ZYXEL
Your Networking Ally

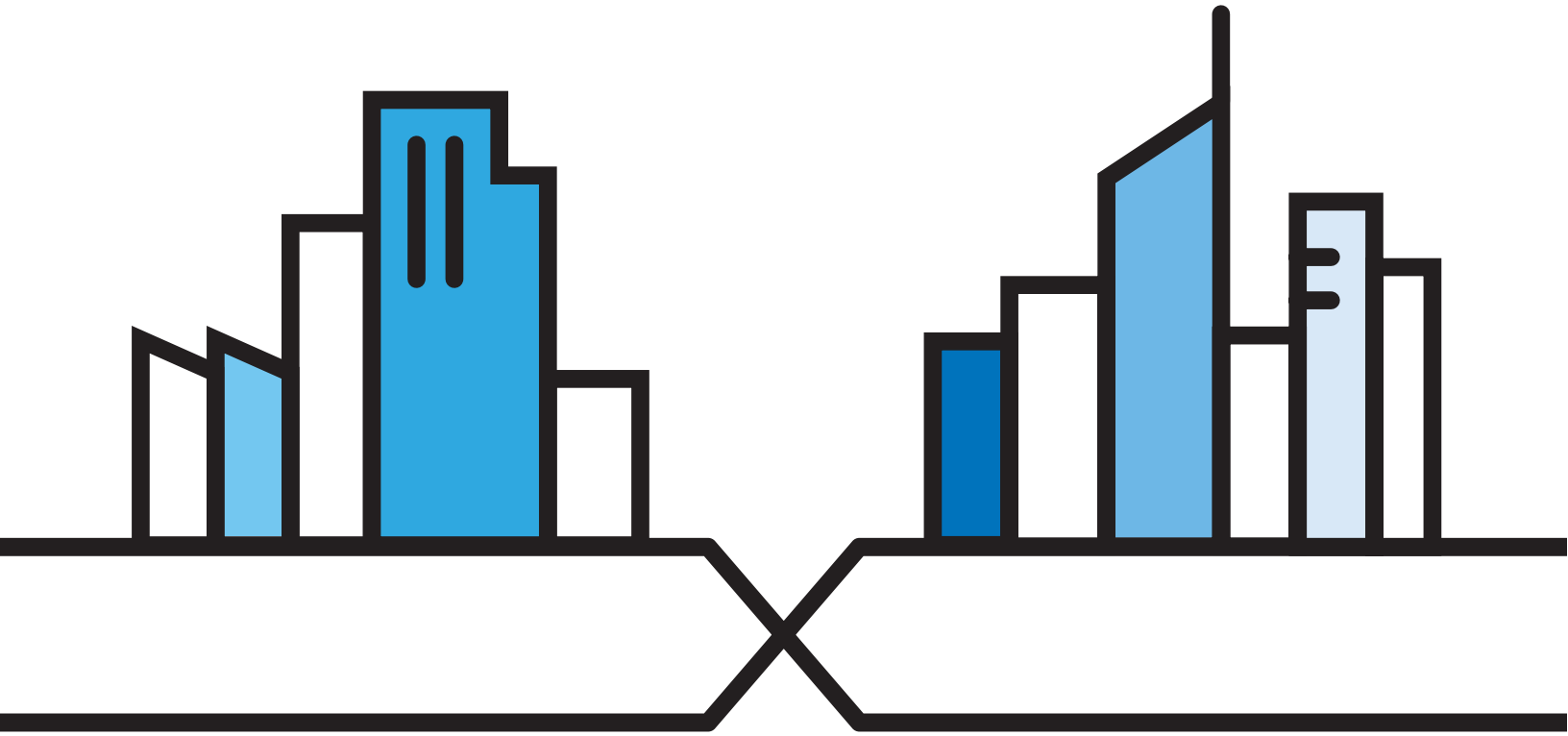
User's Guide

EMG3415-B10A

Dual-Band Wireless AC/N Gigabit Ethernet Gateway

Default Login Details	
LAN IP Address	http://192.168.200.1
Login	Login account and password are not needed. Simply click I Agree to go to the Web Configurator.
Password	

Version 5.12 Edition 1, 02/2017



Copyright © 2017 Zyxel Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for a system managing a series of products. Not all products support all features. Menushots and graphics in this book may differ slightly from what you see due to differences in release versions or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the managed device, such as the Nebula AP, gateway or security gateway.

Contents Overview

User's Guide **12**

Introducing the EMG 13
The Web Configurator 20
Tutorials 27

Technical Reference **44**

Network Map and Status Screens 45
Broadband 50
Wireless 64
Home Networking 88
Routing 102
Quality of Service (QoS) 109
Network Address Translation (NAT) 127
DNS 143
VLAN Group 147
Interface Grouping 149
Firewall 153
MAC Filter 160
Parental Control 162
Scheduler Rule 167
Certificates 169
Log 175
Traffic Status 178
ARP Table 181
Routing Table 183
Multicast Status 185
System 187
User Account 188
Remote Management 191
SNMP 194
Time Settings 196
E-mail Notification 198
Log Setting 200
Firmware Upgrade 203
Backup/Restore 205
Diagnostic 208
Troubleshooting 210

Appendices **215**

Table of Contents

Contents Overview 3

Table of Contents 4

Part I: User's Guide 12

Chapter 1
Introducing the EMG 13

1.1 Overview 13
1.2 Ways to Manage the EMG 13
1.3 Good Habits for Managing the EMG 13
1.4 Applications for the EMG 13
1.4.1 Internet Access 13
1.4.2 Dual-Band 14
1.4.3 Triple Play 15
1.5 LEDs (Lights) 15
1.6 The RESET Button 17
1.7 Wireless Access 17
1.7.1 Using the WPS Button 18
1.8 Wall Mounting 18

Chapter 2
The Web Configurator 20

2.1 Overview 20
2.1.1 Accessing the Web Configurator 20
2.2 Web Configurator Layout 22
2.2.1 Title Bar 22
2.2.2 Navigation Panel 23

Chapter 3
Tutorials 27

3.1 Overview 27
3.2 Setting Up a New WAN Connection 27
3.3 Setting Up a Secure Wireless Network 30
3.3.1 Configuring the Wireless Network Settings 30
3.3.2 Using WPS 32
3.3.3 Without WPS 35
3.4 Configuring Static Route for Routing to Another Network 36

3.5 Configuring QoS Queue and Class Setup 38
3.6 Access the EMG Using DDNS 41
3.6.1 Registering a DDNS Account on www.dyndns.org 41
3.6.2 Configuring DDNS on Your EMG 41
3.6.3 Testing the DDNS Setting 42
3.7 Configuring the MAC Address Filter 42

Part II: Technical Reference 44

Chapter 4
Network Map and Status Screens 45

4.1 Overview 45
4.2 The Network Map Screen 45
4.3 The Status Screen 46

Chapter 5
Broadband 50

5.1 Overview 50
5.1.1 What You Can Do in this Chapter 50
5.1.2 What You Need to Know 50
5.1.3 Before You Begin 53
5.2 The Broadband Screen 53
5.2.1 Add/Edit Internet Connection 54
5.3 Technical Reference 59

Chapter 6
Wireless 64

6.1 Overview 64
6.1.1 What You Can Do in this Chapter 64
6.1.2 What You Need to Know 64
6.2 The General Screen 65
6.2.1 No Security 67
6.2.2 Basic (WEP Encryption) 67
6.2.3 More Secure (WPA(2)-PSK) 68
6.3 MAC Authentication 69
6.4 The WPS Screen 70
6.5 The WMM Screen 72
6.6 The Others Screen 73
6.7 The Channel Status Screen 74
6.8 Technical Reference 75
6.8.1 Wireless Network Overview 75

6.8.2 Additional Wireless Terms 77
6.8.3 Wireless Security Overview 77
6.8.4 Signal Problems 79
6.8.5 BSS 80
6.8.6 Preamble Type 80
6.8.7 WiFi Protected Setup (WPS) 81

Chapter 7
Home Networking 88

7.1 Overview 88
7.1.1 What You Can Do in this Chapter 88
7.1.2 What You Need To Know 89
7.1.3 Before You Begin 90
7.2 The LAN Setup Screen 90
7.3 The Static DHCP Screen 94
7.4 The UPnP Screen 95
7.4.1 Turning On UPnP in Windows 7 Example 96
7.5 The Additional Subnet Screen 98
7.6 The STB Vendor ID Screen 99
7.7 The Wake on LAN Screen 99
7.8 The TFTP Server Name Screen 100
7.9 Technical Reference 100
7.9.1 LANs, WANs and the EMG 100
7.9.2 DHCP Setup 101
7.9.3 DNS Server Addresses 101

Chapter 8
Routing 102

8.1 Overview 102
8.2 The Routing Screen 102
8.2.1 Add/Edit Static Route 103
8.3 The DNS Route Screen 104
8.3.1 The DNS Route Add Screen 105
8.4 The Policy Route Screen 105
8.4.1 Add/Edit Policy Route 107
8.5 RIP 107
8.5.1 The RIP Screen 108

Chapter 9
Quality of Service (QoS) 109

9.1 Overview 109
9.1.1 What You Can Do in this Chapter 109
9.2 What You Need to Know 110

9.3 The Quality of Service General Screen 111
9.4 The Queue Setup Screen 112
9.4.1 Adding a QoS Queue 114
9.5 The Classification Setup Screen 115
9.5.1 Add/Edit QoS Class 115
9.6 The QoS Shaper Setup Screen 119
9.6.1 Add/Edit a QoS Shaper 120
9.7 The QoS Policer Setup Screen 120
9.7.1 Add/Edit a QoS Policer 121
9.8 Technical Reference 122

Chapter 10
Network Address Translation (NAT) 127

10.1 Overview 127
10.1.1 What You Can Do in this Chapter 127
10.1.2 What You Need To Know 127
10.2 The Port Forwarding Screen 128
10.2.1 Add/Edit Port Forwarding 130
10.3 The Applications Screen 131
10.3.1 Add New Application 132
10.4 The Port Triggering Screen 133
10.4.1 Add/Edit Port Triggering Rule 134
10.5 The DMZ Screen 135
10.6 The ALG Screen 136
10.7 The Address Mapping Screen 137
10.7.1 Add/Edit Address Mapping Rule 138
10.8 The Sessions Screen 139
10.9 Technical Reference 139
10.9.1 NAT Definitions 139
10.9.2 What NAT Does 140
10.9.3 How NAT Works 140
10.9.4 NAT Application 141

Chapter 11
DNS 143

11.1 Overview 143
11.1.1 What You Can Do in this Chapter 143
11.1.2 What You Need To Know 143
11.2 The DNS Entry Screen 144
11.2.1 Add/Edit DNS Entry 144
11.3 The Dynamic DNS Screen 145

Chapter 12
VLAN Group 147

12.1 Overview 147
12.1.1 What You Can Do in this Chapter 147
12.2 The VLAN Group Screen 147
12.2.1 Add/Edit a VLAN Group 148

Chapter 13
Interface Grouping 149

13.1 Overview 149
13.1.1 What You Can Do in this Chapter 149
13.2 The Interface Grouping Screen 149
13.2.1 Interface Group Configuration 150
13.2.2 Interface Grouping Criteria 151

Chapter 14
Firewall 153

14.1 Overview 153
14.1.1 What You Can Do in this Chapter 153
14.1.2 What You Need to Know 154
14.2 The Firewall Screen 154
14.3 The Protocol Screen 155
14.3.1 Add/Edit a Service 156
14.4 The Access Control Screen 157
14.4.1 Add/Edit an ACL Rule 157
14.5 The DoS Screen 159

Chapter 15
MAC Filter 160

15.1 Overview 160
15.2 The MAC Filter Screen 160

Chapter 16
Parental Control 162

16.1 Overview 162
16.2 The Parental Control Screen 162
16.2.1 Add/Edit a Parental Control Profile 163

Chapter 17
Scheduler Rule 167

17.1 Overview 167
17.2 The Scheduler Rule Screen 167
17.2.1 Add/Edit a Schedule 167

Chapter 18
Certificates 169

18.1 Overview 169
18.1.1 What You Can Do in this Chapter 169
18.2 What You Need to Know 169
18.3 The Local Certificates Screen 169
18.3.1 Create Certificate Request 170
18.3.2 Load Signed Certificate 171
18.4 The Trusted CA Screen 172
18.4.1 View Trusted CA Certificate 173
18.4.2 Import Trusted CA Certificate 174

Chapter 19
Log 175

19.1 Overview 175
19.1.1 What You Can Do in this Chapter 175
19.1.2 What You Need To Know 175
19.2 The System Log Screen 176
19.3 The Security Log Screen 176

Chapter 20
Traffic Status 178

20.1 Overview 178
20.1.1 What You Can Do in this Chapter 178
20.2 The WAN Status Screen 178
20.3 The LAN Status Screen 179
20.4 The NAT Status Screen 180

Chapter 21
ARP Table 181

21.1 Overview 181
21.1.1 How ARP Works 181
21.2 ARP Table Screen 181

Chapter 22
Routing Table 183

22.1 Overview 183
22.2 The Routing Table Screen 183

Chapter 23
Multicast Status 185

23.1 Overview 185
23.2 The IGMP Status Screen 185
23.3 The MLD Status Screen 185

Chapter 24
System 187

24.1 Overview 187
24.2 The System Screen 187

Chapter 25
User Account 188

25.1 Overview 188
25.2 The User Account Screen 188
25.2.1 The User Account Add/Edit Screen 189

Chapter 26
Remote Management 191

26.1 Overview 191
26.2 The MGMT Services Screen 191
26.3 The Trust Domain Screen 192
26.3.1 The Add Trust Domain Screen 193

Chapter 27
SNMP 194

27.1 Overview 194
27.2 The SNMP Screen 194

Chapter 28
Time Settings 196

28.1 Overview 196
28.2 The Time Screen 196

Chapter 29
E-mail Notification 198

29.1 Overview 198
29.2 The E-mail Notification Screen 198
29.2.1 E-mail Notification Edit 198

Chapter 30
Log Setting 200

30.1 Overview 200
30.2 The Log Settings Screen 200
30.2.1 Example E-mail Log 201

Chapter 31
Firmware Upgrade 203

31.1 Overview 203

31.2 The Firmware Screen 203

Chapter 32
Backup/Restore 205

32.1 Overview 205
32.2 The Backup/Restore Screen 205
32.3 The ROM-D Screen 207
32.4 The Reboot Screen 207

Chapter 33
Diagnostic 208

33.1 Overview 208
33.1.1 What You Can Do in this Chapter 208
33.2 What You Need to Know 208
33.3 Ping & TraceRoute & NsLookup 209

Chapter 34
Troubleshooting 210

34.1 Power, Hardware Connections, and LEDs 210
34.2 EMG Access and Login 211
34.3 Internet Access 212
34.4 Wireless Internet Access 213
34.5 UPnP 214

Part III: Appendices 215

Appendix A Customer Support 216

Appendix B Wireless LANs 222

Appendix C IPv6 234

Appendix D Services 242

Appendix E Legal Information 246

Index 254

PART I
User's Guide

CHAPTER 1
Introducing the EMG

1.1 Overview

The EMG is an Ethernet gateway providing triple-play services and optimized HD IPTV services at home or office. This model offers a Gigabit Ethernet (GbE) WAN with interfaces of Ethernet and WAN ports. The EMG offers 2.4G and 5G Wi-Fi networks that operate simultaneously, providing a simple and unified network management.

Only use firmware for your EMG's specific model.

1.2 Ways to Manage the EMG

Use any of the following methods to manage the EMG.

- Web Configurator. This is recommended for everyday management of the EMG using a (supported) web browser.

