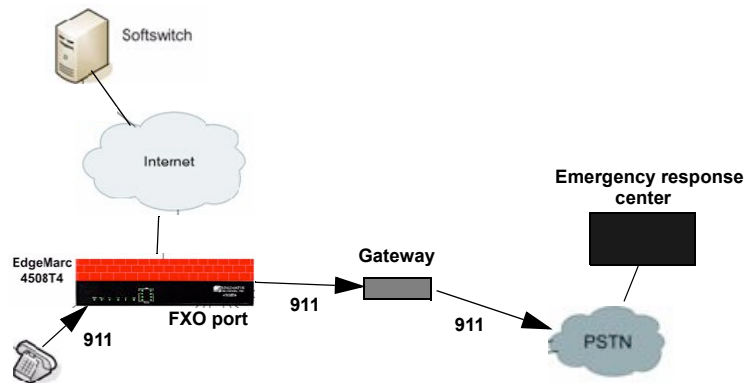
To configure priority redirection, use the SIP Trunking page, as described in “[SIP Trunking Page](#)” on page 218, and also enable Priority Calling services on the FXO/Line Configuration page, as described in “[SIP FXO/Line Port Configuration \(SIP GW\) Page](#)” on page 238.



Note

Priority calls do not support dial string manipulation. They must be sent through as-is.

Figure 4 Priority Redirection



Add a SIP trunking device

1. Choose **VoIP ALG> SIP > Trunking**.
2. In the Add a Trunking Device area, select **Add a new trunking device**.
3. Configure address and port information as described in “[SIP Trunking Page](#)” on page 218.
4. Click **Commit**.

The trunking device is added to the SIP Trunking Devices table on the page.

Delete a SIP trunking device

1. Choose **VoIP ALG> SIP > Trunking**.
2. Click the waste basket icon for the device you want to delete.

Add a SIP trunking rule

1. Choose **VoIP ALG> SIP > Trunking**.
2. In the Add a Rule area, select **Add a new rule**.
3. Configure parameters as described in “[SIP Trunking Page](#)” on page 218.
4. Click **Commit**.

Delete a SIP trunking rule

1. Choose **VoIP ALG > SIP > Trunking**.
2. Click the waste basket icon for the rule you want to delete.

H.323 Configuration

Use the H.323 Settings page to configure the H.323 protocol for the VoIP ALG. The H.323 Settings page includes the following areas:

- Gatekeeper Mode
- WAN/Provider-side gatekeeper mode settings
- LAN/Subscriber-side gatekeeper mode settings
- Embedded gatekeeper mode settings
- LRQ Size
- Default Alias
- Stale Time
- Multicast Messages
- H.460.18 Support
- Alias Restrictions

Configure H.323 settings

1. Choose **VoIP ALG > H.323**.
2. Configure settings as described in [H.323 Settings Page on page 204](#).
3. Click **Submit**.
A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

H.323 Activity

The H.323 Activity page is a read-only page that shows the following information:

- Current time
- WAN Gatekeeper status
- Current payload bandwidth
- Estimated total bandwidth
- Activity log of recent H.323 events

View H.323 activity

- Choose **VoIP ALG > H.323 > Activity**.

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 look-up is performed following alias manipulation.

Configure H.323 alias manipulation

1. Choose **VoIP ALG > H.323 > Alias Manipulation**.
2. Configure settings as described in [H.323 Settings Page on page 204](#).



Note

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.

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

H.323 Neighboring

Neighboring and prefix routing can be used to route calls based on a matching prefix in the destination alias of the call. The call decision is made following alias manipulation and acts on the modified string, similar to other call lookup processes such as registered client look-up. Each prefix is associated with a domain name or IP address that is used in the event that the prefix matches.

To access the H.323 Neighboring page (formerly the Prefix Routing page), select **VoIP ALG > H.323 > Neighboring** in the Configuration Menu.

Configure H.323 alias neighboring

1. Choose **VoIP ALG > H.323 > Neighboring**.
2. Select **Add a new prefix**.
3. Configure settings as described in [H.323 Neighboring Page on page 211](#).
4. Click **Commit**.
A message indicates that service will be temporarily interrupted.
5. Click **OK** to confirm.
6. The new entry is added to the table.

Delete an H.323 neighboring entry

1. Choose **VoIP ALG > H.323 > Neighboring**.
2. Click the waste basket icon for the entry you want to delete.

Regular Expressions

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 set of special expressions.

Alias manipulation patterns can match a sub-string at any location and number of 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.

Regular expressions are listed in [Table 3](#) and [Table 4](#) lists some example expressions.

Table 3 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, e.g. [a-z], [0-9]
()	Matches the literal string given, e.g. (abc)
	Matches the block on either side of the , e.g. 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.

Table 4 Example Regular Expressions

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.

Table 4 Example Regular Expressions (continued)

Expression	Description
#	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.

MGCP Settings

Use the MGCP Settings page to configure the MGCP protocol for the VoIP ALG

Configure MGCP settings

1. Choose **VoIP ALG > MGCP**
2. Configure settings in the following areas, as described in [MGCP Settings Page on page 213](#).
 - In the MCGP protocol area, configure settings for the softswitch where all client traffic will be forwarded.
 - In the Re-Registration area, configure automatic re-registration on behalf of the clients.
 - In the Audit Endpoint area, configure an audit endpoint, to allow the system to detect whether a client is still responsive.
3. Click **Submit**.

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

VoIP Subnet Routing

The EdgeMarc device acts as a proxy for network devices on its own subnet. Because network devices reside on the same subnet as the system, packets proxied by the ALG function and sent to the LAN do not require additional routing information.

Use the VoIP Subnet Routing page, to configure the server to proxy remote networking devices that are not on the same subnet. To system is limited to a total of 20 VoIP subnets.

These subnets reach the system via intermediate routers. The intermediate routers are configured to direct data from network devices to the system. In order for the system to send data to the intermediate router, a return path must be configured on the system.

Configure VoIP Subnet Routing

1. Choose **System > VoIP Subnet Routing**.
2. Configure settings as described in [VoIP Subnet Routing Page on page 290](#).
3. Click **Submit**.
A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

Configuring FXS and FXO Ports

This chapter describes how to use the FXS and FXO ports available on the EdgeMarc device. It contains the following sections:

- Overview
- Example Configurations
- Configuring FXO Ports
- Configuring T38 and G.711 Fax
- Configuring FXS Ports
- Gain Settings
- Configuring SIP Trunking
- Configuring FXS Hunt Group
- Calling Features for Analog Phones on the FXS port

Overview

Foreign eXchange Subscriber (FXS) and Foreign eXchange Office (FXO) are standard analog telephony interfaces 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.

The EdgeMarc appliance 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 appliance 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.

Survivability

The EdgeMarc survivability feature provides call control for local phones and a failover connection to the PSTN. If the connection to the Softswitch is lost, local calls can still be connected, and calls can be routed to the PSTN if the FXO ports are connected or a LAN-side gateway is used.

How Survivability Works

The EdgeMarc appliance creates a dial plan for survivability by monitoring the calls between VoIP endpoints and the network based Feature Server or Softswitch. When a local user dials a phone number, the EdgeMarc appliance collects all the keyed numerals and then sends a message to the Softswitch in the network. The Softswitch verifies that the call is a PSTN call, computes the destination, and arranges for the connection to be made. As part of this process, the local phones register with the Softswitch, and the EdgeMarc stores the registration information before sending it to the Softswitch. If the Softswitch or WAN link goes down, EdgeMarc has sufficient stored information to make connections between the local phones. This makes it possible for all the local phones to continue operating as if the Softswitch were still available.

In addition, if the WAN link is down, EdgeMarc appliance can also route calls destined for any non-local phone to the PSTN through its FXO ports. Up to two outbound calls can be made one time through the two FXO ports on the EdgeMarc appliance.

Session Initiation Protocol (SIP) Trunking

If an enterprise has multiple offices with associated PBXs in geographically separated locations, the EdgeMarc appliance can help provide lower cost service between the offices.

For multiple office connection support, an EdgeMarc appliance 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.

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 device 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.

Transmit/Receive Gain

You can configure the transmit and receive gain setting for each FXS port on the EdgeMarc device. Most devices will operate with the default 0dB Rx gain setting; however, if necessary, you can adjust the setting to interoperate with user endpoints such as phones, fax, or key systems.

It may be necessary to adjust the receive gain settings if, when a user endpoint device is hooked to the FXS port, the port is unable to detect the digits sent from the device. If this occurs, adjust the gain in steps of -4dB until the digits are detected.

Tx gain adjustments could be helpful to support devices that require a specific gain to decipher tones such as CNG or DIS, to support key systems that are connected to the FXS port, or for DTMF detection.

For FXS ports, the TX/RX gain settings will be adjusted at the user endpoint. TX will adjust the gain in the direction from IP WAN to the FXS port. RX will adjust the gain in the direction from the FXS port to IP WAN.

For FXO ports, the TX/RX gain settings will be adjusted at the WAN interface. TX will adjust the gain in the direction from the FXO port to the IP WAN. RX will adjust the gain in the direction from the IP WAN to the FXO port.

Priority Calling Support

Priority calling services provide for the routing of 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. **Note:** 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 SIP Trunking Rules page.



Note

Priority calling services cannot be configured when WAN Link Redundancy is enabled.

FXS Hunt Group

The FXS Hunt Group feature enables the EdgeMarc appliance 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 is returned to the calling party. The following characteristics apply to the Hunt Group feature:

- EdgeMarc can have only one hunt group consisting of all FXS ports.
- Hunt group is identified by a unique DID.
- The DID and authentication credentials are replicated for all ports.
- Supports sequential hunting only

Associated with the FXS Hunt Group feature is Dial-in-Prefix. In deployments where FXS is hooked up to a PBX, Dialed-in prefix provides a way to manipulate the incoming dial-pattern. If dial-in prefix matches the beginning of the incoming dial-string, then the prefix will be stripped from incoming dial-string before forwarding that dial-pattern to the PBX. This may be used to provide abbreviated dialing (i.e. 4 digit dialing). For example:

- If the dial-in prefix is 408555 and dial-in string is 4085551234, then after stripping, the dial-pattern given to the PBX will be 1234 (4-digit dialing).
- If the incoming dial-string is 4085551234 and no stripping occurs, the dial-pattern given to PBX is 4085551234 (10 digit dialing). This will also be the case when dial-in prefix is empty.



Note

For FXS Hunt Group configuration refer to **“Configuring FXS Hunt Group”** on page 88

Ad-Hoc Conferencing

The EdgeMarc appliance supports creating a conference by using ad-hoc SIP means, known as the Conference Factory URI (Conference URI on EM). The conference URI identifies a resource in the SIP/IP network that can handle conferencing and media mixing. Identifying the resource for ad-hoc conferencing is the ISP’s responsibility.

When EM is configured for ad-hoc conferencing, the FXS port uses this network based conferencing capability for 3-Party conferencing. If EM is not configured for ad-hoc conferencing, the FXS port does the local media mixing.

The following example depicts the operation of ad-hoc conferencing using Conference URI:

- Party on FXS port A has a need to 3-way conference with B and C
- Party A calls party B
- Party A puts party B on hold
- Party A calls party C
- Party A initiates a flash-hook and all three parties are put in conference

**Note**

To configure Conference URI refer to “**Configure advanced FXS/phone capabilities**” on page 83.

Example Configurations

The EdgeMarc 4500 series appliance supports these configurations using the FXS and FXO ports:

- IP Centrex Configuration
- SIP Trunking of Analog Ports Configuration
- SIP Trunking of IP PBX Configuration

IP Centrex Configuration

Figure 5 shows a typical configuration IP Centrex configuration.

- In this configuration, the EdgeMarc offers the following capabilities:
- Inbound and outbound dialing are supported.
- For inbound FXO calls, two-stage dialing and call forwarding are supported.
- The Real-time Transport Protocol (RTP) for local calls follows the shortest path directly from one phone to another.
- Calls can be routed out to the WAN side of the EdgeMarc appliance.
- With survivability enabled, it is still possible to route local calls if the WAN link goes down or the Softswitch is unreachable.

**Note**

In all the FXO configurations, the Softswitch must be configured to know that the EdgeMarc appliance is a PSTN gateway and PSTN calls can be routed back to the EdgeMarc appliance.

Figure 5 IP Centrex Configuration on the EdgeMarc Appliance

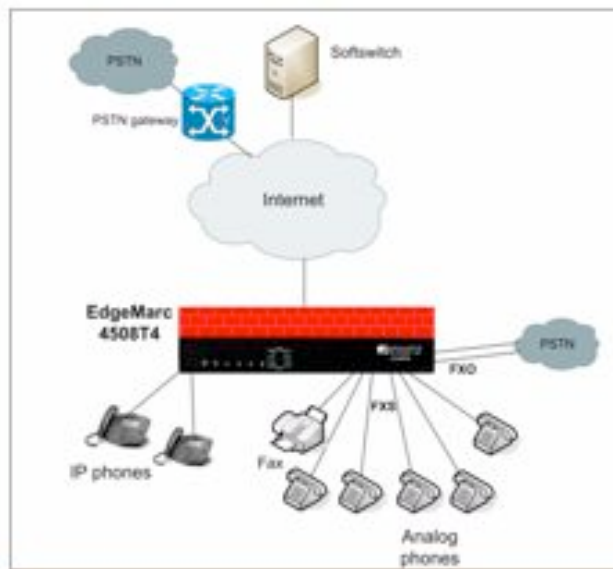
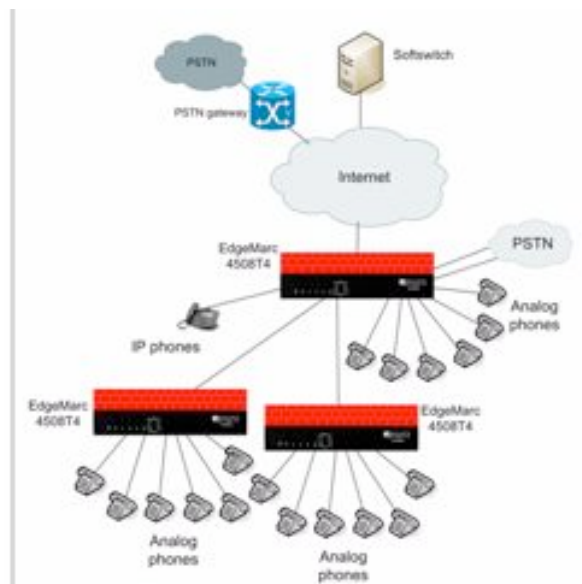


Figure 6 shows how the arrangement in Figure 5 can be expanded in a cascading model with multiple EdgeMarc devices. An EdgeMarc 4500 series appliance is connected to the WAN and also to the PSTN through its FXO ports. Additional EdgeMarc devices provide added FXS ports to service local phones.

Figure 6 Cascaded Model



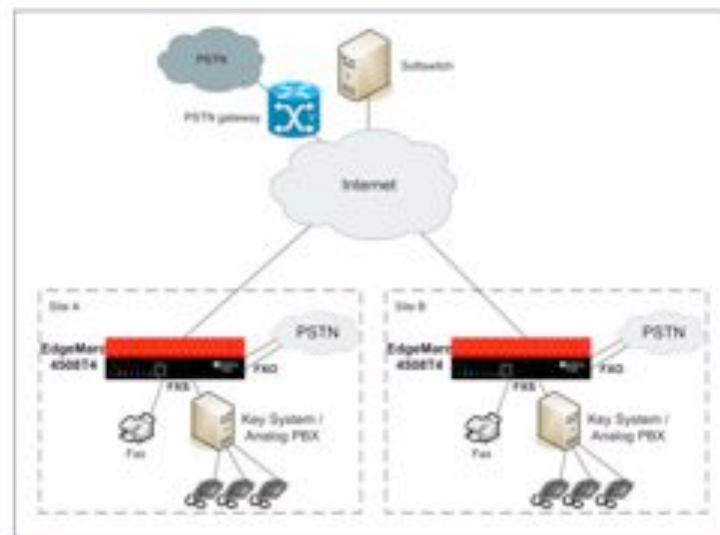
SIP Trunking of Analog Ports Configuration

Figure 7 shows a typical configuration in which the EdgeMarc appliance is used to connect analog or IP based key-systems and PBXs to SIP trunking services. The PBX or existing key system uses the FXS port on the EdgeMarc appliance.

In this configuration, the EdgeMarc offers the following capabilities:

- Inbound and outbound dialing are supported.
- For inbound FXO calls, two-stage dialing and call forwarding are supported.
- The RTP for local calls uses a shortest path rule directly between the two phones involved in a call.
- Calls can be routed out to the WAN side of the EdgeMarc appliance.
- With survivability enabled, it is still possible to still route local calls if the WAN link goes down or the softswitch is unreachable.

Figure 7 SIP Trunking of Analog Ports Configuration



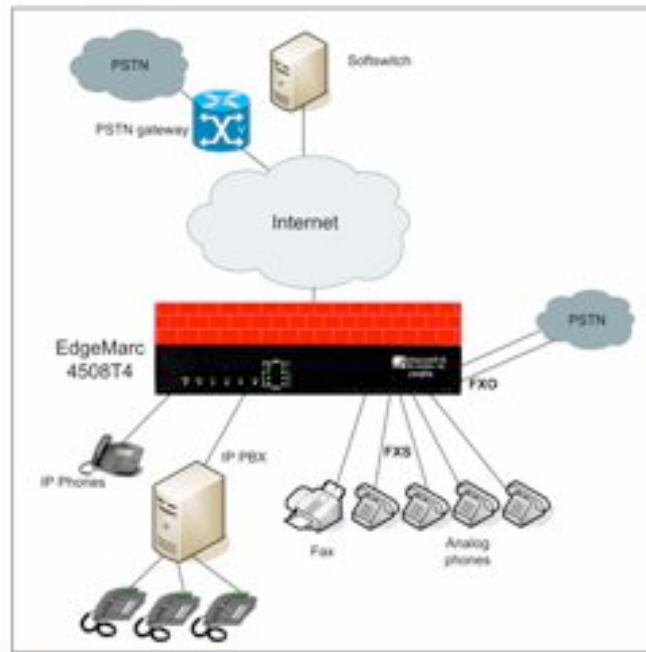
SIP Trunking of IP PBX Configuration

Figure 8 shows a typical configuration in which the EdgeMarc appliance supports SIP trunking dial plans to route PSTN calls out the FXO ports and multiple LAN side gateways. In the figure, an EdgeMarc 4500 series appliance is configured with two LAN side PSTN gateway and two FXO lines. Using the dial plans in the SIP trunking feature, you can now route calls through different gateways based on the rules specified in the dial plan.

In this configuration, the EdgeMarc offers the following capabilities:

- The IP PBX is Ethernet-connected.
- IP PBX does not need to register.
- Call are routed to the IP PBX using the Dial Plan.

Figure 8 Multiple LAN-Side PSTN Gateway Model with Dial Plans



Configuring FXO Ports



Note

Before configuring the FXO ports, verify that survivability is included with your license. To check the license information, click on the system on the left in the configuration menu and then click on the hyperlink in the "Registration Status" section of the web page.

This section describes how to configure the FXO ports on the EdgeMarc appliance to allow voice calls from IP networks to the PSTN.



Note

If the EdgeMarc 250W loses power, only the phone connected to Port 4 is enabled to send voice calls to the PSTN. FXS port 4 must have a phone connected for this feature to be used.

Configure FXO Ports

1. Choose **VoIP ALG > SIP** from the Configuration Menu to open the SIP Configuration page.
2. Enter the IP address and port of the SIP proxy, and click **Submit**.

3. Choose **SIP GW** from the Configuration Menu to open the SIP FXO/Line Port Configuration page. Refer to “**SIP FXO/Line Port Configuration (SIP GW) Page**” on page 240.
4. Select **Enable SIP FXO/Line Port Services**.
5. In the RTP silence delay field, enter a delay, or accept the default setting of 60 seconds. RTP silence delay is the interval used to monitor RTP silence during a call and determines if the PSTN party has been disconnected. If there is a continuous RTP silence for the configured number of seconds, then the FXO/Line port terminates the call.
6. By default, FXO/Line binds to the address of LAN with the last octet of address replaced with 253. For example, if the LAN IP address is configured as 192.168.1.1, the FXO/Line takes the address 192.168.1.253. If the assigned address conflicts with any device on the LAN, then override the FXO/Line the address by entering an address in the SIP GW IP field.
7. Select **Enable Priority Calling Services** to allow special treatment for calls designated as high priority.
8. Enter Callback Extension number.



Note

Enabling ‘Priority Calling Services’ sends all calls to the Callback extension, thus overriding the following settings for individual ports: ‘Enable InBound(from PSTN) two stage dialing’ and ‘Forwarded To’. In addition to enabling priority calling, you must define rules that determine which calls are given priority. See “**Configuring SIP Trunking**” on page 84.

9. Configure the following for each port that will be used:
 - Select **Enable FXO port**.
 - Enter a name and password in the SIP Authentication Name and Password fields only if the SIP FXO/Line port needs to be authenticated.
 - Select **Enable InBound (from IP network) two stage dialing** to allow two-stage dialing for incoming calls from the IP network.
 - Select **Enable InBound (from PSTN) two stage dialing** to allow two-stage dialing for incoming calls from the PSTN and enter the forwarding number in the Forwarded to field.
10. Click **Submit**.
11. Choose **VoIP ALG > SIP Trunking** from the Configuration Menu to open the SIP Trunking page.

The SIP Trunking page includes an entry for the FXO ports in the SIP Trunking Devices table. A default rule should also be included to route all calls to this gateway. If you do not see a default rule, you must create one.
12. Add a Target:
 - Select **Add new target**.
 - Enter a logical name to identify the gateway
 - Enter the IP address of the gateway
 - Keep the default
13. Define a default rule, if one is not already defined:

- Select **Add new rule**.
- Select **Default Rule**.
- Add the pattern match for routing calls through the target gateway.
- Enter the number of digits to be stripped, if any, from the front of the called number if the pattern matches.
- Select the target gateway from the Target pull-down list.

14. Click **Commit**.

The FXO ports are now configured. If survivability is enabled on the EdgeMarc and the Softswitch is unreachable, then the FXO ports can act as a LAN side gateway.

Configuring T38 and G.711 Fax

You can send and receive T38 Fax on FXS port 1 or port 2 on the EdgeMarc appliance. On all the other FXS ports, only G.711 Fax can be send or received.

Configure T38 Fax Settings

- 1.** Choose **SIP UA > Fax** from the Configuration Menu to open the FXS/Phone Port Fax Settings page.
- 2.** Configure the settings as described in [FXS/Phone Port FAX Settings Page on page 236](#).
- 3.** Click **Submit**.

Configuring FXS Ports

This section describes how to configure the FXS ports on the EdgeMarc appliance.



Note

For the EdgeMarc 200 Series, FXS port 1 is connected to the FXO port 1 when the power is off

Configure FXS Ports

- 1.** Choose **VoIP ALG > SIP** to open the SIP Settings page.
- 2.** Enter the IP address of the VoIP provider, and click **Submit**.
- 3.** Choose **SIP UA** from the Configuration Menu to open the FXS/Phone Port Settings page.
- 4.** Configure up to six ports, as described in [FXS/Phone Port FAX Settings Page on page 236](#).
- 5.** Click **Submit**.

It may be necessary to choose SIP UA link again from the Configuration Menu to refresh the page and see the Port Configuration state change from Unregistered to Registered.

A message indicates that service will be temporarily interrupted.

6. Click **OK** to confirm.

**Note**

If the state is still unregistered, check with your VoIP provider to confirm that the Authentication Name and Password is valid.

You can now make and receive calls on the phones that are connected to the configured FXS ports.

Configure advanced FXS/phone capabilities

1. Choose **SIP UA > Advanced** from the Configuration Menu.
2. Configure parameters as described in “**FXS/Phone Port Settings - Advanced Page**” on page 231.

3. Click **Add**.

A message indicates that service will be interrupted while the new interface is added.

4. Click **OK** to confirm.

Gain Settings

Use the next procedure to configure transmit and receive gain settings.

Configure gain settings

1. Choose **SIP UA > Advanced** from the Configuration Menu to open the SIP FXO/Line Port Configuration page.
2. Scroll down to the section for the port that you want to configure.
3. Select gain settings from the Analog Receive Gain and the Analog Transmit Gain pull-down lists, as described in “**FXS/Phone Port Settings - Advanced Page**” on page 231.

4. Click **Submit**.

A message indicates that service will be temporarily interrupted.

5. Click **OK** to confirm.

Configuring SIP Trunking

SIP trunking can be used to configure dial plans or rules to route calls from the softswitch/IP-PBX to client devices that do not register. Each rule points to a device that should receive matching calls, based on the called SIP URI. 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) will be used to match the call.

**Note**

Messages from SIP clients (including trunking devices) are always forwarded to the SIP ALG configured soft-switch/IP-PBX.

SIP Trunking Devices

The available SIP trunking devices must be added to this list. Each device must be configured with its IP address and port number. It can be optionally named to make it easier for the user to associate the entry with the device.

If internal FXO ports are available on appropriate platforms and enabled, they will act as a default device unless configured otherwise.

Rules

Rules match incoming calls to a specific device. A rule is written with a number of explicit digits or pattern that match a range of digits.

**Note**

A default rule can not have a dial string for matching. There can be only one default rule.

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 in the case of a match. Likewise, a string of digits to add will be added to the dialed number in case the rule matches.

Table 5 Matching Patterns for SIP Trunking

Pattern	Description
.	Matches one or more digits.
[x-y]	Matches any single digit between x and y (inclusive). 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]

Examples:

1XXX	Matches any four-digit number starting with 1, e.g. 1000, 1200, 1234
9NXXXXXX	Local calls preceded by a 9, e.g. 95551234
91NXXNXXXXXX	Long distance calls preceded by a 9, e.g. 914085551234
XX	

Priority Redirection

In priority redirection, priority calls are directed to a designated gateway (which can be an FXO port on the EdgeMarc device). If all FXO ports are busy and if any of them is being used for a non-priority call, that call is dropped and one of the FXO ports is freed to make room for the priority call.

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 9](#). 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 FXS port on the EdgeMarc appliance 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.

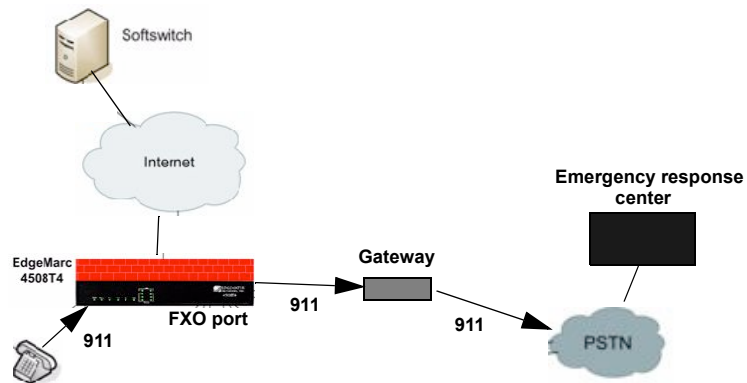
RESTRICTION: Priority calls do not support dial string manipulation. They must be sent through as-is.

FURTHER RESTRICTION: Redirect operations are only performed for SIP INVITE messages. As a result, mid-call features such as transfer, hold or conference may not function as expected.



Note

To configure priority redirection, use the [SIP Trunking](#) page, as described in the section, and also enable Priority Calling services on the [FXO/Line Configuration](#) page, as described in [Configuring FXO Ports on page 80](#).

Figure 9 Priority Redirection

Configuring SIP Trunking Enhancements

This section describes how to configure the SIP trunking enhancements.

Configure SIP trunking enhancements

1. Choose **VoIP ALG > SIP > Trunking** to open the SIP Trunking Configuration page.
2. In the Add a Rule area, select **Redirect** from the Type pull-down list.
3. Configure the rule as described in [SIP Trunking Page on page 220](#).



Note

You cannot specify digits to be stripped or strings to be added in priority rules.

4. Select a gateway from the Trunking Device pull-down list.
5. Click **Commit**.

Distinctive Rings

The EdgeMarc converged network appliance is shipped with five distinctive ring patterns (Ring0 - Ring4) that are available for use when ringing an analog phone on the FXS/phone port. The appliance can automatically select a ring pattern based on the number that is being called or the number that originated the call.

By default, the appliance is configured to use Ring0 for all calls. You can assign different ring patterns based on the following types of rules:

- 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.

Add a distinctive ring pattern rule

1. Choose **SIP UA > Distinctive ring** to open the FXS/Phone Port Distinctive Ring configuration page.
2. Select **Add new rule** from the pull-down list.
3. Enter a pattern in the Caller-Pattern-match field, the Called-Pattern-match field, or both. See **“Pattern Matching Rules”** on page 87 for a description of the matching symbols.
4. Select the ring pattern.
5. Click **Commit**.



Note

For detailed field descriptions, see **“Distinctive Ring Page”** on page 239.

Modify a distinctive ring pattern rule

1. Choose **SIP UA > Distinctive ring** to open the FXS/Phone Port Distinctive Ring configuration page.
2. Choose the rule to modify from the Action: pull-down list.
3. Modify the pattern in the Caller-Pattern-match field, the Called-Pattern-match field, or both. See **“Pattern Matching Rules”** on page 87 for a description of the matching symbols.
4. Select the ring pattern.
5. Click **Commit**.

Delete a distinctive ring pattern rule

1. Choose **SIP UA > Distinctive ring** to open the FXS/Phone Port Distinctive Ring configuration page.
2. Choose the rules to delete from the checkboxes to the left of the rules. **Select: All** selects all the rules; **Select: None** deselects all the rules.
3. Click **Delete**.

Pattern Matching Rules

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.

Rules can include a mix of the digits and patterns listed in [Table 6](#).

Table 6 Number Patterns

Pattern	Description
.	Matches one or more digits.
[x-y]	Matches any single digit between x and y (inclusive). 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]

[Table 7](#) lists some example rules.

Table 7 Example Rules

Caller Pattern match	Called Pattern match	Ring ID	Description
.	408.	1	If any call goes to an FXS/Port extension that starts with 408, ring the phone with Ring 1.
408.	.	3	If the call is from a caller with a number that begins with 408 and is destined for any FXS/Port extension, ring the phone with Ring 3.
.	91NXXNXXXXXXXX	4	if a call is a long distance call (called phone number begins with 91), and terminates on the analog FXS/Phone port, ring the phone with Ring 4.

Configuring FXS Hunt Group

The EdgeMarc appliance could be implemented with the FXS ports connected to analog phones or a PBX. In either implementation, if EM is configured for Hunt Group, softswitch would be route calls to EM using the Hunt Group's unique DID. When EM receives the call from the IP network, it will use the Dial Rules to match the DID and forward the calls to the hunt group.

Use the following guidelines to configure FXS Hunt Group on the EdgeMarc appliance:

- Designate a unique DID for the hunt group (i.e., 408-555-1234)
- Configure FXS/Phone Basic Settings

- Configure SIP Trunking
- Enable Hunt Mode
- Configure Dial-in-Prefix (optional)
- Define an FXS Port to a Hotline Number

Configure FXS/Phone basic settings

1. Choose **SIP UA** from the Configuration Menu to open the FXS/Phone Port Settings - Basic page.
2. Configure the ports, as described in [FXS/Phone Port Settings - Basic \(SIP UA\) Page on page 230](#).
 - a. Enter display name (unique DID)
 - b. Enter username (unique DID)
 - c. Enter authentication name (unique DID)
 - d. Password (if applicable)
3. Click **Submit**.

It may be necessary to choose SIP UA link again from the Configuration Menu to refresh the page and see the Port Configuration state change from Unregistered to Registered.

A message indicates that service will be temporarily interrupted.

4. Click **OK** to confirm



Note

All ports should have the same information

Configure SIP - Trunking

1. Add a device (i.e., Hunt Group). Choose **VoIP ALG> SIP > Trunking**.
2. In the Add a Trunking Device area, select **Add a new trunking device**.
3. Configure address and port information as described in [“SIP Trunking Page”](#) on page 220.
4. Click **Commit**.

The trunking device is added to the SIP Trunking Devices table on the page.
5. Add a rule that will route any inbound traffic matching the unique DID for Hunt Group to the FX ports. All other traffic should use the default.
 - a. Choose **VoIP ALG> SIP > Trunking**.
 - b. In the Add a Rule area, select **Add a new rule**.
 - c. Configure parameters as described in [“SIP Trunking Page”](#) on page 220.
 - d. Click **Commit**.

Enable Hunt Mode

1. Choose **SIP UA > Advanced** from the Configuration Menu.
2. Click **Enable Hunt** as described in “**FXS/Phone Port Settings - Advanced Page**” on page 231.

3. Click **Add**.

A message indicates that service will be interrupted while the new interface is added.

4. Click **OK** to confirm.

Configure Dial-in-Prefix

1. To configure Dial-in-Prefix see “**FXS/Phone Port Settings - Advanced Page**” on page 231



Note

If EM is deployed with FXS ports connected to a PBX, Dial-in-Prefix is an optional configuration.

Define an FXS Port to a Hotline Number

1. Choose **SIP UA > Advanced** from the Configuration Menu.
2. Enter the hotline number in the Hotline Number field. This field is located in the port level configuration section of the FXS port to be defined as a hotline number.
3. Click **Submit** to activate the hotline number.

Calling Features for Analog Phones on the FXS port

All EdgeMarc platforms running VOS 7.x or later support the following mid-calling features for analog phones connected to the FXS port on the EdgeMarc:

- Call hold
- Call Transfer – Unattended
- Call Transfer – Attended
- Call Waiting
- 3-Way Calling

Call hold

1. When in a call perform a flash-hook to hold the call.
2. Press the flash-hook again to resume the call.

3. A on-hook action will end the call.

Call Transfer – Unattended

1. Phone A and Phone B are in call.
2. Phone A presses flash-hook to place Phone B on hold.
3. Phone A receives dialtone, enters the Phone C number and hangs up to transfer the call to Phone C. This also results in Phone A call hang-up.

Call Transfer – Attended

1. Phone A and Phone B are in call.
2. Phone A presses flash-hook to place Phone B on hold.
3. Phone A receives dialtone, enters Phone C number, talks to Phone C and hangs up to transfer the call to Phone C.
4. This also results in Phone A call hang-up.

Please note the following:

- If Phone A hangs up within 3 seconds of completing the dial, the call will be treated as an unattended transfer, and generate a REFER to Phone C.
- If Phone A remains on the line, the call is treated as a consultative transfer, and generate an INVITE to the new number. Phone A should hear a ring-back to indicate that the Phone C is being rung.
- If Phone A hangs up after this point, the call is cancelled and the Phone C gets hung up. Phone B should get hung up too.

Call Waiting

1. Phone A and Phone B are in call.
2. Phone C calls Phone B. Phone B presses cradle hook/flash hook to connect to Phone C.
3. Then presses cradle hook/flash hook to switch back on call with Phone A.

3-Way Calling

There are two ways to perform 3-way calling:

Method 1

1. Phone A and Phone B are in call.
2. Phone A presses the "flash-hook", Phone B is put on hold, Phone A gets dial tone.

3. Phone A dials Phone C number, in call with Phone C, and then Phone A presses flash-hook OR enters “#3” to initiate 3-way conference between Phone A, Phone B & Phone C.
4. If Phone A performs a flash-hook before Phone C answers but after the call rings Phone A will return to the original call with Phone B.

Method 2

1. Phone A and Phone B are in call.
2. Phone C calls Phone B. Phone B presses cradle hook/flash hook to connect to Phone C.
3. Phone B can switch between Phone A and Phone C by pressing cradle hook/flash.
4. Phone B can conference all parties together by pressing “#3”.



Note

When Phone A hangs up, Phone B & Phone C will terminate and get busy tone. But if Phone B or Phone C hangs up, then Phone A will still be in call with active caller.

CODER Behavior

Following behavior applies to the local mode 3-way calling:

1. If an analog phone on one of the FXS ports is engaged in a call and wants to add another party (including an analog phone on one of the FXS ports) to perform a 3-way call and all the other phones on the remaining FXS ports are off-hook, the system terminates the 3-way call and the first party is connected back to the initiator of the 3-way call as an indication that the 3-way call did not go through.
2. For models containing FXS ports, FXS ports 1 and 2 can not simultaneously participate in the same 3-way call, except for model 4508E where multiple FXS ports from ports 1 through 4 can participate in the same 3-way call. Similarly multiple FXS ports from ports 5 through 8 can participate in a 3-way call, but FXS ports from both of these groups can not simultaneously participate in the same 3-way call.

If a free FXO port is selected, that port is marked as busy and will not engage in any PSTN trunking.

This chapter describes how to configure the EdgeMarc appliance as a wireless access point. It contains the following sections:

- [Overview](#)
- [Configuring Wireless Settings](#)
- [Configuring VLAN Settings to Support Wireless Traffic](#)

Overview

The EdgeMarc appliance can be configured as a access point to provide wireless communications for network clients. The EdgeMarc appliance supports the following wireless modes:

- 802.11a
- 802.11b
- 802.11g
- 802.11b/g

When the wireless option is enabled and VLANs are also enabled, a bridge is automatically set up between the wireless connection and a selected VLAN, and the VLAN traffic travels over the wireless link. If VLANs are not enabled, the wireless connection is automatically bridged to eth0.

Security

The EdgeMarc appliance supports Wi-Fi Protected Access security with the pre-shared key (WPA-PSK) security option.

WPA is the family of current-generation wireless security solutions. WPA incorporates improved algorithms and options that are more secure against compromise than earlier generation security solutions. The EdgeMarc appliance supports WPA with pre-shared keys (WPA-PSK), which offers the advantages of the WPA algorithms without the need for an external authentication server.

For encryption, the EdgeMarc appliance supports Temporal Key Integrity Protocol (TKIP).

In WPA-PSK security, a common security key is entered into each network device. When a client requests association to the EdgeMarc appliance using WPA-PSK,

initial authentication is based on the common shared key. During the time that the connection is in place, the devices are synchronized frequently, with the keys automatically changing at each synchronization. The synchronization time is configurable; the default is 3600 seconds.

Service Set Identifiers

Each wireless network is identified by the service set identifier (SSID), a unique name for the network. Client devices select the wireless network established by the EdgeMarc appliance by choosing the SSID that is configured in the EdgeMarc appliance. The EdgeMarc appliance is shipped with the default SSID EWNxxxxxx, where xxxxxx represents the last 6 digits of the appliance's MAC address. The SSID must be no more than 32 characters, and is case-sensitive.

By default, the EdgeMarc device broadcasts the SSID in its wireless beacon, and clients can see the SSID as they scout for available wireless networks. You can opt to disable the SSID broadcast, in which case the clients do not see the SSID as they scan for networks, and they must know the SSID to be able to associate to the EdgeMarc appliance.

Channels and Power Levels

The available multiple radio frequency (RF) channels depend upon the 802.11 wireless mode.

- 802.11a: 36, 40, 44, 48,52, 56, 60, 64.
- 802.11b/g: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11.

The default is 802.11b/g, channel 6.

The power levels for the EdgeMarc appliance radio are configurable. It is best to choose a power level that is high enough to reach the target clients, but not higher than necessary. [Table 8](#) shows the power settings on the EdgeMarc appliance and the associated power levels. The default is 4 (13dBm).

Table 8 Radio Power Settings and Levels

Power Setting	Power Level
1	10dbm
2	11dBm
3	12dBm
4	13dBm (default)
5	14dBm
6	15dBm
7	16dBm
8	17dBm

Table 8 Radio Power Settings and Levels (continued)

Power Setting	Power Level
9	18dBm
10	19dBm

Wireless Status

A link on the Network configuration page indicates whether wireless support is currently enabled. Clicking the underlined [Configure Wireless](#) link opens the Wireless screen and displays the configuration settings.

Configuring Wireless Settings

This section describes how to configure wireless settings.

Configure wireless settings

1. Choose **Wireless**.
2. Select the checkbox at the top of the screen to enable wireless capabilities on the EdgeMarc appliance.
3. In the Network SSID field, enter a unique name for the network established by the EdgeMarc appliance. The wireless client must enter the SSID to connect to the EdgeMarc appliance.
4. Select **Enable SSID Broadcast** if you want the EdgeMarc appliance to advertise the SSID in its 802.11 beacon.
5. Choose the wireless mode that is compatible with the clients to be served.
6. In the Channel field, select the 802.11 operating RF channel.
7. In the Power Level field, choose a level for the strength of the wireless signal transmitted by the EdgeMarc appliance.
8. Enter a key in the Pre-Shared Key field.
9. In the Key Renewal Interval, enter the number of seconds between attempts to automatically synchronize the pre-shared keys.
10. Click **Submit**.
A message indicates that service will be temporarily interrupted.
11. Click **OK** to confirm.

**Note**

If you clear the Enable Security check box, the page is updated to hide the security fields.



Note

For detailed field descriptions, see “[Wireless Configuration Page](#)” on page 293.

Configuring VLAN Settings to Support Wireless Traffic

If VLANs are configured, use the VLAN Configuration page to configure a bridging option for wireless traffic.



Note

If VLANs are not configured, wireless traffic is automatically bridged over the eth0 interface on the EdgeMarc appliance.

Select a VLAN for bridging wireless traffic

1. Choose **VLAN** from the Configuration Menu to open the VLAN Configuration page.
2. In the Wireless column on the right side of the page, select the VLAN to use for the wireless traffic.
3. Click **Modify** to save the modified VLAN settings.

Survivability

This chapter describes how to manage survivability on the EdgeMarc appliance. It contains the following sections:

- Overview
- SIP Server Redundancy
- SIP Server Availability
- MGCP Survivability Configuration
- Survivability in Transparent Mode
- Survivability Voice Mail

Overview

Survivability is a collection of features that enables the system to extend the availability of VoIP services. 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 to a remote softswitch.

Dynamic WAN links (for example, DHCP and PPPoE) 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 will be restarted when a WAN link renegotiation occurs, interrupting any local calls that are in progress. For this reason, survivability is not recommended for systems that use dynamic WAN links.

Survivability allows users connected to an EdgeMarc appliance to make and receive calls when the softswitch or the link to the softswitch is down. Survivability encompasses the following capabilities:

- Detection of when the softswitch is unreachable (Availability)
- Switching to a redundant softswitch (Redundancy)
- Making and receiving station to station calls while the softswitch is unreachable (Survivability)
- Making and receiving PSTN calls while the softswitch is unreachable.

To switch to survivability mode, the EdgeMarc appliance must be able to detect when the softswitch is unreachable. The softswitch may be unreachable for reasons such as the following:

- 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 also up and servicing requests.