1.3 Good Habits for Managing the EMG

Do the following regularly to make the EMG more secure and to manage the EMG more effectively.

- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you backed up an earlier configuration file, you would not have to totally re-configure the EMG. You could simply restore your last configuration.

1.4 Applications for the EMG

Here are some example uses for which the EMG is well suited.

1.4.1 Internet Access

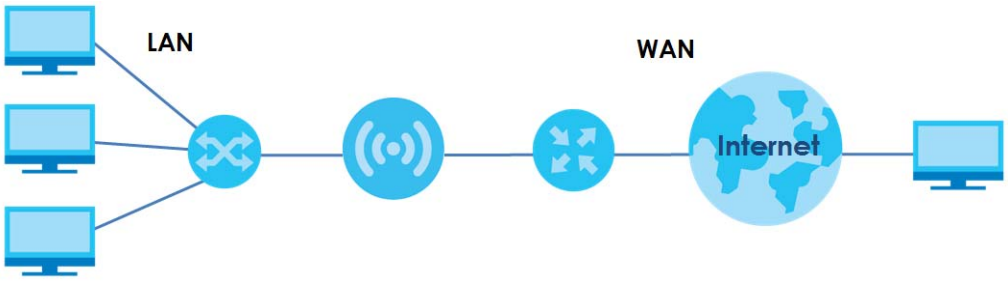
Computers can connect to the EMG's LAN ports (or wirelessly).

You can also configure IP filtering on the EMG for secure Internet access. When the IP filter is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

1.4.1.1 Ethernet WAN

If you have another broadband modem or router available, you can connect the WAN port to the broadband modem or router. This way, you can access the Internet via an Ethernet connection and still use the QoS, Firewall and parental control functions on the EMG.

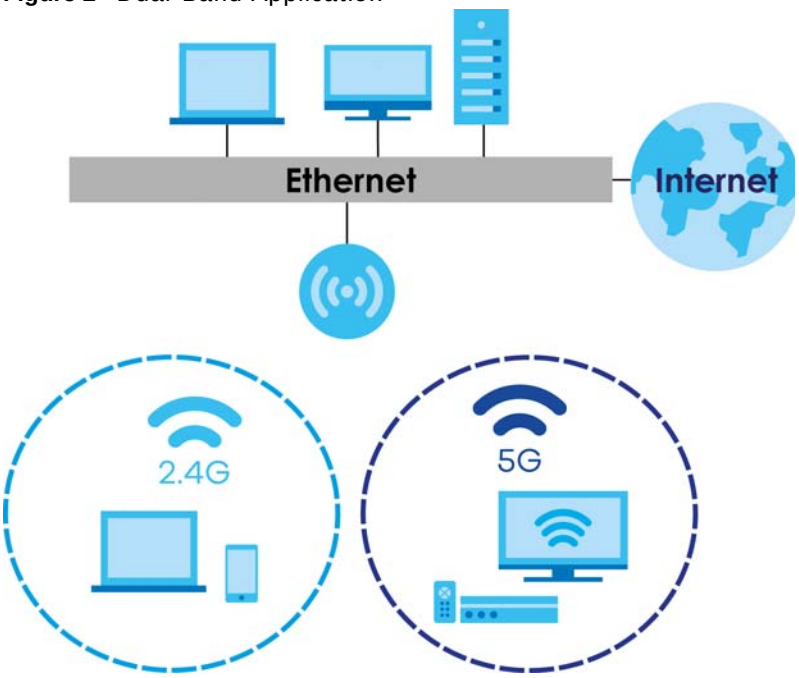
Figure 1 EMG's Internet Access Application: Ethernet WAN



1.4.2 Dual-Band

The EMG is a dual-band gateway and able to function both 2.4G and 5G networks at the same time. You could use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz band for time sensitive traffic like high-definition video, music, and gaming.

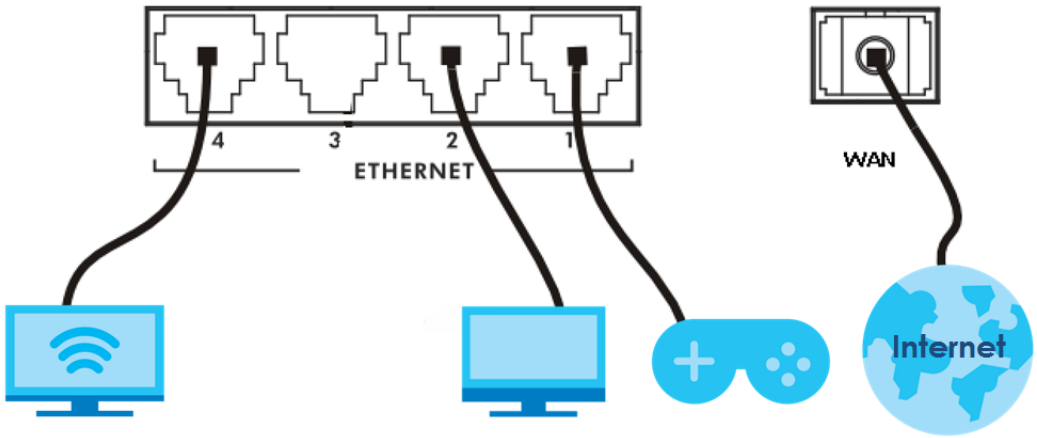
Figure 2 Dual-Band Application



1.4.3 Triple Play

The ISP may provide “triple play” service to the EMG. This allows you to take advantage of such features as broadband Internet access, and streaming video/audio media, all at the same time with no noticeable loss in bandwidth.

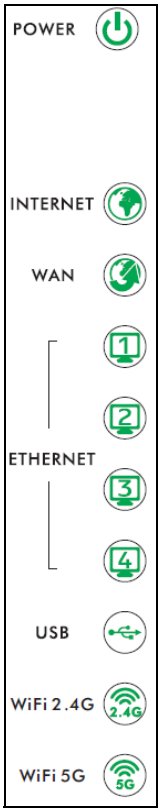
Figure 3 Triple Play Example



1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 4 LEDs on the EMG



None of the LEDs are on if the EMG is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
Power	Green	On	The EMG is receiving power and ready for use.
		Blinking	The EMG is self-testing.
	Red	On	The EMG detected an error while self-testing, or there is a device malfunction.
		Blinking	The EMG is upgrading its firmware.
		Off	The EMG is not receiving power.
Internet	Green	On	The EMG has an IP connection but no traffic.
		Blinking	The EMG is sending or receiving IP traffic.
		Off	There is no Internet connection or the gateway is in bridged mode.
	Red	On	The EMG attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
WAN	Green	On	The EMG has a successful 10/100/1000 Mbps Ethernet connection on the WAN.
		Blinking	The EMG is sending or receiving data to/from the WAN at 10/100/1000 Mbps.
		Off	There is no Ethernet connection on the WAN.

Table 1 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
1 2 3 4 Ethernet 1~4	Green	On	The EMG has a successful 1000 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The EMG is sending or receiving data to/from the LAN at 1000 Mbps.
		Off	The EMG does not have an Ethernet connection with the LAN.
2.4G WiFi 2.4G	Green	On	The 2.4 GHz wireless network is activated.
		Blinking	The EMG is communicating with 2.4 GHz wireless clients.
	Amber	On	The EMG is setting up a WPS connection with a 2.4 GHz wireless client via WPS method 3. See Section 6.4 on page 70 to learn each method.
		Blinking	The EMG is setting up a WPS connection with a 2.4 GHz wireless client via WPS method 1 or 2. See Section 6.4 on page 70 to learn each method.
		Off	The 2.4 GHz wireless network is not activated.
5G WiFi 5G	Green	On	The 5 GHz wireless network is activated.
		Blinking	The EMG is communicating with 5 GHz wireless clients.
	Amber	On	The EMG is setting up a WPS connection with a 5 GHz wireless client via WPS method 3. See Section 6.4 on page 70 to learn each method.
		Blinking	The EMG is setting up a WPS connection with a 5 GHz wireless client via WPS method 1 or 2. See Section 6.4 on page 70 to learn each method.
		Off	The 5 GHz wireless network is not activated.
WPS WPS	Amber	On	The 2.4 Ghz or 5 GHz wireless network and WPS are enabled.
		Off	Both 2.4 Ghz or 5 GHz wireless network and WPS are disabled.

1.6 The RESET Button

You will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously.

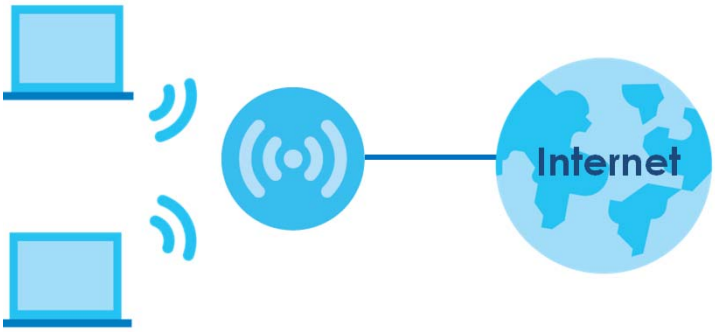
1 Make sure the **POWER** LED is on (not blinking).

2 To set the device back to the factory default settings, press the **RESET** button for five seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

1.7 Wireless Access

You can configure your wireless network in either the built-in Web Configurator, or using the WPS button.

Figure 5 Wireless Access Example



1.7.1 Using the WPS Button

Once the **WiFi** LED turns green, the wireless network is active. If the wireless network is turned off, see Section 6.2 on page 65 for how to enable the wireless network on the EMG.

You can also use the **WPS** button to quickly set up a secure wireless connection between the EMG and a WPS-compatible client by adding one device at a time.

To activate WPS:

1. Make sure the **POWER** LED is on and not blinking.
2. Press the **WPS** button for five seconds and release it.
3. Press the WPS button on another WPS-enabled device within range of the EMG. The **WiFi** LED flashes amber while the EMG sets up a WPS connection with the other wireless device.
4. Once the connection is successfully made, the **WPS** LED shines amber.

   The **WPS** LED turns off when the wireless network is off.

1.8 Wall Mounting

You may need screw anchors if mounting on a concrete or brick wall.

Table 2 Wall Mounting Information

Distance between holes	90 mm
M4 Screws	Two
Screw anchors (optional)	Two

5. Select a position free of obstructions on a wall strong enough to hold the weight of the device.
6. Mark two holes on the wall at the appropriate distance apart for the screws.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

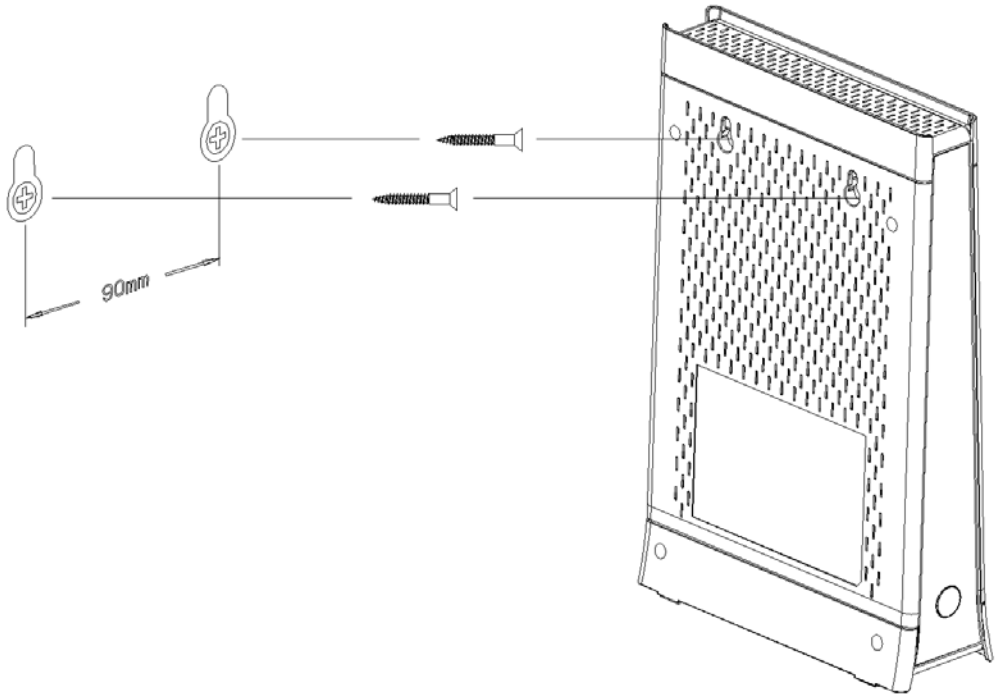
7 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.

8 Make sure the screws are fastened well enough to hold the weight of the EMG with the connection cables.

9 Align the holes on the back of the EMG with the screws on the wall. Hang the EMG on the screws.

Figure 6 Wall Mounting Example



CHAPTER 2
The Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy EMG setup and management via Internet browser. Use Internet Explorer 8.0 and later versions or Mozilla Firefox 3 and later versions or Safari 2.0 and later versions.* The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your EMG. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

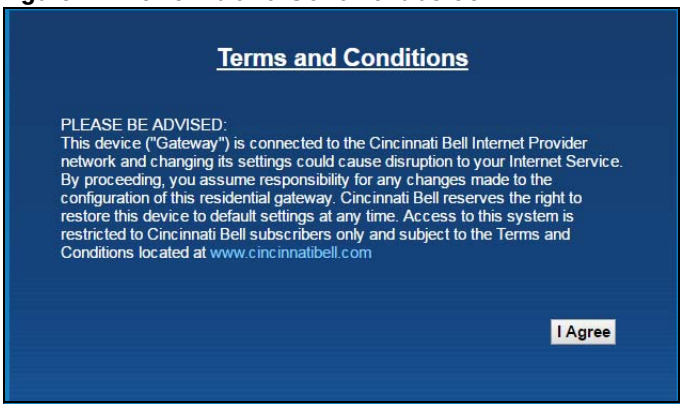
2.1.1 Accessing the Web Configurator

1 Make sure your EMG hardware is properly connected (refer to the Quick Start Guide).

2 Launch your web browser. If the EMG does not automatically re-direct you to the login screen, go to http://192.168.200.1.

3 The **Terms and Conditions** screen displays. To access the administrative Web Configurator and manage the EMG, click on the **I Agree** button as shown below.

Figure 7 The Terms and Conditions Screen



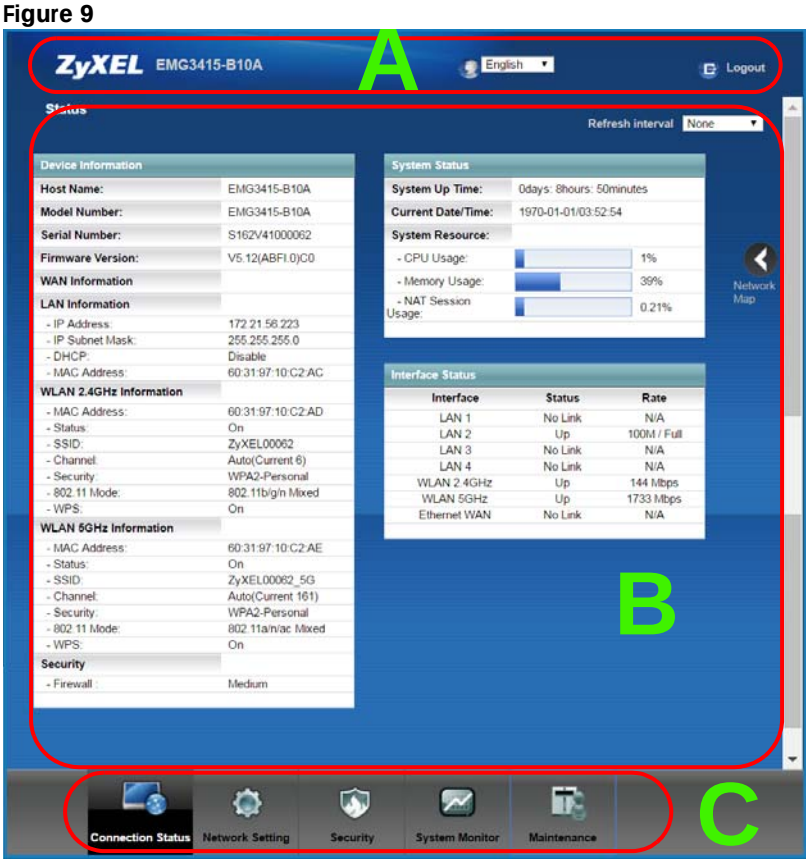
4 The **Network Map** page appears.

Figure 8 The Network Map Screen

5 Click **Status** to display the **Status** screen, where you can view the EMG's interface and system information.

2.2 Web Configurator Layout

Figure 9



As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - main window
- **C** - navigation panel

2.2.1 Title Bar

The title bar provides some icons in the upper right corner.

The icons provide the following functions.

Table 3 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
English	**Language**: Select the language you prefer.
Logout	**Logout**: Click this icon to log out of the web configurator.

2.2.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure EMG features. The following tables describe each menu item.

Table 4 Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		This screen shows the network status of the EMG and computers/devices connected to it.
Network Setting		
Broadband	Broadband	Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections.
Wireless	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the EMG.
	WPS	Use this screen to configure and view your WPS (Wi-Fi Protected Setup) settings.
	WMM	Use this screen to enable or disable Wi-Fi MultiMedia (WMM).
	Others	Use this screen to configure advanced wireless settings.
	Channel Status	Use this screen to scan wireless LAN channel noises and view the results.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to turn UPnP and UPnP NAT-T on or off.
	Additional Subnet	Use this screen to configure IP alias and public static IP.
	STB Vendor ID	Use this screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the EMG automatically create static DHCP entries for the STB devices when they request IP addresses.
	Wake on LAN	Use this screen to remotely turn on a device on the local network.
	TFTP Server Name	Configure a TFTP server name which is sent to clients using DHCP option 66.
Routing	Static Route	Use this screen to view and set up static routes on the EMG.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s).
	Policy Route	Use this screen to configure policy routing on the EMG.
	RIP	Use this screen to configure Routing Information Protocol to exchange routing information with other routers.
QoS	General	Use this screen to enable QoS and traffic prioritizing. You can also configure the QoS rules and actions.
	Queue Setup	Use this screen to configure QoS queues.
	Classification Setup	Use this screen to define a classifier.
	Shaper Setup	Use this screen to limit outgoing traffic rate on the selected interface.
	Policer Setup	Use this screen to configure QoS policers.

Table 4 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Applications	Use this screen to configure servers behind the EMG.
	Port Triggering	Use this screen to change your EMG's port triggering settings.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the **Port Forwarding** screen.
	ALG	Use this screen to enable or disable SIP ALG.
	Address Mapping	Use this screen to change your EMG's address mapping settings.
	Sessions	Use this screen to configure the maximum number of NAT sessions each client host is allowed to have through the EMG.
DNS	DNS Entry	Use this screen to view and configure DNS routes.
	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
Vlan Group	Vlan Group	Use this screen to group and tag VLAN IDs to outgoing traffic from the specified interface.
Interface Grouping	Interface Grouping	Use this screen to map a port to a PVC or bridge group.
Security		
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the EMG.
Parental Control	Parental Control	Use this screen to block web sites with the specific URL.
Scheduler Rules	Scheduler Rules	Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced.
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
System Monitor		

Table 4 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Log	System Log	Use this screen to view the status of events that occurred to the EMG. You can export or e-mail the logs.
	Security Log	Use this screen to view all security related events. You can select level and category of the security events in their proper drop-down list window. Levels include: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debugging Categories include: • Account • Attack • Firewall • MAC Filter
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the EMG.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the EMG.
	NAT	Use this screen to view NAT statistics for connected hosts.
ARP table	ARP table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.
Routing Table	Routing Table	Use this screen to view the routing table on the EMG.
Multicast Status	IGMP Status	Use this screen to view the status of all IGMP settings on the EMG.
	MLD Status	Use this screen to view the status of all MLD settings on the EMG.
Maintenance		
System	System	Use this screen to set Device name and Domain name.
User Account	User Account	Use this screen to change user password on the EMG.
Remote Management	MGMT Services	Use this screen to enable specific traffic directions for network services.
	Trust Domain	Use this screen to view a list of public IP addresses which are allowed to access the EMG through the services configured in the **Maintenance** > **Remote Management** screen.
SNMP	SNMP	Use this screen to configure SNMP (Simple Network Management Protocol) settings.
Time	Time	Use this screen to change your EMG's time and date.
E-mail Notification	E-mail Notification	Use this screen to configure up to two mail servers and sender addresses on the EMG.
Log Setting	Log Setting	Use this screen to change your EMG's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your EMG.

Table 4 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Backup/Restore	Backup/Restore	Use this screen to backup and restore your EMG's configuration (settings) or reset the factory default settings.
	ROM-D	Use this screen to save and/or clean the configuration to/from the ROM-D file which can store customized default settings.
Reboot	Reboot	Use this screen to reboot the EMG without turning the power off.
Diagnostic	Ping&Traceroute &Nslookup	Use this screen to identify problems with the Ethernet WAN connection. You can use Ping, TraceRoute, or Nslookup to help you identify problems.

CHAPTER 3
Tutorials

3.1 Overview

This chapter shows you how to use the EMG's various features.

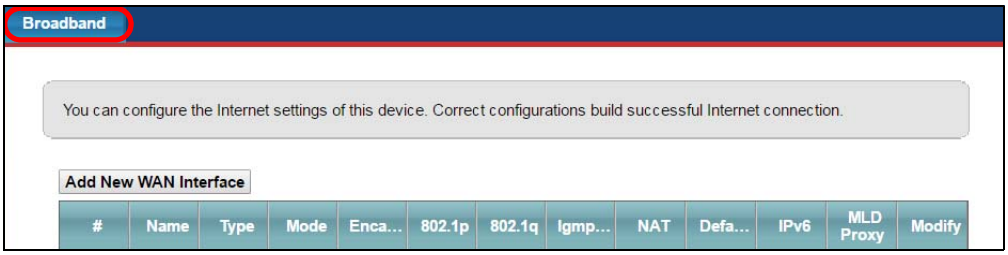
- Setting Up a New WAN Connection, see page 27
- Setting Up a Secure Wireless Network, see page 30
- Configuring Static Route for Routing to Another Network, see page 36
- Configuring QoS Queue and Class Setup, see page 38
- Access the EMG Using DDNS, see page 41
- Configuring the MAC Address Filter, see page 42

3.2 Setting Up a New WAN Connection

This tutorial shows you how to set up a new WAN Internet connection using the Web Configurator.

If you have another broadband modem or router available, you can connect the WAN port to the router and access the Internet via an Ethernet connection.

1 Click **Network Setting > Broadband** to open the following screen. Click **Add New WAN Interface**.



2 In this example, the Ethernet WAN connection has the following information.

General	
Name	MyWANConnection
Type	Ethernet
Connection Mode	Routing
Encapsulation	PPPoE
IPv6/IPv4 Mode	IPv4
Account Information	

PPP User Name	1234@WAN-Ex.com
PPP Password	ABCDEF!
PPPoE Service Name	MyWAN
Static IP Address	192.168.1.32
Others	Authentication Method: AUTO PPPoE Passthrough: Disabled NAT: Enabled IGMP Multicast Proxy: Enabled Apply as Default Gateway: Enabled VLAN: Enabled

3 Select the **Active** check box. Enter the **General** and **Account Information** settings as provided above.

Set the **Type** to **Ethernet**.

Choose the **Encapsulation** specified by your service provider. For this example, the service provider requires a username and password to establish Internet connection. Therefore, select **PPPoE** as the WAN encapsulation type.

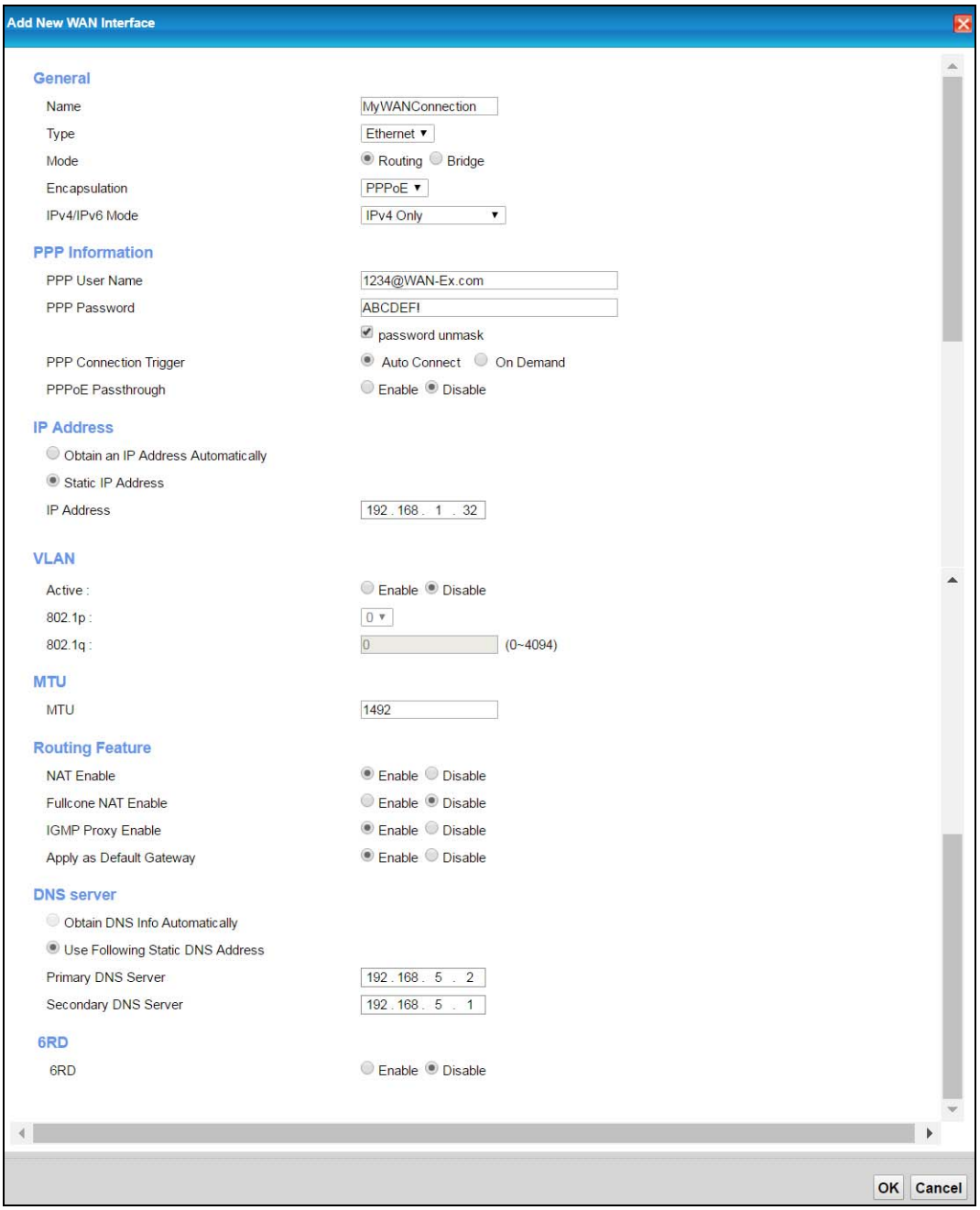
Set the **IPv6/IPv4 Mode** to **IPv4 Only**.

4 Enter the account information provided to you by your service provider.

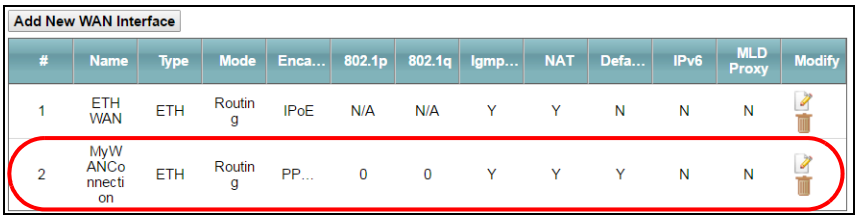
5 Configure this rule as your default Internet connection by selecting the **Apply as Default Gateway** check box. Then select DNS as **Static** and enter the DNS server addresses provided to you, such as **192.168.5.2** (DNS server1)/**192.168.5.1** (DNS server2).

6 Leave the rest of the fields to the default settings.

7 Click **Apply** to save your settings.



8 You should see a summary of your new WAN connection setup in the **Broadband** screen as follows.



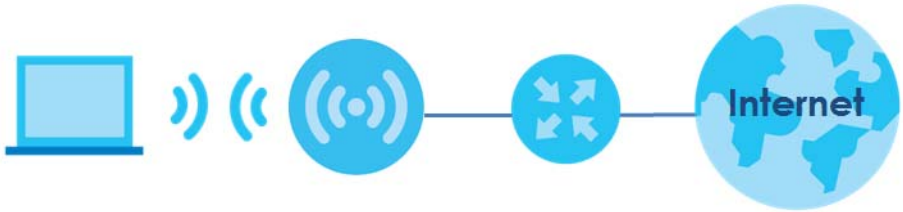
Add New WAN Interface

#	Name	Type	Mode	Enca...	802.1p	802.1q	Igmp...	NAT	Defa...	IPv6	MLD Proxy	Modify
1	ETH WAN	ETH	Routing	IPoE	N/A	N/A	Y	Y	N	N	N	
2	MyWANConnection	ETH	Routing	PP...	0	0	Y	Y	Y	N	N	

Try to connect to a website to see if you have correctly set up your Internet connection.

3.3 Setting Up a Secure Wireless Network

Thomas wants to set up a wireless network so that he can use his notebook to access the Internet. In this wireless network, the EMG serves as an access point (AP), and the notebook is the wireless client. The wireless client can access the Internet through the AP.