The survivability process works as follows:

- 1.** SIP requests sent to the softswitch, and their responses, are monitored to check 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 resending its request. This enables the call to be connected with only a slight delay.
- 2.** 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.
- 3.** When a softswitch is marked as unreachable, the EdgeMarc appliance uses a different keepalive mechanism to determine when it becomes available again. The EdgeMarc appliance 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.
- 4.** An upstream EdgeMarc appliance or EdgeProtect device can send a specially marked keepalive response to inform the downstream EdgeMarc appliance about loss of connectivity to the softswitch. This causes an immediate fallback to the backup server or survivability mode in the downstream EdgeMarc appliance without a time delay.
- 5.** The EdgeMarc appliance 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.
- 6.** If no softswitch is available, the EdgeMarc appliance enters survivability mode and handles call signaling itself. Because the EdgeMarc appliance forwards all messages between the phones and the softswitch, it knows the address of all phones and can direct calls to the phones itself.
- 7.** A SIP PSTN gateway can be installed on the LAN side of the EdgeMarc appliance 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 appliance, and the EdgeMarc appliance can be configured to use the gateway as the default destination for calls not directed to another local phone.

8. When connectivity to the softswitch is restored, the EdgeMarc appliance automatically returns control of all subsequent call requests to the softswitch. Calls in progress that were established while the EdgeMarc appliance was in fallback mode are not disrupted.

Configure Survivability

Follow these steps to configure survivability.

Configure survivability

1. Choose **Survivability** from the Configuration Menu.
2. Scroll down to the Survivability area and select an option.
 - Disabled—Survivability feature is not available.
 - Enabled—Local call switching is enabled between VoIP endpoints and premises based-PSTN gateways during WAN link failures or other failures that prevent connectivity to the softswitch.
 - Always Local—Only local call switching is supported. Calls are not forwarded to network call processing servers.
3. Click **Submit**.

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

SIP Server Redundancy

To configure SIP server redundancy, you must specify the SIP Server address or domain name using one of the following methods:

- DNS Name in the SIP Server Domain Name field—Automatic discovery of primary and backup SIP Servers using DNS SRV lookup.
- IP addresses in the ordered SIP Server list—Manually-entered list of softswitch IP addresses and ports in priority order.

If the first method is used, the EdgeMarc appliance queries the DNS SRV records and collects a list of all SIP proxies for the configured domain.



Note

For detailed field descriptions, see [Survivability Page on page 223](#).

Configure redundancy

1. Choose **VoIP ALG > SIP** from the Configuration Menu to open the SIP Settings page.
2. Choose one of the following methods to specify the SIP Server address:
Method 1:
 - a. Enter the SIP Server domain name and default port.
 - b. Click **Submit**.Method 2:
 - a. Click **Create** to display the fields for manual entry.
 - b. If the domain name is the same for all SIP Servers, enter the domain name in the SIP Server Domain Name field. Otherwise, leave this field blank.
 - c. Click **Add row** as many times as needed to create a row for each SIP server to be added.
 - d. In priority order, enter the IP address and port number of each server or Session Border Controller (SBC). URLs are not permitted when you use manual entry.
 - e. Click the garbage can icon to delete any unneeded rows.
 - f. Click **Submit**.



Note

If all the rows are deleted, the page returns to the single SIP server address and port fields.

3. Choose **Survivability** from the Configuration Menu.
4. (Method 1 only) In the Softswitch/IP PBX Reachability Configuration area, enter the amount of time, in seconds, between DNS lookups.
5. In the SIP Server Redundancy Settings area, choose the options shown below, as described in “[Survivability Page](#)” on page 223.
6. Click **Submit**.

SIP Server Availability

Availability is the mechanism that enables survivability and redundancy. EdgeMarc determines the availability of softswitches in the following ways:

- Monitoring outgoing SIP requests and making sure that a reply is received from the server.

By default, the EdgeMarc appliance monitors all outgoing SIP messages to the active softswitch. If no replies are received from the server within the specified time interval, the switch is marked unreachable and the backup server is selected as the current server. The default time for declaring a SIP message lost is configured so that fallback occurs within the SIP retransmission interval and the clients transaction does not time out.

- Sending periodic SIP OPTIONS messages to the server and monitoring the replies from the server.

Keepalive messages are sent to failed servers using a backoff algorithm that progressively increases the interval until a maximum is reached. By default the maximum interval, when at least one server is reachable is longer than the one when no other backup server is available.

- Listening for specially marked SIP OPTIONS messages that signal loss of connectivity to soft switch from an upstream EdgeMarc appliance or EdgeProtect.

An upstream EdgeMarc appliance or EdgeProtect device can send a specially marked keep-alive response to inform the downstream EdgeMarc appliance about loss of connectivity to the soft-switch. This causes an immediate fallback to the backup server or survivable mode in the downstream EdgeMarc appliance without loss of time. It is not necessary to configure any options to support this capability.

Configure availability

1. Choose **Survivability** from the Configuration Menu.
2. Choose values for the following parameters, as described in “[Survivability Page](#)” on page 223.
 - Time(s) between Keepalive messages
 - Time(s) to declare Keepalive message lost
 - Number of missed messages to declare alarm
 - Number of received messages to clear alarm
 - Interpret error code as success
3. Click **Submit**.

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

MGCP Survivability Configuration

You can configure survivability for the MGCP protocol.

Configure MGCP survivability

1. Choose **VoIP ALG > Survivability** from the Configuration Menu.
2. In the MGCP Survivability area, configure values as described in “[Survivability Page](#)” on page 223.
3. Click **Submit**.

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

Survivability in Transparent Mode

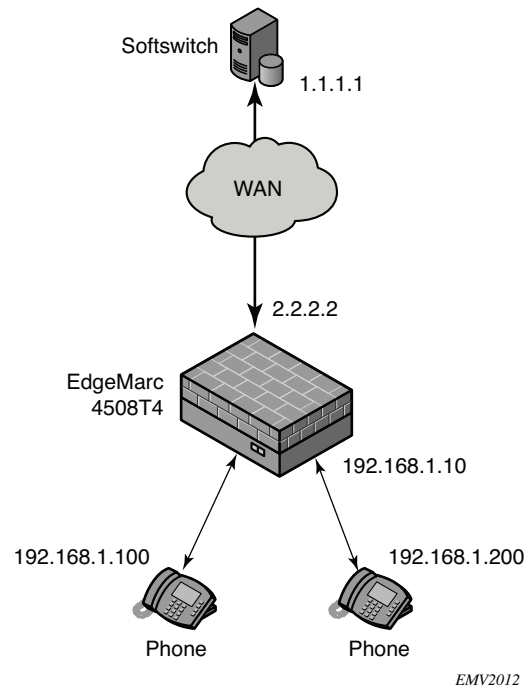
The EdgeMarc appliance now supports survivability when the transparent option is selected for the Session Initiation Protocol (SIP) mode.

An EdgeMarc appliance 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 appliance communicate with the appliance using the private IP address, and the EdgeMarc device 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. [Figure 10](#) shows an example configuration with labeled public and private IP addresses.

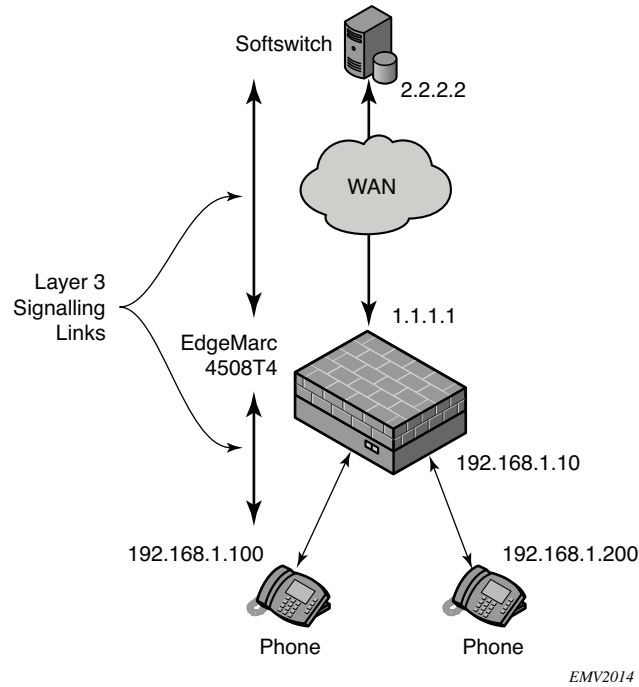
Figure 10 EdgeMarc Configuration with Example IP Addresses



The treatment of traffic sent between phones and the network depends on the choice of SIP mode.

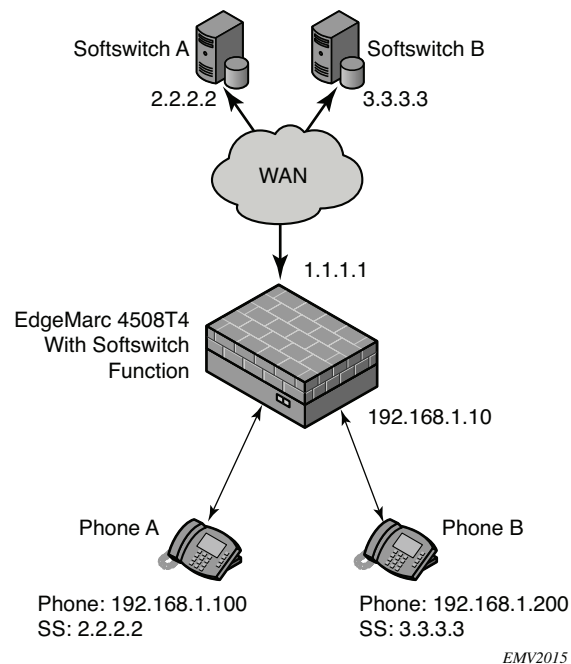
In *normal* (default) mode (Figure 11), a phone connected to the EdgeMarc appliance is configured with a private IP address and views the appliance as if the appliance is a Softswitch. The Layer 3 signalling between the phone and the EdgeMarc appliance is terminated at the appliance, and a separate Layer 3 signalling link is established between the EdgeMarc appliance 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.

Figure 11 Normal Mode



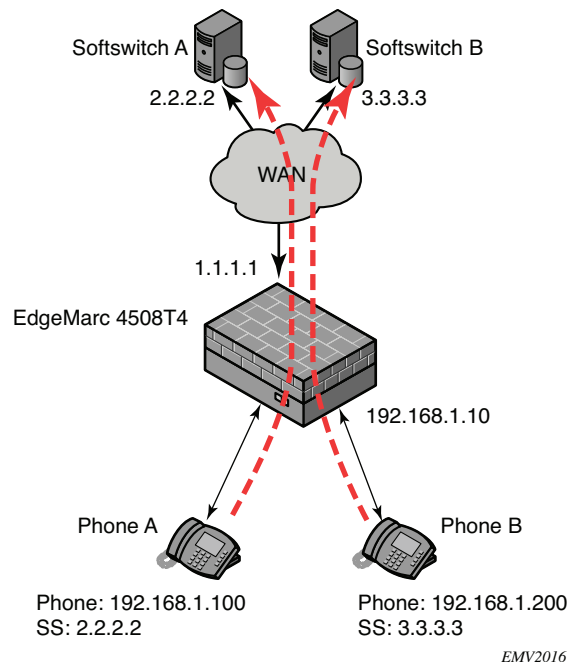
In *multi-homed outbound proxy* mode (Figure 12), the EdgeMarc appliance functions as a proxy server. Each phone connected to the appliance is configured with the IP address of the network Softswitch. An outbound proxy address is also configured, which the EdgeMarc appliance is able to translate. Because the phone includes the Softswitch address in its SIP message, the EdgeMarc appliance 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 appliance to be served by different Softswitches. In addition to performing translation, the EdgeMarc appliance is able to forward the signalling to the correct Softswitch for each phone.

Figure 12 Multi-Homed Proxy Mode



In *transparent mode* (Figure 11), 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 appliance picks up the signals as they are forwarded through the appliance and translates, but does not terminate them. Because the EdgeMarc appliance 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 appliance to be served by different Softswitches.

Figure 13 Transparent Mode



Survivability

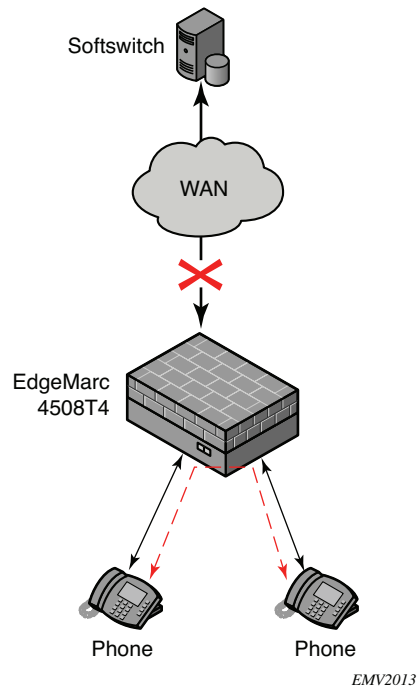
Survivability capabilities are triggered if the EdgeMarc device loses its connection to the WAN or if the network Softswitch is not accessible. When this occurs, the EdgeMarc appliance uses the information that was obtained from the terminated or forwarded phone signals to direct local calls between phones attached to the appliance.

For example, assume that phones A and B are connected to the EdgeMarc appliance and that A attempts to call B. The survivability process works as follows:

1. Phone A sends a request to the EdgeMarc appliance.
2. The EdgeMarc appliance 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 appliance takes over and performs the Softswitch function, connecting phone A to phone B (Figure 14).

Figure 14 Survivability



Note

The EdgeMarc appliance always attempts to connect to the Softswitch that is configured in the appliance. In transparent mode, this could be a different Softswitch from that which is configured in some of the phones. If the Softswitches are different, then the EdgeMarc appliance is unable to perform the survivability function.

Assigning SIP Modes

This section shows how to assign the SIP mode settings. When the SIP mode is assigned, survivability is enabled.



Note

For information on configuring survivability settings, see the *VOS for EdgeMarc Manual*.

Assign the SIP mode

1. Choose **VoIP ALG > Survivability** from the Configuration Menu to open the SIP Settings page.
2. Choose and configure a SIP mode:
 - Normal—Clear the Enable Multi-Homed Outbound Proxy Mode checkbox and the Enable Transparent Proxy Mode checkbox.
 - Multi-Homed Outboard Proxy—Select the Enable Multi-Homed Outbound Proxy Mode checkbox.
 - Transparent mode—Select the Enable Transparent Proxy Mode checkbox, and click **Submit** to enter Softswitch addresses. Enter an IP address in the Allowed SIP Proxies IP Address field, and click **Add**. Add additional addresses as needed.
3. Click **Submit**.

Survivability Voice Mail

The EdgeMarc 5300 survivability voice mail service enables enterprises to provide continued voice mail services even if WAN access is unavailable. The service is intended for enterprises that use voice mail services offered by the Internet Service Provider (ISP) or other WAN-accessible supplier.



Note

Survivability voice mail is available only on Edgemarc 5300 and 5300LF platforms.

If survivability voice mail is enabled, the EdgeMarc 5300 appliance detects when the WAN link is down and activates survivability voice mail as a service on the EdgeMarc 5300. When the WAN link comes back up, the survivability voice mail service is automatically inactivated.

Voice mail messages received while the WAN link is down are stored in the EdgeMarc appliance RAM. Each voice message generates an automated email message to the designated recipient, and the voice message is attached to the message as a .wav file. Windows Media Player or any other player capable of playing .wav files can play the message.

The survivability voice mail service also includes an integrated voice response (IVR) system. If a voice mail message comes in while the survivability voice mail service is active, the message light on the user's telephone lights up. The user can call into the IVR system resident on the EdgeMarc appliance and use the IVR menu prompts to play back the message.



Note

This feature is available as an add-on to the EdgeMarc 5300, and requires a new license key.

Voice Mail Process

The survivability voice mail service operates as follows:

1. On the License page, the EdgeMarc 5300 administrator enables the survivability voice mail feature by entering the correct license key. A SIP and SIP Survivability license is required.
2. On the SIP Client page, the administrator enters the IP phone address, phone extension, and email address for each phone user. This creates a mapping between phone numbers and email addresses. A voice mailbox is automatically created for each SIP client.
3. On the Survivability page, the administrator enters the email address that will be used as the originating address for automated email messages. The administrator can also modify the number of seconds that the phone rings before going to voice mail, the phone extension number for the IVR system, and the maximum number of messages per mailbox.
4. During normal operations, the WAN link is up, and the enterprise obtains voice mail services from the ISP or other external provider. The survivability voice mail service is inactive.
5. When the WAN link goes down, the survivability voice mail service is automatically activated.
6. When the WAN link is down and a voice mail message is received, the EdgeMarc appliance stores the message in local RAM.
7. The system generates an automated email message from the email address that was entered in the Survivability page to the email address that was mapped to the extension receiving the voice mail. The message indicates that a voice mail has been received and directs the user to open the attached .wav file:

```
Hello Mailbox 2222:
```

```
You have a new voice message (0:03sec) in mailbox  
2222.
```

```
The message was left by phone number 2222 on  
Wednesday, September 20, 2006 at 09:40:31 AM.
```

The user can read the message using any standard email client and can perform any functions supported by the media player, such as fast forward, rewind, or pause. The message waiting light on the phone is automatically lit.



Note

Voice mail is received and stored whether or not a phone extension-to-email address mapping has been configured on the SIP Client page; however, the email notification is sent only if the mapping is defined.

8. The user can access the IVR to listen to the .wav file. The user dials the IVR extension that was configured on the Survivability page. The IVR system prompts for the user mailbox number and password. See [Using the IVR System on page 112](#) for information on the user mailbox number and password.

9. When the WAN link comes back up, the survivability voice mail service is automatically inactivated, and the enterprise goes back to using the standard voice mail system.

The EdgeMarc 5300 survivability voice mail service is intended for use only when the WAN is down, and the following restrictions apply:

- Storage space for voice messages is limited. Approximately 120 message minutes can be stored. When this limit is exceeded no additional messages are accepted. The caller hears the message: “I’m sorry, that extension is not accepting messages.”
- Because messages are stored in RAM, messages are deleted when the EdgeMarc appliance is rebooted. If this occurs, users can still access messages by opening the automated email message with the attached .wav file.
- If the EdgeMarc appliance is rebooted or the WAN link comes back up, the IVR system becomes inactive. When this occurs, users must open the automated email message to listen to the voice mail.

Configuring Survivability Voice Mail Settings

This section explains how to configure the survivability voice mail settings:

- [Configuring License Key on page 110](#)
- [Configuring SIP Client Settings on page 110](#)
- [Configuring Survivability Voice Mail Settings on page 112](#)

Configuring License Key

Follow the steps in this section to assign a license key.

Configure license key

1. Choose **System** from the Configuration Menu to open the System page.
2. Click **License Key** in the Registration Status area of the screen.
3. Click **Edit License Key**.
4. Enter the license key.
5. Click **Submit**.

Configuring SIP Client Settings

The phone extension-to-email address mappings are defined on the SIP Client page. You can enter mappings manually on the SIP Clients page, or create an email definition file and upload it to the EdgeMarc appliance.



Note

Because email delivery outside the local domain cannot be guaranteed if the WAN link is down, the Email addresses mapped to phone extensions for the SIP clients should belong to the same local domain as the email address used for of the EdgeMarc device. For example, if the domain of the EdgeMarc device is

edgewaternetworks.com, then each email address using in a phone extension-to-email mapping should also belong to the edgewaternetworks.com domain.

Configure SIP client settings manually

1. Choose **System > Clients List** from the Configuration Menu to open the SIP Clients List page.
2. In the Name field near the bottom of the page, enter the phone extension for the SIP client.
3. In the Address field, enter the IP address of the client.
4. In the Port field, enter 5060 as the port number.
5. In the Email field, enter the email address that will receive notification for voice mail messages sent to the phone extension listed in the Name field.



Note

The email address field is optional. Each phone user is assigned a voice mailbox regardless of whether an email address is assigned. If the email address for a user is not specified, however, the user will not receive email notifications.

6. Click **Add**.
7. Repeat [step 2](#) - [step 6](#) for each phone extension for which you want to support survivability voice mail.

Configure SIP client settings using an mail definition file

1. Create a file with a row for each phone extension. Each row should include the following information, with a space separating each entry.

```
*<space>ip_address<space>port_number<space>phone_number
<space>email_address
```

For example:

```
* 192.168.1.3 5060 222 user1@edgewaternetworks.com
* 192.168.1.4 5060 3333 user2@edgewaternetworks.com
```

...

2. To upload the file, open a Telnet, ssh, or terminal window to the EdgeMarc appliance.
3. Log in, if necessary.

Use echo:

```
“*<space>ip_address<space>port_number<space>phone_number<space>email
_address >> /etc/config/email_defs.conf”
```

For example, to add an email address to the email definition file for phone users 2222 and 1234567890, issue the following “echo” commands while logged in to the EdgeMarc appliance 5300/5300LF through a Telnet or ssh window:

```
# echo '* 192.168.1.55 5060 2222 jack@edgewaternetworks.com' >>
/etc/config/email_defs.conf
# echo '* 192.168.1.31 5060 1234567890 jill@edgewaternetworks.com' >>
/etc/config/email_defs.conf
```

When you are finished adding all the email entries, issue the following command from the same window to save the changes:

```
# /etc/conf/bin/cfg_commit
```

Configuring Survivability Voice Mail Settings

Follow these steps to set up phone extension to email mappings.

Configure survivability voice mail settings

1. Choose **Survivability** from the Configuration Menu.
2. Enter the number of seconds that an incoming call is allowed to ring before going to voice mail. The default is 20 seconds, and the maximum is 50 seconds.
3. Enter the maximum number of messages that will be stored for each mailbox. Because space to store messages is limited, it may be desirable to keep this number low. The default is 2 message, and the maximum is 20 message.
4. Enter the phone extension for the IVR system that phone users can call to retrieve messages. The default extension is 9999.
5. Enter the email address that will be listed as the originator for email notifications. The email address must include a valid domain name; for example: `edgemark@edgewaternetworks.com`.
6. Click **Submit**.



Note

The mailbox password can be reset to default. See [Resetting the Mailbox Password](#) on page 114.

Using the IVR System

Phone users can call into the IVR system to access their survivability voice mailbox. The following functions are available through the IVR system:

- Fast forwarding—Press # while the message is being played to fast-forwarded the message 5 seconds.
- Rewinding—Press * while the message is being played to rewind the message 5 seconds.
- Stop voice prompts, play back the message envelope (caller ID, message timestamp), and speed-up entering of mailbox number and password—Press #.

The following guidelines apply to IVR system messages and mailboxes.

- The maximum message length is 60 seconds.
- The mailbox number for the user is determined by the number of digits for local dialing defined on the Survivability page. For example, if the user name or extension number is 4081234567, and the number of digits for local dialing is set to 5, the mailbox number for the user is 34567. If the user name or extension number is shorter than the number of digits for local dialing, it will be used as-is for the mailbox number. For example, if the user has extension 123, and the number of digits for local dialing is 4, the mailbox number for the user is 123.
- The default password is of the form *0mbox9*, where *mbox* is the mailbox number. For example, if the user mailbox is 4455, the default password is 044559.

The IVR system uses the prompts and messages described in this section.

IVR System Prompts

User Accesses the Voice Mailbox

When a SIP phone user dials the IVR system extension to log in to the IVR system and check messages, the system uses the following prompts:

- “Please enter your mailbox number”—Enter the phone extension
- “Please enter your password”—Enter the password. The default is of the form *0ext9* where *ext* is the phone extension. User presses # after entering the password.
- Press 1 to listen to messages (if there are messages in mailbox)
 - Message plays.
 - “Press 1 to listen to the next message”
 - “Press 2 to hear the current message again”
 - “Press 3 to delete the current message”
- Press 4 to change your password
 - “Please enter your new password”
 - <Enter new password>
 - “Please re-enter your new password”
 - <Re-enter new password>
 - “Password changed” <if new password was entered correctly>
 - “Password mismatched, no change” <if new password was NOT entered correctly>
- “Press # to exit voicemail”
 - “Goodbye”

If a call has been picked up and answered by the voicemail system, the caller can press * to log in instead of leaving message.

- <call made to extension N was not answered and picked up by Voicemail>
- “The person at extension N did not answer”
- <* was pressed>
 - “Please enter your mailbox number”
 - “Please enter your password”

- System continues the prompts listed in [IVR System Prompts on page 113](#).

Caller Leaves Message

When a call is not answered, or the destination extension is busy, the voicemail system answers the call using the following prompts:

- <call was not answered and picked up by voicemail>
- “The person at extension N did not answer”
- “Record your message after the tone”
- <tone>
- <recording of message>
- “Press 1 to send your message”
 - “Message sent”
 - “Thank you”
 - “Goodbye”
- “Press 2 to review your recording”
 - <playing the recorded message>
- “Press 3 to erase and re-record”
 - Record your message after the tone
 - <tone>

Resetting the Mailbox Password

You can reset a user’s mailbox password to the default by entering the client information on the SIP Clients List page and clicking **Add**. If the email address is different (not an exact match), the EdgeMarc appliance treats the Add request as an update for the email address of the user and not as a password reset.

For example, to change the email address “account” of a user to “new-account,” that is, from:

Address: 192.168.1.55
Port: 5060
Name: 2222
Email Address: account@edgewaternetworks.com

enter the address, port, name, and new email address, and click **Add**.

Address: 192.168.1.55
Port: 5060
Name: 2222
Email Address: new-account@edgewaternetworks.com

To reset the password of the same client (address “account”) enter the exact client information:

Address: 192.168.1.55
Port: 5060
Name: 2222

Email Address: account@edgewaternetworks.com

And click **Add**.



Note

If the client doesn't have an email address, adding the client again with (still) no email address will also reset the client mailbox's password.

Stateful Failover

This chapter describes how to configure two EdgeMarc devices to act as a redundant pair. The pair works to eliminate single points of failure in a network configuration.

This chapter contains the following sections:

- Overview
- Configuring Stateful Failover

Overview

You can configure two EdgeMarcs to use automatic, stateful failover in the event of an EdgeMarc failure. One device is designated as the primary device, the other is designated as the backup device. Attached LAN devices, as well as the far-end WAN devices, are unaware that two EdgeMarcs are installed. The two appliances appear as a single device, using a single, constant IP address called a *Virtual IP Address (VIP)*.

Configure the two EdgeMarcs to send status updates to each other by specifying the IP addresses of both the primary and secondary EdgeMarc for the LAN, WAN, or management interfaces. You must enable state transfer for one or more of the IP interfaces. If you enable state transfer for multiple interfaces, you have a higher chance of successful state transfer during link failures. The drawback is that the state transfer causes extra network traffic on that link.

When the master EdgeMarc fails, or one of the links fails, the secondary EdgeMarc will detect the failure and take over in approximately 3 seconds.

When this occurs an event is written to the syslog.

Configuring Stateful Failover

To configure stateful failover with a redundant pair, complete the following tasks on both EdgeMarcs:

1. Configure the LAN and WAN IP addresses.
2. Configure Virtual IP addresses for the redundant pair.
3. Configure the Management Interface.
4. Configure the Stateful Failover page.

Configure the LAN and WAN IP addresses

Configure the LAN and WAN IP addresses. These are real, unique IP addresses.

On each device, complete the following steps:

1. Choose **Network** from the configuration menu to open the Network Configuration page.
2. Enter the IP address for the LAN interface in the **IP Address** field under the LAN Interface Settings section.
3. Enter the IP address for the WAN interface, complete the following fields:
 - a. Select the **Static IP Address** radio button.
 - b. Enter an IP address in the **IP Address** field under the WAN Interface Settings section.
4. Complete any remaining fields as described in [Network Page on page 169](#).
5. Click **Submit** to save your results.

Configure Virtual IP addresses for the redundant pair

Configure the VoIP ALG page on both devices in the redundant pair, specifying the Virtual IP Addresses for the shared LAN and WAN interfaces under **Use ALG Alias IP Addresses**.

On each device, complete the following steps:

1. Choose **VoIP ALG** from the configuration menu.
2. Select the checkbox next to **Use ALG Alias IP Addresses**. If the checkbox is already selected, skip to step 5.
3. Click **Submit**.
4. Click **Ok** when prompted to confirm that it is ok to interrupt all voice and video services. The **VoIP ALG** page is reloaded.
5. In the **ALG LAN Interface IP Address** field, enter a common IP address that will correspond to a LAN IP address to be shared by both devices in the redundant pair.
6. In the **ALG WAN Interface IP Address** field, enter a common IP address that will correspond to a WAN IP address to be shared by both devices in the redundant pair.
7. Complete any remaining fields as described in [VoIP ALG Page on page 202](#).
8. Click **Submit** to save your results.

Configure the Management Interface

Optionally, enable the management interface on each device to enable state transfer between both device's management interfaces.

On each device, complete the following steps:

1. Choose **System > Management Interface** from the primary web configuration menu.
2. Select the **Enable Management Interface** box.
3. Enter a unique management IP address in the **Management Interface IP Address** field.
4. Enter the following subnet mask in the **Subnet Mask** field: 255.255.255.0
5. Click **Submit** to save your results.

Configure the Stateful Failover page

Configure all parameters on the stateful failover page for each device.

On each device, complete the following steps:

1. Choose **System > Management Interface** from the primary web configuration menu.
2. Select the **Enable Stateful Failover** check box.
3. Specify the **Designation** field as **Primary** or **Secondary**.



Note

One device must be designated as the primary device and the other device must be designated as secondary device.

4. Enter the password in the **Password** field.



Note

The password must be the same on both systems.

5. Enter the LAN Virtual IP address (the **ALG LAN Interface IP Address**) into the **LAN Virtual IP address** or **Subscriber Virtual IP address** field.
6. Enter the WAN Virtual IP address (the **ALG WAN Interface IP Address**) into the **WAN Virtual IP address** or **Provider Virtual IP address** field.
7. Enter the real LAN interface address of the other device in the **LAN Remote Address** field.
8. Enter the real WAN interface address of the other device in the **WAN Remote Address** field.

9. Enter the real Management Interface address of the other device in the **Management Remote Address** field.
10. For each link that will transfer state information, select its corresponding **Enable State Transfer** checkbox.



Note

For redundant pairs that process high volumes of SIP signaling and RTP media, enable state transfer of at least two, if not all three, IP interfaces, one of which should be the Management Interface. In the case that one interface should fail, this increases the probability that the state will be successfully transferred between devices.

WAN Link Redundancy

This chapter describes how to configure the EdgeMarc appliance to support the WAN Link Redundancy (WLR) feature. It contains the following sections:

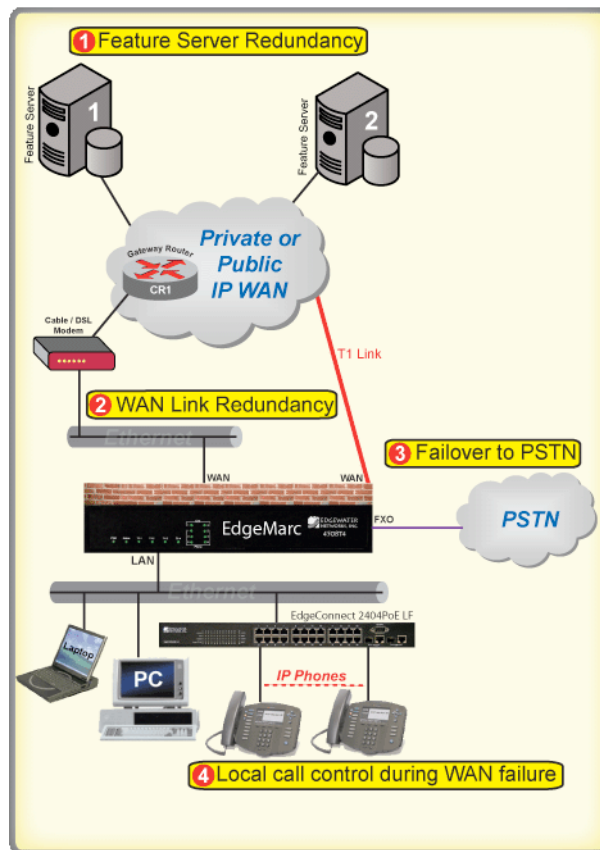
- Overview
- Configuring WAN Link Redundancy

Overview

WLR is a critical part of increasing the reliability of VoIP and data communications. It allows enterprise and service provider customers to take advantage of diverse routing and dual access link connections to private or public IP networks

WLR relies on two separate physical routes, primary and secondary routes to the WAN network. EdgeMarc switches to the secondary route, if a communication failure is detected on the primary route, thus reducing the risk of the WAN link being the single point of failure. As shown in [Figure 15](#), WLR together with “Survivability”, enables the EdgeMarc to provide robust and reliable voice services that meet the needs of both Enterprise and Service Provider deployments.

Figure 15 WLR in conjunction with Survivability.



Data and Voice Interface Switchover

- **Revertive Mode**

If the Primary interface has been defined as main interface (See [Table 77](#)) and the Secondary interface is the currently active interface, then the system will automatically switch to the Primary interface as soon as it is detected to be available.

- **Non-revertive Mode**

The system shall continue to use the currently active interface until it goes down in which case it will switchover to the other interface.

Manual Switchover



Note

Manual Switchover mode is only applicable when the EdgeMarc is configured in non-revertive mode (See [Manual Switchover](#) on page 308).

If the user selects Manual Switchover at any instance then WLR module invokes a network restart setting up the default routes on the system to start using the currently Inactive interface. This switchover takes place irrespective of the status (Up/Down) of the inactive interface.

Supported Interfaces

Wan Link Redundancy can be implemented using two different physical interfaces on the same Edgemarc (e.g. T1 interface and ethernet) or one physical interface with two gateways to the WAN reachable through an intermediate local area network. All tested combinations of a primary and a secondary interface or gateway are provided in [Table 9](#) and [Table 10](#). Any interface or gateway can either be primary or secondary.

Table 9 Primary and secondary gateways on separate WAN interfaces

		WAN Interfaces		
		T1	Ethernet	EVDO
G A T E W A Y I P	S E L E C T I O N	ANSI T1	Static IP	
		PPP T1	PPPoE	
		PPP T1	DHCP	
		PPPoFR T1	PPPoE	
		PPPoFR T1	DHCP	
			PPPoE	EVDO
			Static IP	EVDO

WAN Link Redundancy can be implemented using two different physical interfaces or one physical interface with two gateways to the WAN.

Table 10 Primary and secondary gateways on one WAN interface

		Gateway IP Selection	
Ethernet WAN Interface	Static IP	Static IP	
	Static IP	DHCP	
	Static IP	PPPoE	

Configuring WAN Link Redundancy

This section describes how to configure WAN link redundancy settings.

Configure WLR settings



Note

Priority calling services cannot be configured when WAN Link Redundancy is enabled.

1. Choose **Network** submenu of “**Configuration Menu**” and configure the primary interface and gateway. Also, configure the parameters in the “**Primary WAN Redundancy Settings**” section (See [Network Page](#)) and click **Submit**.
2. Choose “**Configuration Menu**→**Wan-Link Redundancy**” and choose “**Secondary WAN Config**” submenu. Configure the secondary interface and gateway (See [Secondary Interface Settings Configuration Page](#)) and click **Submit**.
3. Choose “**Configuration Menu**→**Wan-Link Redundancy**” and choose “**WLR Parameters Config**” submenu. Change the default values of the parameters if necessary and click **Submit**.
4. Choose “**Configuration Menu**→**Wan-Link Redundancy**” and choose the main interface for data and voice by choosing primary or secondary (See [WAN Link Redundancy Configuration Page](#)).
5. Enable WAN Link Redundancy and if needed enable revertive mode.
6. Click **Submit**.
A message indicates that service will be temporarily interrupted.
7. Click **OK** to confirm.

System Diagnostics

This chapter describes how to use the diagnostic information, troubleshooting tools, and system maintenance utilities on the EdgeMarc appliance. It contains the following sections:

- Viewing Version, Hardware Platform and LAN MAC Address
- Viewing the ALG Registration Code
- Viewing Networking Information
- Viewing Advanced System Information
- Using Troubleshooting Tools
- Rebooting the System
- Using T1 Diagnostics
- Verifying Connectivity with the Test UA

Viewing Version, Hardware Platform and LAN MAC Address

The software version, hardware platform, and LAN MAC address are common pieces of information requested by technical support. You can obtain this information from the System page of VOS for EdgeMarc.

To ensure that you are running the latest software version, visit our website for a complete listing of software releases at:

<http://www.edgewaternetworks.com/Support/SupportDocLanding.html#ReleaseNotes>

Viewing the ALG Registration Code

You will also find a link to the ALG registration code on the System page. The registration code enables the ALG and is pre-installed at the factory.

Entering the Registration Code

If the registration code is inadvertently deleted you can re-enter the code.

Enter license key

1. Choose **System** from the Configuration Menu.
2. Click **License Key**.
3. Click **Edit License Key**.
4. Enter the **License Key** (registration code).

The registration code is printed on the sticker located on the bottom of the EdgeMarc device.

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

Viewing Networking Information

To view the networking configuration and status of the EdgeMarc device, open the Network Information page.

View networking information

- Choose **System > Network Information** from the Configuration Menu.

The Network Information page includes the following information:

- [Routing Information](#)
- [Link Status](#)
- [Interface Information](#)

Routing Information

The system routing table contains the static routes for hosts and networks that are configured on the EdgeMarc device. If only the LAN and WAN IP addresses have been configured multiple lines are displayed:

- The private subnet associated with the LAN interface
- A public subnet present for the WAN interface
- An entry for the EdgeMarc device loopback interface
- An entry for each IPSec tunnel
- The EdgeMarc device's default gateway forwarding to the WAN interface

Additional lines may be displayed depending on the contents of the Route and VoIP Subnet Routing pages. Each entry on one of these pages causes an additional entry in the routing table.

Link Status

Link Status shows the status of the Ethernet interfaces. Ethernet autonegotiation is often unreliable, especially between different vendors or old and new networking equipment. Failure of autonegotiation 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 Set Link page. Intermittent data and voice outages may be caused by link “flapping” when the two endpoints of the Ethernet cable cannot reach agreement using autonegotiation. If the link rate is set manually, make sure 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 EdgeMarc device.

Interface Information

The specific status and configuration information for the system interfaces is displayed in the Interface Information section.

The interface statistics can point to areas of congestion in the network. If the errors statistic is a few percent or more of the total packets sent, it may be an indication of excessive congestion on the network interface. If this congestion is not corrected the quality of voice calls will be affected. The topology of the network attached to the network interface with the errors should be examined and modified to better segment and isolate network traffic.

Viewing Advanced System Information

To view advanced system information for the EdgeMarc device, open the System Information page.

View networking information

- Choose **System > System Information** from the Configuration Menu.

For detailed field descriptions, see “[Subinterfaces Page](#)” on page 171.

Passive Voice Call Monitoring

The EdgeMarc device monitors live voice calls and performs objective speech quality assessment. This information enables the network operator to assess voice quality for the purposes of SLA tracking or problem isolation. Mean Opinion Score (MOS) results for RTP streams in both directions of a VoIP call are calculated at call completion. This information, along with the IP addresses of the VoIP endpoints supporting the call, is logged locally and optionally sent to an external syslog server. In addition, the EdgeMarc device generates a real-time message for any MOS values calculated less than 2.5 (considered poor quality) during an active call.

Voice call quality information is available in the System Logging Messages section of the System Information page. A sample of this information is provided below.

Recent Call Log:

Mar 16 22:15:38 69.169.190.223 E_5300LF mand: Advanced MOS (v1.5);STR=1237241693;STP=1237241738;Call ID=165479;SRC=66.7.123.134;SDD=18013589822;DST=10.221.61.255;DDD=8013751757;MOS=4.36;BTC=0;PJ=0.00;PPL=0.00;LP=4;RR=2190;SRE=2194;OOP=0;PD=0.41;MPJ=2.34;MNJ=-3.72;CLP=3;PLB=2.00;

Mar 16 22:15:38 69.169.190.223 E_5300LF mand: Advanced 2MOS (v1.5);STR=1237241693;Call ID=165479;SRCP=20520;DSTP=16448;SIP-CALL-ID=995a8b51-8f639c90@10.221.61.255;IFACE=eth1;

Mar 16 22:15:38 69.169.190.223 E_5300LF mand: Ending call ID 165479 between 66.7.123.134 and 10.221.61.255. MOS scoring is enabled. Remaining active calls=61.

Mar 16 22:15:39 69.169.190.223 E_5300LF mand: Creating call ID 165491 between 10.221.143.230 and 66.7.123.134. Active calls=62

Mar 16 22:15:40 69.169.190.223 E_5300LF mand: Creating call ID 165492 between 10.221.106.241 and 66.7.123.134. Active calls=63

Mar 16 22:15:43 69.169.190.223 E_5300LF mand: Creating call ID 165493 between 10.221.60.224 and 66.7.123.134. Active calls=63

Mar 16 22:15:43 69.169.190.223 E_5300LF mand: Call ID 165486 10.221.174.240->66.7.123.134: Call complete. Remaining active calls=62. Minimum MOS=4.32 Average MOS=4.35

Mar 16 22:15:43 69.169.190.223 E_5300LF mand: Advanced MOS (v1.5);STR=1237241716;STP=1237241743;Call ID=165486;SRC=10.221.174.240;SDD=8013741283;DST=66.7.123.134;DDD=3196125;MOS=4.35;BTC=0;PJ=0.00;PPL=0.00;LP=3;RR=1362;SRE=1365;OOP=0;PD=0.60;MPJ=18.91;MNJ=-24.34;CLP=2;PLB=1.50;

Using Troubleshooting Tools

The EdgeMarc device provides convenient test tools to facilitate problem isolation and resolution. A network operator can use these tools to verify connectivity to and from the EdgeMarc device and to trace datapaths to endpoints throughout the network.

Verifying Registered Voice Devices

The EdgeMarc device maintains a list of all registered voice devices called a clients list, so that it can properly route voice calls. At startup, voice devices register their IP addresses with the EdgeMarc device. The EdgeMarc device then registers on behalf

of the voice devices by providing its own WAN IP address to the softswitch or IP PBX.

If a user or network operator reconfigures the IP address of the voice device, it re-registers the new address with the EdgeMarc device. In this instance, voice calls may be routed improperly because the EdgeMarc device clients list contains out-of-date information.

To update the clients list, highlight and delete any duplicate or stale entries.