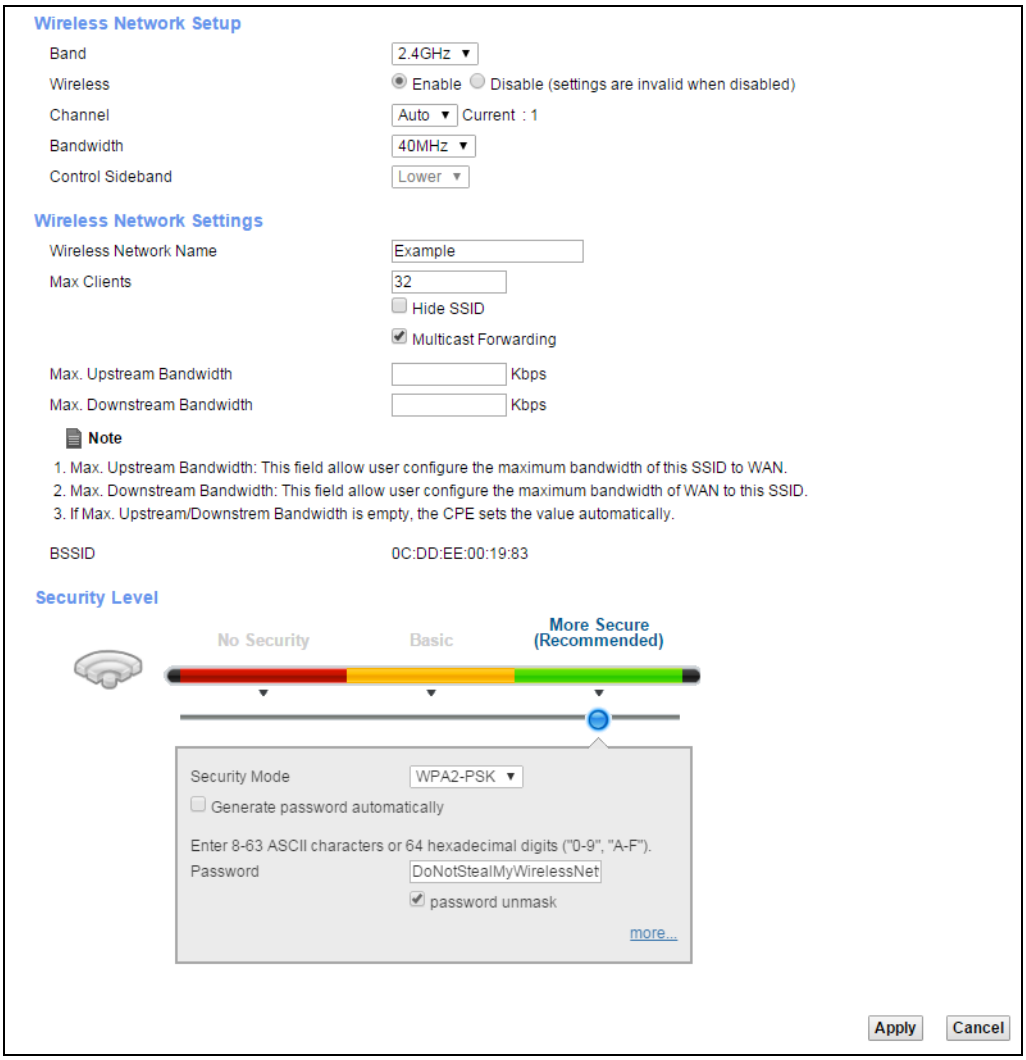
Thomas has to configure the wireless network settings on the EMG. Then he can set up a wireless network using WPS (Section 3.3.2 on page 32) or manual configuration (Section 3.3.3 on page 35).

3.3.1 Configuring the Wireless Network Settings

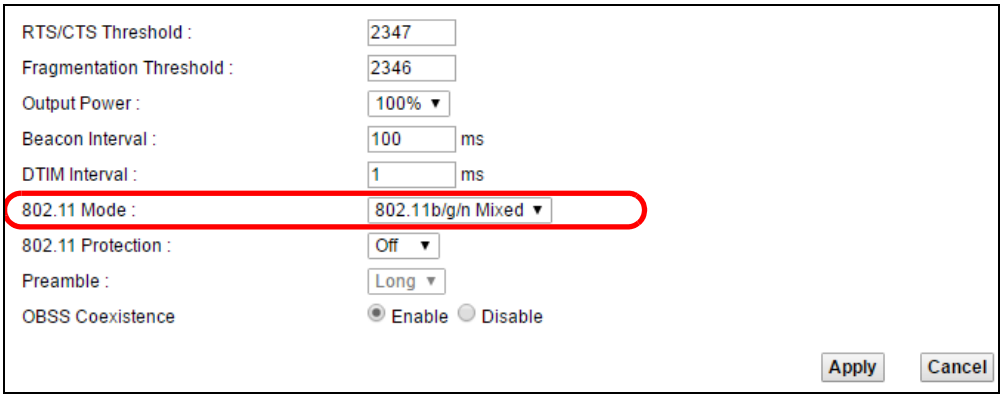
This example uses the following parameters to set up a wireless network.

SSID	Example
Security Mode	WPA2-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork
802.11 Mode	802.11b/g/n Mixed

1 Click **Network Setting** > **Wireless** to open the **General** screen. Select **More Secure** as the security level and **WPA2-PSK** as the security mode. Configure the screen using the provided parameters (see page 30). Click **Apply**.



2 Go to the **Wireless > Others** screen and select **802.11b/g/n Mixed** in the **802.11 Mode** field. Click **Apply**.



Thomas can now use the WPS feature to establish a wireless connection between his notebook and the EMG (see Section 3.3.2 on page 32). He can also use the notebook's wireless client to search for the EMG (see Section 3.3.3 on page 35).

3.3.2 Using WPS

This section shows you how to set up a wireless network using WPS. It uses the EMG as the AP and Zyxel NWD210N as the wireless client which connects to the notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCMCIA card).

There are two WPS methods to set up the wireless client settings:

- **Push Button Configuration (PBC)** - simply press a button. This is the easier of the two methods.
- **PIN Configuration** - configure a Personal Identification Number (PIN) on the EMG. A wireless client must also use the same PIN in order to download the wireless network settings from the EMG.

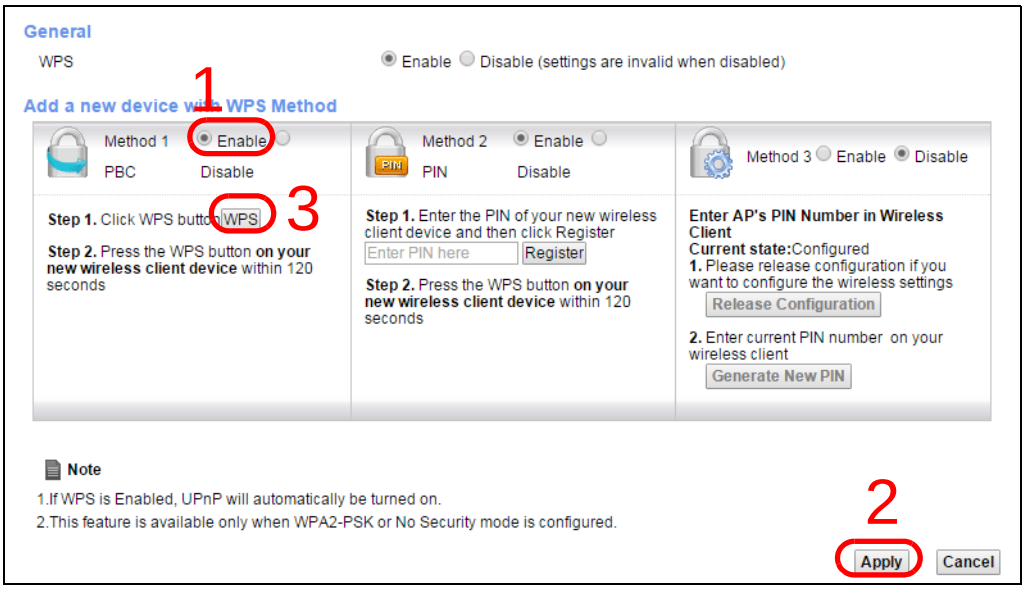
Push Button Configuration (PBC)

1 Make sure that your EMG is turned on and your notebook is within the cover range of the wireless signal.

2 Make sure that you have installed the wireless client driver and utility in your notebook.

3 In the wireless client utility, go to the WPS setting page. Enable WPS and press the WPS button for more than five seconds (**Start** or **WPS** button).

4 Push and hold the **WPS** button located on the EMG's front panel for more than 5 seconds. Alternatively, you may log into EMG's web configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function for method 1 and click **Apply**. Then click the **WPS** button.

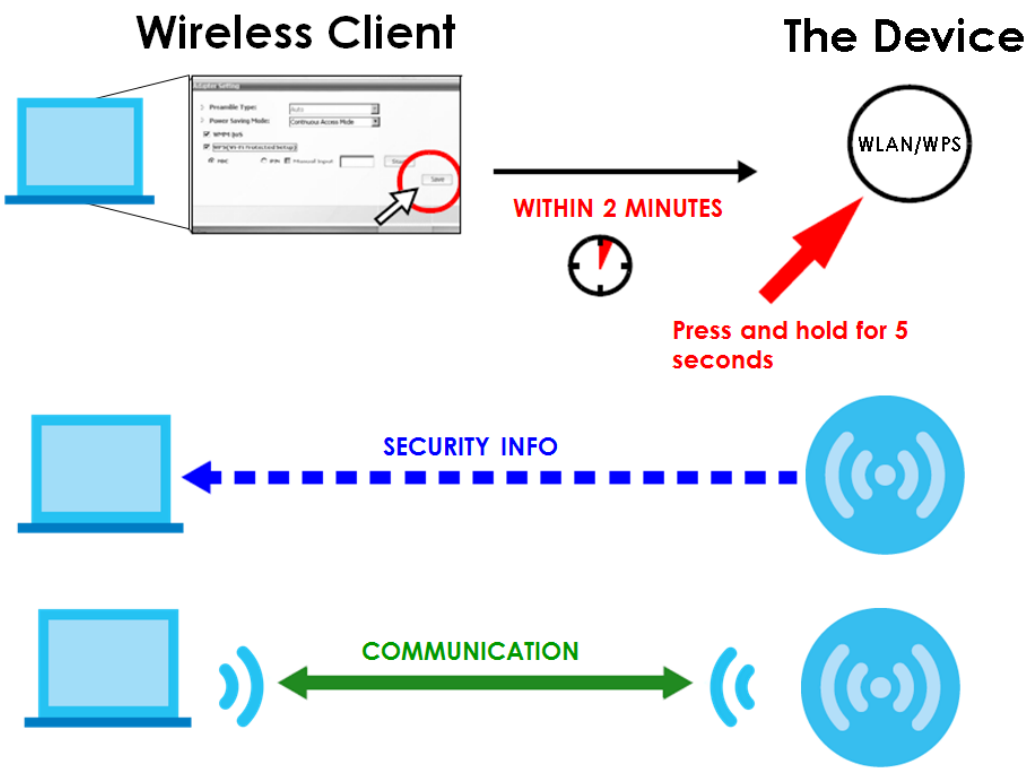


Note: Your EMG has a WPS button located on its front panel as well as a WPS button in its configuration utility. Both buttons have exactly the same function: you can use one or the other.

Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The EMG sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the EMG securely.

The following figure shows you an example of how to set up a wireless network and its security by pressing a button on both EMG and wireless client.

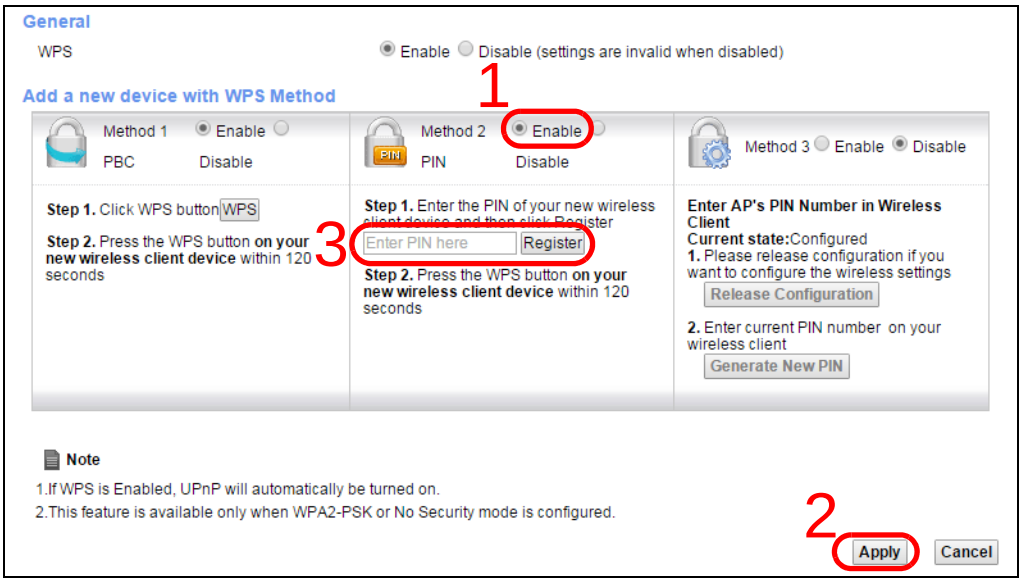


PIN Configuration

When you use the PIN configuration method, you need to use both the EMG's web configurator and the wireless client's utility.

1 Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.

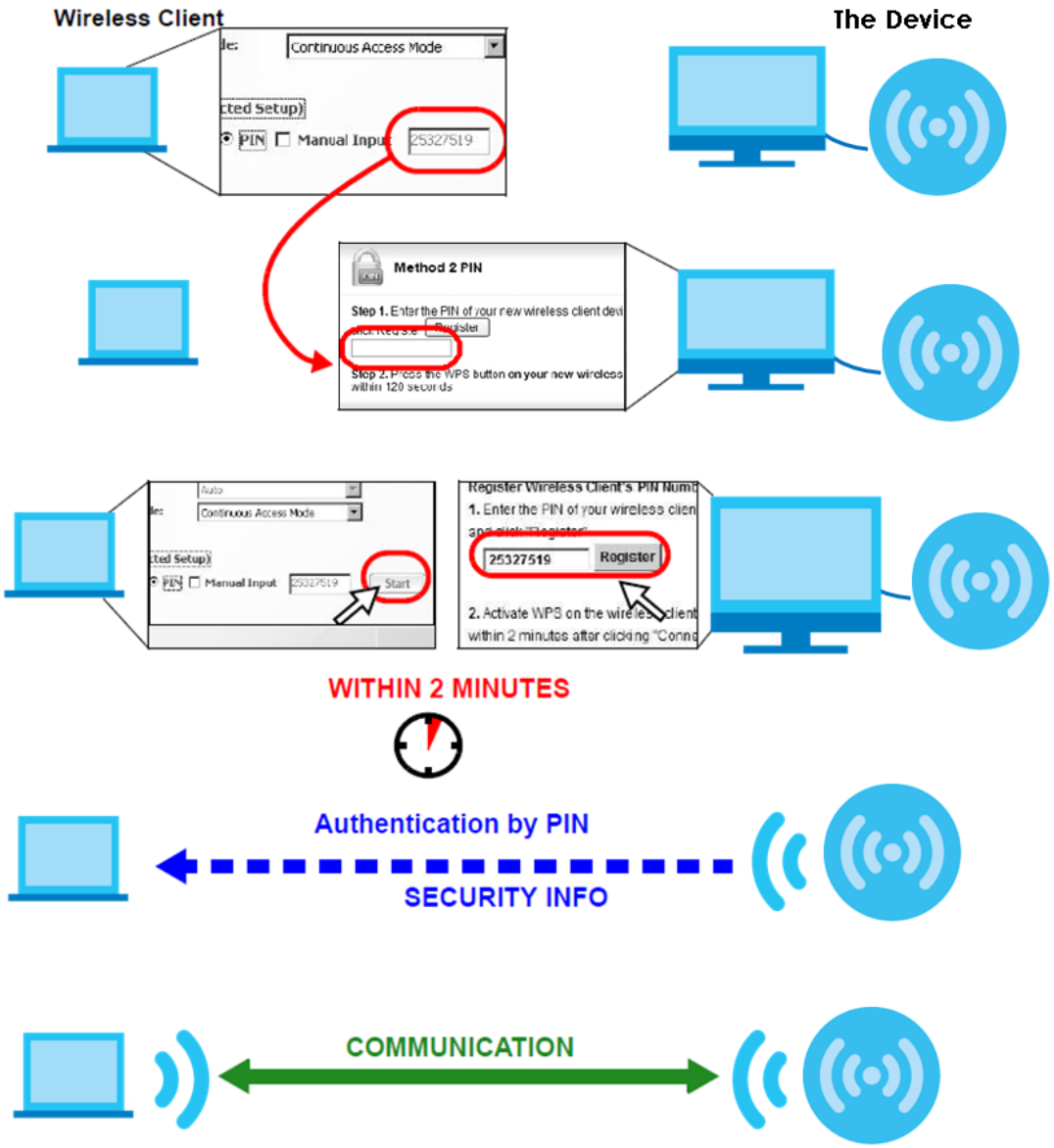
2 Log into EMG's web configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function and click **Apply**.



3 Enter the PIN number of the wireless client and click the **Register** button. Activate WPS function on the wireless client utility screen within two minutes.

The EMG authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the EMG securely.

The following figure shows you how to set up a wireless network and its security on a EMG and a wireless client by using PIN method.



3.3.3 Without WPS

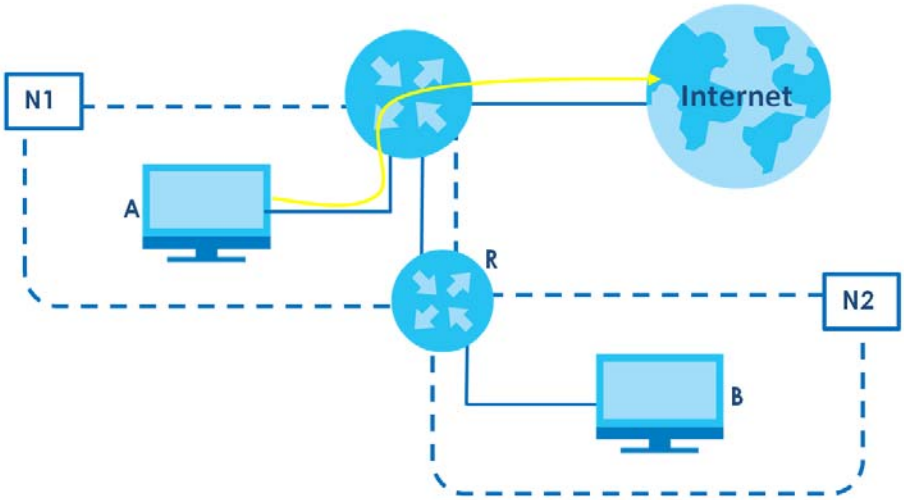
Use the wireless adapter's utility installed on the notebook to search for the "Example" SSID. Then enter the "DoNotStealMyWirelessNetwork" pre-shared key to establish an wireless Internet connection.

Note: The EMG supports IEEE 802.11b and IEEE 802.11g wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

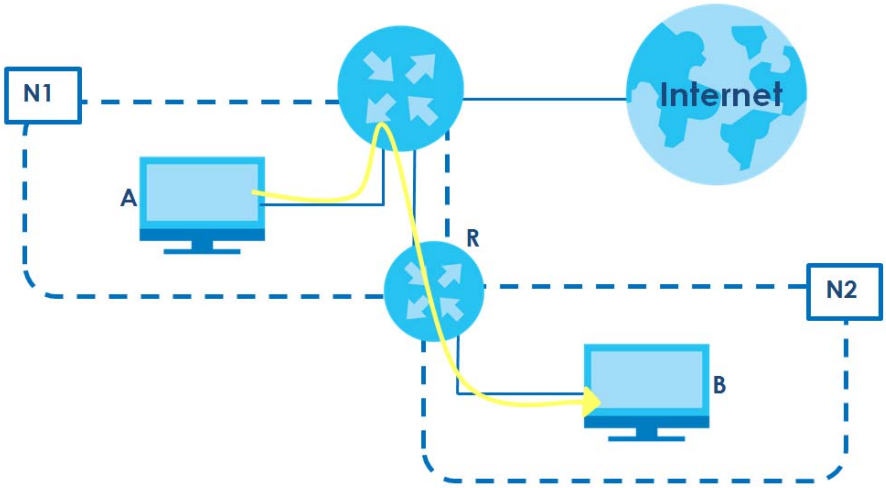
3.4 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the EMG's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the EMG's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the EMG's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the EMG to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the EMG routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

Table 5 IP Settings in this Tutorial

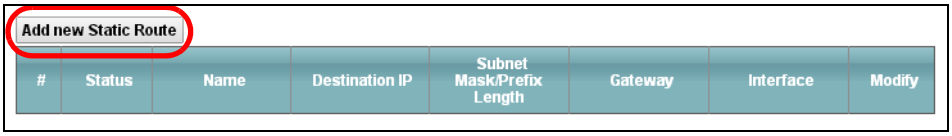
DEVICE / COMPUTER	IP ADDRESS
The EMG's WAN	172.16.1.1
The EMG's LAN	192.168.200.1
IP Type	IPv4
Use Interface	ETHWAN
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

1 Log into the EMG's Web Configurator.

2 Click **Network Setting** > **Routing**.

3 Click **Add new Static Route** in the **Static Route** screen.



4 Configure the **Static Route Setup** screen using the following settings:

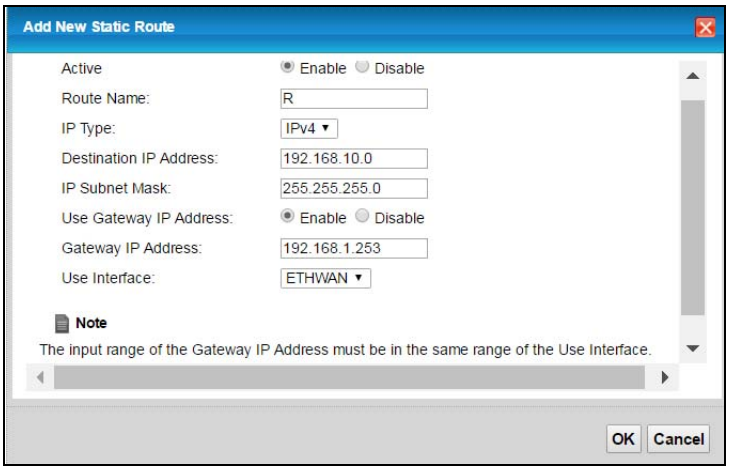
4a Select the **Enable** in the **Active** field. Enter the **Route Name** as **R**.

4b Set **IP Type** to **IPv4**.

4c Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.

4d Select **Enable** in the **Use Gateway IP Address field**. Type **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.

4e Select **ETHWAN** as the **Use Interface**.



4a Click **OK**.

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.

3.5 Configuring QoS Queue and Class Setup

This section contains tutorials on how you can configure the QoS screen.

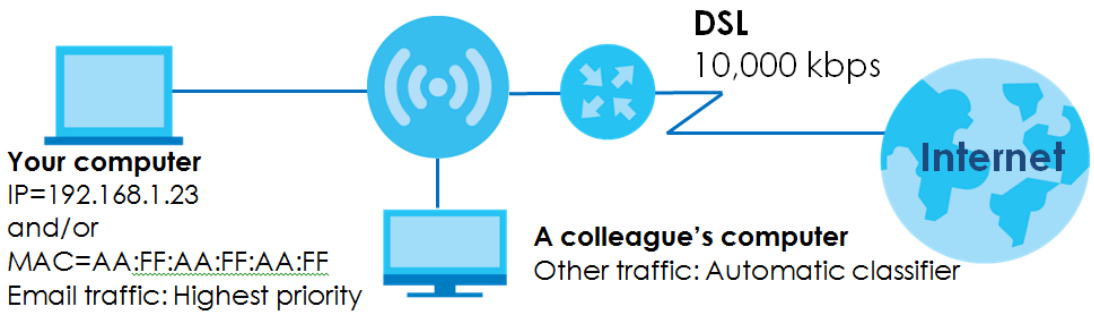
Let's say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues use the Internet for research, as well as chat applications for communicating with other branch offices.

In the following figure, your Internet connection has an upstream transmission bandwidth of 10,000 kbps. For this example, you want to configure QoS so that e-mail traffic gets the highest priority with at least 5,000 kbps. You can do the following:

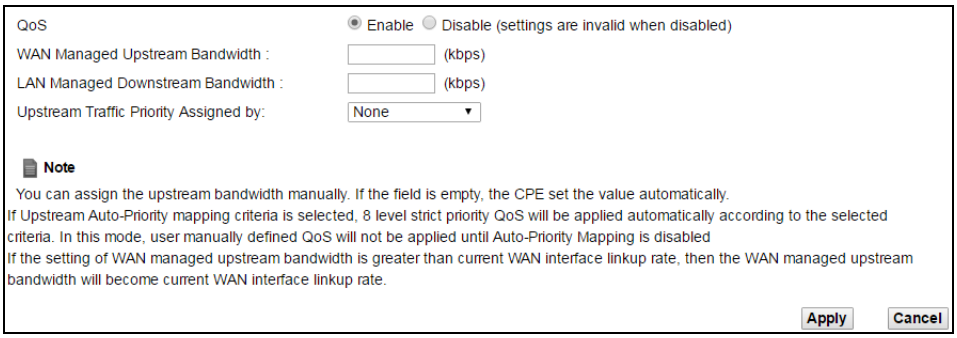
- Configure a queue to assign the highest priority queue (1) to e-mail traffic going to the WAN interface, so that e-mail traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer and map it to queue 7.

Note: QoS is applied to traffic flowing out of the EMG.

Traffic that does not match this class is assigned a priority queue based on the internal QoS mapping table on the EMG.

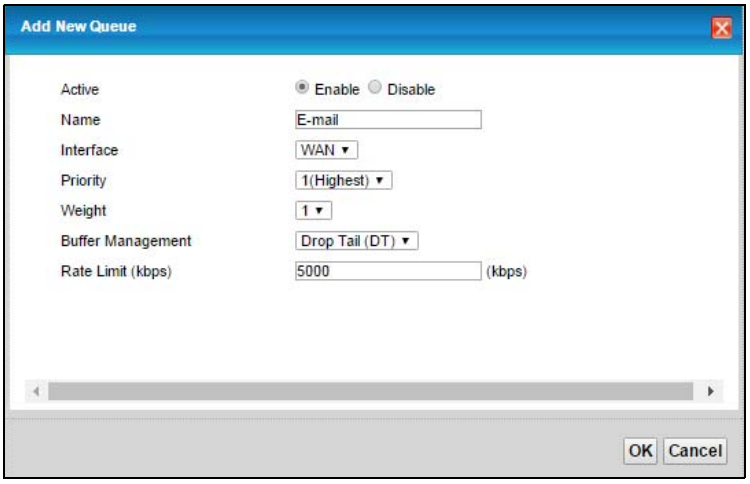


1 Click **Network Setting > QoS > General** and select **Enable**. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the EMG automatically determine this figure). Click **Apply**.

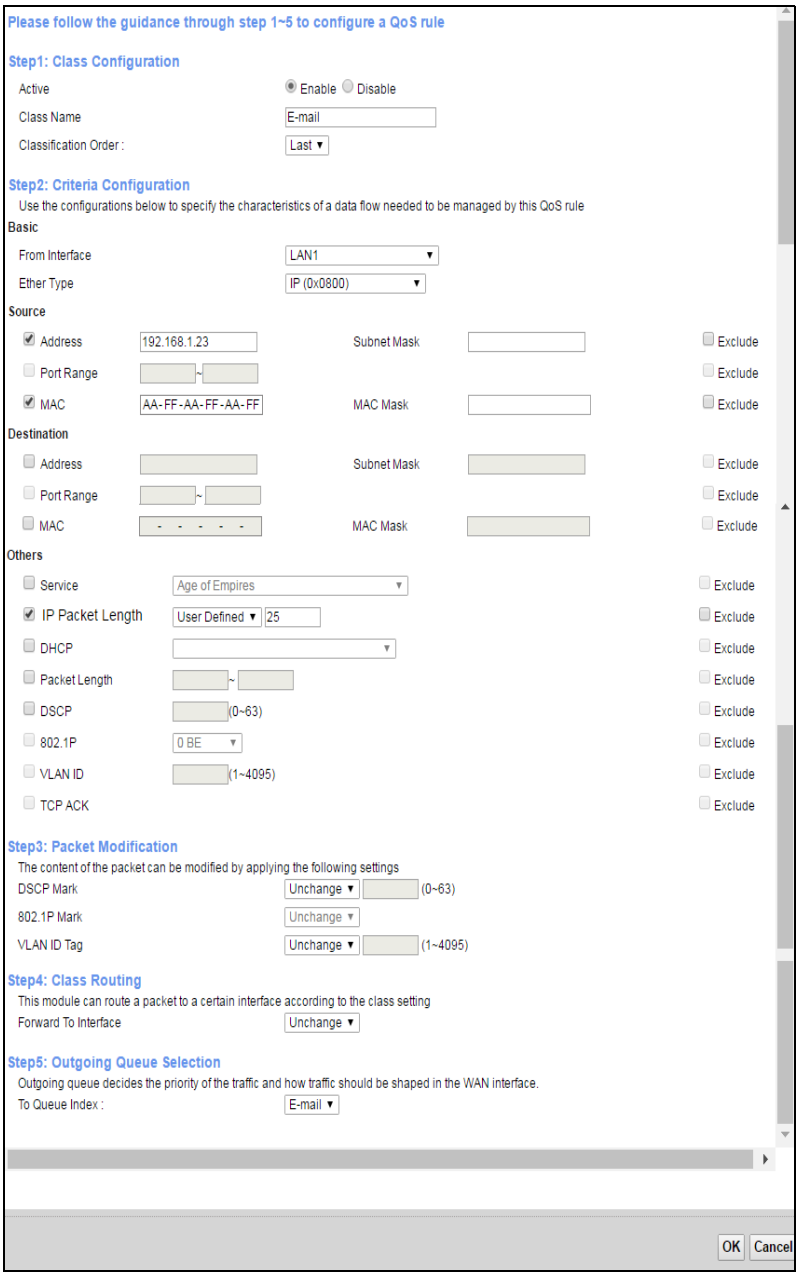


2 Click **Queue Setup** > **Add new Queue** to create a new queue. In the screen that opens, select **Enable** in the **Active** field and enter or select the following values:

- **Name**: E-mail
- **Interface**: **WAN**
- **Priority**: 1 (High)
- **Weight**: 8
- **Rate Limit**: 5,000 (kbps)



3 Click **Classification Setup** > **Add new Classification** to create a new class. Select **Enable** in the **Active** field and follow the settings as shown in the screen below.

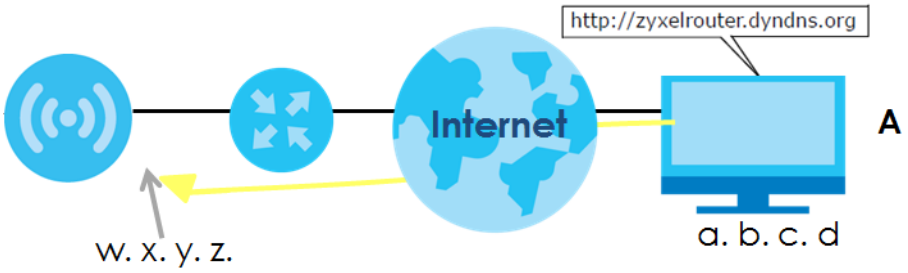


Class Name	Give a class name to this traffic, such as **E-mail** in this example.
From Interface	This is the interface from which the traffic will be coming from. Select **LAN1** for this example.
Ether Type	Select **IP** to identify the traffic source by its IP address or MAC address.
IP Address	Type the IP address of your computer - **192.168.1.23**. Type the **IP Subnet Mask** if you know it.
MAC Address	Type the MAC address of your computer - **AA:FF:AA:FF:AA:FF**. Type the **MAC Mask** if you know it.
To Queue Index	Link this to an item in the **Network Setting > QoS > Queue Setup** screen, which is the **E-mail** queue created in this example.