**Note**

You can configure MGCP and H.323 to age out clients that do not respond to local audits and remove them from the clients list dynamically. To configure this feature, use the appropriate Voip ALG pages.

Verify voice devices

1. Choose **System > Clients List** from the Configuration Menu to open the SIP Clients List page.
By default, the **SIP** clients are shown.
2. Select **MGCP** or **H.323** to view the registered clients for those protocols.
3. In the clients list table, select the checkboxes for any duplicate entries or other entries that required deletion and click **Delete Selected**.
4. Click **Submit**.
5. Restart the VoIP ALG according to the instructions in [Networking Restart on page 130](#).

Ping and Traceroute Tests

The Network Test Tools page provides an easy way to perform a ping test or traceroute test. To access the Network Test Tools page, select **System > Network Test Tools** in the Configuration Menu.

Performing a Ping Test

A 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 EdgeMarc device and the test IP address. A successful ping test does not guarantee that all data traffic is allowed between the EdgeMarc device and the test IP address, but it is useful to verify basic reachability.

Perform a ping test

1. Choose **System > Network Test Tools** from the Configuration Menu.
2. Enter an address in the IP Address to Ping field.
3. Click **Ping**.

The Network Test Tools page reopens to display results of the ping test. (This may take several seconds.)

4. Click **Reset** to clear the data.

Performing a Traceroute Test

A 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, internal network paths can be traced over the LAN to verify the local network topology.

Perform a traceroute test

1. Choose **System > Network Test Tools** from the Configuration Menu.
2. Enter an address in the IP address to Trace field.
3. Select **WAN** or **LAN**.
4. Click **Traceroute**.

The Network Test Tools page reopens to display results of the test. (This may take several seconds.)

5. Click **Reset** to clear the data.

Networking Restart

Technical support may request that networking services be restarted during a troubleshooting session. In this case, you can use the Network Restart page to stop and restart all the networking services that are running on the system.

Restart networking services

1. Choose **System > Restart** to open the Networking Restart page.
2. Click **Submit**.
A message indicates that service will be temporarily interrupted.
3. Click **OK** to confirm.



Warning

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!

Rebooting the System

Rebooting the system stops all networking services and reboots the system. The operating system and networking services will be 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.

**Note**

As an alternative to rebooting, you can perform a reset locally by temporarily disconnecting the power cable from the EdgeMarc device.

Reboot the system

1. Choose **System > Reboot System** from the Configuration Menu.
2. Click **Reboot**.
3. Click **Submit**.

A message indicates warns that rebooting the system will interrupt services for a few minutes.

4. Click **OK** to confirm.

**Caution**

Rebooting the system will interrupt services for a few minutes. All voice, video and data sessions currently in progress will be interrupted! Proceed with caution!

Using T1 Diagnostics

Open the T1 Diagnostics page to display T1 diagnostic information and statistics and run diagnostic commands.

Perform T1 diagnostics

1. Choose **System > T1 Diagnostics** from the Configuration Menu.
2. Select the loopback test you want to run from a pull-down list, and click **Submit** for the desired interface. “[T1 Diagnostics Page](#)” on page 283 describes the available loopback tests.
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 2¹⁵-1 and a QRBS 2²⁰-1 pattern.

**Note**

The EdgeMarc appliance also responds to network generated, AT&T formatted loop up/down codes. Loopback codes sent from far end equipment will loop the T1 interfaces back towards the network.

The T1 Status shows the current alarm state and indicates if there is a loopback or BERT test in progress. For descriptions of alarm and loopback types, see “[T1 Diagnostics Page](#)” on page 283.

The T1 Diagnostics page displays the current 15-minute (CUR) and 24-hour total (SUM) statistics for the T1 interfaces. This information allows you to compare performance from different time intervals. “[T1 Diagnostics Page](#)” on page 283 describes and the interval data.

View T1 Statistics

1. Choose **System > T1 Diagnostics** from the Configuration Menu.
2. Click **Reset** to clear the statistics for the current interval.
A message indicates that service will be temporarily interrupted.
3. Click **OK** to confirm.

View advanced T1 diagnostics

1. Choose **System > T1 Diagnostics** from the Configuration Menu.
2. Click **T1 advanced diagnostics page**
The page displays data for each 15-minute interval over the last 24 hours.



Note

The oldest-15 minute interval is removed from the 24-hour total as each new 15-minute interval is added.

Verifying Connectivity with the Test UA

You can use the Test UA to verify VoIP connectivity. The Test UA allows you to place a call to the EdgeMarc itself. You can confirm that the call was successfully placed and received as well as monitor the quality of service (QOS) for the call in the System Logging Messages.

For information about placing calls to and from the EdgeMarc using an EdgeView appliance, see the *EdgeView VoIP Support System User Manual*.

Placing a call to the EdgeMarc

Prerequisite: A telephone number must be assigned to the Test UA on the softswitch to which the EdgeMarc points.

1. Choose **Test UA** from the primary web configuration menu.
2. Complete the required fields as specified in “[Test UA Settings page](#)” on page 277. 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. Choose **System > System Information** from the primary web configuration menu.
5. Scroll to the section titled **System Logging Messages**. This section provides a message for every logged call.

The successfully placed call will appear as follows 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]
```

Device Configuration Management

This chapter describes the tools available to manage the EdgeMarc appliance configuration. It contains the following sections:

- Overview
- `ewn` Command
- Logging off listed users
- Downloading Files
- Using the Internal TFTP Server

Overview

The EdgeMarc device stores all configuration information for the system in a series of individual files that reside in local flash memory. These files are read at boot time to determine the configuration identity of the EdgeMarc device and then stored in RAM as “running” state. As you configure the EdgeMarc device the **submit** command writes the configuration changes to both RAM and flash so that the files stored in flash are always up to date with the running state of the system.

The EdgeMarc device provides a utility that enables you to copy the individual configuration files stored in flash to a single, consolidated backup file. This single file can then be used as a backup for the entire system and restored at a later date if necessary. Multiple backup files with different system configurations can also be created and stored locally in the EdgeMarc device or on remote TFTP servers.



Note

No more than two backup files can be stored in the EdgeMarc device flash because of size constraints. Also, it is recommended that you create a backup file after any configuration changes are made to the EdgeMarc device. This is to prevent the loss of any configuration changes made since your last backup in the event that you must restore the system configuration.

`ewn` Command

The **ewn** command is used to perform multiple tasks related to backup operations

The syntax for the `ewn` command is as follows:

USAGE:

```
ewn help|list
ewn save|load|restore|delete [file name]
ewn upload|download [file name] [ip address]
```

where file name must use extension .conf1 or .conf2

The **ewn** command can be used with a local terminal connection or remotely using SSH.

- Use a straight-through cable to connect to the console port of the EdgeMarc device.
- Use a terminal emulator such as HyperTerminal set to a baud rate of 9600, 8 data bits, 1 stop bit, and no and parity.

Alternatively you can connect to the EdgeMarc device remotely using SSH. Log on as **root** and enter the **password** provided by Edgewater.

At the command prompt (bash#), you can create the backup file, store it to local flash, copy it to a remote TFTP server, copy it from a remote TFTP server, delete it, load it, restore it, or list all available backup files.

Creating a backup file and save to local flash

The following command creates a backup file of the current running configuration and saves it to local flash memory:

```
bash# ewn save <filename>
```

Filename format (must use extension .conf1 or .conf2):

```
<filename1>.conf1
```

```
<filename2>.conf2
```

<filenameX> can be a combination of both letters and characters. For example, EWNxx_041503.conf1 or location1_Exx00.conf2. Trying to use any other filename format will result in the error message: "EWN_ERROR_BAD_FILE_NAME".



Caution

The *.conf* extensions have special significance. If you save a configuration with <filename-new>.conf1, any existing older <filename-old>.conf1 will be overwritten with the new one.

Copy a backup file to a remote TFTP server

The following commands copies a backup file from the EdgeMarc device to a TFTP server.

```
bash# ewn upload <filename> <tftp server IP Address>
```

Download a backup file from a remote TFTP server

The following command downloads a backup file from a TFTP server to the EdgeMarc device.

```
bash# ewn download <filename> <tftp server IP Address>
```

List available backup files

The following command lists all backup files stored in flash memory. If no file has been saved, the command will only return the bash# prompt.

```
bash# ewn list
```

Delete a backup file

The following command deletes the specified the backup file:

```
bash# ewn delete <filename>
```

Loading a backup file to become the running configuration

The following command loads the specified backup file into RAM and makes it the active running configuration.

```
bash# ewn load <filename>
```



Caution

Issuing this command will automatically restart the EdgeMarc device and therefore interrupt any active voice calls and data sessions.

Restoring a backup file to become the running configuration

The following command deletes all preexisting configurations, restores the specified backup file into RAM, and makes it the active running configuration.

```
bash# ewn restore<filename>
```

Logging off listed users

The following command logs off any listed user logged into the web configuration GUI or the CLI. RADIUS and TACACS users are also tracked.

```
bash# ewn logoff
```

To log off a user, complete the following steps:

1. At the CLI prompt, enter the command **ewn logoff**. A menu appears displaying all listed users who are logged in. Also listed are the ports and ip addresses for those listed users.
2. Enter the number of the assigned user that you wish logoff. A message is displayed confirming that the assigned user has been logged off.

Downloading Files

File Download allows the appliance 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/1.0 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.

When using FTP, File Download will log 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/1.0, 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's RAMDISK by an external management system are not available for HTTP download.



Note

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.

Download files

1. Choose **System > File Download** from the Configuration Menu.
2. Select **Enable File Download**.
3. Enter the IP address of the FTP server and the desired frequency of download.
4. Enter the files to be downloaded. All files must be in the /pub directory on the FTP server.
5. Click **Submit**.
A message indicates that service will be temporarily interrupted.
6. Click **OK** to confirm.

Using the Internal TFTP Server

In some instances, a public TFTP server is not available. Enabling the TFTP server allows configuration and image files to be downloaded from the system by using

TFTP. Configuration and image files can be pushed to the system by a management station using a secure protocol. These files are then served out when an endpoint requests them.

The File Server page is used to enable and configure an internal TFTP file server. The file server is used to store phone configuration information. Enabling the TFTP server will disable the TFTP ALG. Files that are stored on the server are stored in RAM. The files will be lost when the system is rebooted or a Submit is pressed on this page.

Enable the TFTP server

- 1.** Choose **System > File Server** from the Configuration Menu.
- 2.** Configure the server as described in “[File Server Page](#)” on page 256.
- 3.** Click **Submit**.
A message indicates files stored on the RAM disk will be lost and that voice and video services will be interrupted.
- 4.** Click **OK** to confirm.

Edgemarc BGP and Routing Configuration and Troubleshooting

This chapter describes how you can use the EdgeMarc command line interface (CLI) for the EdgeMarc 4500 series to configure and troubleshoot Border Gateway Protocol (BGP). You can use the CLI to enable and configure BGP and routing daemons, as well as troubleshoot existing BGP and routing daemons.

The chapter contains the following sections:

- BGP enablement and configuration
- Troubleshooting using BGP and routing daemons

BGP enablement and configuration

Complete the following steps to enable, connect, and configure the BGP daemon:

1. At the command prompt (**#**), enter the following command:

```
config_routing --bgp --enable
```

The BGP daemon is now enabled.

2. At the command prompt (**#**), complete the following steps:

- a. Enter the following command:

```
config_routing --bgp --connect
```

You are prompted for the BGP password.

- b. Enter the default password: **bgp**

The BGPconsole (**BGP>**) is displayed.

3. At the BGP console (**BGP>**), enter the following command:

```
enable
```

The BGP daemon is now in privileged mode. The BGP privileged mode console (**BGP#**) is displayed.

4. At the BGP privileged mode console (**BGP#**), enter the following command:
config terminal

The BGP daemon is now in BGP terminal configuration mode. The BGP terminal configuration mode console (**BGP(config)#**) is displayed.

5. At the BGP terminal configuration mode console (**BGP(config)#**), add an Autonomous System (AS):
router bgp <AS>

**Note**

<AS> can be any number between 1 and 65535.

The BGP daemon is now in router configuration mode. The router configuration console (**BGP(config-router)#**) is displayed.

6. At the router configuration console (**BGP(config-router)#**) enter the following command:

redistribute connected

The autonomous system is established as a default route for any PE router.

7. To set the BGP router ID and uniquely identify the Edgemarc 4500 device, enter the following command from the router configuration console (**BGP(config-router)#**):

BGP(config-router)# bgp router-id <WAN-IP>

8. To configure a BGP peer, enter the following command from the router configuration console (**BGP(config-router)#**):

neighbor <peer-IP> remote-as <peer-AS>

9. If you are making changes to an existing BGP configuration, you must complete the following additional steps before exiting the BGP daemon:

- a. Exit until you reach the BGP privileged mode console (**BGP#**).

- b. Enter the following command:

clear ip bgp *

The BGP daemon is reset.

10. To save your configuration file, enter the following command from any BGP daemon console:

write file

The configuration file is saved in program memory and its destination is noted.

11. To save your configuration file permanently by storing it in EdgeMarc flash storage, complete the following steps:

- a. Exit from the BGP console by entering exit until you have reached the initial CLI command prompt (#).

- b. At the CLI command prompt (#), enter the following command: **cfg_commit**.

The configuration file is stored in EdgeMarc flash storage.

Troubleshooting using BGP and routing daemons

You can troubleshoot existing routes and configurations using the BGP and routing daemons. Use the BGP daemon to display the current configuration, BGP summary, and BGP neighbors. Use the routing daemon to display all received routes that are mapped by both the provider edge (PE) router and customer edge (CE) router.

The following two topics provide more information

- [Troubleshooting using the BGP daemon](#)
- [Troubleshooting using the routing daemon](#)

Troubleshooting using the BGP daemon

To use the BGP daemon to review existing configurations using the CLI, complete the following steps:

1. At the command prompt (**#**), enter the following command:

```
config_routing --bgp --enable
```

The BGP daemon is now enabled.

2. At the command prompt (**#**), complete the following steps:

- a. Enter the following command:

```
config_routing --bgp --connect
```

You are prompted for the BGP password.

- b. Enter the default password: **bgp**

The BGP console (**BGP>**) is displayed.

3. At the BGP console (**BGP>**), enter the following command:

```
enable
```

The BGP daemon is now in privileged mode. The BGP privileged mode console (**BGP#**) is displayed.

4. To display BGP configuration from the BGP privileged mode console (**BGP#**), enter the following command:

```
show running-config
```

The BGP configuration is displayed.

5. To monitor and debug the BGP daemon, complete the following steps:

- a. From the BGP privileged mode console (**BGP#**), enter the following command:

```
terminal monitor
```

Monitoring the BGP daemon is enabled.

6. At the BGP privileged mode console (**BGP#**), enter the following command:

```
config terminal
```

The BGP daemon is now in BGP terminal configuration mode. The BGP terminal configuration mode console (**BGP(config)#**) is displayed.

- b. .At the BGP terminal configuration mode console (**BGP(config)#**) , enter the following command:

```
log monitor
```

Debugging the BGP daemon is enabled.

7. Exit the BGP terminal configuration mode by entering the following command:

```
exit
```

The BGP privileged mode console (**BGP#**) is displayed

8. To display the BGP summary from the BGP terminal configuration mode (**BGP#**), enter the following command:

```
show ip bgp summary
```

The BGP summary is displayed.

9. To display BGP neighbors from the BGP terminal configuration mode (**BGP#**), enter the following command:

```
show ip bgp neighbors
```

Troubleshooting using the routing daemon

To use the routing daemon to display all received routes that are mapped by both the PE and CE routers, complete the following steps:

1. At the command prompt (**#**), enter the following command:

```
config_routing --bgp --enable
```

The BGP daemon is now enabled.

2. At the command prompt (**#**), complete the following steps:

- a. Enter the following command:

```
config_routing --connect
```

You are prompted for the Routing password.

- b. Enter the default password: **routing**

The routing console (**Routing>**) is displayed.

3. At the routing console (**Routing>**) , enter the following command:

```
show ip route
```

All received routes are displayed.

System Upgrades

This chapter describes how to upgrade the EdgeMarc device to the latest software release available from Edgewater Networks. It contains the following sections:

- Release Information
- Upgrade Procedure for Software Revision 1.3.11 or Later
- Upgrade Procedure for Software Version 1.3.9 or Earlier

Release Information

To display version information for the system, choose **System** from the Configuration Menu. The software version information is presented at the top of the page.

Additional information can be found in the release notes section of our website at:

[http://www.edgewaternetworks.com/Support/SupportDocLanding.html#Release Notes](http://www.edgewaternetworks.com/Support/SupportDocLanding.html#ReleaseNotes)

It is recommended that you reboot the EdgeMarc device before performing an upgrade. The reboot will ensure that enough dynamic memory is available to handle the upgrade process.



Warning

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

Upgrade Procedure for Software Revision 1.3.11 or Later

Use this procedure if your EdgeMarc device is running software revision 1.3.11 or later. The software version is listed on the *System* page of the web GUI.

Upgrade - Revision 1.3.11 or later

1. Select **System > Upgrade Firmware** from the Configuration Menu.
2. Enter the **Download Server** IP address of 204.202.2.188 (the public IP address of the FTP site hosted by Edgewater Networks).
3. Enter the **Filename**: image.bin
4. Click **Submit**.

You can follow the progress of the upgrade by selecting the **refresh the upgrade status** link.



Caution

Do not change the configuration or power off the device until the write is 100 percent complete. The EdgeMarc device may become unusable if the write is interrupted. The flash write can take up to 5 minutes depending on the speed of the download server.

The system will automatically restart after the new image has been loaded.

5. Verify that the upgrade was successful by checking the software revision number found on the *System* page.

Upgrade Procedure for Software Version 1.3.9 or Earlier

Use this procedure if your EdgeMarc device is running software revision 1.3.11 or later. The software version is listed on the *System* page of the web GUI.

We recommend running the upgrade command using the CLI rather than the web GUI. This is because running the command in the CLI provides more feedback to the operator.

Upgrade using local terminal connection

1. Use a straight-through cable to connect to the console port of the EdgeMarc device.
2. Use a terminal emulator such as HyperTerminal set to a baud rate of 9600, 8 data bits, 1 stop bit, and no parity.

Use SSH access

1. Log on as **root**.
2. Enter the **password** (contact Edgewater support for the password)
3. Ping the Edgewater Networks FTP server to determine if you can reach the upgrade server by issuing the following command:
ping 204.202.2.188
4. If the ping was successful enter the upgrade command as follows:
netflash -fk 204.202.2.188 pub/e_<edgemarc device>/flash.bin
You will be prompted for a user ID and password. The user ID is **anonymous** and there is no password. The following is a log of the process:

```
netflash: login to remote host 204.202.2.188
Name (204.202.2.188:root): anonymous
Password:
netflash: ftping file "pub/<dgeMarc device>/flash.bin" from
204.202.2.188
.....
.....
netflash: got "pub/e_<edgemarc device>/flash.bin", netflash: image is
compressed, decompressed length xxxxx
netflash: programing FLASH device /dev/mtd3
.....
.....
Restarting system.
```

The upgrade process takes between 5 and 10 minutes, depending on the speed of the FTP download.



Caution

Do not change the configuration or power off the device until the write operation is 100 percent complete. The EdgeMarc device may become unusable if the write operation is interrupted. The flash write can take up to 5 minutes depending on the speed of the download server.

You may see a “Restarting system” message or your SSH session will exit. This indicates that the system is rebooting. The system takes 1–2 minutes to reboot.

5. Verify that the upgrade was successful by checking the software revision number on the *System* page
6. If you opened an SSH session, you should log out of the EdgeMarc device and close the SSH session by entering **exit** in the command line.

Primary Rate Interface(PRI)

This chapter describes how to configure the ISDN Primary Rate Interface (PRI) on the EdgeMarc appliance. It contains the following sections:

- Overview
- Configuring T1 for PRI
- Configuring Network Side ISDN PRI (PRI/UA)
- Configuring Client Side ISDN PRI (PRI/GW)
- Configuring SIP Trunking for PRI

Overview

The EdgeMarc appliance can be configured to act as a gateway (client device) connecting the IP network to PSTN through a T1 PRI line. It can also work as a network device connecting a PBX to the IP network. The default configuration enables 23 B-channels (64 Kbps each) and 1 D-channel (64 Kbps).

The following applies to the implementation of PRI on the EdgeMarc appliance:

- The appliance can be a client device (gateway) or network device, but not both.
- Supports the following switch types:
 - NISDN-2 or NI2
 - 4ESS
 - 5ESS
 - DMS100
- The highest port number of licensed T1 ports should be used for PRI.

Configuring T1 for PRI

Before PRI can be enabled, following steps must be performed to configure T1:

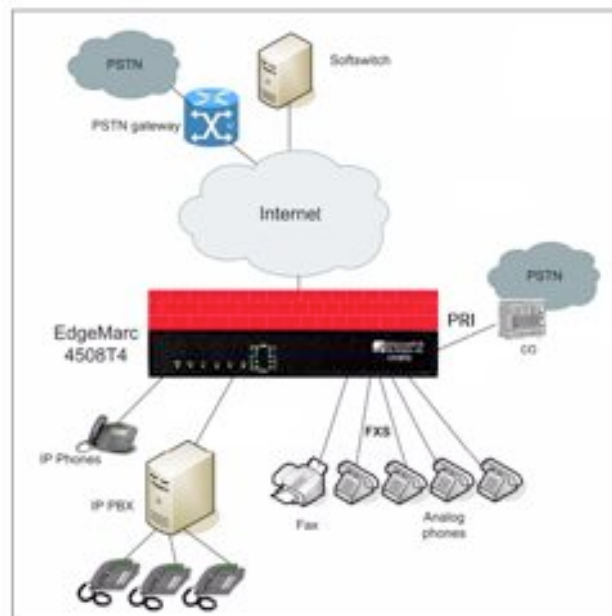
1. Choose the “**T1 configuration**” link under “**System**” on the Configuration menu.
2. If MLPPP is enabled and all licensed T1 ports are used for data, then disable the highest T1 port for data and then select it for PRI/CAS.
3. If MLPPP is not enabled, then choose the highest licensed T1 port for PRI/CAS.

4. The only other parameter that need to be configured is “**LBO**” in the “**Set Interface Configuration**” section. Use the following guidelines when connecting EdgeMarc to a T1 line:
 - DS1 level settings are used when connecting an EdgeMarc to a smartjack or T1 line 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. 0db is used for the longest cable length and -22.5db is used for the shortest cable length.
 - The DSX-1 level settings are used when connecting an EdgeMarc T1 to a private line or a co-resident PBX without a CSU/DSU. The DSX-1 settings can be changed based on the distance between the EdgeMarc and the terminating device.

Configuring Client Side ISDN PRI (PRI/GW)

The Client Side PRI enables the SIP 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. Figure 14 is an example of the Client Side PRI.

Figure 14 Client Side ISDN PRI (PRI/GW)



1. Enable PRI/GW services:
 - a. Choose “**SIP GW**” link from the Configuration Menu
 - b. Check “Enable SIP FXO/Line services” to enable the FXO services

c. Click Submit

- 2.** Choose the “**PRI/Client configuration**” link under “**SIP GW**” from the “**Configuration Menu**”
- 3.** Check “**Enable PRI/GW services**”

- 4.** Click **Submit**.



Note

For complete description of each parameters for Client Side PRI, please refer to [Client Side ISDN PRI \(PRI/GW\) Configuration Page](#)

- 5.** Define the switch type that Client-side PRI will be simulating. The default is NI2.



Note

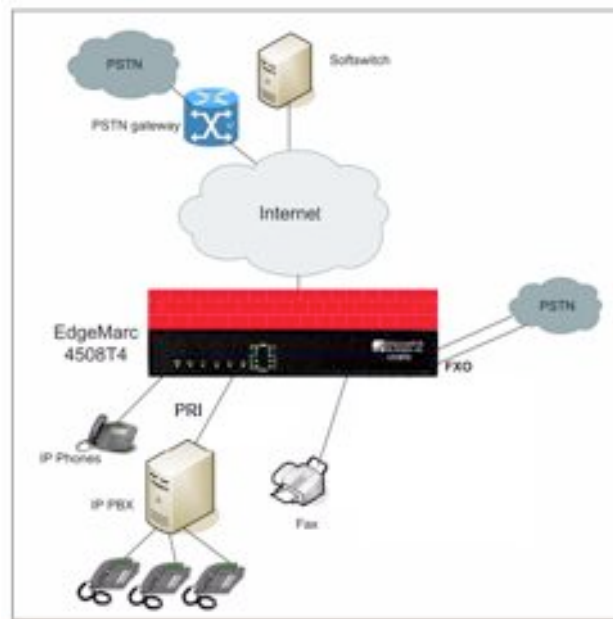
Switch type entry must match the Network-side switch-type to which this interface is connected.

- 6.** Select D-channel number that will be used for Q.931 signaling.
- 7.** Enable/disable each PRI channel.
- 8.** Check PRI connection. If the connection is up, all ports should display a status of “Idle”.
- 9.** If clock signal is provided by the Service Provider then do not check the “**Intenal Clocking**” parameter.
- 10.** If the softswitch requires that endpoint has to be registered before a call can be made, then check the “**Register with SIP server**” parameter and enter all the pertinent information in the following parameters.

Configuring Network Side ISDN PRI (PRI/UA)

The Network Side PRI enables the SIP UA to provide a standard ISDN PRI network side interface to the PBXs and to imitate legacy phone switches. Figure 15 is an example of the Network Side PRI.

Figure 15 Network Side ISDN PRI (PRI/UA)



1. Enable SIP UA services by choosing the “**SIP UA**” link from the “**Configuration Menu**” and checking the “**Enable SIPUA**” parameter.
2. Enable PRI/UA services:
 - a. Choose “**SIP UA**” link from the Configuration Menu
 - b. Choose “**PRI/NET configuration**” submenu.
 - c. Check “**Enable PRI/UA services**”
 - d. Click **Submit**.
 - e. Click **OK** in the warning dialog box.



Note

For complete description of each parameters for Network Side PRI, please refer to [Network Side ISDN PRI \(PRI/UA\) Configuration Page](#)

3. Select the switch type from the drop down list. The default is NI2.



Note

Switch type entry must match the Client-side switch-type to which this interface is connected.

4. Select D-channel number that will be used for Q.931 signaling.

5. Define the device name. This name will be used in the SIP Trunking to define an incoming rule so that all the incoming calls will be handed off to SIP UA which will in turn give it to .



Note

The device name must match the name that will be used in SIP trunking device and dial-rule page for PRI.

6. Enable/disable each PRI channel.
7. Check PRI connection. If the connection is up, all ports should display a status of “Idle”.
8. If clock signal is provided by the PBX then do not check the “**Intenal Clocking**” parameter.
9. If the softswitch requires that endpoint has to be registered before a call can be made, then check the “**Register with SIP server**” parameter and enter all the pertinent information in the following parameters.

Configuring SIP Trunking for PRI

SIP trunking must be configured in order for PRI to work properly. To configure SIP trunking choose the “**VoIP ALG**” link from the “**Configuration Menu**” and then choose the “**SIP>Trunking**” submenu.



Note

For more information on SIP Trunking see “[SIP Trunking](#)” on page 64 or “[SIP Trunking Page](#)” on page 218

Use the following guidelines when configuring SIP trunking for PRI:

Configuration for Client Side PRI

- If SIP GW services have been enabled, then a default route should be set to Internal Gateway whose IP address should be the same address to which SIP GW is attached to.
- Upon enabling the Network Side PRI services, SIP GW will forward all the calls going to the “**Internal Gateway**” to the PRI interface.
- Make sure that the IP address and the port of the “**Internal Gateway**” are the same as *<IP Address>* and *<Port Number>* as displayed in the following message on the “**PRI/Client Configuration**” page: “**SIP/GW is currently bound to address: <IP Address> and port: <Port Number>**”

Configuration for Network Side PRI”

1. Obtain the IP address and port number of the SIP UA from the “**SIP UA>PRI/NET configuration**” page under “**Configuration Menu**” from the following message: **SIP/UA is currently bound to address: <IP Address> and port: <Port Number>**

2. Create a SIP Trunking device for PRI with the same name as the one used on the submenu “**PRI/NET configuration**” of “**SIP UA**” configuration page.



The screenshot shows a web form titled "Add a trunking device". It contains the following fields and controls:

- Action:** A dropdown menu with "Add new trunking device" selected.
- Name:** A text input field containing "pri_net_side".
- Address:** A text input field containing "<IP Address>".
- Port:** A text input field containing "<Port Number>".
- At the bottom left, there are two buttons: "Commit" and "Reset".

3. Associate an inbound default rule with the newly created device.



The screenshot shows a web form titled "Add a rule". It contains the following fields and controls:

- Action:** A dropdown menu with "Add new rule" selected.
- Type:** A dropdown menu with "Inbound" selected.
- Call Party:** A dropdown menu with "Called" selected.
- Default rule:** A checkbox that is checked.
- Priority (redirect only):** An unchecked checkbox.
- Pattern-match (if not default):** An empty text input field.
- Strip digits:** A text input field containing "0".
- Add string:** An empty text input field.
- Trunking device:** A dropdown menu with "pri_net_side {<IP Address>}" selected.
- At the bottom left, there are two buttons: "Commit" and "Reset".



Note

All the inbound traffic coming to SIP UA will be forwarded to the PRI device with the exception of the traffic destined for one of the registered FXS ports.

Syslog Messages

This appendix describes syslog messages for the EdgeMarc appliance.



Note

All firewall-related syslog messages include the string <FW>.

Table 11 Syslog Messages

Message	Description
000:EnableRemoteLog	Allowed Remote Logging
010:Allow-Lan-In	Allowed input packet from the LAN interface
011:Allow-Lan-Tcp-In	Allowed input of TCP packet from the LAN interface
012:Allow-Lan-Udp-In	Allowed input of UDP packet from the LAN interface
013:Allow-Lan-Icmp-In	Allowed input of ICMP packet from the LAN interface
014:Allow-Lan-Out	Allowed output packet from LAN interface
015:Allow-Lan-Tcp-Out	Allowed output of TCP packet from LAN interface
016:Allow-Lan-Udp-Out	Allowed output of UDP packet from LAN interface
017:Allow-Lan-Icmp-Out	Allowed output of ICMP packet from LAN interface
018:Deny-Wan-In	Denied input packet from the WAN interface
019:Deny-Wan-Tcp-In	Denied input of TCP packet from the LAN interface
020:Deny-Wan-Udp-In	Denied input of UDP packet from the LAN interface
021:Deny-Wan-Icmp-In	Denied input of ICMP packet from the LAN interface
022:Deny-Wan-Out	Denied output packet to WAN
023:Deny-Wan-Tcp-Out	Denied output of TCP packet from LAN to WAN
024:Deny-Wan-Udp-Out	Denied output of UDP packet from LAN to WAN
025:Deny-Wan-Icmp-Out	Denied output of Ping/ICMP packet to WAN
026:Allow-Wan-Icmp-Out	Allowed output of Ping/ICMP packet to WAN
027:Allow-Wan-Tcp-Out	Allowed output of TCP packet to WAN

Table 11 Syslog Messages (continued)

Message	Description
030:Deny-Mgcp-Fwd	Denied forwarding of UDP packet to MGCP Softswitch port 2727
034:NoTrack-Lan-Mgcp	No connection tracking of UDP packet from LAN IP to MGCP Softswitch port 2727
038:NoTrack-Wan-Mgcp	No connection tracking of UDP packet from WAN IP to MGCP Softswitch port 2727
042:Allow-Lan-Mgcp	Allowed UDP packet from LAN IP to MGCP Softswitch port 2727
046:Allow-Wan-Mgcp	Allowed UDP packet from WAN IP to MGCP Softswitch port 2727
050:Notrack-Lan-Sip	No connection tracking of UDP packet from LAN IP to SIP Softswitch port 5060
052:Notrack-Wan-Sip	No connection tracking of UDP packet from WAN IP to SIP Softswitch port 5060
054:Allow-Lan-Sip	Allowed UDP packet from LAN IP to SIP port 5050
056:Allow-Wan-Sip	Allowed UDP packet from WAN IP to SIP Softswitch port 5060
058:Deny-Sip-Fwd	Denied forwarding of UDP packet to SIP Softswitch port 5060
070:Allow-Lan-H323-In	Allowed incoming H323 packet from LAN
071:Allow-Lan-H323-Out	Allowed outgoing H323 to LAN
072:Allow-Wan-H323-In	Allowed incoming H323 packet to network port 1718-1719
073:Deny-H323-Fwd	Denied forwarding of UDP packet from LAN to WAN which was destined to H323 port 1718-1719
074:Deny-H323-Fwd	Denied forwarding of TCP packet from LAN to WAN which was destined to H323 port 1720
075:Deny-H323-Fwd	Denied forwarding of UDP packet to H323 port 1718-1719
076:Deny-H323-Fwd	Denied forwarding of TCP packet to H323 port 1720
077:Allow-Wan-H323-Out	Allowed outgoing H323 packet to network port 1718-1719
078:Allow-Wan-H245	Allowed incoming/outgoing H245 packet to/from WAN
079:Allow-Lan-H245	Allowed incoming/outgoing H245 packet to/from LAN
090:NoTrack-Lan-Rtp	No connection tracking for prerouting UDP packet from LAN IP to RTP port 16384-35000

Table 11 Syslog Messages (continued)

Message	Description
091:NoTrack-Lan-Rtp	No connection tracking for output UDP packet from LAN IP to RTP port 16384-35000
092:NoTrack-Wan-Rtp	No connection tracking for prerouting UDP packet from WAN IP to RTP port 16384-35000
093:NoTrack-Wan-Rtp	No connection tracking for output UDP packet from WAN IP to RTP port 16384-35000
094:Deny-Lan-Udp-Fwd	Denied forwarding of UDP packet from LAN IP to RTP port 16384-35000
095:Deny-Wan-Udp-Fwd	Denied forwarding of UDP packet from WAN IP to RTP port 16384-35000
096:Deny-Rtp-Kernel	Denied TCP packet to RTP port 2000
098:Strip-Tos-Bit	Prerouting packet with source address 0000 was stripped off its TOS bit
099:Deny-Icmp-Unreach	Denied ICMP packet of type Port-unreachable
100:Mark-Voice-Pkt	Mark DSCP packet with 0x40
101:Allow-Lan-Udp	Allow UDP packet from/to LAN interface
110:Allow-Lan-Proxy	Allowed LAN packet destined for PROXY ARP IP
111:Allow-Wan-Proxy	Allowed WAN packet from PROXY ARP IP
112:Allow-Proxy-Fwd	Allowed forwarding of packet destined for PROXY ARP IP
113:Allow-Proxy-Fwd	Allowed forwarding of WAN packet from PROXY ARP IP
120:Allow-Nat-Establ	Allowed prerouting NAT packet of an established connection
121:Deny-Wan-Spoof	Denied prerouting WAN packet with spoofed source address
131:Allow-Est-Fwd	Allowed forwarding of packet belongs to an established connection
132:Allow-Lan-Lan-Fwd	Allowed forwarding of packet from LAN to LAN
134:Allow-Lan-Wan-Fwd	Allowed forwarding of packet from LAN to WAN
140:Allow-Nat-Fwd	Allowed posrouting packet from Forward Addresses
141:Allow-Tcpmss-Route	Allowed postrouting TCP packet with flags SYN,RST SYN with TCP Maximum Segment Size adjusted
142:Allow-Fwd	Allowed forwarding of packet destined for Forward Addresses
143:Allow-Fwd	Allowed forwarding of packet destined for Forward Addresses from Input Interface to Output Interface specified in Forward Address menu

Table 11 Syslog Messages (continued)

Message	Description
151:Allow-Dhcp-In	Allowed incoming DHCP packet to LAN interface
152:Allow-Dhcp-Out	Allowed outgoing DHCP packet from LAN interface
153:Allow-BootP-In	Allowed incoming BOOTP packet to LAN interface
154:Allow-BootP-Out	Allowed outgoing BOOTP packet from LAN interface
160:Deny-Port-Scan	Denied Port-scan packet (TCP packet destined for port 0)
161:Deny-Port-Scan	Denied Port-scan packet (UDP packet destined for port 0)
170:Deny-Spoof	Denied Spoofed packet of Local address (127000) from non-local interface
171:Deny-Invalid-Src	Denied packet with Invalid source address (255255255255)
172:Deny-Invalid-Dst	Denied packet with Invalid destination port (0000)
173:Deny-Invalid-Src	Denied packet with Invalid source address (224000)
180:Deny-Invalid-State	Denied packet with state INVALID
182:Deny-Tcp-Invalid	Denied prerouting TCP packet with flags SYN,RST SYN,RST
183:Deny-Tcp-Invalid	Denied prerouting TCP packet with flags SYN,FIN SYN,FIN
184:Deny-Tcp-Invalid	Denied prerouting TCP packet with flag FIN FIN
185:Deny-Tcp-Invalid	Denied prerouting TCP packet with all flags set
186:Deny-Tcp-Invalid	Denied prerouting TCP packet with all flags set
187:Deny-Tcp-Invalid	Denied prerouting TCP packet with flag NONE ALL
188:Deny-Tcp-Invalid	Denied prerouting TCP packet with flag ALL NONE
189:Deny-Tcp-Invalid	Denied prerouting TCP packet requesting new connection with flag RST RST
190:Deny-Tcp-Invalid	Denied prerouting TCP packet with flag FIN FIN that doesn't belong to any connection
191:Deny-Tcp-Invalid	Denied prerouting TCP packet with flag RST RST that doesn't belong to any connection
200:Deny-Http-Wan-In	Denied HTTP packet from WAN due to HTTP Inbound being disabled
202:Allow-Http-Wan-In	Allowed HTTP Inbound packet from WAN
203:Deny-Http-Lan-In	Denied LAN HTTP packet from non-management host
204:Deny-Http-Wan-Out	Denied HTTP packet to WAN due to HTTP Outbound being disabled

Table 11 Syslog Messages (continued)

Message	Description
206:Allow-Http-Wan-Out	Allowed HTTP Outbound packet to WAN
207:Allow-Http-Lan-In	Allowed HTTP Inbound packet from LAN
209:Allow-Http-Lan-Out	Allowed HTTP Outbound packet to LAN
210:Deny-Https-Wan-In	Denied HTTPS packet from WAN due to HTTPS Inbound being disabled
212:Allow-Https-Wan-In	Allowed HTTPS packet from WAN
213:Deny-Https-Lan-In	Denied LAN HTTPS packet from non-management host
214:Deny-Https-Wan-Out	Denied HTTPS Outbound packet to WAN due to HTTPS Outbound being disabled
216:Allow-Https-Wan-Out	Allowed HTTPS Outbound packet to WAN
217:Allow-Https-Lan-In	Allowed HTTPS packet from LAN
219:Allow-Https-Lan-Out	Allowed HTTPS Outbound packet to LAN
220:Deny-Telnet-Wan-In	Denied Telnet packet from WAN due to Telnet Inbound being disabled
222:Allow-Telnet-Wan-In	Allowed Telnet packet from WAN
223:Deny-Telnet-Lan-In	Denied LAN TCP packet from non-management host
224:Deny-Telnet-Wan-Out	Denied Telnet Outbound packet to WAN due to Telnet Outbound being disabled
226:Allow-Telnet-Wan-Out	Allowed Telnet packet from WAN
227:Allow-Telnet-Lan-In	Allowed Telnet packet from LAN
228:Allow-Telnet-Lan-Out	Allowed Telnet packet from LAN
230:Deny-Ssh-Wan-In	Denied SSH packet from WAN due to SSH Inbound being disabled
232:Allow-Ssh-Wan-In	Allowed TCP packet to SSH port
233:Deny-Ssh-Lan-In	Denied LAN SSH packet from non-management host
235:Deny-Ssh-Wan-Out	Denied SSH Outbound packet to WAN due to SSH Outbound being disabled
236:Allow-Ssh-Wan-Out	Allowed SSH Outbound packet to WAN
237:Allow-Ssh-Lan-In	Allowed SSH packet from LAN
239:Allow-Ssh-Lan-Out	Allowed SSH Outbound packet to LAN
240:Deny-Smtp-In	Denied SMTP packet from WAN to LAN
242:Allow-Smtp-In	Allowed SMTP packet from WAN to LAN
245:Deny-Smtp-Wan-Out	Denied SMTP packet to WAN due to SMTP Outbound being disabled
246:Allow-Smtp-Wan-Out	Allowed SMTP packet to WAN

Table 11 Syslog Messages (continued)

Message	Description
247:Allow-Smtp-Lan-Out	Allowed SMTP packet to LAN
251:Allow-Http-In	Allowed HTTP packet to Trusted Management Address
252:Allow-Http-Out	Allowed HTTP packet from Trusted Management Address
261:Allow-Https-In	Allowed TCP packet from Trusted Management Address via HTTPS port
262:Allow-Https-Out	Allowed TCP packet to Trusted Management Address via HTTPS port
271:Allow-Telnet-In	Allowed TCP packet from Trusted Management Address via Telnet port
272:Allow-Telnet-Out	Allowed TCP packet to Trusted Management Address via Telnet port
281:Allow-Ssh-In	Allowed TCP packet from Trusted Management Address via SSH port
282:Allow-Ssh-Out	Allowed TCP packet to Trusted Management Address via SSH port
290:Deny-Snmp-Wan-In	Denied SNMP packet from WAN due to SNMP Inbound being disabled
291:Allow-Snmp-Wan-In	Allowed SNMP packet from WAN
292:Allow-Snmp-In	Allowed UDP packet from Trusted Management Address via SNMP port
293:Allow-Snmp-Out	Allowed UDP packet to Trusted Management Address via SNMP port
295:Deny-Snmp-Wan-Out	Denied SNMP packet to WAN due to SNMP Outbound being disabled
296:Allow-Snmp-Wan-Out	Allowed SNMP packet to WAN
297:Deny-Snmp-Lan-In	Denied LAN SNMP packet from non-management host
298:Allow-Snmp-Lan-In	Allowed SNMP packet from LAN
299:Allow-Snmp-Lan-Out	Allowed SNMP packet to LAN
301:Deny-Dns-In	Denied DNS packet from WAN to LAN
302:Allow-Dns-In	Allowed DNS packet from WAN to LAN
305:Deny-Dns-Wan-Out	Denied DNS packet to WAN due to DNS Outbound being disabled
306:Allow-Dns-Wan-Out	Allowed DNS packet to WAN
307:Allow-Dns-Lan-Out	Allowed DNS packet to LAN
310:Deny-Imap-In	Denied IMAP packet from WAN to LAN due to IMAP protocol being disabled
312:Allow-Imap-In	Allowed IMAP packet from WAN to LAN

Table 11 Syslog Messages (continued)

Message	Description
314:Allow-Imap-Lan-Out	Allowed IMAP packet to LAN
315:Deny-Imap-Wan-Out	Deny IMAP packet to WAN due to IMAP Outbound being disabled
317:Allow-Imap-Wan-Out	Allowed IMAP packet to WAN
320:Deny-Pop3-In	Denied POP3 packet from WAN to LAN
322:Allow-Pop3-In	Allowed POP3 packet from WAN to LAN
325:Deny-Pop3-Wan-Out	Denied POP3 packet to WAN due to POP3 Outbound being disabled
327:Allow-Pop3-Wan-Out	Allowed POP3 packet to WAN
329:Allow-Pop3-Lan-Out	Allowed POP3 packet to LAN
330:Deny-Ntp-In	Denied NTP packet from the network
331:Allow-Ntp-In	Allowed NTP packet from the network
332:Deny-Ntp-Wan-Out	Denied NTP packet to the network due to NTP Outbound being disabled
333:Allow-Ntp-Wan-Out	Allowed NTP packet to the network
334:Allow-Ntp-Lan-Out	Allowed NTP packet to LAN
338:Deny-Ping-In-Limit	Denied Inbound ICMP packet (from WAN) due to Ping limit being exceeded
339:Deny-Ping-Out-Limit	Denied Outbound ICMP packet (to WAN) due to Ping limit being exceeded
340:Deny-Wan-Ping	Denied Inbound ICMP packet (from WAN) due to Ping being disallowed from GUI
341:Allow-Ping-Route	Allowed ICMP type 3 code 3 packet from WAN
342:Deny-Ping-Vlan	Denied Inbound ICMP packet from WAN to VLAN
343:Allow-Ping-Reply	Allowed Inbound ICMP type 0 of an established connection
344:Allow-Ping-Err	Allowed Inbound ICMP type 3-4 (fragmentation, unreachable, source quench,)
345:Allow-Ping-Redir	Allowed Inbound ICMP type 5 (redirection) of an established connection
346:Deny-Ping-Other	Denied Inbound Ping/ICMP packet that are not allowed from WAN
347:Deny-Ping-Wan-Out	Denied Ping/ICMP packet to WAN due to Outbound Ping being disabled from GUI
348:Allow-Ping-Wan-Out	Allowed Ping/ICMP packet to WAN
349:Allow-Ping-Request	Allowed Inbound Ping/ICMP type 8
350:Allow-Vrrp	Allowed VRRP packet
351:Allow-Ping-Lan-Out	Allowed Ping/ICMP packet to LAN

Table 11 Syslog Messages (continued)

Message	Description
353:Deny-Wan-Pptp	Denied Incoming PPTP packet due to PPTP not enabled
354:Deny-Pptp-In-Limit	Denied Incoming PPTP packet due to limit on new connection rate being exceeded
360:Allow-Console	Allowed TCP packet from CONSOLE IP to port 10115
361:Allow-Peer	Allowed TCP packet from PEER IP to port 10115
362:Allow-Peer	Allowed UDP packet from PEER IP to Allowed UDP port
363:Allow-Peer	Allowed UDP packet from PEER IP to Allowed UDP port
364:Allow-Mgmt	Allowed postrouting packet from Trusted Management Address
365:Deny-Eth2	Denied packet from eth2 of EdgeProtect to WAN
366:Deny-Eth2	Denied packet from eth2 of EdgeProtect to LAN
367:Deny-Unknown-Mgmt	Denied packet from unknown Management IP
371:Allow-Wan-Pptp	Allowed WAN PPTP packet
372:Allow-Pptp-Fwd	Allowed forwarding of TCP packet from WAN to PPTP port
374:Allow-Ipsec	Allowed forwarding of UDP packet to port 500 of WAN IP
375:Allow-Ipsec	Allowed forwarding of IPSEC packet to WAN IP
376:Allow-Ipsec	Allowed forwarding of packet from ipsec0 interface
377:Allow-Ipsec	Allowed forwarding of packet to ipsec0 interface
380:Allow-Port-Fwd	Allowed forwarding of packet from WAN to Destination IP
381:Allow-Port-Fwd	Allowed forwarding of packet from WAN to Destination IP & Port
401:Allow-Ftp-In	Allowed FTP packet from WAN to LAN
402:Deny-Ftp-In	Denied FTP packet from WAN to LAN
405:Allow-Ftp-Wan-Out	Allowed FTP packet to WAN
406:Allow-Ftp-Lan-Out	Allowed FTP packet to LAN
407:Deny-Ftp-Wan-Out	Denied FTP packet to WAN due to FTP Outbound being disabled
410:Deny-Tftp-In	Denied incoming TFTP packet from WAN
411:Allow-Tftp-In	Allowed incoming TFTP packet from WAN
412:Deny-Tftp-Wan-Out	Denied outgoing TFTP packet to WAN
413:Allow-Tftp-Wan-Out	Allowed outgoing TFTP packet to WAN

Table 11 Syslog Messages (continued)

Message	Description
416:Allow-Tftp-Lan-Out	Allowed outgoing TFTP packet to LAN
440:Deny-Tcp-In-Ses	Denied new inbound TCP session as Inbound Connection Rate Limit is exceeded
441:Deny-Udp-In-Ses	Denied new inbound UDP session as Inbound Connection Rate Limit is exceeded
450:Deny-Tcp-Out-Ses	Denied new outbound TCP session as Outbound Connection Rate Limit is exceeded
451:Deny-Udp-Out-Ses	Denied new outbound UDP session as Outbound Connection Rate Limit is exceeded
460:Allow-Radius-Wan	Allowed Radius UDP packet from/to WAN
461:Allow-Radius-Lan	Allowed Radius UDP packet from/to LAN
560:Allow-Tacacs-Wan	Allowed Tacacs TCP packet from/to WAN
561:Allow-Tacacs-Lan	Allowed Tacacs TCP packet from/to LAN
600:Masquerade-Out	Masquerade outbound packet
601:Nat-In	Dynamic Nat performed on inbound packet
602:Nat-Out	Static Nat performed on outbound packet
700:Deny-Http-Wan-Fwd	Denied forwarding HTTP packet to WAN due to HTTP being disabled
702:Allow-Http-Wan-Fwd	Allowed forwarding HTTP packet to WAN
705:Deny-Pop3-Wan-Fwd	Denied forwarding POP3/POP3S packet to WAN due to POP3 being disabled
706:Allow-Pop3-Wan-Fwd	Allowed forwarding POP3/POP3S packet to WAN
710:Deny-Https-Wan-Fwd	Denied forwarding HTTPS packet to WAN due to HTTPS being disabled
712:Allow-Https-Wan-Fwd	Allowed forwarding HTTPS packet to WAN
715:Deny-Imap-Wan-Fwd	Denied forwarding IMAP/IMAPS packet to WAN due to IMAP being disabled
716:Allow-Imap-Wan-Fwd	Allowed forwarding IMAP/IMAPS packet to WAN
720:Deny-Telnet-Wan-Fwd	Denied forwarding Telnet packet to WAN due to Telnet being disabled
722:Allow-Telnet-Wan-Fwd	Allowed forwarding Telnet packet to WAN
725:Deny-Wan-Ping-Fwd	Denied forwarding PING packet to WAN due to PING being disabled
730:Deny-Ssh-Wan-Fwd	Denied forwarding SSH packet to WAN due to SSH being disabled
731:Allow-Ping-Wan-Fwd	Allowed forwarding ICMP packet to WAN
732:Allow-Ssh-Wan-Fwd	Allowed forwarding SSH packet to WAN
740:Deny-Snmp-Wan-Fwd	Denied forwarding SNMP packet to WAN due to SNMP being disabled

Table 11 Syslog Messages (continued)

Message	Description
742:Allow-Snmp-Wan-Fwd	Allowed forwarding SNMP packet to WAN
750:Deny-Ftp-Wan-Fwd	Denied forwarding FTP packet to WAN due to FTP being disabled
752:Allow-Ftp-Wan-Fwd	Allowed forwarding FTP packet to WAN
760:Deny-Smtp-Wan-Fwd	Denied forwarding SMTP packet to WAN due to SMTP being disabled
762:Allow-Smtp-Wan-Fwd	Allowed forwarding SMTP packet to WAN
770:Deny-Dns-Wan-Fwd	Denied forwarding DNS packet to WAN due to DNS being disabled
772:Allow-Dns-Wan-Fwd	Allowed forwarding DNS packet to WAN
780:Deny-Ntp-Wan-Fwd	Denied forwarding NTP packet to WAN due to NTP being disabled
782:Allow-Ntp-Wan-Fwd	Allowed forwarding NTP packet to WAN
790:Deny-Tftp-Wan-Fwd	Denied forwarding TFTP packet to WAN due to TFTP being disabled
792:Allow-Tftp-Wan-Fwd	Allowed forwarding TFTP packet to WAN
802:Allow-Wan-Http-Fwd	Allowed forwarding HTTP packet from WAN
805:Deny-Wan-Pop3-Fwd	Denied forwarding POP3/POP3S packet from WAN due to POP3 being disabled
806:Allow-Wan-Pop3-Fwd	Allowed forwarding POP3/POP3S packet from WAN
812:Allow-Wan-Https-Fwd	Allowed forwarding HTTPS packet from WAN
815:Deny-Wan-Imap-Fwd	Denied forwarding IMAP/IMAPS packet from WAN due to IMAP being disabled
816:Allow-Wan-Imap-Fwd	Allowed forwarding IMAP/IMAPS packet from WAN
822:Allow-Wan-Telnet-Fwd	Allowed forwarding Telnet packet from WAN
825:Deny-Wan-Ping-Fwd	Denied forwarding PING packet from WAN due to PING being disabled
826:Deny-Ping-Vlan-Fwd	Denied forwarding PING packet from WAN to VLAN
827:Allow-Ping-Rpl-Fwd	Allowed forwarding of Ping Reply packet from WAN
828:Allow-Ping-Err-Fwd	Allowed forwarding of ICMP Error packet from WAN
829:Allow-Ping-Rdr-Fwd	Allowed forwarding of ICMP Redirection packet from WAN
832:Allow-Wan-Ssh-Fwd	Allowed forwarding SSH packet from WAN
842:Allow-Wan-Snmp-Fwd	Allowed forwarding SNMP packet from WAN
850:Deny-Wan-Ftp-Fwd	Denied forwarding FTP packet from WAN due to FTP being disabled

Table 11 Syslog Messages (continued)

Message	Description
852:Allow-Wan-Ftp-Fwd	Allowed forwarding FTP packet from WAN
860:Deny-Wan-Smtp-Fwd	Denied forwarding SMTP packet from WAN due to SMTP being disabled
862:Allow-Wan-Smtp-Fwd	Allowed forwarding SMTP packet from WAN
870:Deny-Wan-Dns-Fwd	Denied forwarding DNS packet from WAN due to DNS being disabled
872:Allow-Wan-Dns-Fwd	Allowed forwarding DNS packet from WAN
880:Deny-Wan-Ntp-Fwd	Denied forwarding NTP packet from WAN due to NTP being disabled
882:Allow-Wan-Ntp-Fwd	Allowed forwarding NTP packet from WAN
890:Deny-Wan-Tftp-Fwd	Denied forwarding TFTP packet from WAN due to TFTP being disabled
892:Allow-Wan-Tftp-Fwd	Allowed forwarding TFTP packet from WAN
900:Deny-Wan-Syn-Dos	Denied SYN-flood packet from WAN
902:Deny-Wan-Icmp-Dos	Denied ICMP-flood packet from WAN
904:Deny-Wan-Udp-Dos	Denied UDP-flood packet from WAN
906:Deny-Wan-Rst-Dos	Denied RST-flood packet from WAN
950:Allow-Lan-Tcp-In	Allowed incoming LAN TCP packet
951:Allow-Lan-Udp-In	Allowed incoming LAN UDP packet
952:Allow-Lan-Icmp-In	Allowed incoming LAN ICMP packet
954:Allow-Lan-In	Allowed incoming LAN packet
960:Allow-Lan-Tcp-Out	Allowed outgoing LAN TCP packet
961:Allow-Lan-Udp-Out	Allowed outgoing LAN UDP packet
962:Allow-Lan-Icmp-Out	Allowed outgoing LAN ICMP packet
964:Allow-Lan-Out	Allowed outgoing LAN packet
970:Allow-Wan-Tcp-In	Allowed incoming WAN TCP packet
971:Allow-Wan-Udp-In	Allowed incoming WAN UDP packet
972:Allow-Wan-Icmp-In	Allowed incoming WAN ICMP packet
973:Allow-Wan-Pptp-In	Allowed incoming WAN PPTP packet
974:Allow-Wan-In	Allowed incoming WAN packet
980:Allow-Wan-Tcp-Out	Allowed outgoing WAN TCP packet
981:Allow-Wan-Udp-Out	Allowed outgoing WAN UDP packet
982:Allow-Wan-Icmp-Out	Allowed outgoing WAN ICMP packet
983:Allow-Wan-Pptp-Out	Allowed outgoing WAN PPTP packet
984:Allow-Wan-Out	Allowed outgoing WAN packet
991:Allow-Lan-Fwd	Allowed forwarding of packet from LAN interface

Table 11 Syslog Messages (continued)

Message	Description
995:Allow-Wan-Out-Any	Allowed output of packet from WAN interface
996:NoTrack-Local-Msg	No tracking of voice signaling packet from Local interface to LAN IP address
997:Deny-Wan-Fwd	Denied forwarding of packet from WAN to LAN

Configuration Parameters

This appendix describes all the parameters available on the following EdgeMarc device configuration pages:

- Network Page
- Subinterfaces Page
- DHCP Relay Page
- DHCP Server Page
- DHCP Leases Page
- Standard Firewall Page
- Advanced Firewall Page
- Custom Rules Page
- Current Advanced Firewall Rules (Show Rules)
- Forwarding Rules Page
- Message of the Day Page
- NAT Pages
- Traffic Shaper Page
- Advanced Traffic Shaper Page
- H.323 Settings Page
- H.323 Activity Page
- H.323 Alias Manipulation Page
- H.323 Neighboring Page
- MGCP Settings Page
- SIP Settings Page
- SIP Trunking Page
- Survivability Page
- FXS/Phone Port Settings - Basic (SIP UA) Page
- FXS/Phone Port Settings - Advanced Page
- FXS/Phone Port FAX Settings Page
- Distinctive Ring Page
- SIP FXO/Line Port Configuration (SIP GW) Page
- VPN Page
- VPN Subnet Page
- VPN Tunnel Settings Page
- Certificate Page
- Clients List Page
- Dynamic DNS Page

- File Download Page
- File Server Page
- Network Information
- Network Restart Page
- Network Test Tools Page
- Proxy ARP Page
- RADIUS Settings Page
- Reboot System Page
- Route Page
- Services Configuration
- Set Link Page
- Stateful Failover
- System Time Page
- Test UA Settings page
- T1 Configuration Page - MLPPPoFR
- TACACS Settings Page
- Upgrade Firmware Page
- User Commands Page
- VoIP Subnet Routing Page
- VLAN Configuration Page
- Wireless Configuration Page
- Client Side ISDN PRI (PRI/GW) Configuration Page
- Network Side ISDN PRI (PRI/UA) Configuration Page
- WAN Link Redundancy Configuration Page

Network Page

Use this page to configure networking configuration parameters for the public and private networks. [Table 12](#) describes the parameters on the page.

To access this page, choose **Network** from the Configuration Menu.

Network

[Help](#)

Networking configuration information for the public and private networks.

LAN Interface Settings:

IP Address:
 Subnet Mask:
 Enable VLAN support
[VLAN Configuration](#)

WAN Interface Settings:

- ADSL-PPPoE
 DHCP
 Static IP Address
 VLAN
 EVDO
 T1/E1

Note: In case of dynamic links, this DNS server address will override the DNS server address obtained from the Servers. Default value for dynamic links is obtained from the server, if left blank.

Primary DNS Server:
 Secondary DNS Server:

Primary WAN Redundancy Settings:

Enable Ping based status detection:
 Ping Host:
 (Note: If the Ping host is left blank, the default gateway for the interface will be pinged.)

[To configure Secondary Interface click here](#)

Table 12 Network Parameters

Item	Description
LAN Interface Settings	
IP Address	Enter the IP address needed to establish the connection to the LAN. In addition to needing an Internet connection, the system must also be attached to your LAN to serve your voice, video and data needs.
Subnet Mask	Enter the network mask associated with the IP address. The default value is 255.255.255.0.
VLAN Support	Select to enable VLAN support in the LAN.
Configure Wireless	Link to the wireless configuration page. The value shows the status of the wireless link. Note: This link is only visible for the models with WAP.
WAN Interface Settings	
Radio buttons	Select the method used to obtain a connection to the Internet: <ul style="list-style-type: none"> ADSL-PPPoE — When this option is selected, only areas B and C from the above figure are visible. ADSL-PPPoATM — When this option is selected, only areas A, B, and C are visible from the above figure. NOTE: This option is available only on ADSL WAN based models. DHCP — Allows the device to obtain the WAN-side IP address using a DHCP server available from the WAN side of the network. NOTE: To see the WAN IP address for the system, go to the Network Information page. Only area C and F are visible for this option. Static IP Address — Allows you to configure the WAN interface with a static IP address (default). Areas C, D, and F are visible for this option. VLAN - Allows you to use the VLAN defined in EVDO — Allows the device to use select 3G cards. Only area C and F are visible for this option. Note: For a list of specific EVDO cards that are supported by the EdgeMarc, visit http://portal.knowledgebase.net/article.asp?article=291396&p=4739. T1 — Allows you to configure the WAN interface with a static IP address and also configure and test the T1 interface on the system on the T1 Configuration page. You can click the underlined link to open the T1 Configuration page. For information on using the T1 Configuration page, see Test UA Settings page on page 279. Areas C, D, and F are visible for this option.
VPI	Enter the VPI value assigned by your network provider
VCI	Enter the VCI value assigned by your network provider
User Name	Enter the user name assigned by your network provider.

Table 12 Network Parameters (continued)

Item	Description
Password	Enter the password assigned by your network provider.
Keepalive Ping	Select to send an ICMP echo request to its gateway every minute to ensure that the ISP keeps the PPPoE connection open.
PPPoE Link Status (view only)	View the status of the PPPoE line.
IP Address	IP address to be assigned manually.
Subnet Mask	Subnet mask to be assigned manually.

Network Settings

Note: Enter these settings if you selected Static IP Address or T1 in the WAN interface Settings area.

Default Gateway	Enter the default IP gateway for the system. This gateway will be on the same IP subnet as the IP address.
Primary DNS	Enter the primary DNS server as supplied by the ISP.
Secondary DNS	Enter the secondary DNS server as supplied by the ISP. Used if the primary server is unavailable.

Primary WAN Redundancy Settings

Enable Ping based status detection	If WLR is enabled and this field is checked, then the system sends ICMP packets to the "Ping Hot" and if no response is received, then the link is declared as down.
Ping Host	If "Enable Ping based status detection" is checked and WLR is enabled, then ICMP packets will be sent to the host whose IP address is specified in this field.

The Network page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

Subinterfaces Page

Use this page to assign additional IP addresses to a system interface. [Table 13](#) describes the parameters on the page. To access this page, choose **Network > Subinterfaces** from the Configuration Menu.

[Help](#)

Subinterfaces

Subinterfaces allows an administrator to assign additional IP addresses to a system interface. After creating a LAN subinterface, it is often necessary to configure a firewall forwarding rule to permit IP packets through the system. To configure forwarding, visit the [Forwarding Rules](#) page.

Subinterfaces			
Select: All None		Action: <input type="button" value="Delete"/>	
	IP Address	Netmask	Interface
<input type="checkbox"/>	1.1.1.1	255.255.255.0	LAN

Add a Subinterface:

IP Address:

Netmask:

Interface:

Table 13 Network Subinterface Page Parameters

Item	Description
IP Address	Enter the IP address of the subinterface.
Netmask	Enter the network mask associated with the IP address. The default value is 255.255.255.0.
Interface	Select whether the interface is for the LAN or WAN.

The Subinterfaces page contains the following buttons:

Add	Adds the specified entry
Delete	Deletes the selected entries.
Clear	Clears all fields and selections and allows you to enter new information.

WAN VLAN Configuration

Use this page to configure the VLANs that will be connected to the WAN. [Table 15](#) describes the parameters on the page. To access this page, choose **Network > WAN VLAN Configuration** from the Configuration Menu.

Note: This option will only be visible if VLAN has been selected as the specified WAN connection to the Internet.

WAN VLAN Configuration

[Help](#)

WAN VLAN Configuration				
Enable	VLAN ID	IP Address	Subnet Mask	Gateway IP
Data <input checked="" type="checkbox"/>	1	12.48.202.253	255.255.254.0	12.48.202.1
Voice <input type="checkbox"/>	2			

Additional WAN VLANs			
Select: All None		Action: <input type="button" value="Delete"/>	
VLAN ID	IP Address	Subnet Mask	
The list is currently empty			

Create an additional WAN VLAN

VLAN ID:

IP Address:

Subnet Mask:

Table 14 WAN VLAN Configuration

Item	Description
WAN VLAN List	
Enable and disable data or voice VLANs.	
Enable (checkbox)	Select the VLAN that will be enabled or disabled.
Create additional WAN VLANs	
Add another WAN VLAN to the WAN VLAN list.	
VLAN ID	Enter the ID of the VLAN interface
IP Address	Enter the IP address of the VLAN interface.
Netmask	Enter the network mask associated with the IP address. The default value is 255.255.255.0.

The Subinterfaces page contains the following buttons:

Commit	Commits the specified entry
Delete	Deletes the selected entries.
Clear	Clears all fields and selections and allows you to enter new information.

DHCP Relay Page

Use this page to enable DHCP relay. [Table 15](#) describes the parameters on the page. To access this page, choose **DHCP Relay** from the Configuration Menu.

DHCP Relay [Help](#)

Enable DHCP Relay:

DHCP Relay IP Address:

Table 15 DHCP Relay Parameters

Item	Description
Enable DHCP Relay	Select this checkbox to enable DHCP Relay.
DHCP Relay IP Address	Enter the IP address of the DHCP server where the system will forward traffic.

The DHCP Relay page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

DHCP Server Page

Use this page to configure the internal DHCP server. [Table 16](#) describes the parameters on the page.

To access this page, choose **DHCP Server** from the Configuration Menu.

DHCP Server
[Help](#)

DHCP IP Address Ranges		
Start Address	End Address	Action
192.168.1.50	192.168.1.200	
192.168.1. <input style="width: 40px;" type="text" value="2"/>	192.168.1. <input style="width: 40px;" type="text" value="2"/>	<input type="button" value="Add"/>

VLAN:

Enable DHCP Server:

Subnet Mask: 255.255.255.0

Lease Duration (Days):

Time Offset, +/- hours (option 2):

NTP Server Address (option 42):

WINS Address (option 44):

TFTP/FTP Server Name (option 66):

VLAN ID Discovery (option 129):

From [Network](#) page:

Primary DNS: 209.81.59.2

Secondary DNS: 209.81.9.151

Default Gateway: 192.168.1.1

Table 16 DHCP Server Parameters

Item	Description
DHCP IP Address Ranges Table	
	Shows the dynamic addresses to use for the LAN devices.
	Enter individual DHCP IP addresses or a range. Assign static IP addresses for any common-access devices, such as printers or fax machines. To configure an address range, select the appropriate values and click Add . To delete an address, highlight the address and press the Delete key on your keyboard.
VLAN	Select the VLAN served by the DHCP server.
Enable DHCP Server	Select this checkbox to enable the DHCP server.
Subnet Mask	Enter the Subnet Mask address for the DHCP pool. The default implied value is 255.255.255.0.

Table 16 DHCP Server Parameters (continued)

Item	Description
Lease Duration (Days)	Enter the number of days you want to lease the DHCP service. This is the amount of time a DHCP service will remain connected without lapse. Resource allocation and cost might influence the quantity assigned. The value can be 1 day minimum and 30 days maximum.
Time Offset, +/- hours (option 2)	Set the time offset in hours from UTC (Universal time Code) for your local location.
NTP Server Address (option 42)	Set the Network Time Protocol (NTP) address that is served out by DHCP.
WINS Address (option 44)	The Windows Internal Naming Service (WINS) is a service that 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)	Set the TFTP/FTP server name that is served out by DHCP. By default, this option is the same as the TFTP server on the ALG page.
VLAN ID Discovery (option 129)	Set the VLAN ID that Polycom phones will acquire after rebooting. Note: The Polycom phone boots on the Data VLAN “Native VLAN” by default and acquires the 129 Option. Upon learning option 129, the phone re-boots with the correct VLAN ID

The DHCP Relay page contains the following buttons:

Add	Adds the specified entry.
Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

DHCP Leases Page

Use this page to view address information about hosts that are currently leasing DHCP addresses. [Table 17](#) describes the parameters on the page.

To access this page, choose **DHCP Server > DHCP Leases** from the Configuration Menu.

DHCP Leases			
DHCP Leases displays information about hosts who are currently leasing a DHCP address.			
DHCP Leases Table			
Hostname	IP Address	Mac Address	Expires
imran_laptop	192.168.1.50	00:14:22:ae:7e:f7	2007/06/01 00:24:19

Table 17 DHCP Leases Parameters

Item	Description
Hostname	Name of a host that is currently using a DHCP address.
IP Address	IP address of the host.
MAC Address	MAC address of the host.
Expires	Date and time that the DHCP address expires.

There are no buttons on the DHCP Leases page.

Standard Firewall Page

Use this page to configure the basic Edgewater appliance firewall. [Table 18](#) describes the parameters on the page.

To access this page:

- If the standard firewall is currently enabled (default), choose **Standard Firewall** from the Configuration Menu.
- If the advanced firewall has been enabled, choose **Advanced Firewall** from the Configuration Menu, and then click the link at the bottom of the page to open the Standard Firewall page.

[Help](#)

Standard Firewall

Enable Firewall for WAN:

Basic WAN Firewall Settings:
 These settings apply to services that are running on the System.

Allow HTTP access through firewall:

Allow HTTPS access through firewall:

Allow TELNET access through firewall:

Allow SSH access through firewall:

Allow SNMP access through firewall:

Allow TCP Port:

Allow UDP Port:

Trusted Management Addresses:
 Apply basic settings configuration only to the following addresses:

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

Forwarding WAN Firewall Settings:
 These settings apply to packets being forwarded to systems running behind the firewall.

Enable Firewall Logging:

Enable PPTP Server Pass-through:

PPTP Server IP Address:

Firewall Selection:
 To configure using Advanced Firewall, [click here](#)

Table 18 Standard Firewall Parameters

Item	Description
Enable Firewall for WAN	Activates firewall features for the WAN interface.

Table 18 Standard Firewall Parameters (continued)

Item	Description
Basic WAN Firewall Settings	
Allow HTTPS Access Through Firewall	Select this to allow HTTPS management of the system from the WAN interface.
Allow TELNET Access Through Firewall	Select this to allow Telnet management of the system from the WAN interface.
Allow SSH Access Through Firewall	Select this to allow SSH version 2 ONLY management of the system from the WAN interface.
Allow SNMP Access Through Firewall	Select this to allow SNMP V1 and V3 management of the system from the WAN interface.
Allow TCP Port	Specify the TCP port numbers to which access will be granted. Use spaces to separate multiple port values (for example 8070 8080 8090).
Allow UDP Port	Specify the UDP port numbers to which access will be granted. Use spaces to separate multiple port values (for example 8070 8080 8090).
Trusted Management Addresses	
	Use this area to limit the addresses to which the configuration applies. You can specify an IP address (a.b.c.d) or address/mask (a.b.c.d/n). The basic firewall rules will be applied only to those addresses. All other WAN addresses are blocked from accessing the device.
Forwarding WAN Firewall Settings	
Enable Firewall Logging	Select this to enable logging for packets dropped by the firewall. 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.
Enable PPTP Sever Pass-Through	Select this to allow a Point to Point Tunneling Protocol (PPTP) server to be placed on the LAN side with a private IP address. This allows Windows PPTP to pass through to a Windows server, but firewalls the server from other traffic.

Table 18 Standard Firewall Parameters (continued)

Item	Description
PPTP Server IP Address	Enter the private IP address of the PPTP server. 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.

Firewall Selection

This area contains a link to the **Advanced Firewall** page. See ["Advanced Firewall Page"](#) on page 181.

The Standard Firewall page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

Advanced Firewall Page

Use this page to configure the advanced Edgewater appliance firewall. [Table 19](#) describes the parameters on the page.

To access this page:

- If the standard firewall is currently enabled, choose **Standard Firewall** from the Configuration Menu, and then click the link at the bottom of the page to open the Advanced Firewall page.
- If the advanced firewall has been enabled, choose **Advanced Firewall** from the Configuration Menu.

[Help](#)

Advanced Firewall

Submit is required to complete reloading the Advanced Firewall.

Firewall Policy Enable

Firewall Logging (only when Firewall is enabled)

- Log Denied Packet
- Log Allowed Packet
- Log Interface WAN Only

Inbound Session Control:

Inbound Connection Rate Limit: /second

Enable PPTP Server Pass-through:

PPTP Server IP Address:

Outbound Session Control:

Outbound Connection Rate Limit: /second

Outbound protocol(s) to be allowed:

DNS: FTP: HTTP: HTTPS: IMAP: NTP:

PING: POP3: SMTP: SNMP: SSH: TELNET:

ALL OTHERS:

Remote Management:

To configure Remote Management address and options, [click here](#)

Firewall Selection:

To switch to Standard Firewall, [click here](#)

Table 19 Advanced Firewall Parameters

Field	Description
Firewall Policy/Logging	
Firewall Policy	Enable or disable the firewall by selecting from the pull-down list.
Log Denied Packet	Select to enable logging of packets that are blocked by the firewall.
Log Allowed Packet	Select to enable logging of packets that are allowed by the firewall.

Table 19 Advanced Firewall Parameters (continued)

Field	Description
Log Interface	Select a logging interface option: <ul style="list-style-type: none"> • WAN Only—Generates system log messages for traffic handling to and from the network (WAN interface) only. Uses fewest resources. • LAN Only—Generates system log messages for traffic handling to and from the LAN interface only. Resource intensive. • WAN and LAN—Generates system log messages for traffic handling to and from the WAN and LAN interfaces. Highly resource intensive.
Inbound Session Control	
These settings determine the treatment of packets entering the device.	
Inbound Connection Rate Limit	Select a rate in connections per second for inbound connections. This rate is used for automatic detection of denial of service (DoS) attacks from the public network. Packet requests to establish new sessions from the WAN to LAN that exceed this rate are temporarily denied. If this parameter is not defined, the default limit of 20 new sessions is used.
Enable PPTP Sever Pass-Through	Select this option to allow a Point to Point Tunneling Protocol (PPTP) server to be placed on the LAN side with a private IP address. This allows Windows PPTP to pass through to a Windows server, but firewalls the server from other traffic.
PPTP Server IP Address	Enter the private IP address of the PPTP server. 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.
Outbound Session Control	
These settings determine the treatment of packets leaving the device.	
Outbound Connection Rate Limit	Select a rate in connections per second for new outbound connections. This rate is used for automatic detection of denial of service (DoS) attacks from the public network. Packet requests to establish new sessions from the LAN to WAN that exceed this rate are temporarily denied. If this parameter is not defined, the default limit of 20 new sessions is used.
Outbound protocols to be allowed	Select the protocols for which outbound traffic will be allowed by the firewall. To enable any protocol not specifically mentioned, check the ALL OTHERS box.

Table 19 Advanced Firewall Parameters (continued)

Field	Description
The Remote Management	
This area contains a link to the Remote Management page, which is used to configure management protocols and trusted management addresses. See “Remote Management” on page 268.	
Firewall Selection	
This area contains a link to the Firewall page. See “Standard Firewall Page” on page 178.	

The Advanced Firewall page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

Custom Rules Page

Use this page to define custom rules for the advanced firewall. [Table 19](#) describes the parameters on the page.

To access this page, choose **Firewall** from the Configuration Menu, click the advanced firewall link, and then choose **Advanced Firewall > Custom Rules** from the Configuration Menu.

[Help](#)

Custom Rules

The Customized Rule page allows user to define additional firewall policies.

The followings are some sample rule sets:

```
# Allow Inbound and Outbound UDP traffic from/to port 138:
-t filter -A FILTER_WAN_UDP_IN -p udp -m multiport --ports 138 -j ACCEPT
-t filter -A FILTER_WAN_UDP_OUT -p udp -m multiport --ports 138 -j ACCEPT

# Allow Inbound and Outbound traffic on interface "ppp0"
-t filter -A INPUT -i ppp0 -j ACCEPT
-t filter -A OUTPUT -o ppp0 -j ACCEPT

# Allow IP Protocol 1 (ICMP) Inbound and Outbound traffic from/to address 10.10.13.185:
-t filter -A FILTER_WAN_ICMP_IN -p 1 -i eth1 -d 10.10.13.185 -j ACCEPT
-t filter -A FILTER_WAN_ICMP_OUT -p 1 -o eth1 -s 10.10.13.185 -j ACCEPT
```

Custom Rules:

Table 20 Custom Rules

Field	Description
Custom Rules	<p>Enter the custom rules with each rule on a new line.</p> <p>Sample rules:</p> <pre># Allow Inbound and Outbound UDP traffic from/to port 138: -t filter -A FILTER_WAN_UDP_IN -p udp -m multiport --ports 138 -j ACCEPT -t filter -A FILTER_WAN_UDP_OUT -p udp -m multiport --ports 138 -j ACCEPT # Allow Inbound and Outbound traffic on interface "ppp0" -t filter -A INPUT -i ppp0 -j ACCEPT -t filter -A OUTPUT -o ppp0 -j ACCEPT # Allow IP Protocol 1 (ICMP) Inbound and Outbound traffic from/to address 10.10.13.185: -t filter -A FILTER_WAN_ICMP_IN -p 1 -i eth1 -d 10.10.13.185 -j ACCEPT -t filter -A FILTER_WAN_ICMP_OUT -p 1 -o eth1 -s 10.10.13.185 -j ACCEPT</pre>

The Custom Rules page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

Current Advanced Firewall Rules (Show Rules)

Use this page to view the custom rules that are currently in effect. There are no fields or buttons on this page.

To access this page, choose **Firewall** from the Configuration Menu, click the advanced firewall link, and then choose **Advanced Firewall > Show Rules** from the Configuration Menu.

[Help](#)

Current Advanced-Firewall Rules

Filter Table

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
16687 7028K ACCEPT all -- lo * 0.0.0.0/0 0.0.0.0/0
0 0 DROP all -- eth1 * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 DROP tcp -- eth1 * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x16/0x02 recent: CHECK seconds: 5
hit_count: 20 name: syn_dos_in side: source
125 6076 FILTER_WAN_TCP_IN tcp -- eth1 * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x16/0x02 recent: SET
name: syn_dos_in side: source
0 0 DROP all -- eth1 * 0.0.0.0/0 192.168.1.0/24 state INVALID,NEW,UNTRACKED
18 612 FILTER_WAN_UDP_IN udp -- eth1 * 0.0.0.0/0 0.0.0.0/0 multiport sports
5050,5060,1718,1719
0 0 FILTER_WAN_UDP_IN udp -- eth1 * 0.0.0.0/0 0.0.0.0/0 multiport dports
5050,5060,1718,1719
0 0 FILTER_WAN_TCP_IN tcp -- eth1 * 0.0.0.0/0 0.0.0.0/0 multiport sports 1720
0 0 FILTER_WAN_TCP_IN tcp -- eth1 * 0.0.0.0/0 0.0.0.0/0 multiport dports 1720
0 0 DROP tcp -- eth1 * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x16/0x04 recent: CHECK seconds: 5
hit_count: 20 name: rst_dos_in side: source
3 120 FILTER_WAN_TCP_IN tcp -- eth1 * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x16/0x04 recent: SET
name: rst_dos_in side: source
0 0 DROP icmp -- eth1 * 0.0.0.0/0 0.0.0.0/0 recent: CHECK seconds: 5 hit_count: 20 name:
icmp_dos_in side: source
17 1102 FILTER_WAN_ICMP_IN icmp -- eth1 * 0.0.0.0/0 0.0.0.0/0 recent: SET name:
icmp_dos_in side: source
0 0 DROP udp -- eth1 * 0.0.0.0/0 0.0.0.0/0 state INVALID,NEW,UNTRACKED recent: CHECK
seconds: 5 hit_count: 20 name: udp_dos_in side: source
31133 1150K FILTER_WAN_UDP_IN udp -- eth1 * 0.0.0.0/0 0.0.0.0/0 state
INVALID,NEW,UNTRACKED recent: SET name: udp_dos_in side: source
0 0 FILTER_LAN_UDP_IN udp -- eth0.1 * 0.0.0.0/0 0.0.0.0/0
0 0 FILTER_LAN_ICMP_IN icmp -- eth0.1 * 0.0.0.0/0 0.0.0.0/0
0 0 FILTER_LAN_TCP_IN tcp -- eth0.1 * 0.0.0.0/0 0.0.0.0/0
0 0 FILTER_LAN_IN all -- eth0.1 * 0.0.0.0/0 0.0.0.0/0
0 0 FILTER_LAN_UDP_IN udp -- eth0 * 0.0.0.0/0 0.0.0.0/0
0 0 FILTER_LAN_ICMP_IN icmp -- eth0 * 0.0.0.0/0 0.0.0.0/0
0 0 FILTER_LAN_TCP_IN tcp -- eth0 * 0.0.0.0/0 0.0.0.0/0
0 0 FILTER_LAN_IN all -- eth0 * 0.0.0.0/0 0.0.0.0/0
165 25418 FILTER_WAN_UDP_IN udp -- eth1 * 0.0.0.0/0 0.0.0.0/0
319 42072 FILTER_WAN_TCP_IN tcp -- eth1 * 0.0.0.0/0 0.0.0.0/0
0 0 FILTER_WAN_ICMP_IN icmp -- eth1 * 0.0.0.0/0 0.0.0.0/0
165 25418 FILTER_WAN_IN all -- eth1 * 0.0.0.0/0 0.0.0.0/0
0 0 DROP all -- eth1 * 0.0.0.0/0 0.0.0.0/0
```

Forwarding Rules Page

Use this page to configure the rules that determine how the firewall forwards data traffic for a subnet from one interface to another. [Table 21](#) describes the parameters on the page.

To access this page, choose **Firewall > Forwarding Rules** from the Configuration Menu.

[Help](#)

Forwarding Rules

Forwarding Rules permits the firewall to forward data traffic for a subnet from one interface to another. When forwarding a subnet, an IP address needs to be assigned to the system to serve as the default router for the subnet. To add an additional IP address to the system, visit the [Subinterfaces](#) page.

Forwarding Rules						
Select: All None				Action: <input type="button" value="Delete"/>		
IP Address	Netmask	Input Interface	Output Interface	Protocol	Ports	
The list is currently empty						

Add a Forwarding Rule:

IP Subnet:

Netmask:

Input Interface:

Output Interface:

Protocol:

Custom Port:

Table 21 Forwarding Rules Parameters

Item	Description
Forwarding Rules Table	
Forwarding Rules permits the firewall to forward data traffic for a subnet from one interface to another. When forwarding a subnet, an IP address needs to be assigned to the system to serve as the default router for the subnet. To add an additional IP address to the system, visit the Subinterfaces page.	
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.	
Rules	
IP Subnet	Subnet to be forward through the firewall from the Input Interface to the Output Interface.
Netmask	Network mask to apply to the IP Subnet to create the range of IP addresses that are forwarded through the firewall
Input Interface	Interface where data is received that is destined for the forwarded subnet (one or more destination addresses).
Output Interface	Interface where data is received that is sent from the forwarded subnet (one or more source addresses).
Protocol	Can be one of the following: <ul style="list-style-type: none"> • Custom-UDP—For the specified network, allows the specified UDP port to pass through the system • Custom-TCP—For the specified network, allows the specified TCP port to pass through the system • Any—For the specified network, allows all ports and protocols through the system. No ports are required because not all protocols support the concept of ports.
Custom Port	Port Number that is allowed through the system when either Custom-UDP or Custom-TCP protocol is selected. This parameter is not required when Any or a protocol other than Custom-UDP or Custom-TCP is selected

The Forwarding Rules page contains the following buttons:

Add	Adds the specified entry
Delete	Deletes the selected entries.
Clear	Clears all fields and selections and allows you to enter new information.

Message of the Day Page

Use this page to customize the messages that are displayed upon user access and login. [Table 22](#) describes the parameters on the page.

To access this page, choose **Firewall > MOTD** from the Configuration Menu.

[Help](#)

Message of the Day (MOTD)

The messages of the day are displayed when the system is accessed using via HTTP/HTTPS, Telnet, SSH, and console.

System Authorization Message of the Day

The System Authorization MOTD is used to warn users before they log into the system that it is private and requires permission to use the system. This message is displayed when login in via the console, Telnet, and SSH.

HTTP/HTTPS Short System Authorization Message of the Day

The HTTP/HTTPS System Authorization MOTD is used to warn users before they log into the GUI on the system that it is private and requires permission to use the system. The message is limited to 511 characters.

System Greeting Message of the Day

The System Greeting MOTD is used to display a message upon successful login. It is used to display the system greeting and notify authorized users about important events or changes to the system.

Table 22 Message of the Day Parameters

Item	Description
System Authorization Message of the Day	Message used to warn users before they log into the system that it is private and requires permission to use the system. This message is displayed when login in via the console, Telnet, and SSH.
HTTP/HTTPS Short System Authorization Message of the Day	Message used to warn users before they log into the GUI on the system that it is private and requires permission to use the system. The message is limited to 511 characters.
System Greeting Message of the Day	Message that is displayed upon successful login. Includes a greeting and notification to authorized users about important events or changes to the system.

The Message of the Day page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

NAT Pages

Use the NAT pages to configure the address translations for dynamic and static Network Address Translation (NAT):

- NAT for Standard Firewall
- NAT for Advanced Firewall

NAT for Standard Firewall

Table 24 describes the parameters on this page.

To access this page, choose **Standard Firewall > NAT** from the Configuration Menu.

NAT

[Help](#)

Dynamic NAT

Dynamic NAT allows a system with a private address to be mapped to a public address, allowing the system to access the public network.