This maps e-mail traffic coming from port 25 to the highest priority, which you have created in the previous screen (see the **IP Protocol** field). This also maps your computer's IP address and MAC address to the **E-mail** queue (see the **Source** fields).

3.6 Access the EMG Using DDNS

If you connect your EMG to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The EMG's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the EMG using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial covers:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your EMG
- Testing the DDNS Setting

Note: If you have a private WAN IP address, then you cannot use DDNS.

3.6.1 Registering a DDNS Account on www.dyndns.org

1. Open a browser and type **http://www.dyndns.org**.
2. Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.
3. Log into www.dyndns.org using your account.
4. Add a new DDNS host name. This tutorial uses the following settings as an example.
   - Hostname: **zyxelrouter.dyndns.org**
   - Service Type: **Host with IP address**
   - IP Address: Enter the WAN IP address that your EMG is currently using. You can find the IP address on the EMG's Web Configurator **Status** page.

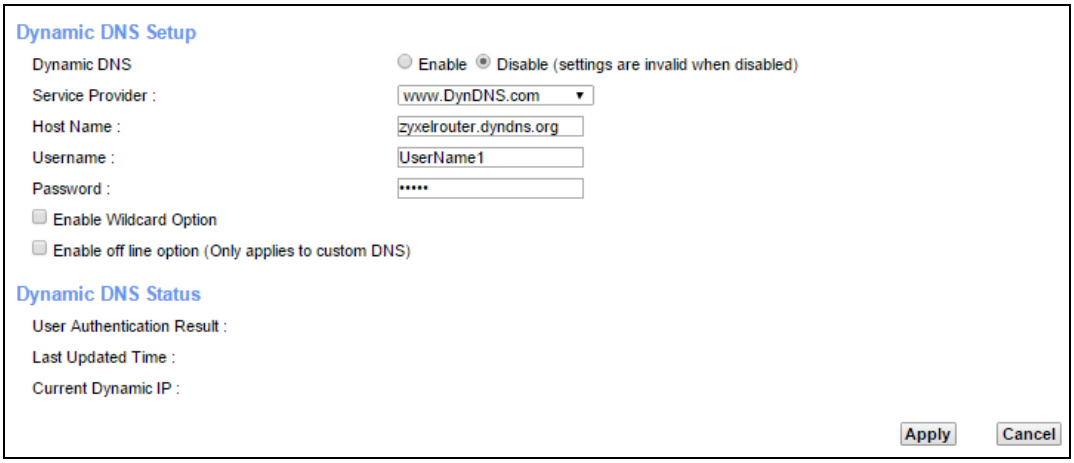
Then you will need to configure the same account and host name on the EMG later.

3.6.2 Configuring DDNS on Your EMG

Configure the following settings in the **Network Setting > DNS > Dynamic DNS** screen.

- Select **Enable Dynamic DNS**.
- Select **www.DynDNS.com** as the service provider.
- Type **zyxelrouter.dyndns.org** in the **Host Name** field.

- Enter the user name (**UserName1**) and password (**12345**).



Click **Apply**.

3.6.3 Testing the DDNS Setting

Now you should be able to access the EMG from the Internet. To test this:

1. Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.
2. Type **http://zyxelrouter.dyndns.org** and press [Enter].
3. The EMG's login page should appear. You can then log into the EMG and manage it.

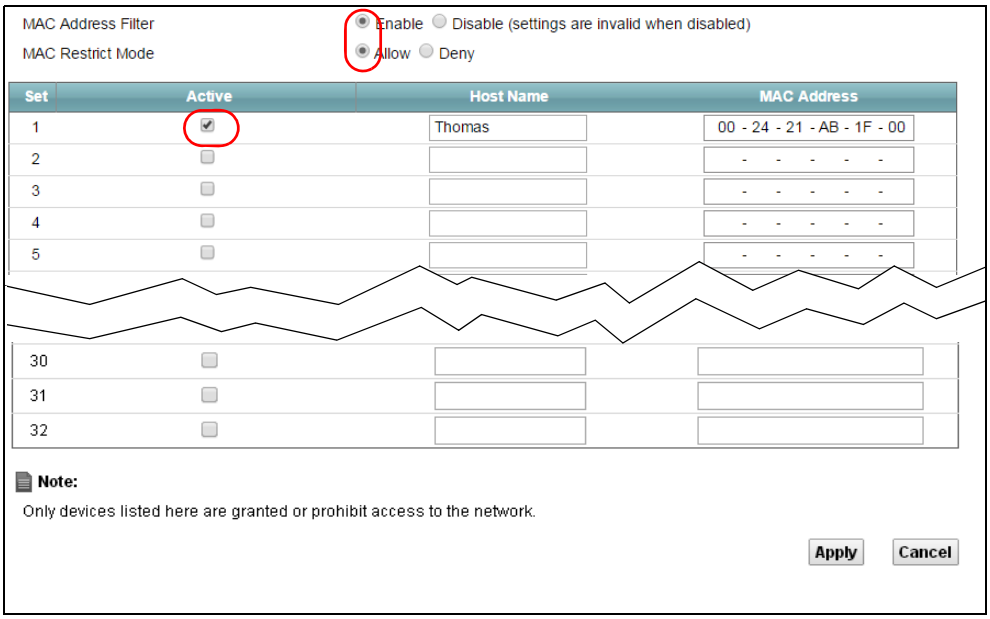
3.7 Configuring the MAC Address Filter

Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

Josephine's computer connects wirelessly to the Internet through the EMG. Thomas decides to use the **Security > MAC Filter** screen to grant wireless network access to his computer but not to Josephine's computer.

1 Click **Security** > **MAC Filter** to open the **MAC Filter** screen. Select the **Enable** check box to activate MAC filter function.

2 Select **Allow**. Then enter the host name and MAC address of Thomas' computer in this screen. Click **Apply**.



Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the EMG.

Part II
Technical Reference

CHAPTER 4
Network Map and Status Screens

4.1 Overview

After you log into the Web Configurator, the **Network Map** screen appears. This shows the network connection status of the EMG and clients connected to it.

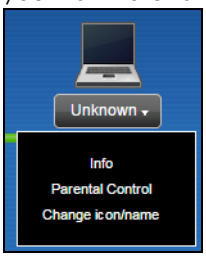
You can use the **Status** screen to look at the current status of the EMG, system resources, and interfaces (LAN, WAN, and WLAN).

4.2 The Network Map Screen

Use this screen to view the network connection status of the device and its clients. A warning message appears if there is a connection problem.

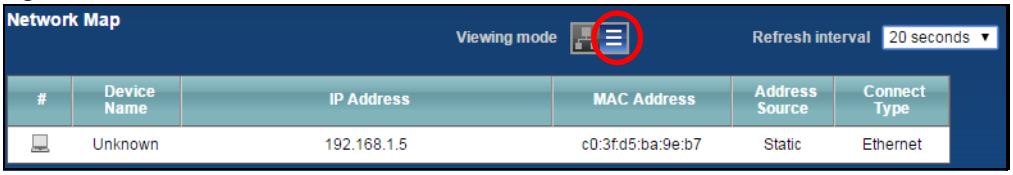
Figure 10 Connection Status: Icon View

If you want to view information about a client, click the client's name and **Info**. Click the IP address if you want to change it. If you want to change the name or icon of the client, click **Change name/icon**.



If you prefer to view the status in a list, click **List View** in the **Viewing mode** selection box. You can configure how often you want the EMG to update this screen in **Refresh interval**.

Figure 11 Connection Status: List View



4.3 The Status Screen

Use this screen to view the status of the EMG. Click **Status** to open this screen.

Figure 12 System Info Screen

Each field is described in the following table.

Table 6 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the EMG to update this screen.
Device Information	
Host Name	This field displays the EMG system name. It is used for identification.
Model Number	This shows the model number of your EMG.
Serial Number	This field displays the serial number of the EMG.
Firmware Version	This is the current version of the firmware inside the EMG.
WAN Information (These fields display when you have a WAN connection.)	
Encapsulation	This field displays the current encapsulation method.
IP Address	This field displays the current IP address of the EMG in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
MAC Address	This shows the WAN Ethernet adapter MAC (Media Access Control) Address of your EMG.
Primary DNS server	This field displays the first DNS server address assigned by the ISP.
Secondary DNS server	This field displays the second DNS server address assigned by the ISP.

Table 6 Status Screen (continued)

LABEL	DESCRIPTION
DHCP	This field displays whether the WAN interface is using a DHCP IP address or a static IP address. Choices are: **Client** - The WAN interface can obtain an IP address from a DHCP server. **None** - The WAN interface is using a static IP address.
LAN Information	
IP Address	This is the current IP address of the EMG in the LAN.
IP Subnet Mask	This is the current subnet mask in the LAN.
IPv6 Link Local Address	This field displays the current link-local address of the EMG for the LAN interface.
DHCP	This field displays what DHCP services the EMG is providing to the LAN. The possible values are: **Server** - The EMG is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The EMG acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **Disable** - The EMG is not providing any DHCP services to the LAN.
MAC Address	This shows the LAN Ethernet adapter MAC (Media Access Control) Address of your EMG.
WLAN 2.4GHz/5GHz Information	
MAC Address	This shows the wireless adapter MAC (Media Access Control) Address of the wireless interface.
Status	This displays whether the WLAN is activated.
SSID	This is the descriptive name used to identify the EMG in a wireless LAN.
Channel	This is the channel number used by the wireless interface now.
Security	This displays the type of security mode the wireless interface is using in the wireless LAN.
802.11 Mode	This displays the type of 802.11 mode the wireless interface is using in the wireless LAN.
WPS	This displays whether WPS is activated on the wireless interface.
Security	
Firewall	This displays the firewall's current security level.
System Status	
System Up Time	This field displays how long the EMG has been running since it last started up. The EMG starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it.
Current Date/ Time	This field displays the current date and time in the EMG. You can change this in **Maintenance> Time Setting**.
System Resource	
CPU Usage	This field displays what percentage of the EMG's processing ability is currently used. When this percentage is close to 100%, the EMG is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS; see Chapter 9 on page 109).
Memory Usage	This field displays what percentage of the EMG's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the EMG is probably becoming unstable, and you should restart the device. See Section 32.2 on page 205, or turn off the device (unplug the power) for a few seconds.
NAT Session Usage	This field displays what percentage of the EMG supported NAT sessions are currently being used. This field also displays the number of active NAT sessions and the maximum number of NAT sessions the EMG can support.
Interface Status	

Table 6 Status Screen (continued)

LABEL	DESCRIPTION
Interface	This column displays each interface the EMG has.
Status	This field indicates the interface's use status. For the LAN and Ethernet WAN interfaces, this field displays **Up** when using the interface and **NoLink** when not using the interface. For a WLAN interface, this field displays the enabled (**Up**) or disabled (**Disable**) state of the interface.
Rate	For the Ethernet WAN and LAN interfaces, this displays the port speed and duplex setting. For the WLAN interface, it displays the maximum transmission rate or **N/A** with WLAN disabled.

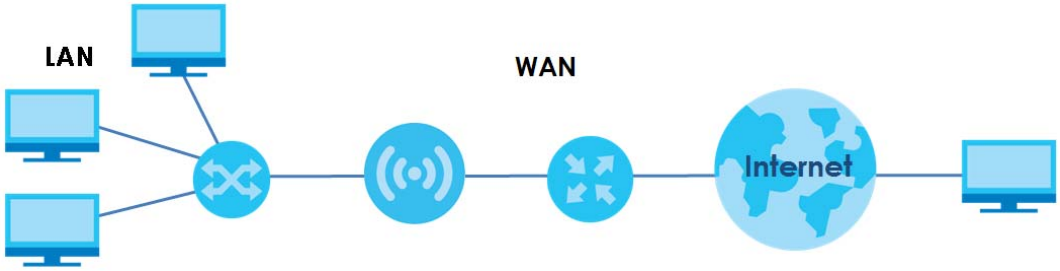
CHAPTER 5
Broadband

5.1 Overview

This chapter discusses the EMG's **Broadband** screens. Use these screens to configure your EMG for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 13 LAN and WAN



5.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view, remove or add a WAN interface. You can also configure the WAN settings on the EMG for Internet access (Section 5.2 on page 53).

Table 7 WAN Setup Overview

LAYER-2 INTERFACE	INTERNET CONNECTION		
CONNECTION	**MODE**	**ENCAPSULATION**	**CONNECTION SETTINGS**
Ethernet	Routing	PPPoE	PPP user name and password, WAN IPv4/IPv6 IP address, routing feature, DNS server, VLAN, and MTU
		IPoE	WAN IPv4/IPv6 IP address, NAT, DNS server and routing feature
	Bridge	N/A	VLAN

5.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

WAN IP Address

The WAN IP address is an IP address for the EMG, which makes it accessible from an outside network. It is used by the EMG to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the EMG tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es).

IPv6 Introduction

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses. The EMG can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

IPv6 Subnet Masking

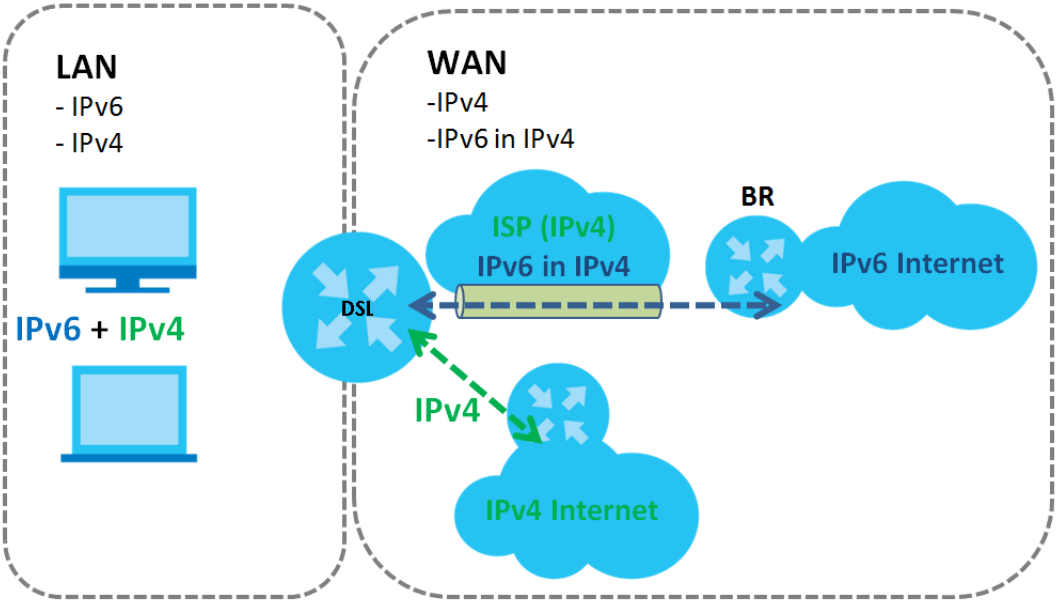
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

IPv6 Rapid Deployment

Use IPv6 Rapid Deployment (6rd) when the local network uses IPv6 and the ISP has an IPv4 network. When the EMG has an IPv4 WAN address and you set **IPv4/IPv6 Mode** to **IPv4 Only**, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.