Enable LAN NAT:

Static NAT

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

Add a Static NAT Rule:

Protocol:	<input type="button" value="TCP"/> ▾
Src IP:	<input type="text"/>
Src Netmask:	<input type="text"/>
Src Port:	<input type="text"/>
Dest IP:	<input type="text"/>
Dest Port:	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Clear"/>	

Static NAT Rules						
Select: All None				Action: <input type="button" value="Delete"/>		
	Protocol	Src IP	Src Mask	Src Port	Dest IP	Dest Port
The list is currently empty						

Table 23 NAT Parameters for Standard Firewall

Item	Description
Enable LAN NAT	Select to allow the EdgeMarc appliance to provide WAN IP addresses for devices on the local LAN.
Add a Static NAT Rule	

Table 23 NAT Parameters for Standard Firewall (continued)

Item	Description
Protocol	Select the protocol for traffic over the interface. Note: When 'any' is selected as the protocol type, all data to the source IP address will be forwarded to the destination IP address. Restriction: When 'any' is used as the Protocol, the specified ports for the source IP address and the destination IP address must also be able to process any protocol type.
Src IP	Enter the IP address of the source interface. Note: When the system's own IP address is a dynamic WAN IP address and will be used as the source interface, use the token "WAN_IP".
Src Netmask	Enter the network mask for the source interface. Note: If the token "WAN_IP" is used to specify the source IP address, use the token "WAN_SUBNET". The token "WAN_SUBNET" specifies that the system use its own WAN subnet as the source netmask.
Src Port	Enter the port on the source interface to which the Static NAT rule should apply.
Dest IP	Enter the port on the destination interface to which the Static NAT rule should apply.
Dest Port	Enter a port to be used to route traffic to specific devices.

Static NAT rules

This table contains an entry for each static NAT rule.

The NAT page for standard firewall contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

NAT for Advanced Firewall

Table 24 describes the parameters on this page.

To access this page, choose **Advanced Firewall > NAT** from the Configuration Menu.

[Help](#)

NAT

Dynamic NAT

Dynamic NAT maps private IP addresses on LAN side to the public IP address on the WAN interface.

Enable Dynamic NAT:

Static NAT

Static NAT maps address/port on the WAN side to address/port on the LAN side. Static NAT requires Dynamic NAT to be enabled.

Static NAT Entries:

Proto	WAN Address	WAN Netmask	WAN Port	LAN Address	LAN Port

WAN Address Netmask WAN Port
 LAN Address Protocol Any Custom Port

Table 24 NAT Parameters for Advanced Firewall

Item	Description
Enable Dynamic NAT	Select to map private IP addresses on the LAN side to public IP addresses on the WAN interface.
Static NAT	
Static NAT Client Entries	Enter values in the following fields for static NAT:
WAN Address	Enter the IP address of the WAN interface.
Netmask	Enter the network mask for the WAN interface.
WAN Port	Enter a port to be used to route traffic to specific devices.
LAN Address	Enter the IP address for the LAN side.

Table 24 NAT Parameters for Advanced Firewall (continued)

Item	Description
Protocol	Select the protocol for traffic over the interface.
Custom Port	Enter a custom port if one of the custom options is selected for Protocol.

The NAT page for advanced firewall contains the following buttons:

Add	Adds the entry to the table.
Delete	Removes an entry from the table.
Submit	Applies the settings configured on this page.

Traffic Shaper Page

Use this page to configure rules that govern the behavior and priority of network traffic. [Table 25](#) describes the parameters on the page.

To access this page, choose **Traffic Shaper** from the Configuration Menu.

[Help](#)

Traffic Shaper

Enable Traffic Shaping:

WAN Downstream Bandwidth: Kbps
 WAN Upstream Bandwidth: Kbps

Enable Priority IP Addresses:

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

Enter an individual IP address or a range or the token WAN_IP (to specify dynamic WAN IP Address). Examples:

- 192.168.1.2
- 192.168.1.3-9
- WAN_IP

To delete an entry, highlight and delete it.

Differentiated Services Code Point (DSCP)

Expedited Forwarding (default)

IP Precedence

Assured Forwarding

Custom Value (1-63)

Enable TOS based routing:

Enable TOS Byte Stripping:

Note: Call admission control settings impacts H.323 video calls uniquely, see the [Help](#) page before enabling.

Enable Call Admission Control:

Maximum number of calls allowed:

Note: See the [Help](#) page for help determining how many calls your WAN link can support.

Enable SIP Inactivity Monitor:

SIP Inactivity Timeout (min):

Table 25 Traffic Shaper Parameters

Item	Description
Traffic shaping	
Enable Traffic Shaping	Select this checkbox to enable traffic shaping. NOTE: With traffic shaping disabled, the VoIP devices that are registered to the system's ALG will still have their layer 3 packets marked as TOS 0xb8 or DIFFServ AF46. Data traffic by default will be re-written to 0x00 (See Enable TOS Byte Stripping.)
WAN Bandwidth	
WAN Downstream Bandwidth	Enter the total actual downstream bandwidth that applies to your WAN connection. This value is entered in Kbps; for example, 1024 = 1 Mbps.
WAN Upstream Bandwidth	Enter the total actual upstream bandwidth the applies to your WAN connection. This value is entered in Kbps; for example 1024 = 1 Mbps.
Priority IP Addresses	
Enable Priority IP Address	To specify a device in the network as high priority, you can manually add its IP address to the list of high priority devices. Use care when entering IP addresses in this list. Devices that consume all the bandwidth may cause media quality problems. Enter an individual IP or range, for example 192.168.1.10-150. To delete an entry, highlight it and press the Delete key on your keyboard.
Enable TOS based routing	By default, this option is not selected. When enabled, this causes all VoIP related packets to be forcefully routed through the main WAN interface. 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.
Enable TOS Byte Stripping	By default, this option is selected. For all RTP traffic (voice and video) the system marks the TOS byte as High Priority, and strips (set to 0) the TOS byte for all other traffic. When this option is not selected, the TOS byte will not be stripped from non-RTP traffic, but will remain unchanged. Note: Devices that use the VoIP ALG function (phones, video stations, etc.) are already marked as high priority and do not need to be in this list. All data from IP addresses in this list has the same priority as voice data. Poorly behaved data may cause voice quality problems. Use with caution!
Differentiated Services Code Point (DSCP)	
Expedited Forwarding (Default)	This setting uses expedited forwarding as the forwarding rule.

Table 25 Traffic Shaper Parameters (continued)

Item	Description
IP Precedence	This setting uses classification of IP layer packets to determine priority.
Assured Forwarding	This setting assures that the packets will be forwarded.
Custom Value	For non-standard per-hop behavior, this field permits the use of a custom rule.

Call Admission Control (CAC)

Enable Call Admission Control	Select this checkbox to enable the Call Admission Control.
Maximum Number of Calls Allowed	Enter the total number of VoIP calls allowed to traverse the system, for example as RTP streams from VoIP devices. Use CAC to ensure that the system will NOT over subscribe the total amount of WAN bandwidth. 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

Enable SIP Inactivity Monitor	Select this checkbox to enable monitoring of RTP activity on all calls.
SIP Activity Timeout (min)	Enter the time in minutes after which SIP activity is deemed to have timed out. The SIP call is torn down and deallocated by the system. Note: The default and recommended timeout value is 90 minutes.

The Traffic Shaper page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

Advanced Traffic Shaper Page

Use this page to configure rules that govern the behavior and priority of network traffic. Table 25 describes the parameters on the page.

To access this page, choose **Traffic Shaper > Advanced** from the Configuration Menu.

Advanced Traffic Shaping

[Help](#)

Hit submit to apply the new CoS configuration.

| [Classes of Service](#) | [Classification Rules](#) |

Classes of Service			
Select: All None			Action: Delete
	Name	Priority Class	Bandwidth %
<input type="checkbox"/>	Voice_Video	EF / IP5	50
<input type="checkbox"/>	priority	AF4x / IP4	20
<input type="checkbox"/>	Real_Time_Data	AF3x / IP3	10
<input type="checkbox"/>	Best_Effort	Best Effort	20

[Submit](#)

Create a new Class

Name:

Priority Class: [AF1x / IP1](#) ▾

Bandwidth Percentage (%):

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

[Help](#)

Advanced Traffic Shaping

Hit submit to apply the new CoS configuration.

| [Classes of Service](#) | [Classification Rules](#) |

Classification Rules						
Select: All None				Action: Delete		
	Direction	IP Address	Source Port	Destination Port	Protocol	DSCP
<input type="checkbox"/>	N/A	0.0.0.0	any	5060	udp	AF41
<input type="checkbox"/>	N/A	0.0.0.0	any	22	tcp	AF42
<input type="checkbox"/>	N/A	0.0.0.0	any	80	tcp	AF42
<input type="checkbox"/>	N/A	0.0.0.0	any	23	tcp	AF42
<input type="checkbox"/>	N/A	0.0.0.0	any	179	tcp	AF41
<input type="checkbox"/>	N/A	0.0.0.0	any	3389	udp	AF31

Create a new Classification Rule

Traffic can be classified by a single or a range of IP addresses and/or ports.
For example: 192.168.1.100-105, 1000-1005.

IP Address:

Direction:

Protocol:

Source Port:

Destination Port:

Differentiated Services Code Point:

Expedited Forwarding

IP Precedence

Assured Forwarding

Custom Value (1-63)

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

[Submit](#)

Table 26 Advanced Traffic Shaper Parameters

Item	Description
Classes of Service Table	
Note: This table is featured by default. The table can be refreshed by clicking on the “Class of Service” link, located at the top of the page. Each row is an entry for a priority class.	
Create a new Class	
Name	Specifies the name of the class of service and its associated priority queue.
Priority Class	Specifies the Per-Hop Behavior (PHB) for the associated class of service.
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 can not exceed 100 percent.
Classification Rules Table	
Note: This table is featured on the page when you select the “Classification Rules” link, located at the top of the page. Each of the table’s rows contains an entry for a classification rule.	
Create a new Classification Rule	
IP Address	Specifies the IP address.
Direction	Specifies the direction of the traffic.
Protocol	Specifies the transport protocol: TCP, UDP or any.
Source Port	Specifies the source port.
Destination Port	Specifies the destination port.
Differentiated Services Code Point	Specifies the DSCP value used to mark the traffic flow.

The Advanced Traffic Shaper page contains the following buttons:

Delete	Deletes the entry for the selected row or rows in the table.
Commit	Commits the entry for the selected
Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

VoIP ALG Page

Use this page to configure parameters that allow the EdgeMarc device to recognize and register network devices. [Table 27](#) describes the parameters on the page.

To access this page, choose **VoIP ALG** from the Configuration Menu.

VoIP ALG

[Help](#)

ALG allows the system to recognize and register network devices.

TFTP Server IP address:

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

Use ALG Alias IP Addresses:
 ALG LAN Interface IP Address: 192.168.1.1
 ALG WAN Interface IP Address: 66.52.177.178

Do strict RTP source check:
 Enable Client List lockdown:
 Allow Shared Usernames:
 Use Unique Ports for Shared users:
 Strip G.729 from calls:
 Allow clients on WAN:

Allow non-translated RTP to be MOS scored:
 RTP range:

Bandwidth Settings for H.323

The maximum bandwidth to be used. The total bandwidth is counted as RTP payload plus IP header overhead, i.e. the actual link bandwidth set aside for RTP streams. The per-call bandwidth is the RTP payload bandwidth only, i.e. the value used in the client to specify the bandwidth of the call.

Maximum total bandwidth (kbps):
 Maximum per-call bandwidth (kbps):
 Default audio stream bandwidth (kbps):
 Default video stream bandwidth (kbps):
 Current payload bandwidth: 0
 Estimated current total bandwidth: 0

The ALG feature is registered. View [license key](#).

Table 27 VoIP ALG Parameters

Item	Description
Application Layer Gateway (ALG) Support	
ALG is on VLAN ID	Select a VLAN for the ALG to support. The ALG can only support one VLAN.
TFTP server IP address	Select to allow the system to act as a TFTP server providing subsequent configuration information to other VoIP phones or devices.
Use ALG Alias IP Address	<p>Select to enable the use of the IP address of the ALG alias. When this checkbox is selected, you can change the following parameters:</p> <ul style="list-style-type: none"> • ALG LAN Interface IP—Enter the IP address on the LAN that endpoints communicate with. Generally, this is the same as the LAN IP address. In some cases, the ALG addresses will not correspond to the addresses of the LAN or the WAN ports (e.g. when VRRP is enabled). The addresses will be alias addresses that have been configured on the ports. In general, you should leave this feature disabled. • ALG WAN Interface IP—Enter the IP address on the WAN that communicates with the soft switch. Generally, this is the same as the WAN IP address. <p>Note: ALG is enabled on your system, allowing the system to recognize and register a network appliance before it presents the IP telephone or data device through its public WAN port. When the ALG is not registered this text will read “Invalid License Key. The device has to be registered.”</p>
Do strict RTP source check	Select to help prevent a specific RTP-based denial-of-service attack as well as address network based gateways that periodically fail to stop sending an RTP stream when 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 to prevent new clients from registering. First a client list must be established, either by manually entering all clients that are allowed to use the system, or by running the system without the Client List lockdown feature until all desired clients have registered, and then enabling this feature. To use the Client List Lockdown feature with clients using dynamic IP address assignment (DHCP) you must disable Allow Shared Usernames so that Client List IP addresses can be updated if client addresses change over time.

Table 27 VoIP ALG Parameters (continued)

Item	Description
Allow Shared Usernames	Select to allow multiple clients to register using the same username. A new entry and a unique contact field will be generated for each client. If Client List Lockdown and Allow Shared Usernames are enabled at the same time, new phones using an existing username will not be added to the clients list and will fail to work.
Use unique ports for shared users	Allows the system to assign a unique port for clients using the same IP address and port. Note: This option is applicable to SIP clients only. If you enable this feature, you will have to clear the SIP clients list.
Strip G.729 from calls	Select 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 SDP (session description protocol). When you enable the G.729 feature, the codecs are removed from the SDP.
Allow clients on WAN	Select this checkbox to allow clients to register from the WAN side of the device. If you have no clients on the WAN side, you should leave this option disabled.
RTP Range	if the application requires that traffic shaping and MOS scoring should be performed on the calls initiated by non-translated signaling protocols, then enter the RTP ranges that will be associated with these calls. It can be specified as RTP port, RTP range, or any combinations of these separated by commas as can be seen below. 2000,30000-32000,40002,45000-46000 Currently this functionality is only supported for VoIP VPN application. A license must be obtained for VoIP VPN before this functionality can be operational.

Application Layer Gateway (ALG) Support

Maximum total bandwidth (kbps)	Enter the maximum available bandwidth. Bandwidth includes the RTF payload plus the IP header overhead.
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).
Default audio stream bandwidth (kbps)	Enter the bandwidth available for streaming audio traffic.
Default video stream bandwidth (kbps)	Enter the bandwidth available for streaming video traffic.

Table 27 VoIP ALG Parameters (continued)

Item	Description
Current payload bandwidth	Indicates the current bandwidth used for traffic payloads (read only).
Estimated current total bandwidth	Indicates the current total bandwidth (RTF payload plus IP header) (read only).

The VoIP ALG page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

H.323 Settings Page

Use this page to configure parameters for the H.323 protocol. Table 28 describes the parameters on the page.

To access this page, choose **VoIP ALG > H.323** from the Configuration Menu.

[Help](#)

H.323 Settings

H.323 protocol settings.

Gatekeeper mode
The gatekeeper mode configuration specifies whether the system should work in WAN/Provider-side gatekeeper mode, Peering-Proxy mode, or embedded gatekeeper mode.

- None (H.323 is disabled)
- WAN/Provider-side gatekeeper mode
- LAN/Subscriber-side gatekeeper mode
- Peering-Proxy mode (configure [prefixes](#))
- Embedded gatekeeper mode

WAN/Provider-side gatekeeper mode settings
The H.323 gatekeeper that all client traffic shall be forwarded to.

WAN/Provider-side GK address:

Modify Time-To-Live:

New Time-To-Live (s):

Gatekeeper reachability: N/A (Not in WAN GK mode)

LAN/Subscriber-side gatekeeper mode settings
The H.323 gatekeeper that all incoming calls should be forwarded to. It is possible to have a LAN side gatekeeper configured for peering-proxy mode as well.

LAN/Subscriber-side GK address:

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.

Allow public IP in LCF:

Embedded gatekeeper mode settings
These settings control the embedded gatekeeper behavior.

Time-To-Live (s):

Prevent calls from unregistered endpoints:

LRQ size
Some gatekeepers do not accept more than 2 source aliases in the LRQ message.
Limit LRQ size:

Default Alias
A default alias can be added to incoming calls without a destination alias in the Q.931 Setup message. By adding this alias, the embedded gatekeeper, or a LAN/Subscriber-side gatekeeper can route the call to a default endpoint.
Default alias:
 E.164
 H.323

Stale Time
The system can automatically delete clients when they have not sent any registration requests for a given period of time.
Delete stale clients:
Stale time (m):

Multicast Messages
Some RAS messages can be multicast in order to automatically detect gatekeepers.
Listen to multicast messages:

Alias Restrictions
The maximum number of aliases to be allowed to register
Max Aliases:

Table 28 H.323 Parameters

Item	Description
Gatekeeper Mode	
None	H.323 is disabled.
WAN/Provider-side gatekeeper mode	Specifies that the system will forward all client RAS messages to the gatekeeper. If this is selected, you must configure the settings in the WAN/Provider-side gatekeeper mode settings area.
LAN/Subscriber-side gatekeeper mode	Specifies that the system will act as a gatekeeper. If this option is selected, you must configure the settings in the LAN/Subscriber-side gatekeeper mode settings area.

Table 28 H.323 Parameters (continued)

Item	Description
Peering-Proxy mode	<p>Allows calls to be forwarded to other endpoints based on the information sent from the endpoints. All the information about routing the call must be sent as part of the request or prefixes must be configured.</p> <p>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.</p> <p>The prefixes are searched in order, that is, the first prefix is tried first, and then the next one on the list until the system finds a matching prefix. This means that if there are multiple matching prefixes, the first one is used.</p> <p>Prefixes use regular expressions to match the destination alias. Prefixes are always searched from the left of the alias and cannot match a middle part or the end of the alias. A regular expression can be a string of literal characters to match or a number of special expressions.</p>
Embedded gatekeeper mode	<p>Provides gatekeeper functions and accepts endpoint registrations. If this option is selected, you must configure the settings in the Embedded gatekeeper mode settings area.</p>

WAN/Provider-Side Gatekeeper Mode

If WAN/Provider-side gatekeeper mode is selected, you must configure the following parameters:

WAN/Provider-side GK address	Specifies the IP address of the gatekeeper
Modify Time-To-Live	Allows you to override the value for time-to-live returned by the gatekeeper before forwarding the response to the endpoint.
New Time-To-Live	Specifies how long an endpoint's registration should be valid.

LAN/Subscriber-Side Gatekeeper Mode

If LAN/Subscriber-side gatekeeper mode is selected, you must configure the following parameters:

LAN/Subscriber-side GK address	Enter the IP address of the gatekeeper.
Allow public IP in LCF	<p>Select the checkbox if the gatekeeper has been deployed with multiple outbound proxies and must decide which proxy to use based on the IP address returned in the LCF.</p> <p>This is an advanced configuration option and should usually not be selected.</p>

Table 28 H.323 Parameters (continued)

Item	Description
Embedded Gatekeeper Mode	
If embedded gatekeeper mode is selected, you must configure the following parameters:	
Time-to-Live(s)	Enter a time in seconds. This setting controls how long an endpoint's registration should be valid. At the end of this period the endpoint sends another registration request.
GK routed mode	Specifies whether the system should allow signaling to go directly between endpoints when possible (disabled) or always route signaling between endpoints (enabled).
Prevent calls from unregistered endpoints:	Blocks unregistered LAN-side endpoints from making calls through the device.
Location Request (LQR) Size	
You can limit the number of source aliases in a forwarded LRQ message to a maximum of two to allow interoperability with gatekeepers that cannot handle more than two source aliases.	
Limit LRQ Size	Enter a number of source aliases (maximum 2).
Default Alias	
Default alias	Enter a default alias to be added to incoming calls without a destination message in the Q.931 Setup message. This alias allows the embedded gatekeeper or a LAN/Subscriber-side gatekeeper to route the call to a default endpoint. Enter a default alias and select one of the following types: <ul style="list-style-type: none"> <li data-bbox="808 1268 899 1289">• E.164 <li data-bbox="808 1310 899 1331">• H.323
Stale Time	
Delete stale clients	Select if you want to delete clients that have not sent any registration requests in the specified interval.
Stale time (m)	Enter the interval in minutes.
Multicast Messages	
Listen to multicast messages	Enable the process of listening to multicast messages. Some RAS messages can be multicast in order to automatically detect gatekeepers.
H.460/18 Support	
Disabled	Disables H.460.18 support.

Table 28 H.323 Parameters (continued)

Item	Description
Enabled	Enables H.460.18 support. This allows the system to do NAT/Firewall traversal for clients behind NAT or firewall devices. This area includes the following configurable parameters:
Keep-alive time(s)	Specifies the keep-alive time if H.460.18 support is enabled.
Alias Restrictions	
Max Aliases	Enter the maximum number of allowed aliases. If the value is set to 0, the maximum is not enforced.

The H.323 Settings page includes the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

H.323 Activity Page

Use this page to view time, status, bandwidth, and log information for the H.323 protocol. [Table 29](#) describes the information on the page.

To access this page, choose **VoIP > H.323 > H.323 Activity** from the Configuration Menu.

H.323 Activity
[Help](#)

Current time: **Fri Jun 15 11:11:10 2007**
 WAN Gatekeeper status: **N/A (Not in WAN GK mode)**
 Current payload bandwidth: **0**
 Estimated total bandwidth: **0**

The H.323 activity logs shows recent H.323 events such as call terminations and registration rejects.

H.323 activity logs		
Event/Time	Source	Destination
The list is currently empty		

Table 29 H.323 Activity Parameters

Item	Description
Current time	Current local device time.
WAN Gatekeeper status	Indication of the WAN gatekeeper status, if WAN GK mode is used.
Current payload bandwidth	Current bandwidth of H.323 data.
Estimated total bandwidth	Estimation of total available bandwidth for H.323 data.
Activity log of recent H.323 events	List of recent H.323 activity, including time, source, and destination of the transmission.

H.323 Alias Manipulation Page

Use this page to configure aliases that are used for H.323 IDs or E.164. [Table 30](#) describes the parameters on the page.

To access this page, choose **VoIP > H.323 > Alias Manipulation** from the Configuration Menu.

[Help](#)

H.323 Alias Manipulation

Destination H323-ID or E.164 Alias Modification

The alias modification table can be used to modify aliases before they are acted on.

Destination H323-ID or E.164 Alias Modification		
Select: All None		Action: <input type="button" value="Delete"/>
Index	Pattern	Replace
The list is currently empty		

Add a rule

Action:

Pattern:

Index:

Replace:

Table 30 H.323 Alias Manipulation Parameters

Item	Description
Destination H323-ID or E.164 Alias Modification table	
	Lists alias manipulation rules.
	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.
Rules	
	Allows you to add new prefixes to the Prefix Routing and Gatekeeping Neighboring table.
Action	Indicates whether the rule is to be added or edited.
Pattern	Specifies the pattern to be matched. See “Regular Expressions” on page 69 for details on 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	Specifies the string that will replace the matched pattern.

The H.323 Alias Manipulation page contains the following buttons:

H.323 Neighboring Page

Use this page to configure rules for neighboring and prefix routing. [Table 31](#) describes the parameters on the page.

To access this page, choose **VoIP > H.323 > Neighboring** from the Configuration Menu.

H.323 Neighboring
[Help](#)

Prefix Routing and Gatekeeper Neighboring

The prefix routing table can be used to forward incoming calls based on their dialed alias.

Neighbor prefixes will not be used in this mode.

Prefix and Gatekeeper Neighboring table							
Select: All None				Action: Delete			
Index	Prefix	Strip	Add	Neighbor	Local Zone	Address	
The list is currently empty							

Add a prefix

Action: Add new prefix

Prefix:

Index:

Strip:

Add:

Neighbor:

Local Zone:

Address:

Table 31 H.323 Neighboring Parameters

Item	Description
Prefix Routing and Gatekeeping Neighboring table	
Lists rules for forwarding incoming calls based on their dialed alias. 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.	
Add a Prefix Allows you to add new prefixes to the Prefix Routing and Gatekeeper Neighboring table.	
Action	Indicates whether the rule is to be added or edited.
Prefix	Specifies the prefix pattern to be matched against the dialing string. See “Regular Expressions” on page 69 for details on valid patterns.
Index	Determines the order in which the rule is scanned in the Prefix and Gatekeeper Neighboring table. To add a rule between two rules with consecutive indexes (n and m), use the higher index (m).
Strips	Indicates whether the matching prefix is stripped from the dialing string.
Add	Specifies a string to be prepended to the dialing string.
Neighbor	Determines whether a location request (LRQ) is sent when this prefix matches. <ul style="list-style-type: none">• If enabled, the prefix becomes a neighboring statement.• If disabled, the incoming Q.931 Setup is forwarded to the given address without a preceding LRQ. This field is used for interoperability with other gatekeepers that may not accept a Setup without a preceding LRQ.
Local Zone	Provides compatibility with remote gatekeepers that are configured to accept LRQs only from sources that match its configured remote zone. If a gatekeeper is configured to accept requests only from a known source, enter the zone in this field.
Address	Specifies the IP address or domain name of the device to which the call is to be forwarded.

The H.323 Neighboring page contains the following buttons:

MGCP Settings Page

Use the MGCP Settings page to configure parameters for the MGCP protocol. Table 32 describes the parameters on the page.

To access this page, choose **VoIP > MGCP** from the Configuration Menu.

MGCP Settings		Help
MGCP protocol settings.		
The MGCP server settings specify the soft-switch that all client traffic shall be forwarded to.		
MGCP Server IP Address:	<input type="text" value="0.0.0.0"/>	
MGCP Call Agent Port:	<input type="text" value="2727"/>	
MGCP Media Gateway Port:	<input type="text" value="2427"/>	
MGCP Notified Entity Port:	<input type="text" value="2432"/>	
Re-registration		
Re-registration controls the automatic re-registration on behalf of the clients.		
Automatic MGCP Re-registration:	<input checked="" type="checkbox"/>	
MGCP Re-registration Rate (s):	<input type="text" value="5"/>	
MGCP Re-registration Retry Delay (s):	<input type="text" value="30"/>	
Audit Endpoint		
Audit Endpoint allows the system to detect whether a client is still responsive.		
Automatic MGCP Audit:	<input checked="" type="checkbox"/>	
Audit Cycle Interval (m):	<input type="text" value="15"/>	
Stale Time (m):	<input type="text" value="1440"/>	
Prevent stale re-registration:	<input checked="" type="checkbox"/>	
Automatic Client Deletion:	<input type="checkbox"/>	
Deletion Time (m):	<input type="text" value="2880"/>	
<input type="button" value="Submit"/> <input type="button" value="Reset"/>		

Table 32 MGCP Parameters

Item	Description
MGCP Protocol Settings	
MGCP Server IP Address	If a MGCP ALG is needed, enter the IP address for the MGCP Server as provided. The MGCP server provides media gateway control protocol service to IP phones, client adapters and gateways.
MGCP Call Agent Port	Call Agent Port specifies the port number that the Call Agent (soft-switch) listens to for messages from the phones. (Default is 2727)
MGCP Media Gateway Port	The Media Gateway Port specifies the port number the Media Gateway (phones) listens to for messages from the soft-switch. (Default is 2427)
MGCP Notify Entity Port	The Notified Entity port specifies the port number that the soft-switch uses for notifications from the phones, e.g. hook up, hook down, digits. (Default is 2432)
Reregistration	
This section allows you to configure automatic re-registration on behalf of clients.	
Automatic MGCP Re-registration	Re-registers MGCP endpoints every time the network or system restarts. Enable this feature to automatically synchronize the softswitch and phones immediately after a restart. The default is Enabled (checkbox selected).
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. Generally, this value does not need to be modified. If the MGCP Re-registration Rate needs to be changed, enter a value between 1 and 5. The default value is 5 messages per second.
MGCP Re-Registration Retry Delay (s)	The system re-registers clients when it starts up. If any re-registration request fails, the system will wait for the configured number of seconds and then retry the re-registration for the clients that failed. The system will make at most 10 re-registration requests for failed attempts. Generally, this value does not need to be modified. If the MGCP Re-registration Retry Delay needs to be changed, enter a value between 30 and 60 seconds. The default value is 30 seconds.
Audit Endpoint	
This section allows you to set an audit endpoint to help the appliance detect whether a client is still responsive.	
Automatic MGCP Audit	Select this to specify that MGCP clients will be automatically audited by sending a message to each client and waiting for a response.

Table 32 MGCP Parameters

Item	Description
Audit Cycle Interval (m)	Specifies in minutes how often these messages should be sent out to the clients. At each cycle, all endpoints will be audited so the rate of messages being sent is dependent on the number of clients currently registered. The default value is 15 minutes.
Stale Time (m)	This value in minutes is used to decide when a client is supposed to be deemed stale, or unavailable. The value is entered in minutes. The default value is 1440 minutes.
Prevent Stale Registration	Select this to disable the automatic MGCP re-registration feature for stale clients.
Automatic Client Deletion	Deletes clients that have been unavailable for the period of time specified by the Deletion Time parameter.
Deletion Time (m)	Specifies the time in minutes for the automatic client deletion feature.

The MGCP Settings page contains the following buttons:

Item	Description
Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

SIP Settings Page

Use this page to configure parameters for the SIP protocol. Table 33 describes the parameters on the page.

To access this page, choose **VoIP > SIP** from the Configuration Menu.

[Help](#)

SIP Settings

SIP protocol settings.

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

SIP Server Domain name:

List of SIP Servers:

Priority	Sip Server Address	Port	x
0	63.152.12.98	5060	

Enable Multi-homed Outbound Proxy Mode:

Enable Transparent Proxy Mode:

Limit Allowed Proxies:

Allowed SIP Proxies

This is the list of outbound proxies or registrars that are allowed through Transparent Proxy Mode. The SIP Server Address above is always included and does not have to be in this list.

66.52.177.135	
---------------	--

IP Address:

Stale Timer

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

Stale client time (m):

Registration Rate-Pacing parameters are available on the [Survivability page](#).

Table 33 SIP Parameters

Item	Description
SIP Protocol Settings	
SIP Server Domain Name	Specifies the domain name of the SIP server that accepts forwarded client traffic.

Table 33 SIP Parameters (continued)

Item	Description
List of SIP Servers	Specifies the address (either an IP or URL) for the SIP Server and port number as provided, if a SIP ALG is needed. The SIP server provides session-initialization protocol service to IP phones, client adapters and gateways.
Enable Multi-homed Outbound Proxy Mode	Allows phones behind the same System to utilize the default softswitch or one of their own choosing.
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 Allowed Proxies	Restricts the number of permitted proxies that are specified in the Allowed SIP Proxies area.
Allowed SIP Proxies	
Stale Timer	Lists the IP addresses of outbound proxies or registrars that are allowed in transparent proxy mode.
Stale Timer	
Stale Timer	Sets the inactivity timer interval in minutes after which the system deletes SIP clients that have not registered within the specified time.

The SIP Settings page includes the following buttons:

Add Row	Adds a new row to the list of SIP servers.
Add	Adds a new IP address.
Submit	Applies the settings configured on this page.
Reset	Clears the indicated fields and selections and allows you to enter new information.

SIP Trunking Page

Use this page to configure parameters for SIP trunking devices. Table 34 describes the parameters on the page.

To access this page, choose **VoIP > SIP > Trunking** from the Configuration Menu. See the next two figures.

SIP Trunking

[Help](#)

Configuration of SIP trunking devices.

SIP Trunking devices

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

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

SIP Trunking Devices		
Select: All None		Action: Delete
Address	Port	Name
192.168.1.253	1026	Internal Gateway

Add a trunking device

Action: [Add new trunking device](#) ↓

Name:

Address:

Port:

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

Header Transformation

These header transformation rules are applied to all SIP trunking devices. They define how specified SIP headers should be transformed when forwarding to the SIP Server.

From Header

Select the domain to use in From header when sending requests to the SIP Server:

- SIP Server Address (default)
- System WAN IP

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

Rules

Rules are used to forward and/or modify incoming and outgoing calls. There are 3 types of rules:

- Inbound: from server to trunking device
- Outbound: from trunking device to server
- Redirect: from local phone to trunking device (w/o routing to server)

Dial Rules							
Select: All None							Action: Delete
	Type	Party	PRIQ	Pattern-match	Strip	Add	Trunking device
<input type="checkbox"/>	Redirect			888880X			Internal Gateway (192.168.1.253:1026)
<input type="checkbox"/>	Redirect		Yes	911			Internal Gateway (192.168.1.253:1026)

Add a rule

Action:

Type:

Call Party:

Default rule:

Priority (inbound & redirect only):

Pattern-match (if not default):

Strip digits:

Add string:

Use SIP proxy as secondary target:

Trunking device:

Table 34 SIP Trunking Configuration Parameters

Item	Description
SIP Trunking Devices table	
This area allows you to add new SIP trunking devices. A SIP trunking device can be a PSTN gateway, or similar device, that does not issue REGISTER messages. Calls will be forwarded to the device based on the dial-plan rules below.	
Action	Indicates whether the device is to be added or modified.
Name	Specifies the name of the trunking device.
Address	Specifies the IP address of the device.
Port	Specifies the port for the SIP traffic.

Table 34 SIP Trunking Configuration Parameters (continued)

Item	Description
Header Transformation	
This area allows you to transform the header of a SIP message sent by a SIP endpoint so that it is forwarded to either the SIP Server or the system IP's address.	
SIP Server Address (default)	Specifies that the SIP message will be forwarded to the SIP Server. By default, registered SIP endpoints send messages to the SIP Server.
System WAN IP	Specifies that the SIP message will be forward to the system's IP address. Unregistered SIP endpoints typically send messages to the WAN IP address.
Rules table	
This area allows you to forward incoming and outgoing calls to and from a specific SIP trunking device based on a pattern-matching string for the called number. It is also possible to redirect calls from a local device to go directly to the trunking device without being routed to the soft-switch first by using the redirect rules.	
Action	Indicates whether the rule is to be added or modified.
Type	Indicates the type of rule: <ul style="list-style-type: none"> Inbound —Determines the trunking device to use for an inbound call from the soft-switch through the voice system to the trunking device. Outbound—Determines a dial string modification rule to use for calls from a specified trunking device through the voice system to the softswitch <p>Specify the Call Party as "Called" or "Calling" to assign the rule to the corresponding outbound call.</p> <ul style="list-style-type: none"> Redirect—Determines how to directly connect a local device to a trunking device without sending the signaling to the soft-switch first. <p>NOTE: Redirect operations are only performed for SIP INVITE messages. As a result, mid-call features such as transfer, hold or conference may not function as expected.</p>
Default rule	Indicates that this is the default trunking rule. Only one default rule can be specified.
Priority (inbound & redirect only)	Indicates that an inbound or redirect call will preempt any other call that is not priority. Non-priority calls in progress may be dropped.
Pattern-Match	Specifies the pattern that must be matched for the rule to apply. See " Regular Expressions " on page 69 for details on valid patterns.
Strip digits	Specifies the number of digits to be stripped from the front of the called number when the pattern matches.
Add string	Specifies a string to be added to the called number when the pattern matches.

Table 34 SIP Trunking Configuration Parameters (continued)

Item	Description
Use SIP proxy as secondary target	Specifies that the Sip Server be used a secondary target.
Trunking device	Specifies a SIP trunking device from the SIP Trunking Devices table on this page.

The SIP Trunking page contains the following buttons:

Commit	Applies the settings configured on this page.
Delete	Deletes the selected entry.
Reset	Clears all fields and selections and allows you to enter new information.

Survivability Page

Use this page to configure parameters that extend the availability of VoIP services. [Table 35](#) describes the parameters on the page.

To access this page, choose **Survivability** from the Configuration Menu. See the next two figures.

[Help](#)

Survivability

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

Enable Common Survivability Defaults

Softswitch/IP PBX Reachability Configuration

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

Time (s) between DNS lookups:

Time (s) between Keepalive messages:

Softswitch Recovery Timer (MGCP Only):

Time (s) to declare Keepalive message lost:

Number of missed messages to declare alarm:

Number of received messages to clear alarm:

Interpret error code as success:

Enable Local-Mode Indicator:

Enable Shared Call:

Current SIP Server reachability status:

	Name	Address	Port	P	W	Lost	Rcvd	Status
●	63.152.12.98	63.152.12.98	5060	0	1	872	0	Unreachable

Current MGCP Server reachability status:
No information available.

MGCP Survivability Settings:

Fill in the Blanks (requires Submit):

RM Message for RSIP:

Local Endpoint Name for RSIP:

Domain Name for RSIP:

Number of NTFY resends to declare alarm:

Immediate Switch Back to Softswitch:

SIP Server Redundancy Configuration

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

SIP Server Redundancy Settings:

Enable SIP server redundancy:

Enable forward next REGISTER:

Enable sticky failover mode:

Enable keepalive messages for active server:

Time for declaring SIP messages lost (seconds)

Call Control Configuration

Call Control Status:
Current Call Control is: Local

Survivability Configuration:
 Disabled
 Enabled
 Always Local

Local Dialing Plan:
Number of digits for local dialing:

Request Subscriber Information:
The system can request subscriber information from the SIP Server and use this information in survivable mode
 Request Subscriber Information:

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

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

Codec Choice:
The Codec choice option is limited to G.711 ulaw for system with MGCP Survivability enabled.
 Codec Choice:

Table 35 Survivability Parameters

Item	Description
Enable Common Survivability Defaults	Enables the survivability features on the device.
Softswitch/IP PBX Reachability Configuration	
<small>These settings control how often messages are sent to the Softswitch/IP PBX and how quickly a Softswitch/IP PBX will be declared unreachable or reachable. This determines Softswitch/IP PBX reachability for redundancy and local or remote call control functions.</small>	
Time (s) Between DNS Lookups	Specifies the number of seconds that lapse between DNS lookups.
Time (s) Between Keepalive Messages-	Specifies the number of seconds between consecutive keepalive messages sent to the softswitch to determine connectivity.
Time (s) To Declare Keepalive message Lost	Specifies the number of seconds after which a message is considered lost if no keepalive message is sent during that period.

Table 35 Survivability Parameters (continued)

Item	Description
Number of Missed Messages To Declare Alarm	Specifies the number of missed messages after which a loss of connectivity to the remote switch is declared.
Number of received messages to clear alarm	Specifies the number of consecutively received keepalive messages required for the system to declare successful connectivity to the remote softswitch.
Interpret error code as success	Specifies 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.
Enable Local-Node Indicator	Specifies that the EdgeMarc device will ignore register messages from the phone to trigger the phone into displaying a different icon or line-appearance symbol while it is in Local mode.
Enable Shared Call	Allows the EdgeMarc device to route all calls to the first (primary) line appearance of the phone while in Local mode, if 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, will be ignored by the EdgeMarc device while it is in Local mode.

Current SIP and MGCP Server Reachability Status (view only)

This section reports on the current ability of the device to reach the configured SIP and MGCP servers.

The following information is reported for each configured server;

- Name—Name of the server as returned by DNS server
- Address—IP address of the server
- Port—Port for the configured protocol (SIP or MGCP)
- 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—This column can have one of the following values:

Fill in the Blanks (requires Submit)

Fills most fields with the default values. You must click Submit for this setting to take effect.

Heartbeat RM Message for RSIP

Specifies the exact character string to be sent as part of the “RM:” option in the RSIP message to the softswitch. The default RM message is survping. Alternatively, disconnected can be used depending on your specific environment.

For example, if survping is specified, the RSIP message to the softswitch is similar to the following:

```
RSIP 332 00c002e0f8f8@edgewater.com MGCP 1.0
RM: survping
```


Table 35 Survivability Parameters (continued)

Item	Description
Local Endpoint Name for RSIP	Specifies the endpoint name to be embedded in the RSIP message that is used as the heartbeat. The endpoint name can be a real/physical endpoint in the system, or it can be a virtual endpoint whose name is user determined, as long as the name syntax is acceptable to the softswitch. The default value for this field is the MAC Address of the LAN Interface in the system.
Domain Name for RSIP	Specifies the domain name to be embedded in the RSIP message. This domain name can be a real domain name, or it can be any character string that is acceptable to the softswitch.
Number of NTFY resends to declare alarm-	Specifies the number of times a NTFY messages sent to the softswitch can go un-acknowledged before the system considers the communications with the Softswitch to be lost (causing a switch over to the system's local mode). The minimum number of resends is 1, and the recommended value is 4 (most MGCP devices retransmit at most 4 times).
Immediate Switch Back to Softswitch	<p>Disconnects all local calls and immediately switches out of the local mode when communication is reestablished with the softswitch.</p> <p>If this checkbox is unchecked, the calls are left running, but the system still switches out of local mode without waiting for the calls to end. (Default is checked.)</p>

SIP Server Redundancy Configuration

These settings allow 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.

Enable SIP server redundancy	Indicates whether the SIP redundancy feature is enabled.
Enable forward next REGISTER	Indicates whether the EdgeMarc appliance will forward the first REGISTER from the client to the server after the active server has been changed, even if the rate pacing interval is not over.
Enable sticky failover mode	Indicates whether the EdgeMarc appliance will fail over to the next available softswitch and not monitor the failed ones. This does not affect the monitoring of failed switches in survivability mode.
Enable Keep-Alive messages to active server	Indicates whether the active softswitch will be monitored with keepalive messages. If both survivability and redundancy are disabled, then no keepalive messages are sent, even if "Enable keepalive messages for active server" is checked.
Time for declaring SIP messages lost	Specifies the number of seconds after which a SIP message will be considered lost.