The EMG generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router (BR in the figure) to connect to the native IPv6 Internet. The local network can also use IPv4 services. The EMG uses it's configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 14 IPv6 Rapid Deployment

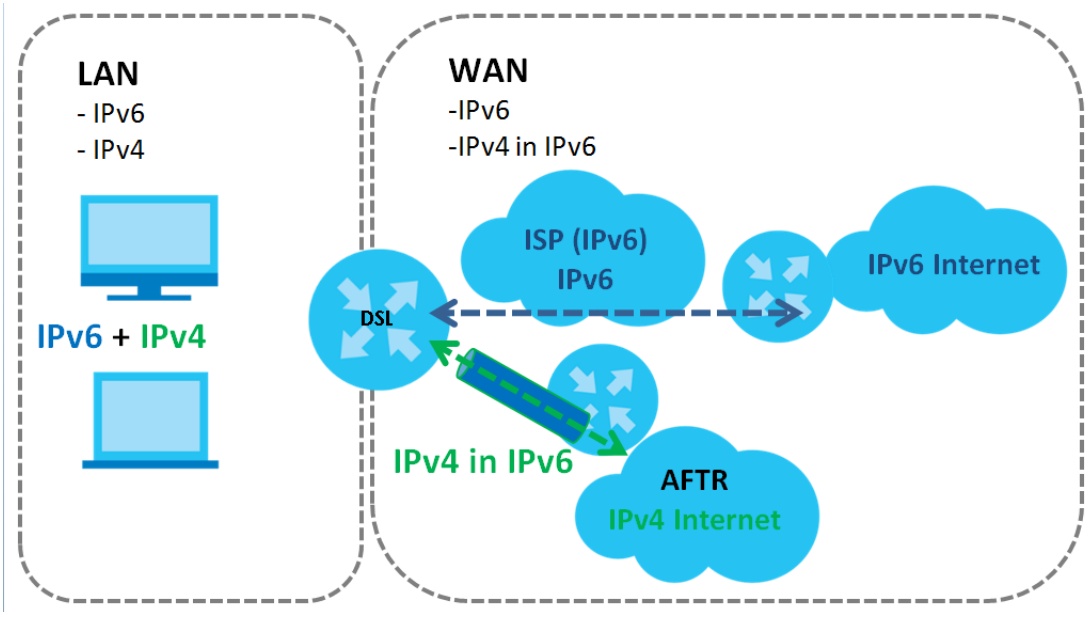


Dual Stack Lite

Use Dual Stack Lite when local network computers use IPv4 and the ISP has an IPv6 network. When the EMG has an IPv6 WAN address and you set **IPv4/IPv6 Mode** to **IPv6 Only**, you can enable Dual Stack Lite to use IPv4 computers and services.

The EMG tunnels IPv4 packets inside IPv6 encapsulation packets to the ISP's Address Family Transition Router (AFTR in the graphic) to connect to the IPv4 Internet. The local network can also use IPv6 services. The EMG uses it's configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

Figure 15 Dual Stack Lite



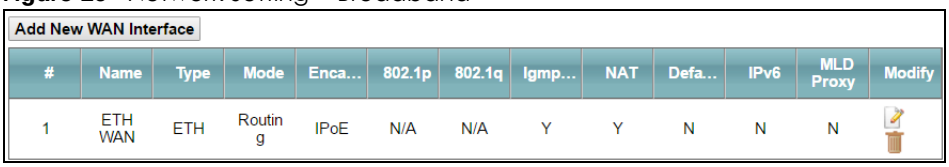
5.1.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

5.2 The Broadband Screen

Use this screen to change your EMG's Internet access settings. Click **Network Setting** > **Broadband** from the menu. The summary table shows you the configured WAN services (connections) on the EMG.

Figure 16 Network Setting > Broadband



The following table describes the labels in this screen.

Table 8 Network Setting > Broadband

LABEL	DESCRIPTION
Add New WAN Interface	Click this button to create a new connection.
#	This is the index number of the entry.
Name	This is the service name of the connection.
Type	This shows whether it is an ATM, Ethernet or a PTM connection.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.

Table 8 Network Setting > Broadband (continued)

LABEL	DESCRIPTION
802.1p	This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
802.1q	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
IGMP Proxy	This shows whether the EMG act as an IGMP proxy on this connection.
NAT	This shows whether NAT is activated or not for this connection.
Default Gateway	This shows whether the EMG use the WAN interface of this connection as the system default gateway.
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service.
MLD Proxy	This shows whether Multicast Listener Discovery (MLD) is activated or not for this connection. MLD is not available when the connection uses the bridging service.
Modify	Click the **Edit** icon to configure the WAN connection. Click the **Delete** icon to remove the WAN connection.

5.2.1 Add/Edit Internet Connection

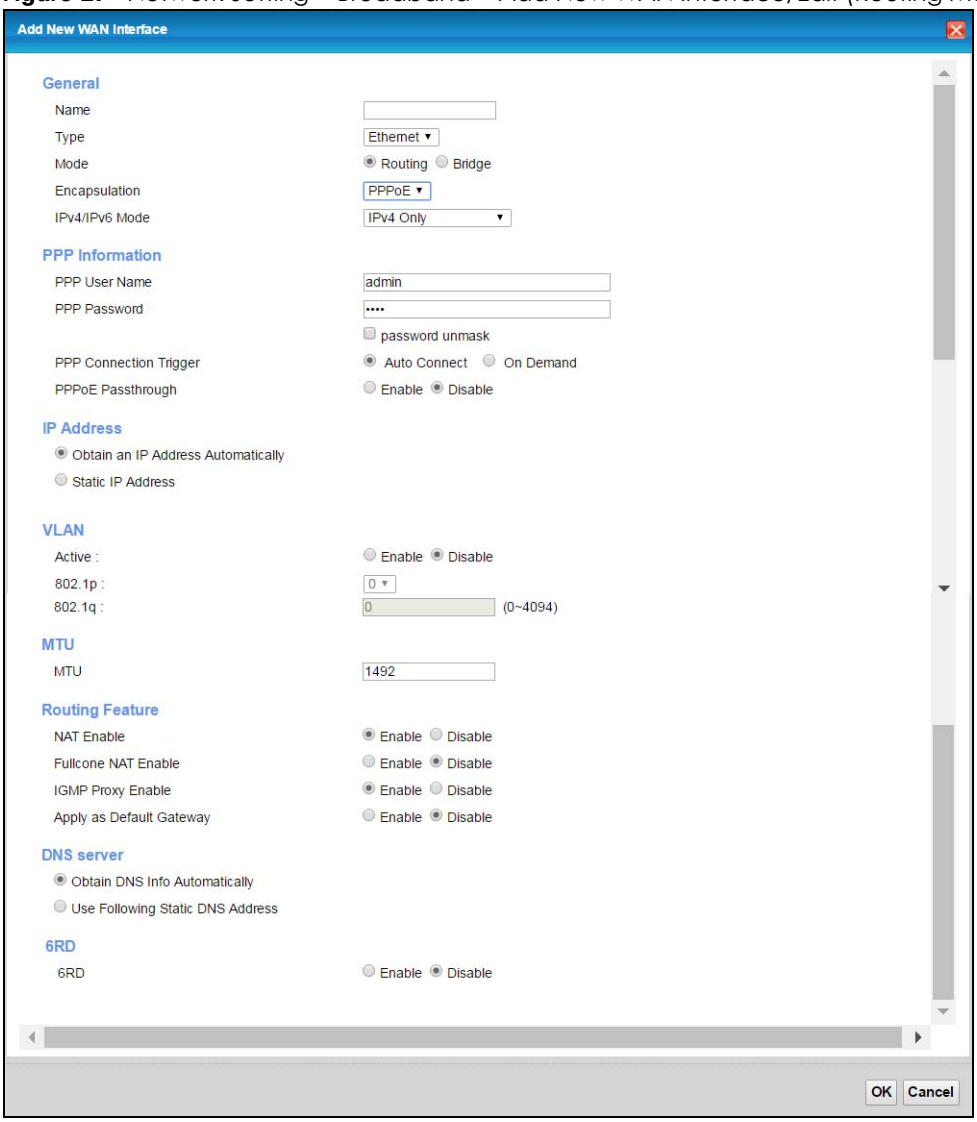
Click **Add New WAN Interface** in the **Broadband** screen or the **Edit** icon next to an existing WAN interface to configure a WAN connection. The screen varies depending on the interface type, mode, encapsulation, and IPv6/IPv4 mode you select.

5.2.1.1 Routing Mode

Use **Routing** mode if your ISP give you one IP address only and you want multiple computers to share an Internet account.

The following example screen displays when you select the **Ethernet** connection type, **Routing** mode, and **PPPoE** encapsulation. The screen varies when you select other encapsulation and IPv4/IPv6 mode.

Figure 17 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode)



The following table describes the labels in this screen.

Table 9 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode)

LABEL	DESCRIPTION
General	
Name	Specify a descriptive name for this connection.
Type	Select an Ethernet connection.
Mode	Select **Routing** if your ISP give you one IP address only and you want multiple computers to share an Internet account.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select **Routing** in the **Mode** field. The choices are **PPPoE** and **IPoE**.
IPv4/IPv6 Mode	Select **IPv4 Only** if you want the EMG to run IPv4 only. Select **IPv4 IPv6 DualStack** to allow the EMG to run IPv4 and IPv6 at the same time. Select **IPv6 Only** if you want the EMG to run IPv6 only.

Table 9 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
PPP Information (This is available only when you select **PPPoE** in the **Mode** field.)	
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above. Select **password unmask** to show your entered password in plain text.
PPP Connection Trigger	Select when to have the EMG establish the PPP connection. **Auto Connect** - select this to not let the connection time out. **On Demand** - select this to automatically bring up the connection when the EMG receives packets destined for the Internet.
Idle Timeout	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server. This field is not available if you select **On Demand** in the **PPP Connection Trigger** field.
PPPoE Passthrough	This field is available when you select **PPPoE** encapsulation. In addition to the EMG's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the EMG. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
IP Address (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Static IP Address	Select this option If the ISP assigned a fixed IP address
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the gateway IP address provided by your ISP.
VLAN	
Active	Select this to enable VLAN on this WAN interface.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
MTU	
MTU	Enter the MTU (Maximum Transfer Unit) size for this traffic.
Routing Feature (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
NAT Enable	Select this option to activate NAT on this connection.
Fullcone NAT Enable	Select this option to enable full cone NAT on this connection. This field is available only when you activate NAT. In full cone NAT, the EMG maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The EMG also maps packets coming to that external IP address and port to the internal IP address and port.

Table 9 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
IGMP Proxy Enable	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Select this option to have the EMG act as an IGMP proxy on this connection. This allows the EMG to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the EMG use the WAN interface of this connection as the system default gateway.
DNS Server (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
	Select **Obtain DNS Info Automically** if you want the EMG to use the DNS server addresses assigned by your ISP. Select **Use Following Static DNS Address** if you want the EMG to use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
Tunnel The DS-Lite (Dual Stack Lite) fields display when you set the **IPv4/IPv6 Mode** field to **IPv6 Only**. Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network. See Dual Stack Lite on page 52 for more information.	
Enable DS-Lite	This is available only when you select **IPv6 Only** in the **IPv4/IPv6 Mode** field. Select **Enable** to let local computers use IPv4 through an ISP's IPv6 network.
DS-Lite Relay Server IP	Specify the transition router's IPv6 address.
6RD The 6RD (IPv6 rapid deployment) fields display when you set the **IPv6/IPv4 Mode** field to **IPv4 Only**. See IPv6 Rapid Deployment on page 52 for more information.	
6RD	Select **Enable** to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.
	Select **Manually Configured** if you have the IPv4 address of the relay server. Otherwise, select **Automatically configured by DHCPC** to have the EMG detect it automatically through DHCP. The **Automatically configured by DHCPC** option is configurable only when you set the method of encapsulation to **IPoE**.
Service Provider IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet.
IPv4 Mask Length	Enter the subnet mask number (1~32) for the IPv4 network.
Border Relay IPv4 Address	When you select **Manually Configured**, specify the relay server's IPv4 address in this field.
DHCPC Options (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
Request Options	Select **Option 43** to have the EMG automatically add vendor specific information in the DHCP packets to request the vendor specific options from the DHCP server. Select **Option 121** to have the EMG push static routes to clients.
Sent Options	
option 60	Select this and enter the device identity you want the EMG to add in the DHCP discovery packets that go to the DHCP server.
Vendor ID	Enter the Vendor Class Identifier, such as the type of the hardware or firmware.

Table 9 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

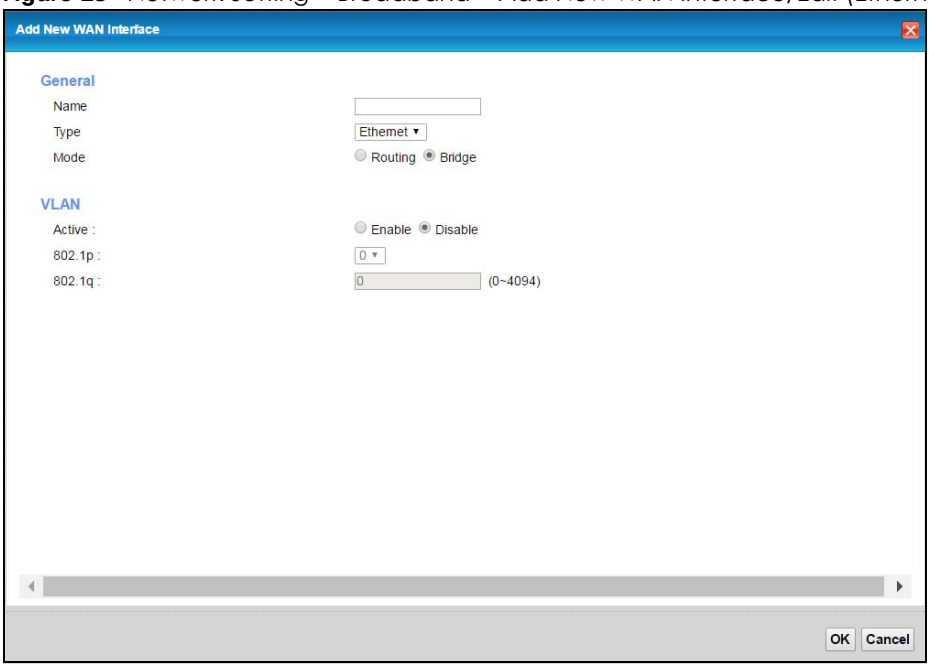
LABEL	DESCRIPTION
option 61	Select this and enter any string that identifies the device.
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DUID	Enter the hardware type, a time value and the MAC address of the device.
option 125	Select this to have the EMG automatically generate and add vendor specific parameters in the DHCP discovery packets that go to the DHCP server.
IPv6 Address (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field.)	
Obtain an IPv6 Address Automatically	Select **Obtain an IPv6 Address Automatically** if you want to have the EMG use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Static IPv6 Address	Select **Static IPv6 Address** if you have a fixed IPv6 address assigned by your ISP. When you select this, the following fields appear.
IPv6 Address	Enter an IPv6 IP address that your ISP gave to you for this WAN interface.
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
IPv6 Default Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your EMG's interface(s). The gateway helps forward packets to their destinations.
IPv6 Routing Feature (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field. You can enable IPv6 routing features in the following section.)	
MLD Proxy Enable	Select this checkbox to have the EMG act as an MLD proxy on this connection. This allows the EMG to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the EMG use the WAN interface of this connection as the system default gateway.
IPv6 DNS Server This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field. Configure the IPv6 DNS server in the following section.	
Obtain IPv6 DNS Info Automatically	Select **Obtain IPv6 DNS Info Automatically** to have the EMG get the IPv6 DNS server addresses from the ISP automatically.
Use Following Static IPv6 DNS Address	Select **Use Following Static IPv6 DNS Address** to have the EMG use the IPv6 DNS server addresses you configure manually.
Primary DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.
Apply	Click **Apply** to save your changes back to the EMG.
Cancel	Click **Cancel** to exit this screen without saving.

5.2.1.2 Bridge Mode

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **Bridge** as the encapsulation mode. The screen varies depending on the interface type you select.