Call Control Configuration (view only)

Table 35 Survivability Parameters (continued)

Item	Description
	<p>Shows the current status of call control. This can be one of the following:</p> <ul style="list-style-type: none"> • Remote--There is connectivity to a remote softswitch. Calls are being processed by the softswitch. • Local--Connectivity to the remote softswitch is lost. Calls are being processed locally by the system.
Survivability Configuration	<p>Determines local call switching for survivability.</p> <ul style="list-style-type: none"> • Disabled--The system does not check for connectivity of the softswitch and will not provide local call switching in the event of a loss of connectivity to the softswitch. By default, survivability configuration is disabled. • Enabled--The system checks the connectivity of the softswitch and automatically performs local call switching when the softswitch becomes unavailable. • Always Local--The system always provides local call switching even when the softswitch is available to process calls. In this mode subscribers will only be able to make local, station-to-station phone calls. This setting is typical when troubleshooting-- it allows you to force the system into local call switching.
Number of digits for local dialing	<ul style="list-style-type: none"> • Specifies the number of digits the system uses for local call switching when in survivability mode. <p>PSTN-Gateway Prefix for Outdial--The number of digits that the system will use to process local calls when providing local call switching. For example if 4 is entered then the last four digits are used as the phone extension. If 0 is entered, the whole phone number is used.</p>
Request Subscriber Information	<p>Allows the device to request subscriber information as part of the phone registration process, if the softswitch supports such a request.</p> <p>The softswitch returns additional information about the phone that can be used in survivability mode, such as additional extensions.</p>

Table 35 Survivability Parameters (continued)

Item	Description
Registration Rate-Pacing	<p>Specifies the rate at which registration messages are forwarded to the Softswitch/IP PBX:</p> <ul style="list-style-type: none"> • Expires override (s)—Number of seconds a registration is valid. The system uses this value to re-write the expires value returned from the SIP Server. • Softswitch/IP PBX Expires override (s)—Number of seconds used when forwarding registration messages to the SIP Server. This should be higher than the rate pacing value, otherwise, the SIP Server may consider the phones registration to have expired. • Register rate pacing (s)—Number of seconds to wait before forwarding a register message from one phone to the SIP Server. <p>Note: It is possible for registration messages to overload the SIP Server. To prevent this, set the SIP Register pacing 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 are answered locally by the system. For example, you can set the expires value to 60 and the 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.</p>
Codec Choice	<p>Specifies the codec should to be used for signaling in survivability mode. The codec choice is limited to G.711 ulaw for a system with MGCP Survivability enabled.</p>

The Survivability page contains the following buttons:

Enable Common Survivability Defaults	Enables the survivability features on the appliance.
Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

FXS/Phone Port Settings - Basic (SIP UA) Page

Use this page to configure basic parameters that allow analog phones at each FXS port to make IP or PSTN calls. [Table 36](#) describes the parameters on the page.

To access this page, choose **SIP UA** from the Configuration Menu.

[Help](#)

FXS/Phone Port Settings - Basic

SIP UA allows voice call from Analog port to IP or PSTN
UA is currently bound to 192.168.1.252:1025

Global configuration:

Enable SIPUA:

Use SIP Username for SIP authentication:

Codec Preference:

Use Preferred codec only:

Use REFER for transfer:

Register with proxy:

Port 1 Configuration: (Registered)

Hook state: **On-hook**

SIP Display name:

SIP Username:

SIP Authentication name:

Password:

Table 36 FXS/Phone Port Settings - Basic

Item	Description
Global Configuration	
These settings apply to all ports.	
Enable SIPUA	Enables the SIP UA features. If the checkbox is not checked, the configuration on this page can still be saved, but the SIP UA functions are not available.
Use SIP Username for SIP authentication	Specifies that the SIP username is used for SIP authentication.
Codec Preference	Specifies the codec that to be given preference when making or receiving a call. 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

Table 36 FXS/Phone Port Settings - Basic (continued)

Item	Description
Use preferred codec only	Allows only the preferred codec to be used. No preference is given to the other codecs.
Use REFER for transfer	Indicates that the VoIP switch supports REFER requests for call transfer, as described in RFC3515.
Register with proxy	Instructs each configured FXS ports to register by sending a REGISTER request to the configured domain through a configured outbound proxy. Note: Some VoIP deployments use the static registration for the FXS ports and do not require port registration. If this checkbox is not checked, FXS ports will not register.

Port Configuration

This section includes a set of parameters for each port.

SIP Display Name	Specifies the name used by the FXS port to authentication itself, if the "Use SIP Username for SIP authentication" field is checked in global configuration area on this page.
SIP Username	Identifies the analog phone connected to the FXS port. This value can be either a name or a number that people use to reach to the analog phone.
SIP Authentication name	Specifies the name used to authenticate the SIP UA against the softswitch or outbound proxy.
Password	Specifies the passwords to authenticate the SIP UA against the softswitch or outbound proxy.

The FXS/Phone Port Settings - Basic page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

FXS/Phone Port Settings - Advanced Page

Use this page to configure advanced parameters that allow analog phones at each FXS port to make and receive IP or PSTN calls. [Table 37](#) describes the parameters on the page.

To access this page, choose **SIP UA > Advanced** from the Configuration Menu.

FXS/Phone Port Settings - Advanced

[Help](#)

This Page allows advance configuration of FXS/Phone ports..

[Reset to Defaults](#)

Global configuration:

Enable SIPUA:
 Bind to LAN:
 SIPUA IP Address:
 SIPUA bind Port:
 Conference URI:
 Domain:
 RTP Min Port:
 RTP Max Port:
 Outbound Proxy Server IP:
 Outbound Proxy Server Port:
 Termination Impedance:
 Dialed in prefix(Incoming from IP network):
 CPC(Call Party Control) timer (in milliseconds):
 Inter Digit Delay timer(in seconds):
 Enable Call Waiting:
 Internal Call Ring:
 External Call Ring:
 Hunt Group DID:
 VAD Enable:
 Caller ID Time offset:

Port 1 Configuration:

Codec Preference:
 Use Preferred codec only:
 Domain:
 Outbound Proxy Server IP:
 Outbound Proxy Server Port:
 Analog Receive gain:
 Analog Transmit gain:
 Member of HUNT group:
 Enable Call Waiting:
 VAD Enable:
 Hotline number:

Port 2 Configuration:

Codec Preference:
 Use Preferred codec only:
 Domain:
 Outbound Proxy Server IP:
 Outbound Proxy Server Port:
 Analog Receive gain:
 Analog Transmit gain:
 Member of HUNT group:
 Enable Call Waiting:
 VAD Enable:
 Hotline number:

Extended Hunt Group Members

Name:
 Address:
 Add to list:

	<input type="button" value="Move Up"/> <input type="button" value="Delete"/> <input type="button" value="Move Down"/>
--	---

[Submit](#) [Reset](#)

Table 37 FXS Phone Port Settings - Advanced

Item	Description
Global Configuration	
These settings apply to all ports.	
Note: Values set for individual FXS/Phone ports on this page override the global settings.	
Enable SIPUA	Enables the SIP UA features. If the checkbox is not checked, the configuration on this page can still be saved, but the SIP UA functions are not available.
SIPUA bind Port	Define a port number to which the SIP UA will bind and listen for SIP messages. If this field is empty, the SIP UA binds to internal port 5060.
Bind to LAN	Select to internally bind the UA to the LAN IP of the EdgeMarc, processing all signaling through the EdgeMarc's ALG. If not selected, the UA will internally bind to the WAN IP, bypassing the EdgeMarc's ALG. The later setting is used in special circumstances only. By default, this option is selected.
SIPUA IP Address	Specifies the LAN side IP address with which the SIP UA will bind. When this field is blank, the IP address will be set to the class C subnet of the VoIP ALG LAN plus 252.
Conference URI	SIP Conference Factory URI supplied by ISP. It should be identified in the same manner as a SIP end-point (user@host). Note: Conference URI is applicable only if your soft-switch supports creating a conference using Ad-Hoc SIP methods.
Domain	Specifies the domain of the softswitch where the SIP UA is provisioned. The domain is also the authentication domain for SIP UA.
RTP Min Port, RTP Max Port	Defines the range of RTP ports that SIP UA will use for media.
Outbound Proxy Server IP	Specifies the IP address of the outboard proxy server.
Outbound Proxy Server Port	Specifies the outbound proxy server port that SIP UA uses to register each FXS port and make outbound calls. If VoIP-ALG is enabled, the outbound proxy must point to the VOIP-ALG LAN interface.
Termination Impedance	Specifies the impedance on the outboard port.
Dialed in Prefix	Applicable only when HUNT mode is enabled. When a dial pattern is defined, that pattern is looked for in the dialed in number (TO field of SIP message). If the pattern is found as prefix, that prefix is stripped out and the remaining digits are given to the PBX as the dial pattern.

Item	Description
Call Party Control (CPC) timer (in milliseconds)	A timer value ranging from 250-800 milliseconds. The Call Party Control (CPC) indicates that the “calling party” has hung up. APBX/Key-system connected to the FXS port can make use of the CPC as a call disconnect signal.
Inter Digit Delay timer (in seconds)	Defines the maximum delay between two digits when dialed. When dialing, If a key is not pressed within the defined delay, dialing is auto-completed and the collected digits are dialed out. The default value for this field is set to 4 seconds.
Enable Call Waiting	Check this box to enable the call-waiting feature globally on all FXS ports. By default, this box is checked and call-waiting is enabled on all ports. To control feature at port level, disable the global setting and select the settings a port level.
Internal Call Ring	Associates a distinctive ring with all internal calls. The ring and the rules defining an internal call are specified on the FXS/Phone Port Distinctive Ring configuration page.
External Call Ring	Associates a distinctive ring with all external calls. The ring and the rules defining an external call are specified on the FXS/Phone Port Distinctive Ring configuration page.
VAD Enable	Globally enables voice activity detection. By default, VAD is enabled.
Caller ID Time offset	Defines 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.

Port Configuration

This section includes a set of parameters for each port.

Codec Preference	Specifies the codec that to be given preference when making or receiving a call. 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	Allows only the preferred codec to be used. No preference is given to the other codecs.
Domain	Specifies the domain of the softswitch where the SIP UA is provisioned. The domain is also the authentication domain for SIP UA.
Outbound Proxy Server IP	Specifies the IP address of the outboard proxy server.
Outbound Proxy Server Port	Specifies the outbound proxy server port that SIP UA uses to register each FXS port and make outbound calls. If VoIP-ALG is enabled, the outbound proxy must point to the VOIP-ALG LAN interface.
Analog Receive Gain	Specifies the 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.

Item	Description
Analog Transmit Gain	Specifies the 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.
Member of Hunt Group	Check this box to enable the associated FXS port to answer Incoming calls that are placed to the hunt group from an IP network. The port will still receive calls that are placed to it directly.
Enable Call Waiting	Check this box to enable call-waiting feature at the port level.
VAD Enable	Enables voice activity detection for the FXS port.
Hotline Number	Configures the FXS port such that when the phone goes off hook, the port will automatically dial the specified destination.

The FXS/Phone Port Settings - Advanced page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset to Defaults	Changes all the settings on the page to their factory defaults.
Reset	Clears all fields and selections and allows you to enter new information.

FXS/Phone Port FAX Settings Page

Use this page to configure FAX settings for the FXS/Phone ports. [Table 38](#) describes the parameters on the page.

To access this page, choose **SIP UA > FAX** from the Configuration Menu.

[Help](#)

FXS/Phone Port FAX Settings

FAX configuration for FXS/Phone port 1 and 2. FAX hookup is currently only available on FXS/Phone port 1 and 2. If T38 is enabled, T38 version 0 over UDP is supported.

Use T38 for FAX:

Fax Bit rate(bps):

Fax TCF:

Fax Options:

UDP Max buffer:

UDP Max Datagram size:

Fax Error Correction:

Table 38 FXS/Phone Port FAX Settings

Item	Description
Use T38 for FAX	<p>Uses the T38 to send and received faxes, if this checkbox is selected.</p> <p>If this checkbox is not selected, G711ulaw is used to send and receives faxes.</p>
Fax Bit rate (bps)	Specifies the data rate that the fax machine support (bps). Maximum is 14400 bps.
Fax TCF	<p>Defines the Data Rate Management Method for TCF (Training Check Function) signal:</p> <ul style="list-style-type: none"> • Local—Requires that the TCF training signal is generated locally by the receiving gateway (the entity that receives the T38 data and translates it into T30 data, Port 1 or 2). Data rate management is done by the emitting gateway (entity that 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. • Transferred—Requires that the TCF signal is transferred from the emitting gateway to the receiving gateway. In this case, the speed selection is done by the G3FEs in the same way as for a PSTN connection. This method is mandatory for UDP.

Table 38 FXS/Phone Port FAX Settings (continued)

Item	Description
Fax Options	Specifies special settings for the fax machine: <ul style="list-style-type: none">• 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 MMR and the line format to increase data compression and reduce bandwidth in the packet network.• JBIG Transcoding—Use JBIG conversion to reduce bandwidth.
UDP Max buffer	Defines 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	Defines the maximum size of a 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	Defines the error correction method used by the fax machine.

The FXS/Phone Port FAX Settings page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

Distinctive Ring Page

Use this page to configure distinctive ring tones for FXS/Phone ports. Table 39 describes the parameters on the page.

To access this page, choose **SIP UA > Distinctive Ring** from the Configuration Menu.

[Help](#)

FXS/Phone Port Distinctive Ring configuration

Configure distinctive rings for FXS/Phone ports. User can configure rules to select a distinctive ring based on who is calling or who is being called.

Distinctive Ring Rules		
Select: All None		Action: <input type="button" value="Delete"/>
Callee Pattern-match	Called Pattern-match	RingId
The list is currently empty		

Add a Distinctive ring rule

Action: ▼

Caller Pattern-match:

Called Pattern-match:

Ring Type: ▼

Table 39 FXS/Phone Port Distinctive Ring Parameters

Item	Description
Action	Applicable task (Add a Rule, Edit a Rule)
Caller-Pattern-Match	Caller pattern that triggers the distinctive ring.
Called-Pattern-Match	Called pattern that triggers the distinctive ring.
Ring Type	Selection of the specific distinctive ring for this rule.

The Distinctive Ring page contains the following buttons:

Commit	Applies the settings configured on this page.
Delete	Deletes the selected entry.
Reset	Clears all fields and selections and allows you to enter new information.

SIP FXO/Line Port Configuration (SIP GW) Page

Use this page to configure the SIP FXO/Line port to allow SIP IP phones or analog phone at FXS ports to make or receive PSTN calls. [Table 40](#) describes the parameters on the page.

To access this page, choose **SIP GW** from the Configuration Menu.

SIP FXO/Line port configuration

[Help](#)

SIP FXO/Line port allows voice call from IP networks to PSTN.

GW is currently bound to 192.168.1.253:1026

(If you enable or disable the SIP FXO/Line port services, you also must configure the [SIP trunking rules](#).)

Enable SIP FXO/Line services:

RTP Silence delay:

SIPGW IP Address:

Add Dial Out Prefix (To IP network):

Enable Priority Calling services:

Callback extension(Mandatory):

Priority Call Window(sec):

(You must also configure Priority calling [SIP trunking rules](#) for these services to work.)

Register with SIP server:

Override FROM Username(To IP network):

Sip Authentication Name(optional):

Password(optional):

Refer to [Header Transformation](#) page if you want to override FROM domain name.

PSTN CO Auto-Disconnect timer(sec):

Override FROM Display Name(To IP network):

Port 1 Configuration:

Enable FXO port:

Analog Receive gain:

Analog Transmit gain:

Enable InBound(from IP Network) two stage dialing:

Port 2 Configuration:

Enable FXO port:

Analog Receive gain:

Analog Transmit gain:

Enable InBound(from IP Network) two stage dialing:

Table 40 SIP FXO/Line port configuration

Item	Description
Enable SIP FXO/Line port services	Select this checkbox to enable SIP FXO/Line port services.
RTP Silence delay	A value used to monitor RTP silence packets when in call and determine if a PSTN party has been disconnected. By default the value is 120 seconds. If there is a continuous RTP silence from the PSTN side for the duration of this interval, the FXO/Line port will terminate the call.

Table 40 SIP FXO/Line port configuration (continued)



Item	Description
SIPGW IP Address	Specifies 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. 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. Otherwise, the default configuration is sufficient.
Enable Priority Calling services	Enables 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, will be routed on priority basis to FXO port and connected.  Note: Enabling 'Priority Calling Services' will override (or hide) the following settings for individual ports: Enable InBound(from PSTN) two stage dialing and 'Forwarded To'.  Additional Note: Priority calling services cannot be configured when WAN Link Redundancy is enabled.
Callback extension	Only visible when Priority Calling services are enabled. Define a callback number that will receive Callbacks from Priority calling services operators, if such services are available. This field is mandatory and make sure it is set to an extension (which MUST be an FXS port or an extension on LAN side that is always up. Note: When 'Priority calling' is enabled, 'Callback extension' overrides any 'Forwarding number' configured for FXO ports.
Priority Call Window	Only visible when Priority Calling services are enabled. Each port can feature a Priority call window. The priority call window field defines a time period during which an Inbound call from the PSTN will be forwarded to the last IP caller that made an Outbound priority call through the FXO port. The time period is measured in seconds. The time period starts when a caller makes an Outbound priority call through a FXO port and ends when the window has expired.
Register with SIP server	Enables the FXO/GW to register with SIP server, using the 'Override SIP FROM' as SIP user name.
Override FROM Username (To IP Network)	Overrides FROM field in SIP messages with the SIP username. Note: When the Override FROM field is specified with the SIP username, it replaces any Dial Out Prefix and CallerID.
Sip Authentication Name (optional)	Defines the SIP authentication name.
Password (optional)	Supplies optional credentials which may be required for successful SIP logon.

Table 40 SIP FXO/Line port configuration (continued)

Item	Description
PSTN CO Auto-Disconnect timer (sec)	The time in seconds it will take the PSTN CO line to terminate a call when the call originated from the PSTN through the FXO port and the SIP caller has hung up the call.
Override FROM Display Name (To IP network)	Overrides FROM field in SIP messages with the SIP Display Name. Note: When Override FROM field is specified with the Display Name, CallerID is replaced with the display name "anonymous".

Port Configuration

This section includes a set of parameters for each port.

Enable FXO Port	Enables the FXO/Line port for incoming and outgoing calls. When this field is not checked, the FXO/Line port will be disabled.
Analog Receive gain	Adjusts the gain to optimize echo cancellation in a call. The default value is 0db. Note: In cases where the default value does not optimize echo cancellation, adjust the gain with -6DB in steps to -10DB till echo is gone.
Analog Transmit gain	Identifies the SIP FXO/Line port. The field is optional and only needed if the SIP FXO/Line port must be authenticated
Enable InBound (from IP Network) two stage dialing	Identifies the password to authenticate the SIP FXO/Line port against the SIP softswitch or outbound proxy. This field is optional and only needed if SIP FXO/Line port must be authenticated
Enable InBound (from PSTN) two stage dialing	Supports two-stage dialing for incoming PSTN calls: <ul style="list-style-type: none"> • Provides dial tone when a call is answered. Caller can then dial an extension to further complete the call or hang up. • Forwards an incoming call from PSTN to the configured number.
Forwarded to	Specifies the forwarding number if two-stage dialing is disabled.

The SIP FXO/Line Port Configuration page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

**Note**

The following diagram is an example of the SIP FXO/Line port configuration page when Enable Priority Calling services is not enabled. Table 36 describes the parameters for this page.

SIP FXO/Line port configuration

SIP FXO/Line port allows voice call from
GW is currently bound to 192.168.1.

(If you enable or disable the SIP FXO/Line
configure the SIP trunking rules.)

Enable SIP FXO/Line services:

RTP Silence delay:

SIPGW IP Address:

Add Dial Out Prefix (To IP network):

Enable Priority Calling services:

Callback extension(Mandatory):

Priority Call Window(sec):

**(You must also configure Priority cal
these services to work.)**

VPN Page

Use this page to add, edit, or delete VPN tunnels. [Table 41](#) describes the settings on this page.

To access this page, choose **VPN** from the Configuration Menu.

VPN Configuration

[Help](#)

Global Settings:

Enable the VPN module:

[Refresh Status](#) Current time: Tue Dec 23 20:04:03 2008

VPN Tunnels		
Select: All None		Action: <input type="button" value="Delete"/>
	Tunnel Name	Status
<input type="checkbox"/>	t10to30	Tunnel negotiation initiated <input type="button" value="i"/>
<input type="checkbox"/>	t10to40	Tunnel negotiation initiated <input type="button" value="i"/>
<input type="checkbox"/>	t10to50	Tunnel negotiation initiated <input type="button" value="i"/>

Add a new tunnel:

Table 41 VPN page settings

Item	Description
Enable the VPN module	Enables the VPN module. If this box is not checked, no VPN tunnels will be available for use.

The VPN page contains the following buttons and links:

Submit	Applies the settings configured on this page.
Delete	Deletes the selected entry or entries.
Refresh Status	Refreshes the status information for all VPN tunnels.
Status	Displays the current status of the tunnel listed in each row of the VPN Tunnels table. If more information is available, such as the time the status event occurred, the IP address of the remote party, or a detailed help text, then an information icon will be displayed.
Add Tunnel	Creates a new tunnel.

VPN Subnet Page

Use this page to allow traffic between a local and remote subnet to be sent through a given tunnel. [Table 42](#) describes the parameters on the page.



Note

The remote side of the tunnel must have a similar configuration.

To access this page, choose **VPN > VPN Subnets** from the Configuration Menu.

[Help](#)

VPN Subnet Management

Additional VPN subnets can be added to route traffic through existing VPN tunnels.

VPN Subnets			
Select: All None		Action: Delete	
Subnet Name	Local Subnet	Remote Subnet	Remote Gateway
<input type="checkbox"/> syslog	192.168.1.10/32	172.16.30.0/24	192.168.1.30

Add a new subnet

Action:

Name:

Local Subnet:

Remote Subnet:

Remote VPN gateway:

Table 42 VPN Subnet Management Parameters

Item	Description
Action	Add or edit an existing subnet
Name	Enter or edit a unique name for the subnet
Local Subnet	Specify the local subnet. Must be in a network/mask or network/bits format.
Remote Subnet	Specify the remote subnet. Must be in a network/mask or network/bits format.
Remote VPN gateway	The remote VPN gateway to use when processing packets matching the specified local and remote subnets.

The VPN Subnet Management Parameters page contains the following buttons:

Commit	Applies the settings configured on this page.
Delete	Deletes the selected entry.
Reset	Clears all fields and selections and allows you to enter new information.

VPN Tunnel Settings Page

Use this page to configure a new or existing VPN tunnel. [Table 43](#) describes the parameters on the page.

To access this page, choose **VPN** from the Configuration Menu, and then click on the **Add Tunnel** button. If tunnels are listed in the VPN Tunnels table, you can also click on a tunnel name listed in the **Tunnel Name** column to access this page.

Add New VPN Tunnel

[Help](#)

[Back to VPN overview](#)

Name:	<input type="text" value="Tunnel_1"/>
Enabled:	<input checked="" type="checkbox"/>
Shared Secret:	<input type="text"/>
Local VPN Gateway:	<input type="text" value="WAN_IP"/>
Protected Local Network:	<input type="text"/>
Remote VPN Gateway:	<input type="text"/>
Protected Remote Network:	<input type="text"/>
DH Group:	<input type="text" value="DH Group 2 - 1024 bits"/>
Phase 1:	<input type="text" value="3DES"/> - <input type="text" value="SHA1"/>
Phase 2:	<input type="text" value="AES128"/> - <input type="text" value="SHA1"/>
Phase 1 Lifetime:	<input type="text" value="28800"/> seconds
Phase 2 Lifetime:	<input type="text" value="86400"/> seconds
Perfect Forward Secrecy:	<input checked="" type="checkbox"/>
Early Start:	<input checked="" type="checkbox"/>
Keepalive Ping (Optional)	
Source IP address:	<input type="text"/>
Destination IP address:	<input type="text"/>

Table 43 Add New VPN Tunnel Page Settings

Item	Description
Status	Displays the current status of the tunnel. If more information is available, such as the time the status event occurred, the IP address of the remote party, or a detailed help text, an information icon is displayed.
Name	Enter the name of the VPN tunnel. The name must be unique per device, with maximum length of 32 characters.
Enabled	Select this checkbox to enable this tunnel.
Local VPN Gateway	To use a static IP address, enter the WAN IP address of this device. To use dynamic WAN IP address assignment, enter the string "WAN_IP" to permit dynamic assignment of the WAN-side IP address.
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 .
Remote VPN Gateway	Enter the static IP address of the remote VPN gateway .
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.
PerfectForward Secrecy	Select this checkbox to enable Perfect Forward Secrecy for IKE negotiation.
DH Group	Enter the Diffie-Hellman Group to use for Phase 1 and Phase 2. Supported values are "DH Group 2" (1024-bit key) and "DH Group 5" (1536-bit key).
Phase 1	Enter the cipher and hash algorithms to use for Phase 1 (IKE) encryption. Supported settings are 3DES or AES for the cipher, and MD5 or SHA1 for the hash.
Phase 2	Enter the cipher and hash algorithms to use for Phase 2 (ESP) encryption. Supported settings are 3DES or AES for the cipher, and MD5 or SHA1 for the hash.
Phase 1 lifetime	Specify 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	Specify the time that the connection (IPsec SA) should last before being renegotiated. Valid range for the Phase 2 Lifetime is 600-86400 seconds.

Item	Description
Early Start	<p>Select this checkbox to cause the VPN gateway to start key negotiation when you click Apply or when the gateway reboots. The Keepalive Ping settings are displayed if Early Start is selected.</p> <p>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.</p>
Keepalive Ping (Optional)	<p>Enter the source and destination IP addresses of a host that belongs to the remote protected VPN. The system sends pings messages to this address to detect VPN tunnels that are down and renew those tunnels automatically. Keepalive ping is active only when user enables Early Start. To disable this feature, leave the fields blank or disable Early Start.</p> <p>Source IP Address: The source IP address to use when sending the pings. This must be a configured address of the local system.</p> <p>Destination IP Address: The Destination IP address to use when sending the pings.</p>

System Page

Use this page to view information about the EdgeMarc appliance and configure passwords for the administrator and read-only user. [Table 44](#) describes the parameters on the page.

To access this page, choose **System** from the Configuration Menu.

System	Help
<hr/>	
Software Version:	Version 7.3.0jdoan -- Tue Jun 12 14:03:08 PDT 2007
<hr/>	
Hostname:	E_4500atVON
<hr/>	
Model:	EdgeMarc 4508T4
<hr/>	
LAN Interface MAC Address:	00:03:6D:DF:32:60
<hr/>	
Registration Status:	The ALG feature is registered. View license key .
<hr/>	
System Date:	06/15/2007 11:18:42 UTC
<hr/>	
Change Administrative Password:	The password of the read-write administrative user can be changed .
<hr/>	
Change Read-Only Password:	The password of the read-only user can be changed .

Table 44 System Information

Item	Description
Software Version	Current running system firmware version.
Hostname	Currently assigned Hostname of the system.
Model Number (view only)	Model number of the system.
LAN Interface MAC Address (view only)	LAN interface MAC address of the system.
Registration Status	Registration status for the ALG feature; this information 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.

Table 44 System Information (continued)

Item	Description
System Date	Current System Time of the system.
Change Administrative Password	Allows you to navigate to the Reset 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.
Change Read-Only Password	Allows you to change the password for read-only users.

This page contains no buttons.

Certificate Page

Use this page to configure the device certificate used by HTTPS for secure remote management. [Table 45](#) describes the parameters on the page.

To access this page, choose **System > Certificate** from the Configuration Menu.

[Help](#)

Certificate

Configure the device certificate used by HTTPS.
[Click here for online Certificate help.](#)

Certificate:

Private Key:

Password:

Table 45 Certificate Parameters

Item	Description
Certificate	X.509 certificate for HTTPS-based device authentication. You should obtain a certificate from a trusted CA and enter the certificate in this field. The system only supports certificates in .pem format.
Private Key	Private key associated with the device certificate. The system only supports private keys in .pem format.
Password	The password that protects the private key file. The Certificate page includes the following button: Submit—Applies the settings configured on this page.

The Certificate Parameters page contains the following buttons:

Submit	Applies the settings configured on this page.
--------	---

Clients List Page

Use this page to configure the entries for devices that have registered with the EdgeMarc devices. When you select a protocol on the page, the page refreshes to show information for the selected protocol. [Table 46](#) describes the parameters on the page.

To access this page, choose **System > Clients List** from the Configuration Menu.

[Help](#)

SIP Clients List

Protocol to display: [SIP](#) [MGCP](#) [H.323](#)

Client List Filter:

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

	No Sort	Address	Port	Name
<input type="checkbox"/>		192.168.1.252	1025	4074017626
<input type="checkbox"/>		192.168.1.252	1025	0002
<input type="checkbox"/>		192.168.1.252	1025	0003
<input type="checkbox"/>		192.168.1.252	1025	0004
<input type="checkbox"/>		192.168.1.252	1025	0005
<input type="checkbox"/>		192.168.1.252	1025	0006

|<<< 1 >>>|

Displaying page 1 of 1.
Number of clients: 6

Add a SIP client to the client list

Name:

Address:

Port:

Table 46 SIP Clients List

Item	Description
Client List Filter	Applies a filter on the client list before displaying it, making it possible to search for a subset of clients. The Apply button applies the currently typed string, and the Clear button clears the filter.

Client Information table

- **Clients can be selected manually by clicking on the check-box of each client, or by pressing the Select: All link. Clients can be cleared by pressing the Select: None link. The select all and none links only apply to the currently displayed clients. A certain subset of clients can be selected by first applying a filter and then selecting all displayed clients.** Trashcan icon—Deletes the entry.
- Info icon—Display additional information about the client.
- MGCP specific icons—Allows you to modify the extension number of the client. The client's extension number is required only if the MGCP Survivability feature is enabled. Otherwise, it can be left blank.
- Warning icon—Client has not responded to audits for the given amount of time.
- H.323 lock icon—lock or unlock the endpoint. A locked endpoint is not automatically deleted by the system (if that feature is enabled).

Add a SIP Client to the Clients List

Name	Specifies the name of the client.
Address	Specifies the IP address of the client.
Port	Specifies the port used by the client.

Add an MCGCP Client to the Clients List

Name	Specifies the name of the client.
Address	Specifies the IP address of the client.
Extension	Specifies the client's phone extension.

Add an H.323 Client to the Clients List

Address	Specifies the static IP address of the H.323 client.
Q.931 Port	Specifies the Q.931 call signaling port on which the endpoint sends call setup. Port 1720 is generally used.
RAS Port	Specifies the Registration, Admission and Status (RAS) port. Port 1719 is generally used.
Alias	Specifies the H.323 or E.164 alias for the static client that you are adding.
Alias Type	Specifies the type of alias entered in the Alias field.

The Clients List page contains the following buttons:

Apply	Applies the settings configured on this page.
Clear	Clears the value entered but not saved in the Client List Filter field.
Delete Selected	Deletes the selected entry.
Delete All	Deletes all the client list entries.
Add	Adds a SIP client to the client list.
Reset	Clears the information entered but not added for the SIP clients.

Dynamic DNS Page

Use this page to configure dynamic DNS parameters. [Table 47](#) describes the parameters on the page.

To access this page, choose **System > Dynamic DNS** from the Configuration Menu.

Dynamic DNS [Help](#)

Dynamic DNS allows a user to associate a name with the public address of the system. When a change occurs to the public interface of the system, the Dynamic DNS service is notified of the change.

Enable Dynamic DNS:

Service Name:

User ID:

Password:

Host Id:

Table 47 Dynamic DNS Parameters

Item	Description																
Enable Dynamic DNS	Select this checkbox to enable the system to notify the external DNS server that the systems IP address has changed.																
Service Name	Enter the service name that the system is using. Use one of the names from the following table.																
	<table border="1"><thead><tr><th>Service Name</th><th>URL for Service Provider</th></tr></thead><tbody><tr><td>dhs</td><td>www.dhs.org</td></tr><tr><td>dyndns</td><td>www.dyndns.org</td></tr><tr><td>ods</td><td>www.ods.org</td></tr><tr><td>tzo</td><td>www.tzo.com</td></tr><tr><td>easydns</td><td>www.easydns.com</td></tr><tr><td>justlinux</td><td>www.justlinux.com</td></tr><tr><td>zoneedit</td><td>www.zoneedit.com</td></tr></tbody></table>	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
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	Enter the user ID. User ID and Password are used together 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.																
Password	See User ID.																
Host ID	Enter the domain name chosen by the user to identify the name of the system. This name is usually created in the user's portal on the service provider's site. 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).																

The Dynamic DNS page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

File Download Page

Use this page to download image and configuration files from a central FTP server and store them locally on the EdgeMarc appliance. [Table 48](#) describes the parameters on the page.

To access this page, choose **System > File Download** from the Configuration Menu.

[Help](#)

File Download

File Download allows the system to download image and configuration files from a central FTP server and store them locally on the system. To enable local storage of files, first enable the [File Server](#).

Enable File Download:

File Server Address:

File Refresh Frequency: hours

List the files to download from the server. (FTP files assumed to be in /pub.)

Table 48 File Download

Item	Description
Enable File Download	Check this box to enable file download.
File Server Address	Enter the IP address of the remote FTP server.
File Refresh Frequency	Enter the value in hours that the system will contact the remote FTP server for these files.
List the Files to Download from the Server	List the files in this text box to download from the remote server. (FTP files are assumed to be in /pub.) Enter the file names in one of the following formats: <ul style="list-style-type: none"> • <filename> space <filename> or • <filename> • <filename>

The File Download page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

File Server Page

Use this page to enable and configure FTP and/or TFTP file servers on the EdgeMarc appliance. Table 49 describes the parameters on the page.

To access this page, choose **System > File Server** from the Configuration Menu.

File Server
[Help](#)

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

Files that are stored on the server are stored in RAM. The files will be lost when the system is rebooted or a Submit is pressed on this page.

Enable TFTP Server:

Enable FTP Server:

RAMDISK Size (in Kbytes):

Server Maintenance:

Enable Read-Write Server:

Enable Automatic Cleanup:

Automatic Cleanup Interval:

Filenames to Cleanup:

Filesystem usage:

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
tmpfs	16384	156	16228	1%	/etc/images

Files on server:

```

274 0000000000000.cfg
5518 SIPDefault.cnf
1 fileconfig
4672 gpu0000000000000.cfg
112822 ipmid.cfg
2372 sipedgemarc.cfg
                
```


Table 49 File Server Parameters

Item	Description
Enable TFTP Server	Check this box to enable the TFTP Server.
Enable FTP Server	Check this box to enable the FTP Server. Either the TFTP ALG or TFTP server can be enabled. Enabling the TFTP server automatically disabled the TFTP ALG function. By default, the TFTP ALG is enabled and the TFTP server is disabled.
RAMDISK Size	Select the size of the systems RAMDISK, values are in Kbps. <ul style="list-style-type: none"> • 512Kbps • 1024Kbps • 2048Kbps • 4096Kbps • 8192Kbps • 16384Kbps

Server Maintenance

Enable Read-Write Server	Check to allow the file server to allow files to be uploaded to it via FTP. Use caution when enabling this feature. If the server file system fills up, phone configuration and image files could be lost. The default is disabled (a read-only file system).
Enable Automatic Cleanup	Check to cause the files listed in Filenames to Cleanup to be automatically deleted from the server.
Automatic Cleanup Interval	Enter the interval between file cleanup operations. The default cleanup interval is 15 minutes.
Filenames to Cleanup	Add the list of files to clean up. The filename can include wild cards such as "*". For example, to remove all log files, enter *.log.

The File Server page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

Network Information

Use this read-only page to display the low-level network configuration for the EdgeMarc appliance. [Table 50](#) lists the types of information presented.

To access this page, choose **System > Network Information** from the Configuration Menu.

[Help](#)

Network Information

Networking Information displays the low level network configuration for the system.

Routing Information:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.252	0.0.0.0	255.255.255.255	UH	0	0	0	lo
192.168.1.253	0.0.0.0	255.255.255.255	UH	0	0	0	lo
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
66.52.177.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
1.1.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	66.52.177.1	0.0.0.0	UG	0	0	0	eth1

Link Status:

```
eth0(1): no link
eth0(2): no link
eth0(3): no link
eth0(4): no link
eth1: negotiated 100baseTx-HD, link ok
```

Interface Information:

```
eth0      Link encap:Ethernet  HWaddr 00:03:6D:DF:32:60
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:256

eth0.1    Link encap:Ethernet  HWaddr 00:03:6D:DF:32:60
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1496  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0

eth0.1:252 Link encap:Ethernet  HWaddr 00:03:6D:DF:32:60
          inet addr:192.168.1.252  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1496  Metric:1

eth0.1:253 Link encap:Ethernet  HWaddr 00:03:6D:DF:32:60
          inet addr:192.168.1.253  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1496  Metric:1

eth0:100  Link encap:Ethernet  HWaddr 00:03:6D:DF:32:60
          inet addr:1.1.1.1  Bcast:1.255.255.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1

eth0:253  Link encap:Ethernet  HWaddr 00:03:6D:DF:32:60
          inet addr:192.168.1.253  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1

eth1      Link encap:Ethernet  HWaddr 00:03:6D:DF:32:61
          inet addr:66.52.177.178  Bcast:66.255.255.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:418288 errors:0 dropped:4 overruns:0 frame:0
          TX packets:23156 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:256

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:63530 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63530 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

Table 50 Network Information

Area	Description
Routing Information	Static routes for hosts and networks configured on the EdgeMarc device.
Link Status	Status of the Ethernet interfaces.
Interface Information	Status and configuration information for the system interfaces

Network Restart Page

This page is used to restart the network. It contains the following buttons:

To access this page, choose **System > Network Restart** from the Configuration Menu.

Networking Restart [Help](#)

Restarting the network services will interrupt the system for up to a minute. Proceed with caution!

Submit	Restarts the network.
--------	-----------------------

Reset

Network Test Tools Page

Use this page to verify connectivity of the EdgeMarc appliance and trace the path of data throughout the network. [Table 51](#) describes the parameters on the page.

To access this page, choose **System > Network Test Tools** from the Configuration Menu.

[Help](#)

Network Test Tools

A network administrator may use the test tools on this page to verify connectivity of the System and trace the path of data throughout the network.

Ping Test:

IP Address to Ping:

Traceroute Test:

IP Address to Trace:

Interface: LAN WAN

Table 51 Network Test Tools

Item	Description
Ping Test	
IP Address to Ping	Enter the destination IP address for the ping command. 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. Enter the IP address (IPv4 addresses only) of the device to send an ICMP ping to. Select Ping to execute the ping test. Select Reset to clear the IP address field so you can test a different path.

Table 51 Network Test Tools (continued)

Item	Description
Traceroute Test	
IP Address to Trace	Enter 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.

The Network Test Tools page contains the following buttons:

Ping	Perform a ping test.
Traceroute	Perform a traceroute test.
Reset	Clears selections and allows you to enter new information.

Proxy ARP Page

Use this page to configure bridges between the WAN and the LAN for an IP address or network. [Table 52](#) describes the parameters on the page.

To access this page, choose **System > Proxy ARP** from the Configuration Menu.

[Help](#)

Proxy ARP

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

Edit Proxy ARP List:

IP Address/Bitmask: /

On Interface:

Gateway:

Respond to ARP requests from: Interface

Configured Proxy ARP Entries:

IP Address/Bitmask	On IF	Proxy on IF	Gateway

Table 52 Proxy ARP Parameters

Item	Description
Edit Proxy ARP List	
In addition to proxying individual addresses, a range of addresses can be proxied by specifying a network netmask rather than a host netmask.	
IP Address /Bitmask	The IP address and netmask of the subnet to be proxied e.g. 67.40.40.1/32 for this single address.
On Interface	The specific interface of the system where the proxy target is connected. When VLAN (4300 only) is not enabled, this is always the LAN interface. When VLAN (4300 only) is enabled, you should choose the VLAN interface that the target is connected to.

Table 52 Proxy ARP Parameters (continued)

Item	Description
Gateway	The IP address of the gateway for the proxy target. The IP address should belong to the subnet of the target's interface that is connected to EdgeMarc device. 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 request's source IP address belong 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's subnet and also does not conflict with existing IP address.
Respond To ARP Requests From	The interface that the system will use to respond to ARP requests. The interface to use is the one that does not have access to the host system using the proxied address. Currently this interface must be the WAN interface of the system.

Configured Proxy ARP List

Shows a list of configured Proxy ARP entries.

The Proxy ARP page contains the following buttons:

Add	Adds the entry to the configured ARP entries list.
Delete	Deletes the selected entry.

RADIUS Settings Page

Use this page to configured RADIUS authentication settings. [Table 53](#) describes the parameters on the page.

To access this page, choose **System > RADIUS Settings** from the Configuration Menu.

[Help](#)

Radius Settings

Configuration parameters for using RADIUS server authentication for HTTP, HTTPS, SSH, Telnet and console login.

Important: you must re-Submit the Firewall configuration for changes to take effect.

Enable RADIUS:

Primary RADIUS Server Address:

Server Retries:

Retransmit Interval (in seconds):

Shared Secret:

Shared Secret (confirm):

RADIUS Port:

RADIUS Authorization Mode: ▼

Table 53 RADIUS Settings

Item	Description
Enable RADIUS	Select this checkbox to enable RADIUS authentication.
Primary RADIUS Server Address	IP address of the primary RADIUS server.
Server Retries	Number of times to try again to reach the RADIUS server if an attempt fails
Retransmit Interval (in seconds)	Delay in seconds between Server Retries. The default value is 2 seconds.
Shared Secret	A value used for authentication of the RADIUS request. The client and the server must have the same secret. There is no default for the shared secret.
Shared Secret (confirm)	Enter the shared secret a second time to confirm the value.

Table 53 RADIUS Settings (continued)

Item	Description
RADIUS Port	Port for local clients to use for communication with the RADIUS servers. The default is 1812.
RADIUS Authorization Mode	Mode for RADIUS authorization. Basic mode confirms the shared secret with the server. CHAP mode also shares the secret with the server but includes a built-in challenge as part of the CHAP protocol. The default is Basic.

The RADIUS Settings page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

Reboot System Page

This page is used to reboot the system.

To access this page, choose **System > Reboot System** from the Configuration Menu.

Reboot System [Help](#)

Rebooting the system interrupts all services for several minutes. Proceed with caution!

The Reboot System page contains the following buttons:

Reboot	Reboots the EdgeMarc appliance.
--------	---------------------------------

Remote Management

Use this page to specify the protocols that are permitted for management traffic and to restrict management access to defined subnets. [Table 54](#) describes the parameters on the page.

To access this page, choose **System > Remote Management** from the Configuration Menu.

[Help](#)

Remote Management

Configure Management Protocols and Trusted Management Addresses

Management Protocols:
Allow the following Management protocols.

HTTP: HTTPS: PING: SNMP: SSH: TELNET:

Remote Management Addresses:
Restrict management access to defined subnets. Default is to allow all
Warning: misconfiguration may block legitimate access requests.

Management Address	Address	Bitmask
	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>

Table 54 Remote Management

Item	Description
Management Protocols	Specifies the protocols to be allowed for management traffic.
Remote Management Addresses	Restricts management access to the defined subnets. Enter each IP address and bit mask.

The Route page contains the following buttons:

Add	Adds the new entry
Delete	Removes the selected entry
Submit	Applies the settings configured on this page.

Route Page

Use this page to create static routes. [Table 55](#) describes the parameters on the page.

To access this page, choose **System > Route** from the Configuration Menu.

Route

[Help](#)

Route allows the user to apply a static route to the system.

Apply Route:

IP Network:

Netmask:

Gateway:

To configure routing to support the transfer of VoIP data for more than one subnet, go to the [VoIP Subnet Routing](#) page.

Table 55 Static Routes

Item	Description
Apply Route	Select to activate this route.
IP Network	Enter the IP address of the remote network.
Netmask	Enter the subnet mask of the remote network.
Gateway	Enter the IP address of the gateway for the remote network.

The Route page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

Services Configuration

Use this page to configure SNMP and other services. [Table 56](#) describes the parameters on the page.

To access this page, choose **System > Services** from the Configuration Menu.

[Help](#)

Services Configuration

Customize the configuration of the services accessible on the System.

Enable SNMPv1:

SNMPv1 Read-Only Community:

SNMPv1 Trap Agent IP Address:

Trap Destinations:

IP Address	Version	Community	Delete

Enable SNMPv3:

SNMPv3 User Name:

SNMPv3 Passphrase:

SNMPv3 Security:

SNMPv3 Trap Context:

SNMPv3 Trap Destination IP Address:

SNMP Common Configuration:

System Location:

System Contact:

Port:

Enable Remote System Logging:

Remote Syslog Hosts:
[Syslog Hosts are Space delimited]

Syslog filter:

Current Hostname:

Set Hostname:

Admin Inactivity Timeout (seconds):

Enable MOS Scoring:

Current MOS Threshold:

Set MOS Threshold:

Table 56 Services Configuration

Item	Description
SNMPv1	
Enable SNMPv1	Indication that SNMPv1 is enabled.
SNMPv1 Read-Only Community	The community string that the management station uses when accessing read-only objects from the system.
SNMPv1 Trap Community	Trap community string place in trap PDUs.
SNMPv1 Trap Agent IP Address	When sending an SNMPv1 trap, set the trap agent field 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 will use the WAN/Provider address of the system.
SNMPv3	
Enable SNMPv3	Indication that SNMPv3 is enabled.
SNMPv3 User Name	If SNMPv3 is enabled, this field defines the SNMPv3 user name for SNMPv3 USM based authentication and VACm access control.
SNMPv3 Passphrase	The SNMPv3 passphrase is optionally used to authenticate the user as well as encrypt the payload based on the SNMPv3 Security setting below. The minimum length of a valid passphrase is 8.
SNMPv3 Security	The SNMPv3 security level for user authentication and encryption of both synchronous requests as well as asynchronous traps. "None" means neither SNMPv3 authentication or encryption are used. "Auth(MD5)" means authenticating user using MD5 hash algorithm. "AuthPriv(MD5/DES)" means authentication as well as encryption using the DES encryption algorithm. The default value is None.
SNMPv3 Trap Context	The SNMPv3 trap context defaults to nothing but can be set to any string.
Common Configuration	
System Location	A comment string that can be used to indicate the location of the system. By default, no value is set.
System Contact	The administrative contact information for the system. By default, no value is set.
SNMP Port	The port that the system monitors to read and send SNMP data. The default is 161.
Trap Destination IP	The IPv4 address to send traps to. Specifying this address enables cold start, authentication and linkUp/linkDown traps.

Table 56 Services Configuration (continued)

Item	Description
Enable Remote System Logging	Indication that syslog messages can be sent to a remote system.
Remote Syslog Host	The address or addresses systems running a system 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.
Syslog Filter	The current logging level for the syslog service on the system. The priorities are Debug, Informational, Notice, Warning, Error, Critical, Alert and Emergency. Choosing a higher priority excludes lower level syslog messages. Debug is the lowest logging level meaning it will log all the log levels. Emergency is the highest level and it will exclude all levels except Emergency. The default priority is Debug.
Local Hostname	Set the hostname for this system. By default, the hostname is the system type.
Admin Inactivity Timeout	This timer terminates login sessions that are inactive for the number of second specified. 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. The empty command resets the timer (i.e. pressing enter). The timer is not active when a command is running (e.g. a continuous ping). A value of '0' disables the inactivity timer. The largest allowed timeout value is 86400 seconds. The default is '0'.
Enable MOS Scoring	Enable MOS scoring for media that is passing through the system. Disabling MOS scoring will improve system performance. By default, MOS scoring is Enabled.
MOS Threshold	Set 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.

The Services Configuration page contains the following buttons:

Add New Destination	Adds the specified SNMP information.
Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

Set Link Page

Use this Set Link page to display and choose the current Ethernet interface link settings. Table 57 describes the parameters on the page.

To access this page, choose **System > Set Link** from the Configuration Menu.

Set Link
[Help](#)

Set Link displays the current ethernet interface link settings for the system. Use caution when adjusting the ethernet link rate. The device may become unreachable if an incompatible rate is set.

Link Rate Settings:
 Modification of WAN ethernet link parameters is not supported by this prototype hardware. Contact an Edgewater sales representative to obtain a production hardware upgrade.

LAN1 Ethernet:

LAN2 Ethernet:

LAN3 Ethernet:

LAN4 Ethernet:

WAN Ethernet:

Detailed Link Rate Information:

```
eth0(1): no link
product info: vendor 00:07:32, model 5 rev 2
basic mode: autonegotiation enabled
basic status: no link
capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
advertising: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-control
link partner: flow-control
eth0(2): no link
product info: vendor 00:07:32, model 5 rev 2
basic mode: autonegotiation enabled
basic status: no link
capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
advertising: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-control
link partner: flow-control
eth0(3): no link
product info: vendor 00:07:32, model 5 rev 2
basic mode: autonegotiation enabled
```

Table 57 Set Link

Item	Description
Link Rate Settings	Displays the current settings for the LAN and WAN interfaces. The default setting is autonegotiate.
Detailed Link Rate Information	Ethernet autonegotiation is often unreliable, especially between different vendors or old and new networking equipment. Failure of autonegotiation 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, video and data outages.

Table 57 Set Link (continued)

Item	Description
Set Ethernet Link Rate	The link rate of an interface can be assigned to a desired rate. A network administrator may want to set the rate manually if autonegotiation fails to select a rate consistently or it selects a rate that is slower than the maximum rate supported by both interfaces.
Set WAN MTU size	<p>On the 5300 and 6400 platforms, the WAN MTU size may be set 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.</p> <p>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.</p>

There are no buttons on the Set Link page.

Stateful Failover

Use this page to enable or disable stateful failover configuration parameters. [Table 58](#) describes the type of information on the page.

To access this page, choose **System > Stateful Failover** from the Configuration Menu.



Table 58 Stateful Failover

Item	Description
Administratively Disabled	<p>Administratively Disabled Select this checkbox on the primary or secondary system to bring it out of active mode and cause the other device in the redundant pair to take over.</p> <p>Note: Administratively disable the system during an upgrade. Additional Note: If a secondary system has not been enabled, voice services will be disrupted.</p>
Stateful Failover Configuration	<p>Enable Stateful Failover Select this checkbox to enable stateful failover.</p> <p>Note: This box should be checked on both the primary and the secondary system that will act as participants in a redundant pair.</p>

Table 58 Stateful Failover

Item	Description
Designation	Specify the device as the primary or secondary system in a redundant pair.
Password	Enter the password used by both the primary and secondary system.
LAN Virtual IP Address	Specify the common virtual IP address for the LAN that is shared between both the primary and secondary system.
WAN Virtual IP Address	Specify the common virtual IP address for the WAN that is shared between both the primary and secondary system.
LAN Remote Address	Specify the actual LAN address of the other system in the redundant pair. Note: Stateful failover must be enabled on the remote device.
WAN Remote Address	Specify the actual WAN address of the other system in the redundant pair. Note: Stateful failover must be enabled on the remote device.
Management Remote Address	Specify the actual management IP address of the other system in the redundant pair. Note: Stateful failover must be enabled on the remote device.
Enable State Transfer	Select this box for each address that will transfer state information to the other address in the redundant pair. Note: To eliminate the possibility of incomplete state transfer, enable state transfer on more than one link. If the redundant pair processes high volumes of traffic, enable state transfer on the management address, as this address is reserved and not used for SIP signalling or RTP media.

The Stateful Failover page contains the following buttons:

Commit	Saves the settings configured on this page to the EdgeMarc.
Reset	Clears all fields and selections and allows you to enter new information.

System Information

Use this page to view detailed operating system and device information. [Table 59](#) describes the types of information on the page.

To access this page, choose **System > System Information** from the Configuration Menu.

System Information

[Help](#)

System Information displays detailed operating system and device information.

System Uptime:

11:24:00 up 1 day, 12:18, load average: 0.00, 0.02, 0.00

Number of Active Streams:

0

Recent Call Log: [click here for online MOS help](#)

Process Information:

```

PID  Uid      VmSize  Stat  Command
  1  root      404    S    /bin/init
  2  root           SW    [keventd]
  3  root           SWN   [ksoftirqd_CPU0]
  4  root           SW    [kswapd]
  5  root           SW    [bdflush]
  6  root           SW    [kupdated]
  8  root           SW    [mtdblockd]
 78  root           SW    [ixp425 eth0]
 79  root           SW    [ixp425 eth1]
451  root      512    S    /bin/inetd
    
```

Table 59 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.
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 will be 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 link click here for online MOS help .
Process Information	Active processes in the EdgeMarc device.
Memory Usage	Detailed memory allocation information that may be of use to technical support.
System Logging Messages	Information logged during system boot and normal operation. Logging messages may include information about unauthorized attempts to access the EdgeMarc device; process restart messages; and excessive resource utilization messages.

There are no buttons on the System Information page.

System Time Page

Use this page to set the stem time. [Table 60](#) describes the parameters on the page.

To access this page, choose **System > System Time** from the Configuration Menu.

[Help](#)

System Time

Configure the system time of the System.

Current System Date: 06/15/2007 11:25:33 UTC

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 using [ping](#).

Enable SNTP:

SNTP Server:

Set Date (UTC time):

Month	Day	Year	Hour	Min.	Sec.
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Table 60 System Time

Item	Description
Enable SNTP	Select the checkbox to use SNTP
SNTP Server	Enter the IP address of the SNTP server. The server address can be either an IP address or the DNS name of the SNTP server.
Set Date	<p>The date on the device can be set manual using this option. The values are entered in numeric form.</p> <p>Month range: 1-12</p> <p>Day range: 1-31</p> <p>Year range: 1970-2034</p> <p>Hour range: 0-23</p> <p>Minute range: 0-59</p> <p>Second range: 0-59</p>

The System Time page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

Test UA Settings page

Use this page to make a call to or from the EdgeMarc itself. [Table 60](#) describes the parameters on the page.



Note

You must first have enabled the Test UA to access this page.

To access this page, choose **Test UA** from the Configuration Menu.

Test UA Settings

[Help](#)

Global configuration:

- Enable Test UA:
- Use SIP Username for SIP authentication:
- Register with proxy:

Test UA Configuration: (Unregistered)

SIP Display name:

SIP Username:

SIP Authentication name:

Password:

Domain:

Table 61 Test UA Settings

Item	Description
Enable Test UA	Enables the Test UA function. Note: Unchecking this box will not delete any pre-existing Test UA configuration.
Use SIP Username for SIP authentication	Enables the use of the SIP username for SIP authentication.
Register with proxy	Enables the Test UA to register with a configured domain using a configured outbound proxy.
SIP Display name	Defines the identity of the Test UA.
SIP Username	Defines the name that is used by the Test UA for SIP authentication.
SIP Authentication Name	Specifies the SIP Authentication Name. May be the same as the SIP username.
Password	Provides authentication credentials to the soft-switch.
Domain	Specifies the IP address assigned to the user agent.

T1 Configuration Page

Use this page to view and configure T1 parameters. [Table 62](#) describes the parameters on the page.

To access this page, choose **System > T1 Configuration** from the Configuration Menu.

[Help](#)

T1 Configuration

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

MLPPP Settings

Enable MLPPP

Current Settings:

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

Framing and Line Encoding:

Framing Mode:
 Line Encoding: B8ZS

Set Interface Configuration:

Type: T1
 T1-1 Name:
 T1-2 Name:
 T1-3 Name:
 T1-4 Name:
 Protocol:
 Clock: External Internal
 LBO:

Fractional Settings:

Enable Fractional Support:

Table 62 T1 Configuration

Item	Description
MLPPP Settings	
Enable MLPPP	Indicates whether MLPPP is enabled.
Framing and Line Encoding:	
Framing Mode	Defines the number of frames that are grouped together. ESF (F24) and D3/D4 (F12) are supported. ESF has 24 frames and D3/D4 has 12 frames.

Table 62 T1 Configuration (continued)

Item	Description
Set Interface Configuration	
T1 Name	Specifies the interface name.
Protocol	Specifies the protocol for the T1 interfaces.
Clock	Specifies an internal or external clock.
LBO	Determines the power and attenuation level (dB) for the transmit signal from the EdgeMarc T1 interfaces.
Fractional Settings	
<i>These settings are visible if MLPPP is disabled.</i>	
Enable Fractional Support	Allows configuration of a fractional T1 links.
Frame Relay Settings	
<i>These settings are visible if MLPPP is enabled and one of the PPPoFR protocol options is selected.</i>	
Frame Relay Mode	Specifies the DCE or DTE mode for frame relay.
Frame Relay DLCI	Specifies the DLCI value (channel number). Values 0-15 and 1023 are reserved and should not be used.
PPPoFR User Name	Specifies the user name for authentication by the PPPoFR switch.
PPPoFR Password	Specifies the password for authentication by the PPPoFR switch.
Frame Relay Secondary Settings	
<i>These settings are visible if MLPPP is disabled and fractional support is enabled.</i>	
Enable Secondary DLCI	Specifies the DCE or DTE mode for frame relay.
Secondary DLCI	Specifies the DLCI value (channel number). Values 0-15 and 1023 are reserved and should not be used.
PPPoFR User Name	Specifies the user name for authentication by the PPPoFR switch.
PPPoFR Password	Specifies the password for authentication by the PPPoFR switch.
Enable Auto DS0 Detection	Allows automatic detection of currently-used timeslots based on the pre-configured IDLE value that the T1 service provider provides for unused timeslots.

Table 62 T1 Configuration (continued)

Item	Description
Bandwidth	Specifies the bandwidth for the fractional link as a multiple of 64kbps.
Starting DS0	Specifies the beginning timeslot for the DS0 link (1-23).

The T1 Configuration page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

T1 Configuration Page - MLPPPoFR

The following page is an example of the T1 configuration for MLPPPoFR.



Note

If PPP Authentication is enabled, you can enter the PPPoFr Username and password and also have an option to enable secondary DLCI.

[Help](#)

T1 Configuration

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

MLPPP Settings

Enable MLPPP	<input checked="" type="checkbox"/>
Enable T1-1	<input checked="" type="checkbox"/>
Enable T1-2	<input checked="" type="checkbox"/>
Enable T1-3	<input type="checkbox"/>
Enable T1-4	<input type="checkbox"/>

Current Settings:

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

Framing and Line Encoding:

Framing Mode:
Line Encoding: B8ZS

Set Interface Configuration:

Type: T1

T1-1 Name:	<input type="text" value="527839"/>
T1-2 Name:	<input type="text" value="527781"/>
T1-3 Name:	<input type="text"/>
T1-4 Name:	<input type="text"/>

Protocol: Use PPP Authentication

Clock: External Internal
LBO:

Frame Relay Settings:

Frame Relay Mode: DCE DTE
Frame Relay DLCI:

T1 Diagnostics Page

Use this page to perform T1 diagnostic testing. [Table 63](#) lists the loopback tests, [Table 64](#) lists the alarm types, [Table 65](#) lists the loopback types, [Table 66](#) lists diagnostics counters, and [Table 67](#) lists the interval data.

To access this page, choose **System > T1 Diagnostics** from the Configuration Menu.

T1 Diagnostics

[Help](#)

The T1 Diagnostics page displays detailed T1 information that can assist in troubleshooting T1 interfaces.

Diagnostic Commands

T1-1	
Loopback:	Deactivate
BERT:	Deactivate
<input type="button" value="Submit-1"/>	

T1 Status

T1-1	
Alarms:	NONE
Loopback:	Deactivate
BERT:	OFF

T1 Statistics

For complete interval statistics, visit the [T1 advanced diagnostics page](#).

Counters	
T1-1	
Framing Errors:	0
Code Violation Errors:	0
CRC Errors:	0
Bit Errors:	0
Seconds Since Last:	0
ESF Error Events:	0
Current Status:	0
Valid Intervals:	0

Interval Data		
T1-1		
	CUR	SUM
Errored (s):	0	0
Unavailable (s):	0	0
Severely Errored (s):	0	0
Bursty Errored (s):	0	0
Loss of Frame (s):	0	0
Controlled Slip (s):	0	0
Valid (s) in Interval:	0	0
(s) w/ Actual Data:	0	0
<input type="button" value="Reset-1"/>		
Reset all stats	<input type="button" value="Reset"/>	

Table 63 Loopback Tests

Item	Description
Local	Tests the inward loopback such that the interface on the EdgeMarc can synchronize on the signal it is sending. Used to verify the proper operation of the T1 interface on the EdgeMarc appliance.
Network line	Loops the data back towards the network before the framer chip in the EdgeMarc appliance.
Network payload	Loops the data back towards the network at the T1 framer chip in the EdgeMarc appliance.
Remote line (AT&T or ANSI)	Causes the EdgeMarc 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)	The EdgeMarc 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.

Table 64 Alarm Types

Type	Description
Red Alarm	The EdgeMarc is not receiving a valid framing pattern from the network. Something is usually broken with the receive (of the EdgeMarc) path of the T1 line or with the sending equipment.
Yellow Alarm	The remote end (network side T1 interface) is not able to synchronize to the signal sent by the EdgeMarc. Something is usually broken with the transmit (from the EdgeMarc) path of the T1 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.

Table 65 Loopback Types

Type	Description
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 framer chip in the EdgeMarc.
Remote line (AT&T or ANSI)	Causes the EdgeMarc appliance to send 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)	Causes the EdgeMarc appliance to send 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.

Table 66 T1 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 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.

Table 67 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 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 appliance and the received T1 signal.
Valid Intervals	Number of elapsed seconds in the current interval.
(s) w/ Actual Data	Number of seconds for which there is data.

The T1 Diagnostics page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

TACACS Settings Page

Use this page to configure parameters for TACACS+ server authentication and logging for HTTP, HTTPS, SSH, Telnet, and console login. [Table 68](#) describes the parameters on the page.

To access this page, choose **System > TACACS Settings** from the Configuration Menu.

[Help](#)

TACACS+ Settings

Configuration parameters for using TACACS+ server authentication and logging for HTTP, HTTPS, SSH, Telnet and console login.

Important: you must relaunch your browser window for authentication changes to take effect.

Enable TACACS+ Authentication:

TACACS+ Server Address:

Shared Secret:

Shared Secret (confirm):

Server Timeout(in seconds):

TACACS+ Authentication Mode:

Enable TACACS+ Logging:

Table 68 TACACS Settings

Item	Description
Enable TACACS+ Authentication	Select the checkbox to activate TACACS+ authentication.
TACACS+ Server Address	Enter the IP address of the TACACS server to contact for authentication.
Shared Secret	is a value used for authentication of the TACACS+ request. The client and the server must have the same secret. There is no default for the shared secret.
Shared Secret (confirm)	Reenter the shared secret to confirm.
Server Timeout (in seconds)	If the TACACS+ server does not respond to a request within this period of time, it is deemed to be unavailable. The range is 1-100 seconds, and the default is 5 seconds.

Table 68 TACACS Settings (continued)

Item	Description
TACACS+ Authentication Mode	Select one of the following TACACS+ authentication modes: <ul style="list-style-type: none">• 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.
Enable TACACS+ Logging	If enabled, all configuration changes done by user over HTTP, HTTPS, SSH, Telnet, and system console are logged.

The TACACS page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

Upgrade Firmware Page

Use this page to upgrade the firmware on the EdgeMarc appliance. [Table 69](#) describes the parameters on the page.

To access this page, choose **System > Upgrade Firmware** from the Configuration Menu.

[Help](#)

Upgrade Firmware

Current Version:
Version 7.3.0jdoan -- Tue Jun 12 14:03:08 PDT 2007

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

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

Download Server:

Filename:

Table 69 Upgrade Firmware

Item	Description
Download Server	Enter the IP address of the server from which the new firmware will be downloaded.
Filename	Enter the name of the firmware file.

The Upgrade Firmware page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

User Commands Page

Use this page to enter specialized commands or enable features that are not available through other GUI pages. [Table 70](#) describes the parameters on the page.

To access this page, choose **System > User Commands** from the Configuration Menu.

[Help](#)

User Commands

The User Commands page is used to enter specialized commands or enable features that are not available through other GUI pages. User commands are stored in the file `/etc/config/user_defs.conf`, as described in a number of Edgewater Knowledgebase articles. They are automatically executed whenever the box starts or a Network Restart is performed. User commands are commonly used to create user specific firewall and routing rules.

The user should use caution when adding user commands. The system may become unreachable if an incorrect command is entered.

Once user commands have been entered, if changes are later made on other GUI pages, it is recommended that a [Network Restart](#) be performed.

User Commands:

Table 70 User Commands

Item	Description
User Commands	Area to enter specialized commands or enable features that are not available through the GUI.

The User Command page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

VoIP Subnet Routing Page

Use this page to configure the EdgeMarc appliance to proxy remote networking devices that are not on the same subnet. [Table 71](#) describes the parameters on the page.

To access this page, choose **System > VoIP Subnet Routing** from the Configuration Menu.

[Help](#)

VoIP Subnet Routing

Allow ALG routing of VoIP data for multiple subnets.

Update Subnet List:

IP Network:

Netmask:

Gateway:

Delete Subnet:

Currently Configured Subnets:
There are no subnets configured.

Table 71 VoIP Subnet Routing

Item	Description
IP Network	Enter the IP address of the remote network.
Netmask	Enter the subnet mask for the remote network.
Gateway	Enter the IP address of the gateway for the remote network.
Delete Subnet	Select the checkbox to delete the subnet.

The VoIP Subnet Routing page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

VLAN Configuration Page

Use this page to configure VLAN support. Table 72 describes the parameters on the page.

To access this page, choose **System > VLAN Configuration** from the Configuration Menu.

[Help](#)

VLAN Configuration

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

View and modify existing VLAN configuration.

ID	IP Address	Network Mask	LAN Port Membership			
			1	2	3	4
1	192.168.1.1	255.255.255.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Link Status			●	●	●	●

Add and configure a new VLAN.

ID	IP Address	Network Mask
<input type="text"/>	<input type="text"/>	<input type="text"/>

Table 72 VLAN Configuration

Item	Description
View and modify existing VLAN Configuration	
ID	VLAN ID.
IP Address	IP address of the VLAN.
Network Mask	Network make of the VLAN

Table 72 VLAN Configuration (continued)

Item	Description
LAN Port Membership	Selection of protocols for each LAN port: 802.1 or 802.1q. The mode of the physical port determines the rules for VLAN assignment: <ul style="list-style-type: none">• 802.1 mode: Assign the port to a single VLAN.• 802.1q mode: Assign the port to multiple VLANs Note: Port 4 is reserved for 802.1.

Add and configure a new VLAN

ID	VLAN ID.
IP Address	IP address of the VLAN.
Network Mask	Network make of the VLAN

The VLAN Configuration page contains the following buttons:

Add	Adds a new VLAN.
Modify	Modifies and existing VLAN.
Reset	Clears all fields and selections in this area of the page and allows you to enter new information.

Wireless Configuration Page

Use this page to configure the EdgeMarc appliance as a wireless access point. Table 73 describes the parameters on the page.

To access this page, choose **System > Wireless** from the Configuration Menu.

The screenshot shows the 'Wireless' configuration page. At the top right is a 'Help' link. Below the title, there is a checkbox for 'Enable Wireless' which is currently checked. A horizontal line separates this from the 'Current Settings' section. Under 'Current Settings', several parameters are listed with their current values: 'Wireless' (Enabled), 'Network SSID' (EWNdf3264), 'Wireless Mode' (802.11b/g), 'Channel' (6), 'Power Level' (4), and 'Security' (Disabled). Another horizontal line follows. The 'Settings' section contains input fields for 'Network SSID' (EWNdf3264), 'Enable SSID Broadcast' (checked), 'Wireless Mode' (802.11b/g), 'Power Level' (4 (1.3 dBm)), and 'Channel' (6). A final horizontal line separates this from the 'Security Settings' section, which has an unchecked 'Enable Security' checkbox. At the bottom are 'Submit' and 'Reset' buttons.

Table 73 Wireless Configuration

Item	Description
Enable Wireless	Indication that the appliance can be used as a wireless access point.
IP Address	IP address of the VLAN.
Settings	
Network SSID	Unique name for the wireless network. Wireless client must enter the SSID to connect to the network.
Enable SSID Broadcast	Indication that the SSID is advertised in the 802.11 beacon.
Wireless Mode	Wireless mode that is compatible with the served clients.
Power Level	Level of power provided for the 802.11 signals (dBm)
Channel	801.11 operating RF channel.

Table 73 Wireless Configuration (continued)

Item	Description
Security Settings	
Enable Security	Indication that security is checked when a client accesses the wireless network.
Pre-Shared Key	Key for initial access to the wireless network.
Key Renewal Interval	Number of seconds between attempts to automatically synchronize the pre-shared keys.

The Wireless Configuration page contains the following buttons:

Add	Adds a new VLAN.
Modify	Modifies and existing VLAN.
Reset	Clears all fields and selections in this area of the page and allows you to enter new information.

Client Side ISDN PRI (PRI/GW) Configuration Page

Use this page to configure the Client Side ISDN PRI (PRI/GW) on the EdgeMarc appliance. Table 66 describes the parameters on this page.

To access this page, choose “*SIP-GW* → *PRI Client configuration*” from the Configuration Menu

[Help](#)

Client Side ISDN PRI (PRI/GW) configuration

Client Side PRI enables the SIP/GW(SIP Gateway) to provide a standard ISDN PRI Client-side interface to the PSTN. SIP/GW will receive calls from IP side and connect call to PSTN.

Enable PRI/GW services:

SIP/GW is currently bound to address: 192.168.1.253 and port: 1026

PRI is configured for T1 line:4

Trunk Switch Type:

D Channel:

B Channel order descending(optional):

Internal clocking:

Register with SIP server(optional):

Override SIP FROM Username(To IP network):

SIP Authentication name(Optional):

SIP Password(Optional):

Refer to [Header Transformation](#) page if you want to override FROM domain name.

Define configuration for each PRI channel:

Channel No.	Enable	Status
1	<input checked="" type="checkbox"/>	Not-connected
2	<input checked="" type="checkbox"/>	Not-connected
3	<input checked="" type="checkbox"/>	Not-connected
4	<input checked="" type="checkbox"/>	Not-connected

To be continued on the next page...

5	<input checked="" type="checkbox"/>	Not-connected
6	<input checked="" type="checkbox"/>	Not-connected
7	<input checked="" type="checkbox"/>	Not-connected
8	<input checked="" type="checkbox"/>	Not-connected
9	<input checked="" type="checkbox"/>	Not-connected
10	<input checked="" type="checkbox"/>	Not-connected
11	<input checked="" type="checkbox"/>	Not-connected
12	<input checked="" type="checkbox"/>	Not-connected
13	<input checked="" type="checkbox"/>	Not-connected
14	<input checked="" type="checkbox"/>	Not-connected
15	<input checked="" type="checkbox"/>	Not-connected
16	<input checked="" type="checkbox"/>	Not-connected
17	<input checked="" type="checkbox"/>	Not-connected
18	<input checked="" type="checkbox"/>	Not-connected
19	<input checked="" type="checkbox"/>	Not-connected
20	<input checked="" type="checkbox"/>	Not-connected
21	<input checked="" type="checkbox"/>	Not-connected
22	<input checked="" type="checkbox"/>	Not-connected
23	<input checked="" type="checkbox"/>	Not-connected
24	<input type="checkbox"/>	D-channel

Submit Reset

Table 74 ISDN PRI (PRI/GW) Configuration Parameters

Item	Description
Enable PRI/GW services	Enables Client side ISDN PRI interface and SIP trunking on IP side.
Trunk Switch Type	Switch type that Client-side ISDN PRI will be simulating. Default is NI2. Note: Switch type must match Network-side switch-type to which this interface is connected.
D Channel	D-channel number that will be used for Q.931 signaling.

Table 74 ISDN PRI (PRI/GW) Configuration Parameters

Item	Description
B Channel order descending (optional)	For an outgoing call, it enables the system to select the highest free B-Channel from 24 to 1, bypassing the channel configured as D-Channel by "D Channel" parameter above.
Internal Clocking	The PRI line requires a synching time source which can be "internal" or "external". The "internal" time source can be a local system clock and the "external" clocking signal is provided by the service provider or the PBX connected on the other side of the PRI line. This option enables the use of internal clock for synching time signal.
Register with SIP server	This optional parameter enables the device to register with the SIP server. If specified, the value of "Override SIP FROM" parameter below is used, otherwise its default value is used for SIP user name. If authentication is required, "SIP Authentication name" and "SIP Password" parameters below must also be provided.
Override SIP FROM Username	When an incoming call from PSTN to the Client side PRI gateway is terminated on the IP network, the FROM field in the SIP message towards the IP network contains the value of this parameter. If no value is specified for this parameter, then gateway's LAN MAC address is used by default.
SIP Authentication name	This parameter is required if "Register with SIP Server" is enabled and authentication is required. It defines the name to be used in the authentication process of the Client side PRI gateway registration with the SIP server.
SIP Password	This parameter is required if "Register with SIP Server" is enabled and authentication is required. It defines the password to be used in the authentication process of the Client side PRI gateway registration with the SIP server.
Define configuration for each PRI channel.	
Channel No.	B-channel number
Enable	Enables the B-channel as part of the call. By default all the 23 channels are enabled. Note: Fraction of B-channels on the PRI interface can be selected.
Status	Provides the read-only status for a given PRI channel. Status can be Unknown, Idle, Busy, Not-connected.

Client Side ISDN CAS (CAS/GW) Configuration Page

Use this page to configure the Client Side ISDN CAS (CAS/GW) on the EdgeMarc appliance. Table 66 describes the parameters on this page.

To access this page, choose **SIP/GW > CAS Client configuration** from the Configuration Menu

Client Side (CAS/GW) configuration [Help](#)

Client Side CAS enables the SIP/GW(SIP Gateway) to provide a standard CAS interface to the PSTN. SIP/GW will receive calls from IP side and connect call to PSTN.

Enable CAS/GW services:

SIP/GW is currently bound to address: 192.168.1.253 and port: 1026

CAS is configured for T1 line:4

CAS signaling model:

Internal clocking:

Register with SIP server(optional):

Override SIP FROM Username(To IP network):

SIP Authentication name(Optional):

SIP Password(Optional):

Refer to [Header Transformation](#) page if you want to override FROM domain name.

Define configuration for each CAS channel:

Channel No.	Enable	Status
1	<input checked="" type="checkbox"/>	Not-connected
2	<input checked="" type="checkbox"/>	Not-connected
3	<input checked="" type="checkbox"/>	Not-connected
4	<input checked="" type="checkbox"/>	Not-connected
5	<input checked="" type="checkbox"/>	Not-connected

To be continued on the next page...

6	<input checked="" type="checkbox"/>	Not-connected
7	<input checked="" type="checkbox"/>	Not-connected
8	<input checked="" type="checkbox"/>	Not-connected
9	<input checked="" type="checkbox"/>	Not-connected
10	<input checked="" type="checkbox"/>	Not-connected
11	<input checked="" type="checkbox"/>	Not-connected
12	<input checked="" type="checkbox"/>	Not-connected
13	<input checked="" type="checkbox"/>	Not-connected
14	<input checked="" type="checkbox"/>	Not-connected
15	<input checked="" type="checkbox"/>	Not-connected
16	<input checked="" type="checkbox"/>	Not-connected
17	<input checked="" type="checkbox"/>	Not-connected
18	<input checked="" type="checkbox"/>	Not-connected
19	<input checked="" type="checkbox"/>	Not-connected
20	<input checked="" type="checkbox"/>	Not-connected
21	<input checked="" type="checkbox"/>	Not-connected
22	<input checked="" type="checkbox"/>	Not-connected
23	<input checked="" type="checkbox"/>	Not-connected
24	<input checked="" type="checkbox"/>	Not-connected

Submit Reset

Table 75 Client Side ISDN CAS Configuration Parameters

Item	Description
CAS signaling model	Specifies the type of CAS signaling to be used in the call setup and tear down.
Internal Clocking	<p>The CAS line requires a synching time source which can be "internal" or "external". The "internal" time source can be a local system clock and the "external" clocking signal is provided by the service provider or the PBX connected on the other side of the CAS line.</p> <p>This option enables the use of internal clock for synching time signal.</p>

Table 75 Client Side ISDN CAS Configuration Parameters

Item	Description
Register with SIP server	This optional parameter enables the device to register with the SIP server. If specified, the value of "Override SIP FROM" parameter below is used, otherwise its default value is used for SIP user name. If authentication is required, "SIP Authentication name" and "SIP Password" parameters below must also be provided.
Override SIP FROM Username	When an incoming call from PSTN to the Client side CAS gateway is terminated on the IP network, the FROM field in the SIP message towards the IP network contains the value of this parameter. If no value is specified for this parameter, then gateway's LAN MAC address is used by default.
SIP Authentication name	This parameter is required if "Register with SIP Server" is enabled and authentication is required. It defines the name to be used in the authentication process of the Client side CAS gateway registration with the SIP server.
SIP Password	This parameter is required if "Register with SIP Server" is enabled and authentication is required. It defines the password to be used in the authentication process of the Client side CAS gateway registration with the SIP server.
Define configuration for each PRI channel.	
Channel No.	CAs channel number
Enable	Enables the CAS channel as part of the call. By default all the 24 channels are enabled. Note: Fraction of CAS channels can be selected.
Status	Provides the read-only status for a given CAS channel. Status can be Unknown, Idle, Busy, Not-connected.

Network Side ISDN PRI (PRI/UA) Configuration Page

Use this page to configure the Network Side ISDN PRI (PRI/UA) on the EdgeMarc appliance. Table 67 describes the parameters on this page.

To access this page, choose **SIP/UA > PRI/NET configuration** from the Configuration Menu.

Network Side ISDN PRI (PRI/UA) configuration [Help](#)

Network Side ISDN PRI enables the SIP-UA to provide a standard ISDN PRI Network-side interface to the PBXs and to mimic the behavior of legacy phone switches.

Enable PRI/UA services:

SIP/UA is currently bound to address: 192.168.1.252 and port: 1025

Note: *If you enable Network side PRI/UA service, you must also configure the SIP trunking device and dial-rule to terminate VoIP traffic to Network side PRI/UA. Use SIP/UA Binding information to configure trunking device and define a dial-rule. If you want, you can change the default binding address at [UA Advance Page](#) by defining field 'SIPUA IP Address'.*

PRI is configured for T1 line:4

Trunk Switch Type:

D Channel:

Note: *Device name MUST match the device name defined in [SIP trunking device and dial-rule page](#) for PRI trunking.*

Device name:

B Channel order descending(optional):

Internal clocking:

International Prefix:

Register with SIP server(optional):

Override SIP FROM Username(To IP network):

SIP Authentication name(Optional):

SIP password(Optional):

Refer to [Header Transformation](#) page if you want to override FROM domain name.

To be continued on the next page...

Define configuration for each PRI channel:

Channel No.	Enable	Status
1	<input checked="" type="checkbox"/>	Unknown
2	<input checked="" type="checkbox"/>	Unknown
3	<input checked="" type="checkbox"/>	Unknown
4	<input checked="" type="checkbox"/>	Unknown
5	<input checked="" type="checkbox"/>	Unknown
6	<input checked="" type="checkbox"/>	Unknown
7	<input checked="" type="checkbox"/>	Unknown
8	<input checked="" type="checkbox"/>	Unknown
9	<input checked="" type="checkbox"/>	Unknown
10	<input checked="" type="checkbox"/>	Unknown
11	<input checked="" type="checkbox"/>	Unknown
12	<input checked="" type="checkbox"/>	Unknown
13	<input checked="" type="checkbox"/>	Unknown
14	<input checked="" type="checkbox"/>	Unknown
15	<input checked="" type="checkbox"/>	Unknown
16	<input checked="" type="checkbox"/>	Unknown
17	<input checked="" type="checkbox"/>	Unknown
18	<input checked="" type="checkbox"/>	Unknown
19	<input checked="" type="checkbox"/>	Unknown
20	<input checked="" type="checkbox"/>	Unknown
21	<input checked="" type="checkbox"/>	Unknown
22	<input checked="" type="checkbox"/>	Unknown
23	<input checked="" type="checkbox"/>	Unknown
24	<input type="checkbox"/>	D-channel

Submit Reset

Table 76 Network Side ISDN PRI Configuration Parameters

Item	Description
Enable PRI/GW services	Enables Network side ISDN PRI interface and SIP trunking on IP side.
PRI line	T1 line (port 1) for ISDN PRI.
Trunk Switch Type	Switch type that Network-side ISDN PRI will be simulating. Default is NI2. Note: Switch type must match Client-side switch-type to which this interface is connected.
D Channel	D-channel number that will be used for Q.931 signaling.
Device Name	Device name as it is configured in VoIP ALG->SIP->Trunking page . Note: It is advisable to change this field, if device name in trunking page is changed.

Table 76 Network Side ISDN PRI Configuration Parameters

Item	Description
B Channel order descending (optional)	For an outgoing call, it enables the system to select the highest free B-Channel from 24 to 1, bypassing the channel configured as D-Channel by "D Channel" parameter above.
Internal Clocking	The PRI line requires a synching time source which can be "internal" or "external". The "internal" time source can be a local system clock and the "external" clocking signal is provided by the service provider or the PBX connected on the other side of the PRI line. This option enables the use of internal clock for synching time signal.
Register with SIP server	This optional parameter enables the device to register with the SIP server. If specified, the value of "Override SIP FROM" parameter below is used, otherwise its default value is used for SIP user name. If authentication is required, "SIP Authentication name" and "SIP Password" parameters below must also be provided.
Override SIP FROM Username	When an incoming call from PSTN to the Network side PRI UA is terminated on the IP network, the FROM field in the SIP message towards the IP network contains the value of this parameter. If no value is specified for this parameter, then gateway's LAN MAC address is used by default.
SIP Authentication name	This parameter is required if "Register with SIP Server" is enabled and authentication is required. It defines the name to be used in the authentication process of the Network side PRI UA registration with the SIP server.
SIP Password	This parameter is required if "Register with SIP Server" is enabled and authentication is required. It defines the password to be used in the authentication process of the Network side PRI UA registration with the SIP server.
Define configuration for each PRI channel.	
Channel No.	B-channel number
Enable	Enables the B-channel as part of the call. By default all the 23 channels are enabled. Note: Fraction of B-channels on the PRI interface can be selected.
Status	Provides the read-only status for a given PRI channel. Status can be Unknown, Idle, Busy, Not-connected.

Network Side ISDN CAS (CAS/UA) Configuration Page

Use this page to configure the Network Side ISDN CAS (CAS/UA) on the EdgeMarc appliance. Table 67 describes the parameters on this page.

To access this page, choose “SIP UA→CAS/NET configuration“ from the Configuration Menu.

[Help](#)

Network Side (CAS/UA) configuration

CAS/Net enables the SIP-UA to provide a standard CAS/T1 Network-side interface to the PBXs and to mimic the behavior of legacy phone switches.

Enable CAS/UA services:

SIP/UA is currently bound to address: 192.168.1.252 and port: 1025

Note: If you enable Network side CAS/UA service, you must also configure the SIP trunking device and dial-rule to terminate VoIP traffic to Network side CAS/UA. Use SIP/UA Binding information to configure trunking device and define a dial-rule. If you want, you can change the default binding address at [UA Advance Page](#) by defining field 'SIPUA IP Address'.

CAS is configured for T1 line:4

CAS signaling model:

Note: Device name MUST match the device name defined in [SIP trunking device and dial-rule](#) page for CAS trunking.

Device name:

Internal clocking:

International Prefix:

Register with SIP server(optional):

Override SIP FROM Username(To IP network):

SIP Authentication name(Optional):

SIP password(Optional):

Refer to [Header Transformation](#) page if you want to override FROM domain name.

Define configuration for each CAS channel:

Channel No.	Enable	Status
1	<input checked="" type="checkbox"/>	Not-connected
2	<input checked="" type="checkbox"/>	Not-connected
3	<input checked="" type="checkbox"/>	Not-connected

To be continued on the next page...

4	<input checked="" type="checkbox"/>	Not-connected
5	<input checked="" type="checkbox"/>	Not-connected
6	<input checked="" type="checkbox"/>	Not-connected
7	<input checked="" type="checkbox"/>	Not-connected
8	<input checked="" type="checkbox"/>	Not-connected
9	<input checked="" type="checkbox"/>	Not-connected
10	<input checked="" type="checkbox"/>	Not-connected
11	<input checked="" type="checkbox"/>	Not-connected
12	<input checked="" type="checkbox"/>	Not-connected
13	<input checked="" type="checkbox"/>	Not-connected
14	<input checked="" type="checkbox"/>	Not-connected
15	<input checked="" type="checkbox"/>	Not-connected
16	<input checked="" type="checkbox"/>	Not-connected
17	<input checked="" type="checkbox"/>	Not-connected
18	<input checked="" type="checkbox"/>	Not-connected
19	<input checked="" type="checkbox"/>	Not-connected
20	<input checked="" type="checkbox"/>	Not-connected
21	<input checked="" type="checkbox"/>	Not-connected
22	<input checked="" type="checkbox"/>	Not-connected
23	<input checked="" type="checkbox"/>	Not-connected
24	<input checked="" type="checkbox"/>	Not-connected

Submit Reset

Table 77 Network Side ISDN CAS Configuration Parameters

Item	Description
CAS signaling model	Specifies the type of CAS signaling to be used in the call setup and tear down.
Device name	Specifies the device name as it is configured in 'VoIP ALG->SIP->Trunking" page. It is advisable to change this field, if device name in trunking page is changed.

Table 77 Network Side ISDN CAS Configuration Parameters

Item	Description
Internal Clocking	<p>The CAS line requires a synchronizing time source which can be "internal" or "external". The "internal" time source can be a local system clock and the "external" clocking signal is provided by the service provider or the PBX connected on the other side of the CAS line.</p> <p>This option enables the use of internal clock for synchronizing time signal.</p>
International Prefix	This parameter specifies the digits to be added at the beginning of an international number before it is sent to the SIP server.
Register with SIP server	This optional parameter enables the device to register with the SIP server. If specified, the value of "Override SIP FROM" parameter below is used, otherwise its default value is used for SIP user name. If authentication is required, "SIP Authentication name" and "SIP Password" parameters below must also be provided.
Override SIP FROM Username	When an incoming call from a PBX to the Network side CAS UA is terminated on the IP network, the FROM field in the SIP message towards the IP network contains the value of this parameter. If no value is specified for this parameter, then gateway's LAN MAC address is used by default.
SIP Authentication name	This parameter is required if "Register with SIP Server" is enabled and authentication is required. It defines the name to be used in the authentication process of the Network side CAS UA registration with the SIP server.
SIP Password	This parameter is required if "Register with SIP Server" is enabled and authentication is required. It defines the password to be used in the authentication process of the Network side CAS UA registration with the SIP server.
Define configuration for each PRI channel.	
Channel No.	CAs channel number
Enable	<p>Enables the CAS channel as part of the call. By default all the 24 channels are enabled.</p> <p>Note: Fraction of CAS channels can be selected.</p>
Status	Provides the read-only status for a given CAS channel. Status can be Unknown, Idle, Busy, Not-connected.

WAN Link Redundancy Configuration Page

Use this page to configure the WAN Link Redundancy on the EdgeMarc appliance. Table 78 describes the configurable parameters on this page.

To access this page, choose “**Wan-Link Redundancy**” submenu from “**Configuration Menu**”

[Help](#)

Wan Link Redundancy

This section allows administrators to configure various WLR parameters and view WLR status values.

If you want to attach Data/Voice Services to a specific interface then use the dropdown settings below.

Data Interface Primary ▼

Voice Interface Primary ▼

Enable WAN Link Redundancy:

Enable Revertive Mode:

Interface details:

Primary Interface name: eth1
 Primary Interface IP address: 10.10.66.1
 Secondary Interface name: eth1:0
 Secondary Interface IP address: 10.10.10.120

WAN Link Redundancy Status

Current Active Data Interface: PRIMARY
 Current Active Voice Interface: PRIMARY
 Primary Interface Status: **DOWN**
 Secondary Interface Status: **DOWN**

Table 78 WAN Link Redundancy

Item	Description
Data Interface	Allows the user to choose Primary or Secondary interface as the active interface for data. If Revertive Mode is enabled, then the chosen interface will also be treated as the main interface for data services. The only time this interface will not be used is when it is down.
Voice Interface	Allows the user to choose Primary or Secondary interface as the active interface for voice. If Revertive Mode is enabled, then the chosen interface will also be treated as the main interface for voice services. The only time this interface will not be used is when it is down.

Table 78 WAN Link Redundancy

Item	Description
Enable WAN Link Redundancy	Enable WAN Link Redundancy by selecting the check box. WAN Link Redundancy is disabled if the check box is cleared.
Enable Revertive Mode	Select the checkbox to delete the subnet.



Note: Priority calling services cannot be configured when WAN Link Redundancy is enabled.

The WAN Link Redundancy page contains the following buttons:

Submit	Applies the settings configured on this page.
Manual Switchover	Switches voice and data services from their currently active interfaces over to their inactive interfaces. This action will result in a network restart.



Note: Only works when Revertive Mode is disabled.

Secondary Interface Settings Configuration Page

Use this page to configure the Secondary interface for the WAN Link Redundancy feature on EdgeMarc. Table 79 describes the configurable parameters on this page.

To access this page, choose “**Wan-Link Redundancy**→**Secondary WAN Config**” submenu from “**Configuration Menu**”

Secondary Interface Settings [Help](#)

Secondary WAN interface configuration

Secondary WAN Interface Settings:

- ADSL-PPPoE
- DHCP
- Static IP Address
- EVDO
- T1

Enter the username and password given to you by your network provider.

User Name:

Password:

Keepalive Ping:

PPP Link Status: down

To see the IP address given to the WAN port, check the [Network Information page](#).

IP Address:

Subnet Mask:

Secondary WAN Network Settings:

Default Gateway:

Primary DNS Server:

Secondary DNS Server:

Secondary WAN Redundancy Settings:

Enable Ping based status detection:

Ping Host:

Table 79 Secondary Interface Settings

Item	Description
Radio buttons	Select the method used to obtain a connection to the Internet: <ul style="list-style-type: none"> ADSL-PPPoE — When this option is selected, only areas B and C from the above figure are visible. DHCP — Allows the device to obtain the WAN-side IP address using a DHCP server available from the WAN side of the network. NOTE: To see the WAN IP address for the system, go to the Network Information page. Only area C is visible for this option. Static IP Address — Allows you to configure the WAN interface with a static IP address (default). Areas C and D are visible for this option. EVDO — Allows the device to use a 3G card from Verizon Wireless. Only area C is visible for this option. T1 — Allows you to configure the WAN interface with a static IP address and also configure and test the T1 interface on the system on the T1 Configuration page. You can click the underlined link to open the T1 Configuration page. For information on using the T1 Configuration page, see Test UA Settings page on page 279. Areas C and D are visible for this option.
User Name	Enter the user name assigned by your network provider.
Password	Enter the password assigned by your network provider.
Keepalive Ping	Select to send an ICMP echo request to its gateway every minute to ensure that the ISP keeps the PPPoE connection open.
PPPoE Link Status (view only)	View the status of the PPPoE line.
IP Address	IP address to be assigned manually.
Subnet Mask	Subnet mask to be assigned manually.

Secondary WAN Network Settings

Note: Enter these settings if you selected Static IP Address or T1 in the WAN interface Settings area.

Default Gateway	Enter the default IP gateway for the system. This gateway will be on the same IP subnet as the IP address.
Primary DNS	Enter the primary DNS server as supplied by the ISP.
Secondary DNS	Enter the secondary DNS server as supplied by the ISP. Used if the primary server is unavailable.

Secondary WAN Redundancy Settings

Table 79 Secondary Interface Settings

Item	Description
Enable Ping based status detection	If WLR is enabled and this field is checked, then the system sends ICMP packets to the "Ping Hot" and if no response is received, then the link is declared as down.
Ping Host	If "Enable Ping based status detection" is checked and WLR is enabled, then ICMP packets will be sent to the host whose IP address is specified in this field.

The Secondary Interface Settings page contains the following buttons:

Submit	Applies the settings configured on this page.
Reset	Clears all fields and selections and allows you to enter new information.

WAN Link Parameters Configuration Page

Use this page to configure the various parameters effecting the behavior of WAN Link Redundancy feature on the EdgeMarc. Table 80 describes the configurable parameters on this page.

To access this page, choose “**Wan-Link Redundancy**→**WLR Parameters Config**” submenu from “**Configuration Menu**”

Wan-Link Redundancy Configuration [Help](#)

This section allows administrators to configure various WLR parameters.

Link Detection Module

Up Link Timer (seconds):

Up Link Attempts:

Down Link Timer(seconds):

Down Link Attempts:

Ping Detection Module

Up Ping Timer (seconds):

Up Ping Attempts:

Down Ping Timer (seconds):

Down Ping Attempts:

Table 80 WLR Parameters Configuration

Item	Description
Link Detection Module	
Up Link Timer	Specifies the time interval in seconds before the module polls a physically up interface for its status.
Up Link Attempts	Specifies the number of UP responses from a previously down interface before it can be declared as up.
Down Link Timer	Specifies the time interval in seconds before the the module polls a physically down interface for its status.
Down Link Attempts	Specifies the number of DOWN responses from a previously physically up interface before it can be declared as down.
Ping Detection Module	
Up Ping Timer	Specifies the time interval in seconds before the module sends an ICMP packet on a physically up link to the “Ping Host”.
Up Ping Attempts	Specifies the number consecutive responses for ICMP requests from the “Ping Host” on a previously down link before the link can be declared as up.

Item	Description
Down Ping Timer	Specifies the time interval in seconds before the the module sends an ICMP request on a down link with physically up interface.
Down Ping Attempts	Specifies the number of consecutive ICMP requests with no responses from the "Ping Host" on a physically up interface with a previously up link status.

License Information

The following sections contain license information related to the operation of EdgeMarc™ hardware and software:

- EdgeMarc Software License Agreement
- Asterisk Copyright
- Data Encryption Standard Copyright
- XML 1.0 Parser Library License
- Open LDAP Copyright
- Open LDAP License
- Open H.323 Copying Permission
- Henry Spencer Regex License
- Berkeley Source Distribution License
- Sleepycat Software License
- Perl Compatible Regular Expressions License
- Vovida Software License
- Blowfish License
- Open SSL License
- Open SSL Toolkit License
- Net SNMP License
- Point-to-Point Protocol Daemon License
- SSH License
- Shadow Utilities License
- Asterisk Copyright
- GNU General Public License Version 2.1

EdgeMarc Software License Agreement

EDGEWATER NETWORKS, INC. IS WILLING TO LICENSE THIS SOFTWARE AND THE ACCOMPANYING DOCUMENTATION TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS IN THIS AGREEMENT.

PLEASE READ THE TERMS CAREFULLY BEFORE INSTALLING, USING, OR ACCESSING THE SOFTWARE, AS BY SUCH ACTIONS YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS.

IF YOU DO NOT AGREE TO THESE TERMS, EDGEWATER NETWORKS IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND WE ASK THAT YOU IMMEDIATELY RETURN THIS PRODUCT FOR A FULL REFUND.

LICENSE. You are permitted to install, perform and display the Software and use the Software only on the EdgeMarc™ converged network appliance that accompanies this Software. You may copy the Software only for backup purposes, provided that you reproduce all copyright and other proprietary notices that are on the original copy of the Software.

1. **RESTRICTIONS**. You may not use, copy, modify, or transfer the Software, or any copy thereof, in whole or in part, except as expressly provided in this Agreement. You may not reverse engineer, disassemble, decompile, or translate the Software, or otherwise attempt to derive the source code of the Software, except to the extent allowed under any applicable law. Any attempt to transfer any of the rights, duties or obligations hereunder is void. You may not rent, lease loan, resell for profit, or distribute the Software, or any part hereof.

2. **OWNERSHIP**. The Software is licensed, not sold, to you for use only under the terms of this Agreement, and Edgewater Networks reserves all rights not expressly granted to you.

3. **TERM**. This Agreement will terminate immediately upon notice to you if you materially breach any term or condition of this Agreement. You agree upon termination to promptly destroy the Software and all copies.

4. **WARRANTY DISCLAIMER**. Edgewater Networks warrants to You that the Software, when operated in an environment supported by Edgewater Networks, will perform substantially in accordance with its user documentation for the ninety (90) day period immediately following your receipt of the Software (the "Warranty Period"). If You notify Edgewater Networks during the Warranty Period that the Software does not perform substantially in accordance with the user documentation and Edgewater Networks is able to reproduce such failure, the entire and exclusive liability and remedy shall be limited to either, at Edgewater Networks' sole discretion: (i) providing a correction or a workaround for such failure; (ii) replacing the Software with conforming software; or (iii) refunding of the license fee paid for the Software.

EXCEPT AS EXPRESSLY PROVIDED, THE SOFTWARE IS PROVIDED TO YOU "AS IS" AND EDGEWATER NETWORKS AND ITS SUPPLIERS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS INCLUDING THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. NO ORAL OR WRITTEN INFORMATION OR WRITTEN INFORMATION OR ADVICE GIVEN BY EDGEWATER NETWORKS, ITS EMPLOYEES, DISTRIBUTORS, DEALERS, OR AGENTS SHALL INCREASE THE SCOPE OF THE ABOVE WARRANTIES OR CREATE ANY NEW WARRANTIES. Some states or jurisdictions do not allow the disclaimer of certain implied warranties, so the above disclaimer may not apply to You.

5. LIMITATION OF REMEDIES. REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL EDGEWATER NETWORKS OR ITS SUPPLIERS BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOST PROFITS, LOST DATA, INTERRUPTION OF BUSINESS, OR OTHER SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE OR ANY DATA SUPPLIED THEREWITH, EVEN IF EDGEWATER NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES AND WHETHER OR NOT SUCH LOSS OR DAMAGES ARE FORESEEABLE. IN NO EVENT SHALL THE LIABILITY OF EDGEWATER NETWORKS EXCEED THE AMOUNT RECEIVED BY EDGEWATER NETWORKS FROM YOU FOR THIS SOFTWARE LICENSE. Some states or jurisdictions do not allow the exclusion or limitation of incidental, consequential, indirect or special damages, so the above limitations may not apply to You.

6. EXPORT LAW. The Software and related technology are subject to U.S. export control laws and may be subject to export or import regulations in other countries. You agree to strictly comply with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export or import as may be required.

7. U.S. GOVERNMENT END USERS. The Software is a "commercial item" as that term is defined at FAR 2.101 (Oct 1995), consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212 (Sep 1995) and is provided to the U.S. Government only as a commercial end item. Consistent with FAR.12.212 and DFARS 227.7202 (Jun 1995), all U.S. Government End Users acquire the Software with only those rights set forth herein.

8. GENERAL. This Agreement will be governed by the laws of the State of California, without regard to or application of conflicts of law rules or principles. The State and Federal Courts located in Santa Clara County shall have sole jurisdiction over any disputes arising hereunder. If any provision of this Agreement is held to be unenforceable, that provision will be removed and the remaining provision will remain in full force. This Agreement is the complete and exclusive statement of the agreement between us which supersedes any proposal or prior agreement, oral or written, and any other communications between us in relation to the subject matter of this Agreement.

If you have any questions regarding this Agreement, please contact Edgewater Networks, Inc. at 2730 San Tomas Expressway, suite 200, Santa Clara, CA 95051 or call 408.351.7200.

THE SOFTWARE AND ACCOMPANYING USER DOCUMENTATION ARE PROTECTED BY UNITED STATES COPYRIGHT LAW AND INTERNATIONAL TREATY. UNAUTHORIZED REPRODUCTION OR DISTRIBUTION IS SUBJECT TO CIVIL AND CRIMINAL PENALTIES.

Software included in this product contains a module called PsyVoIP which is protected by copyright and by European, US and other patents and is provided under licence from Psytechnics Limited.

Asterisk Copyright

Copyright 1992, 1993, 1994 by Jutta Degener and Carsten Bormann, Technische Universitaet Berlin

Any use of this software is permitted provided that this notice is not removed and that neither the authors nor the Technische Universitaet Berlin are deemed to have made any representations as to the suitability of this software for any purpose nor are held responsible for any defects of this software. THERE IS ABSOLUTELY NO WARRANTY FOR THIS SOFTWARE.

As a matter of courtesy, the authors request to be informed about uses this software has found, about bugs in this software, and about any improvements that may be of general interest.

Berlin, 28.11.1994 Jutta Degener Carsten Bormann

Data Encryption Standard Copyright

Copyright (C) 1995-1997 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an DES implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with MIT's libdes.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution.

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of that the SSL library. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Eric Young (eay@cryptsoft.com)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE

AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The reason behind this being stated in this direct manner is past experience in code simply being copied and the attribution removed from it and then being distributed as part of other packages. This implementation was a non-trivial and unpaid effort.

XML 1.0 Parser Library License

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper

Copyright (c) 2001, 2002, 2003 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Open LDAP Copyright

Copyright 1998-2003 The OpenLDAP Foundation All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License. A copy of this

license is available at <http://www.OpenLDAP.org/license.html> or in the file LICENSE in the top-level directory of the distribution.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by other parties and subject to additional restrictions.

This work is derived from the University of Michigan LDAP v3.3 distribution. Information concerning this software is available at:
<http://www.umich.edu/~dirsvcs/ldap/>

This work also contains materials derived from public sources.

Additional information about OpenLDAP can be obtained at:
<http://www.openldap.org/>

or by sending e-mail to: info@OpenLDAP.org

Portions Copyright 1998-2003 Kurt D. Zeilenga. Portions Copyright 1998-2003 Net Boolean Incorporated. Portions Copyright 1999-2003 Howard Y.H. Chu. Portions Copyright 1999-2003 Symas Corporation. Portions Copyright 2001-2003 IBM Corporation. Portions Copyright 1998-2003 Hallvard B. Furuseth. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that this notice is preserved. The names of the copyright holders may not be used to endorse or promote products derived from this software without their specific prior written permission. This software is provided "as is" without express or implied warranty.

Portions Copyright (c) 1992-1996 Regents of the University of Michigan. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty.

Open LDAP License

The OpenLDAP Public License Version 2.7, 7 September 2001

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

Open H.323 Copying Permission

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Xiph.org Foundation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Henry Spencer Regex License

Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

Berkeley Source Distribution License

License: BSD Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Sleepycat Software License

/*- * \$Id: LICENSE,v 11.12 2004/03/30 20:49:44 bostic Exp \$ */

The following is the license that applies to this copy of the Berkeley DB software. For a license to use the Berkeley DB software under conditions other than those described here, or to purchase support for this software, please contact Sleepycat Software by email at info@sleepycat.com, or on the Web at <http://www.sleepycat.com>.

```

===== /* * Copyright (c)
1990-2004 *Sleepycat Software. All rights reserved. * * Redistribution and use in
source and binary forms, with or without * modification, are permitted provided that
the following conditions * are met: * 1. Redistributions of source code must retain
the above copyright * notice, this list of conditions and the following disclaimer. *
2. Redistributions in binary form must reproduce the above copyright * notice, this
list of conditions and the following disclaimer in the * documentation and/or other
materials provided with the distribution. * 3. Redistributions in any form must be
accompanied by information on * how to obtain complete source code for the DB
software and any * accompanying software that uses the DB software. The source
code * must either be included in the distribution or be available for no * more
than the cost of distribution plus a nominal fee, and must be * freely redistributable
under reasonable conditions. For an * executable file, complete source code means
the source code for all * modules it contains. It does not include source code for
modules or * files that typically accompany the major components of the operating
* system on which the executable file runs. * * THIS SOFTWARE IS PROVIDED
BY SLEEPYCAT SOFTWARE "AS IS" AND ANY EXPRESS * OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED *
WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR
PURPOSE, OR * NON-INFRINGEMENT, ARE DISCLAIMED. IN NO EVENT
SHALL SLEEPYCAT SOFTWARE * BE LIABLE FOR ANY DIRECT,
INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR * CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF *
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY
OF LIABILITY, WHETHER IN * CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) * ARISING IN ANY WAY OUT
OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF * THE
POSSIBILITY OF SUCH DAMAGE. *//* * Copyright (c) 1990, 1993, 1994, 1995
*The Regents of the University of California. All rights reserved. * * Redistribution
and use in source and binary forms, with or without * modification, are permitted
provided that the following conditions * are met: * 1. Redistributions of source code
must retain the above copyright * notice, this list of conditions and the following
disclaimer. * 2. Redistributions in binary form must reproduce the above copyright *
notice, this list of conditions and the following disclaimer in the * documentation
and/or other materials provided with the distribution. * 3. Neither the name of the
University nor the names of its contributors * may be used to endorse or promote
products derived from this software * without specific prior written permission. *

```

* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE * ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF * SUCH DAMAGE. */* * Copyright (c) 1995, 1996 *The President and Fellows of Harvard University. All rights reserved. * * Redistribution and use in source and binary forms, with or without * modification, are permitted provided that the following conditions * are met: * 1. Redistributions of source code must retain the above copyright * notice, this list of conditions and the following disclaimer. * 2. Redistributions in binary form must reproduce the above copyright * notice, this list of conditions and the following disclaimer in the * documentation and/or other materials provided with the distribution. * 3. Neither the name of the University nor the names of its contributors * may be used to endorse or promote products derived from this software * without specific prior written permission. * * THIS SOFTWARE IS PROVIDED BY HARVARD AND ITS CONTRIBUTORS "AS IS" AND * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE * ARE DISCLAIMED. IN NO EVENT SHALL HARVARD OR ITS CONTRIBUTORS BE LIABLE * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF * SUCH DAMAGE. */

Perl Compatible Regular Expressions License

PCRE LICENCE -----

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service, Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2004 University of Cambridge All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

End

Vovida Software License

/*

```
=====
* The Vovida Software License, Version 1.0 * * Copyright (c) 2000
Vovida Networks, Inc. All rights reserved. * * Redistribution and use in source and
binary forms, with or without * modification, are permitted provided that the
following conditions * are met: * * 1. Redistributions of source code must retain the
above copyright * notice, this list of conditions and the following disclaimer. * *
2. Redistributions in binary form must reproduce the above copyright * notice, this
list of conditions and the following disclaimer in * the documentation and/or other
materials provided with the * distribution. * * 3. The names "VOCAL", "Vovida
Open Communication Application Library", * and "Vovida Open Communication
Application Library (VOCAL)" must * not be used to endorse or promote products
derived from this * software without prior written permission. For written *
permission, please contact vocal@vovida.org. * * 4. Products derived from this
software may not be called "VOCAL", nor * may "VOCAL" appear in their name,
without prior written * permission of Vovida Networks, Inc. * * THIS
SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED *
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
```

WARRANTIES * OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND * NON-INFRINGEMENT ARE DISCLAIMED. IN NO EVENT SHALL VOVIDA * NETWORKS, INC. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT DAMAGES * IN EXCESS OF \$1,000, NOR FOR ANY INDIRECT, INCIDENTAL, SPECIAL, * EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, * PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR * PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY * OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE * USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH * DAMAGE. * *

=====

===== */

Blowfish License

Copyright (C) 1995-1997 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an Blowfish implementation written by Eric Young (eay@cryptsoft.com).

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution.

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Eric Young (eay@cryptsoft.com)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The reason behind this being stated in this direct manner is past experience in code simply being copied and the attribution removed from it and then being distributed as part of other packages. This implementation was a non-trivial and unpaid effort.

Open SSL License

LICENSE ISSUES =====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License -----

/*

```
===== * Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved. *
* Redistribution and use in source and binary forms, with or without * modification,
are permitted provided that the following conditions * are met: * * 1.
Redistributions of source code must retain the above copyright * notice, this list of
conditions and the following disclaimer. * * 2. Redistributions in binary form must
reproduce the above copyright * notice, this list of conditions and the following
disclaimer in * the documentation and/or other materials provided with the *
distribution. * * 3. All advertising materials mentioning features or use of this *
software must display the following acknowledgment: * "This product includes
software developed by the OpenSSL Project * for use in the OpenSSL Toolkit.
(http://www.openssl.org/)" * * 4. The names "OpenSSL Toolkit" and "OpenSSL
Project" must not be used to * endorse or promote products derived from this
software without * prior written permission. For written permission, please contact
* openssl-core@openssl.org. * * 5. Products derived from this software may not be
called "OpenSSL" * nor may "OpenSSL" appear in their names without prior
written * permission of the OpenSSL Project. * * 6. Redistributions of any form
whatsoever must retain the following * acknowledgment: * "This product
includes software developed by the OpenSSL Project * for use in the OpenSSL
Toolkit (http://www.openssl.org/)" * * THIS SOFTWARE IS PROVIDED BY THE
OpenSSL PROJECT "AS IS" AND ANY * EXPRESSED OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE * IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL
PROJECT OR * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
INDIRECT, INCIDENTAL, * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT * NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; * LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) * HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, * STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) * ARISING IN ANY
```

WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED * OF THE
POSSIBILITY OF SUCH DAMAGE. *

=====
***** * * This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim * Hudson
(tjh@cryptsoft.com). * */

Original SSLeay License -----

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) * All rights reserved.
* * This package is an SSL implementation written * by Eric Young
(eay@cryptsoft.com). * The implementation was written so as to conform with
Netscapes SSL. * * This library is free for commercial and non-commercial use as
long as * the following conditions are aheared to. The following conditions * apply
to all code found in this distribution, be it the RC4, RSA, * lhash, DES, etc., code;
not just the SSL code. The SSL documentation * included with this distribution is
covered by the same copyright terms * except that the holder is Tim Hudson
(tjh@cryptsoft.com). * * Copyright remains Eric Young's, and as such any
Copyright notices in * the code are not to be removed. * If this package is used in a
product, Eric Young should be given attribution * as the author of the parts of the
library used. * This can be in the form of a textual message at program startup or * in
documentation (online or textual) provided with the package. * * Redistribution and
use in source and binary forms, with or without * modification, are permitted
provided that the following conditions * are met: * 1. Redistributions of source code
must retain the copyright * notice, this list of conditions and the following
disclaimer. * 2. Redistributions in binary form must reproduce the above copyright *
notice, this list of conditions and the following disclaimer in the * documentation
and/or other materials provided with the distribution. * 3. All advertising materials
mentioning features or use of this software * must display the following
acknowledgement: * "This product includes cryptographic software written by *
Eric Young (eay@cryptsoft.com)" * The word 'cryptographic' can be left out if the
rouines from the library * being used are not cryptographic related :-). * 4. If you
include any Windows specific code (or a derivative thereof) from * the apps
directory (application code) you must include an acknowledgement: * "This
product includes software written by Tim Hudson (tjh@cryptsoft.com)" * * THIS
SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND * ANY EXPRESS
OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE *
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE * ARE DISCLAIMED. IN NO EVENT SHALL THE
AUTHOR OR CONTRIBUTORS BE LIABLE * FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL * DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) * HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT * LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY * OUT
OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF * SUCH DAMAGE. * * The licence and distribution terms for any publically
available version or * derivative of this code cannot be changed. i.e. this code cannot
simply be * copied and put under another distribution licence * [including the GNU
Public Licence.] */

Open SSL Toolkit License

LICENSE ISSUES =====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License -----

/*

```
===== * Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved. *
* Redistribution and use in source and binary forms, with or without * modification,
* are permitted provided that the following conditions * are met: * * 1.
Redistributions of source code must retain the above copyright * notice, this list of
conditions and the following disclaimer. * * 2. Redistributions in binary form must
reproduce the above copyright * notice, this list of conditions and the following
disclaimer in * the documentation and/or other materials provided with the *
distribution. * * 3. All advertising materials mentioning features or use of this *
software must display the following acknowledgment: * "This product includes
software developed by the OpenSSL Project * for use in the OpenSSL Toolkit.
(http://www.openssl.org/)" * * 4. The names "OpenSSL Toolkit" and "OpenSSL
Project" must not be used to * endorse or promote products derived from this
software without * prior written permission. For written permission, please contact
* openssl-core@openssl.org. * * 5. Products derived from this software may not be
called "OpenSSL" * nor may "OpenSSL" appear in their names without prior
written * permission of the OpenSSL Project. * * 6. Redistributions of any form
whatsoever must retain the following * acknowledgment: * "This product
includes software developed by the OpenSSL Project * for use in the OpenSSL
Toolkit (http://www.openssl.org/)" * * THIS SOFTWARE IS PROVIDED BY THE
OpenSSL PROJECT "AS IS" AND ANY * EXPRESSED OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE * IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL
PROJECT OR * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
INDIRECT, INCIDENTAL, * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT * NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; * LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) * HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, * STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) * ARISING IN ANY
WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED * OF THE
POSSIBILITY OF SUCH DAMAGE. *
```

```
===== * * This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim * Hudson
(tjh@cryptsoft.com). * */
```

Original SSLeay License -----

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) * All rights reserved.
* * This package is an SSL implementation written * by Eric Young
(eay@cryptsoft.com). * The implementation was written so as to conform with
Netscapes SSL. * * This library is free for commercial and non-commercial use as
long as * the following conditions are aheared to. The following conditions * apply
to all code found in this distribution, be it the RC4, RSA, * lhash, DES, etc., code;
not just the SSL code. The SSL documentation * included with this distribution is
covered by the same copyright terms * except that the holder is Tim Hudson
(tjh@cryptsoft.com). * * Copyright remains Eric Young's, and as such any
Copyright notices in * the code are not to be removed. * If this package is used in a
product, Eric Young should be given attribution * as the author of the parts of the
library used. * This can be in the form of a textual message at program startup or * in
documentation (online or textual) provided with the package. * * Redistribution and
use in source and binary forms, with or without * modification, are permitted
provided that the following conditions * are met: * 1. Redistributions of source code
must retain the copyright * notice, this list of conditions and the following
disclaimer. * 2. Redistributions in binary form must reproduce the above copyright *
notice, this list of conditions and the following disclaimer in the * documentation
and/or other materials provided with the distribution. * 3. All advertising materials
mentioning features or use of this software * must display the following
acknowledgement: * "This product includes cryptographic software written by *
Eric Young (eay@cryptsoft.com)" * The word 'cryptographic' can be left out if the
rouines from the library * being used are not cryptographic related :-). * 4. If you
include any Windows specific code (or a derivative thereof) from * the apps
directory (application code) you must include an acknowledgement: * "This
product includes software written by Tim Hudson (tjh@cryptsoft.com)" * * THIS
SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND * ANY EXPRESS
OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE *
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE * ARE DISCLAIMED. IN NO EVENT SHALL THE
AUTHOR OR CONTRIBUTORS BE LIABLE * FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL * DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) * HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT * LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY * OUT
OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF * SUCH DAMAGE. * * The licence and distribution terms for any publically
available version or * derivative of this code cannot be changed. i.e. this code cannot
simply be * copied and put under another distribution licence * [including the GNU
Public Licence.] */
```

Net SNMP License

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts. Up until 2001, the project was based at UC Davis, and the first part covers all code written during this time. From 2001

onwards, the project has been based at SourceForge, and Networks Associates Technology, Inc hold the copyright on behalf of the wider Net-SNMP community, covering all derivative work done since then. An additional copyright section has been added as Part 3 below also under a BSD license for the work contributed by Cambridge Broadband Ltd. to the project since 2001. An additional copyright section has been added as Part 4 below also under a BSD license for the work contributed by Sun Microsystems, Inc. to the project since 2003.

Code has been contributed to this project by many people over the years it has been in development, and a full list of contributors can be found in the README file under the THANKS section.

---- Part 1: CMU/UCD copyright notice: (BSD like) ----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000 Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----

Copyright (c) 2001-2003, Networks Associates Technology, Inc All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) ----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) ----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) ----

Copyright (c) 2003-2004, Sparta, Inc All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) ----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that

the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Point-to-Point Protocol Daemon License

See the respective source files to find out which copyrights apply.

----- Copyright (C) 2002
Roaring Penguin Software Inc.

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Roaring Penguin Software Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Roaring Penguin Software Inc..

Roaring Penguin Software Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

----- Copyright (C)
1995,1996,1997,1998 Lars Fenneberg <lf@elemental.net>

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Lars Fenneberg not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Lars Fenneberg.

Lars Fenneberg makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

----- Copyright 1992
Livingston Enterprises, Inc. Livingston Enterprises, Inc. 6920 Koll Center Parkway
Pleasanton, CA 94566

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Livingston Enterprises, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Livingston Enterprises, Inc.

Livingston Enterprises, Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

----- [C] The Regents of
the University of Michigan and Merit Network, Inc. 1992, 1993, 1994, 1995 All
Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies of the software and derivative works or modified versions thereof, and that both the copyright notice and this permission and disclaimer notice appear in supporting documentation.

THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE REGENTS OF THE UNIVERSITY OF MICHIGAN AND MERIT NETWORK, INC. DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET LICENSEE'S REQUIREMENTS OR THAT OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. The Regents of the University of Michigan and Merit Network, Inc. shall not be liable for any special, indirect, incidental or consequential damages with respect to any claim by Licensee or any third party arising from use of the software.

----- Copyright (C)
1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software. -----

SSH License

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1) * Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland *
All rights reserved * * As far as I am concerned, the code I have written for this software * can be used freely for any purpose. Any derived versions of this * software must be clearly marked as such, and if the derived work is * incompatible with the protocol description in the RFC file, it must be * called by a name other than "ssh" or "Secure Shell".

[Tatu continues] * However, I am not implying to give any licenses to any patents or * copyrights held by third parties, and the software includes parts that * are not under my direct control. As far as I know, all included * source code is used in accordance with the relevant license agreements * and can be used freely for any purpose (the GNU license being the most * restrictive); see below for details.

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "<http://www.cs.hut.fi/crypto>".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE

PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2) The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

```
* Cryptographic attack detector for ssh - source code * * Copyright (c) 1998
CORE SDI S.A., Buenos Aires, Argentina. * * All rights reserved.
Redistribution and use in source and binary * forms, with or without modification,
are permitted provided that * this copyright notice is retained. * * THIS
SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED *
WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE
* LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY OR * CONSEQUENTIAL DAMAGES RESULTING FROM THE
USE OR MISUSE OF THIS * SOFTWARE. * * Ariel Futoransky
<futo@core-sdi.com> * <http://www.core-sdi.com>
```

3) ssh-keyscan was contributed by David Mazieres under a BSD-style license.

```
* Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>. * *
Modification and redistribution in source and binary forms is * permitted provided
that due credit is given to the author and the * OpenBSD project by leaving this
copyright notice intact.
```

4) The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

```
* @version 3.0 (December 2000) * * Optimised ANSI C code for the
Rijndael cipher (now AES) * * @author Vincent Rijmen
<vincent.rijmen@esat.kuleuven.ac.be> * @author Antoon Bosselaers
<antoon.bosselaers@esat.kuleuven.ac.be> * @author Paulo Barreto
<paulo.barreto@terra.com.br> * * This code is hereby placed in the public
domain. * * THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS"
AND ANY EXPRESS * OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED * WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE * ARE DISCLAIMED. IN
NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE * LIABLE
```

FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR * BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, * WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE * OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, * EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5) One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

* Copyright (c) 1983, 1990, 1992, 1993, 1995 * The Regents of the University of California. All rights reserved. * * Redistribution and use in source and binary forms, with or without * modification, are permitted provided that the following conditions * are met: * 1. Redistributions of source code must retain the above copyright * notice, this list of conditions and the following disclaimer. * 2. Redistributions in binary form must reproduce the above copyright * notice, this list of conditions and the following disclaimer in the * documentation and/or other materials provided with the distribution. * 3. Neither the name of the University nor the names of its contributors * may be used to endorse or promote products derived from this software * without specific prior written permission. * * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE * ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF * SUCH DAMAGE.

6) Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl Theo de Raadt Niels Provos Dug Song Aaron Campbell Damien Miller
Kevin Steves Daniel Kouril Wesley Griffin Per Allansson Nils Nordman Simon
Wilkinson

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

Ben Lindstrom Tim Rice Andre Lucas Chris Adams Corinna Vinschen Cray Inc.
Denis Parker Gert Doering Jakob Schlyter Jason Downs Juha Yrjölä Michael Stone
Networks Associates Technology, Inc. Solar Designer Todd C. Miller Wayne

Schroeder William Jones Darren Tucker Sun Microsystems The SCO Group Daniel Walsh

* Redistribution and use in source and binary forms, with or without * modification, are permitted provided that the following conditions * are met: *

1. Redistributions of source code must retain the above copyright * notice, this list of conditions and the following disclaimer. *
2. Redistributions in binary form must reproduce the above copyright * notice, this list of conditions and the following disclaimer in the * documentation and/or other materials provided with the distribution. *

* * THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8) Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

* "THE BEER-WARE LICENSE" (Revision 42): * <phk@login.dknet.dk> wrote this file. As long as you retain this * notice you can do whatever you want with this stuff. If we meet * some day, and you think this stuff is worth it, you can buy me a * beer in return. Poul-Henning Kamp

b) snprintf replacement

* Copyright Patrick Powell 1995 * This code is based on code written by Patrick Powell * (papowell@astart.com) It may be used for any purpose as long as this * notice remains intact on all source code distributions

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code in the openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following copyright holders:

Todd C. Miller Theo de Raadt Damien Miller Eric P. Allman The Regents of the University of California Constantin S. Svintsoff

* Redistribution and use in source and binary forms, with or without * modification, are permitted provided that the following conditions * are met: *

- * 1. Redistributions of source code must retain the above copyright * notice, this list of conditions and the following disclaimer.
- * 2. Redistributions in binary form must reproduce the above copyright * notice, this list of conditions and the following disclaimer in the * documentation and/or other materials provided with the distribution.
- * 3. Neither the

name of the University nor the names of its contributors * may be used to endorse or promote products derived from this software * without specific prior written permission. * * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE * ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF * SUCH DAMAGE.

Some code is licensed under an ISC-style license, to the following copyright holders:

Internet Software Consortium. Todd C. Miller Reyk Floeter Chad Mynhier

* Permission to use, copy, modify, and distribute this software for any * purpose with or without fee is hereby granted, provided that the above * copyright notice and this permission notice appear in all copies. * * THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL * WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES * OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE * FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES * WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION * OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN * CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Some code is licensed under a MIT-style license to the following copyright holders:

Free Software Foundation, Inc.

* Permission is hereby granted, free of charge, to any person obtaining a * * copy of this software and associated documentation files (the * * "Software"), to deal in the Software without restriction, including * * without limitation the rights to use, copy, modify, merge, publish, * * distribute, distribute with modifications, sublicense, and/or sell * * copies of the Software, and to permit persons to whom the Software is * * furnished to do so, subject to the following conditions:
* * * * * The above copyright notice and this permission notice shall be included * * in all copies or substantial portions of the Software. * * * * * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS * * OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF * * MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. * * IN NO EVENT

SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,
 * * DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF
 CONTRACT, TORT OR * * OTHERWISE, ARISING FROM, OUT OF OR IN
 CONNECTION WITH THE SOFTWARE OR * * THE USE OR OTHER
 DEALINGS IN THE SOFTWARE. * *

* * Except as contained in this notice, the name(s) of the above copyright * * holders
 shall not be used in advertising or otherwise to promote the * * sale, use or other
 dealings in this Software without prior written * * authorization.

*

 *****/

----- \$OpenBSD: LICENCE,v 1.19 2004/08/30 09:18:08 markus Exp \$

Shadow Utilities License

The shadow utilities license:

This software is copyright 1988 - 1994, Julianne Frances Haugh. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of Julianne F. Haugh nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY JULIE HAUGH AND CONTRIBUTORS
 "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT
 NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
 AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO
 EVENT SHALL JULIE HAUGH OR CONTRIBUTORS BE LIABLE FOR ANY
 DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
 PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
 DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED
 AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
 ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This source code is currently archived on ftp.uu.net in the comp.sources.misc portion of the USENET archives. You may also contact the author, Julianne F. Haugh, at jfh@tab.com if you have any questions regarding this package.

THIS SOFTWARE IS BEING DISTRIBUTED AS-IS. THE AUTHORS
 DISCLAIM ALL LIABILITY FOR ANY CONSEQUENCES OF USE. THE
 USER IS SOLELY RESPONSIBLE FOR THE MAINTENANCE OF THIS
 SOFTWARE PACKAGE. THE AUTHORS ARE UNDER NO OBLIGATION TO
 PROVIDE MODIFICATIONS OR IMPROVEMENTS. THE USER IS
 ENCOURAGED TO TAKE ANY AND ALL STEPS NEEDED TO PROTECT

AGAINST ACCIDENTAL LOSS OF INFORMATION OR MACHINE RESOURCES .

Special thanks are due to Chip Rosenthal for his fine testing efforts; to Steve Simmons for his work in porting this code to BSD; and to Bill Kennedy for his contributions of LaserJet printer time and energies. Also, thanks for Dennis L. Mumaugh for the initial shadow password information and to Tony Walton (olapw@olgb1.oliv.co.uk) for the System V Release 4 changes. Effort in porting to SunOS has been contributed by Dr. Michael Newberry (miken@cs.adfa.oz.au) and Micheal J. Miller, Jr. (mke@kaber.drain.com). Effort in porting to AT&T UNIX System V Release 4 has been provided by Andrew Herbert (andrew@werple.pub.uu.oz.au). Special thanks to Marek Michalkiewicz (marekm@i17linuxb.ists.pwr.wroc.pl) for taking over the Linux port of this software.

Source files: login_access.c, login_desrpc.c, login_krb.c are derived from the logdaemon-5.0 package, which is under the following license:

```
/*
*****
**** * Copyright 1995 by Wietse Venema. All rights reserved. Individual files *
may be covered by other copyrights (as noted in the file itself.) * * This material was
originally written and compiled by Wietse Venema at * Eindhoven University of
Technology, The Netherlands, in 1990, 1991, * 1992, 1993, 1994 and 1995. * *
Redistribution and use in source and binary forms are permitted * provided that this
entire copyright notice is duplicated in all such * copies. * * This software is
provided "as is" and without any expressed or implied * warranties, including,
without limitation, the implied warranties of * merchantability and fitness for any
particular purpose.
*****
*****/
```

This software is copyright 1988 - 1994, Julianne Frances Haugh. All rights reserved.

GNU General Public License Version 2

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other

Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does

not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and

each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

To obtain a complete machine-readable copy of the corresponding source code covered under GNU GPL please send mail to info@edgewaternetworks.com

GNU General Public License Version 2.1

GNU GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes

a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example,

permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

2. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) The modified work must itself be a software library.
 - b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
 - c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
 - d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then

you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

5. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

6. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

7. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of

the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

8. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
 - a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
 - b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
9. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
10. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
11. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
12. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

13. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
14. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

15. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

16. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE

LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

17. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free

Software Foundation, Inc., 59 Temple Place, Suite 330, Boston,
MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James
Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

To obtain a complete machine-readable copy of the corresponding source code covered under GNU GPL please send mail to info@edgewaternetworks.com

Product Warranties

Hardware Warranty

For a period of one (1) year after shipment of the Product, Edgewater warrants that such Hardware will substantially conform to Edgewater's published specifications for such Hardware on the date of order if properly used in accordance with procedures described in the documentation supplied by Edgewater. 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's exclusive obligations with respect to nonconforming Hardware shall be, at Edgewater's option, to advance replace such Hardware, if it is determined to be defective, or to refund to End-user the purchase price paid for the Product. Advance replacement units are shipped same business day for next-day delivery (within the US) when hardware failure is determined by 1pm PST. Failed components must be returned to Edgewater within 14 days or End-user will be charged for new product purchase.

Software Warranty

Edgewater warrants that the Software on the Product will substantially conform with Edgewater's 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. Edgewater's exclusive obligation with respect to nonconforming Software shall be, at Edgewater's 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 Product on which the Software is installed. Defects in the Software must be reported during the warranty period and be reported to Edgewater in a form and with supporting information reasonably requested by Edgewater to enable it to verify, diagnose and correct the defect.

Edgewater Networks
2895 Northwestern Parkway
Santa Clara, CA 95051
Phone: 408-351-7200
info@edgewaternetworks.com
<http://www.edgewaternetworks.com>