If you select **Ethernet** as the interface type, the following screen appears.

Figure 18 Network Setting > Broadband > Add New WAN Interface/Edit (Ethernet-Bridge Mode)



The following table describes the fields in this screen.

Table 10 Network Setting > Broadband > Add New WAN Interface/Edit (Ethernet-Bridge)

LABEL	DESCRIPTION
General	
Name	Enter a service name of the connection.
Type	Select **Ethernet** as the interface that you want to configure.
Mode	Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
VLAN	This section is available only when you select **ADSL/VDSL over PTM** in the **Type** field.
Active	Select **Enable** to enable VLAN on this WAN interface.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

5.3 Technical Reference

The following section contains additional technical information about the EMG features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The EMG can work in bridge mode or routing mode. When the EMG is in routing mode, it supports the following methods.

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

PPP over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the EMG (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the EMG does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

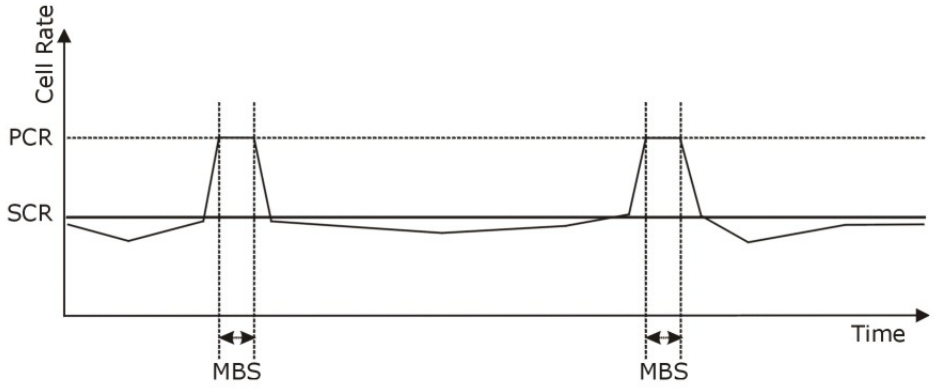
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 19 Example of Traffic Shaping



IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and default gateway.

Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

Multicast

IP packets are transmitted in either one of two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

At start up, the EMG queries all directly connected networks to gather group membership. After that, the EMG periodically updates this information.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The EMG can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the EMG's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

CHAPTER 6
Wireless

6.1 Overview

This chapter describes the EMG's **Network Setting > Wireless** screens. Use these screens to set up your EMG's wireless connection.

6.1.1 What You Can Do in this Chapter

This section describes the EMG's **Wireless** screens. Use these screens to set up your EMG's wireless connection.

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode (Section 6.2 on page 65).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the EMG (Section 6.3 on page 69).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 6.4 on page 70).
- Use the **WMM** screen to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications (Section 6.5 on page 72).
- Use the **Others** screen to configure wireless advanced features, such as the RTS/CTS Threshold (Section 6.6 on page 73).
- Use the **Channel Status** screen to scan wireless LAN channel noises and view the results (Section 6.7 on page 74).

6.1.2 What You Need to Know

Wireless Basics

"Wireless" is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwowaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there a number of wireless networking standards available with different methods of data encryption.

Finding Out More

See Section 6.8 on page 75 for advanced technical information on wireless networks.

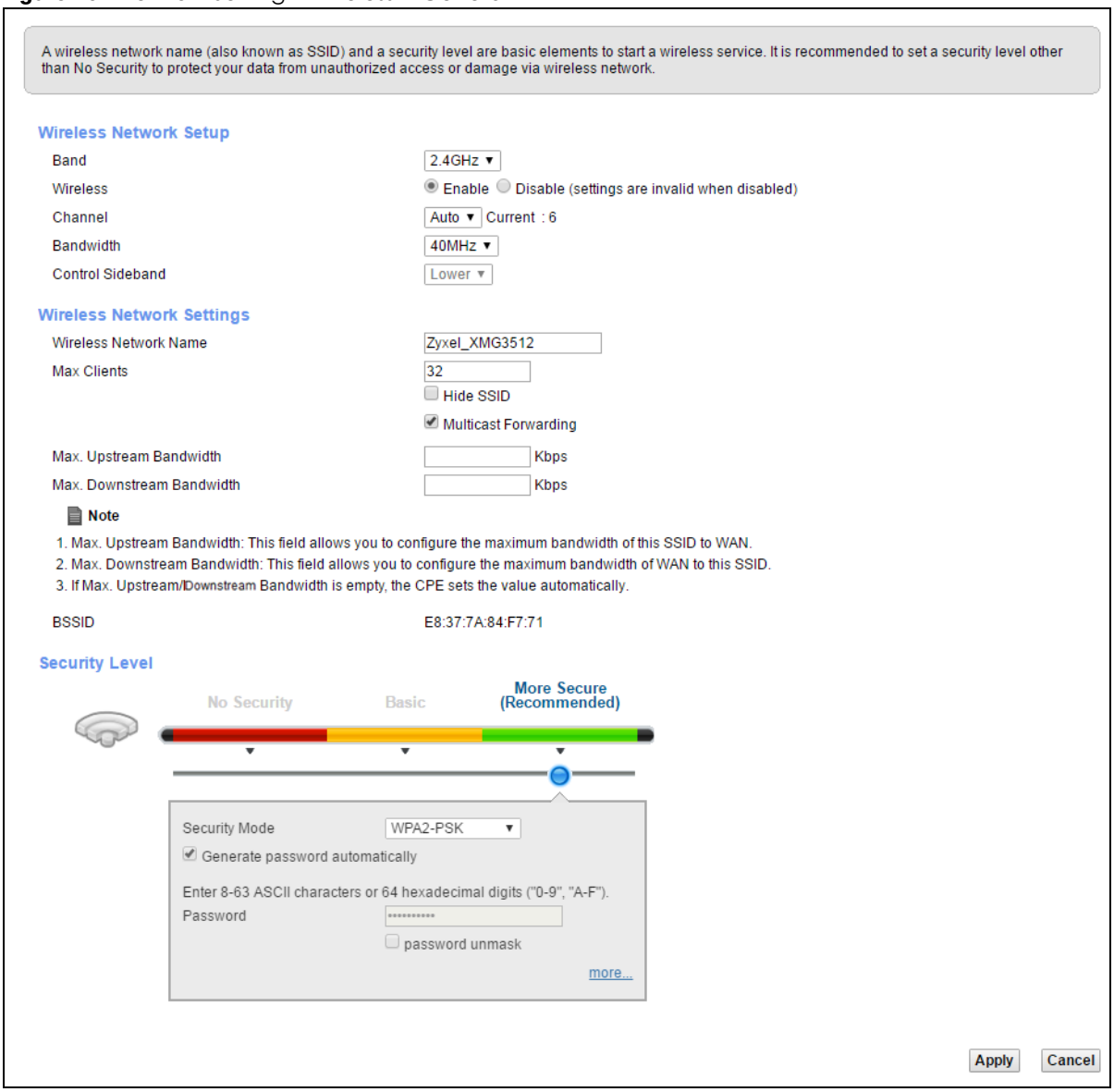
6.2 The General Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the EMG from a computer connected to the wireless LAN and you change the EMG's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the EMG's new settings.

Click **Network Setting** > **Wireless** to open the **General** screen.

Figure 20 Network Setting > Wireless > General



The following table describes the general wireless LAN labels in this screen.

Table 11 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless Network Setup	
Band	This shows the wireless band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n wireless clients while **5GHz** is used by IEEE 802.11a/ac wireless clients.
Wireless	You can **Enable** or **Disable** the wireless LAN in this field.
Channel	Use **Auto** to have the EMG automatically determine a channel to use.
Bandwidth	Select whether the EMG uses a wireless channel width of **20MHz**, **40MHz** or **80MHz**. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. An 80MHz channel groups adjacent 40MHz channels into pairs to increase bandwidth even higher. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.
Control Sideband	This is available for some regions when you select a specific channel and set the Bandwidth field to **40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
Wireless Network Settings	
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Multicast Forwarding	Select this check box to allow the EMG to convert wireless multicast traffic into wireless unicast traffic.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the EMG when wireless LAN is enabled.
Security Level	Select **Basic (WEP)** or **More Secure (WPA(2)-PSK)** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the EMG. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.2.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption or authentication.

Note: If you do not enable any wireless security on your EMG, your network is accessible to any wireless networking device that is within range.

Figure 21 Wireless > General: No Security

The following table describes the labels in this screen.

Table 12 Wireless > General: No Security

LABEL	DESCRIPTION
Security Level	Choose **No Security** to allow all wireless connections without data encryption or authentication.

6.2.2 Basic (WEP Encryption)

WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

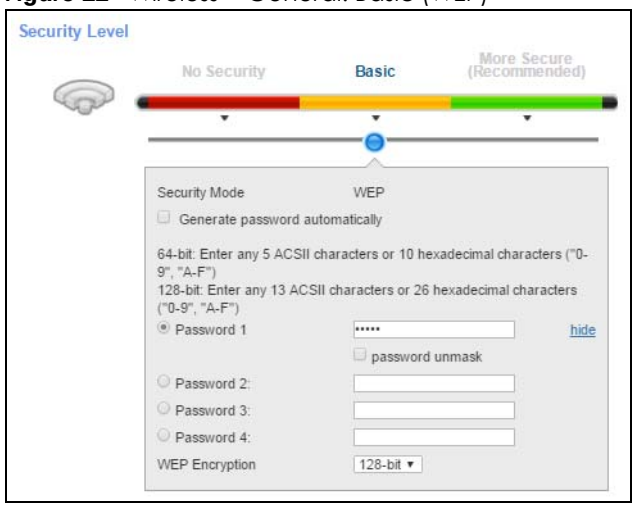
Note: WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. For example, use WPA-PSK or WPA2-PSK if all your wireless devices support it, or use WPA or WPA2 if your wireless devices support it and you have a RADIUS server. If your wireless devices support nothing stronger than WEP, use the highest encryption level available.

Your EMG allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

Note: **WEP** is not available when you set the wireless band to **5GHz**.

In order to configure and enable WEP encryption, click **Network Setting** > **Wireless** to display the **General** screen, then select **Basic** as the security level.

Figure 22 Wireless > General: Basic (WEP)



The following table describes the labels in this screen.

Table 13 Wireless > General: Basic (WEP)

LABEL	DESCRIPTION
Security Level	Select **Basic** to enable WEP data encryption.
Security Mode	This shows **WEP** when you set **Security Level** to **Basic**.
Generate password automatically	Select this option to have the EMG automatically generate a password. The password field will not be configurable when you select this option.
Password 1~4	The password (WEP keys) are used to encrypt data. Both the EMG and the wireless stations must use the same password (WEP key) for data transmission. If you chose **64-bit** WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit** WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one password, only one password can be activated at any one time. Select **password unmask** to display the entered password in plain text. Clear it to hide the password to avoid shoulder surfing.
more.../hide	Click **more...** to show more fields in this section. Click **hide** to hide them.
WEP Encryption	Select **64-bit** or **128-bit**. This dictates the length of the security key that the network is going to use.

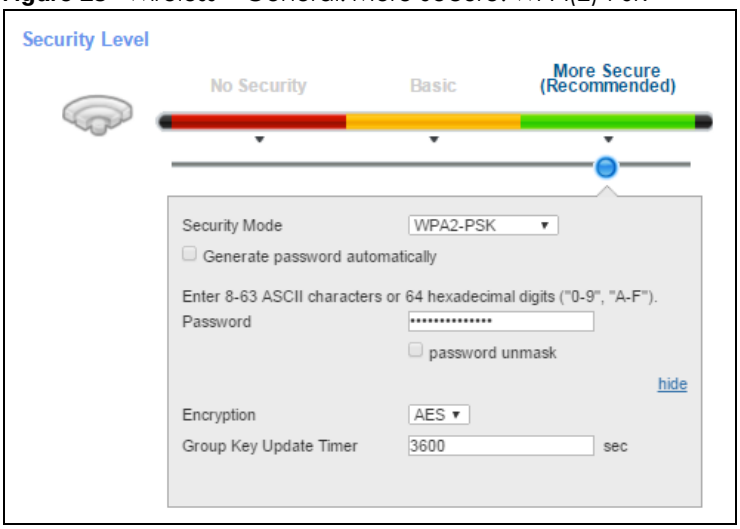
6.2.3 More Secure (WPA(2)-PSK)

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the EMG and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be.

Note: **WPA-PSK** is not available if you enable WPS before you configure them.

Click **Network Setting** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 23 Wireless > General: More Secure: WPA(2)-PSK



The following table describes the labels in this screen.

Table 14 Wireless > General: More Secure: WPA(2)-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2)-PSK data encryption.
Security Mode	Select **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
Generate password automatically	Select this option to have the EMG automatically generate a password. The password field will not be configurable when you select this option.
Password	The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. If you did not select **Generate password automatically**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters. Select **password unmask** to display the entered password in plain text. Clear it to hide the password to avoid shoulder surfing.
more.../hide	Click **more...** to show more fields in this section. Click **hide** to hide them.
Encryption	Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption. Select **TKIP** if your wireless clients can all use TKIP. Select **AES** if your wireless clients can all use AES. Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the RADIUS server sends a new group key out to all clients.

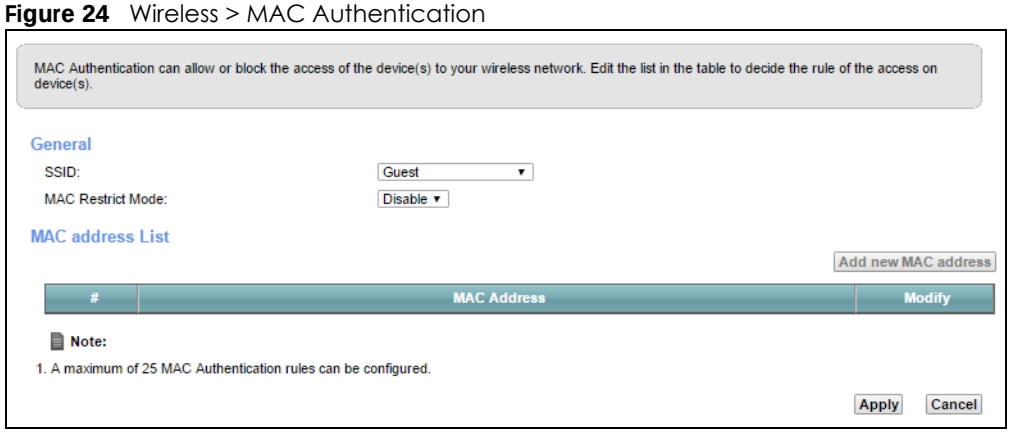
6.3 MAC Authentication

This screen allows you to configure the Zyxel Device to give exclusive access to specific devices **(Allow)** or exclude specific devices from accessing the Zyxel Device **(Deny)**. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six

pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

Use this screen to view your EMG's MAC filter settings and add new MAC filter rules. Click **Network Setting > Wireless > MAC Authentication**. The screen appears as shown.

Figure 24 Wireless > MAC Authentication



The following table describes the labels in this screen.

Table 15 Wireless > MAC Authentication

LABEL	DESCRIPTION
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Disable** to turn off MAC filtering. Select **Deny** to block access to the EMG. MAC addresses not listed will be allowed to access the EMG. Select **Allow** to permit access to the EMG. MAC addresses not listed will be denied access to the EMG.
Add new MAC address	Click this if you want to add a new MAC address entry to the MAC filter list below. Enter the MAC addresses of the wireless devices that are allowed or denied access to the EMG in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the EMG.
Modify	Click the **Edit** icon and type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc). Click the **Delete** icon to delete the entry.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

6.4 The WPS Screen

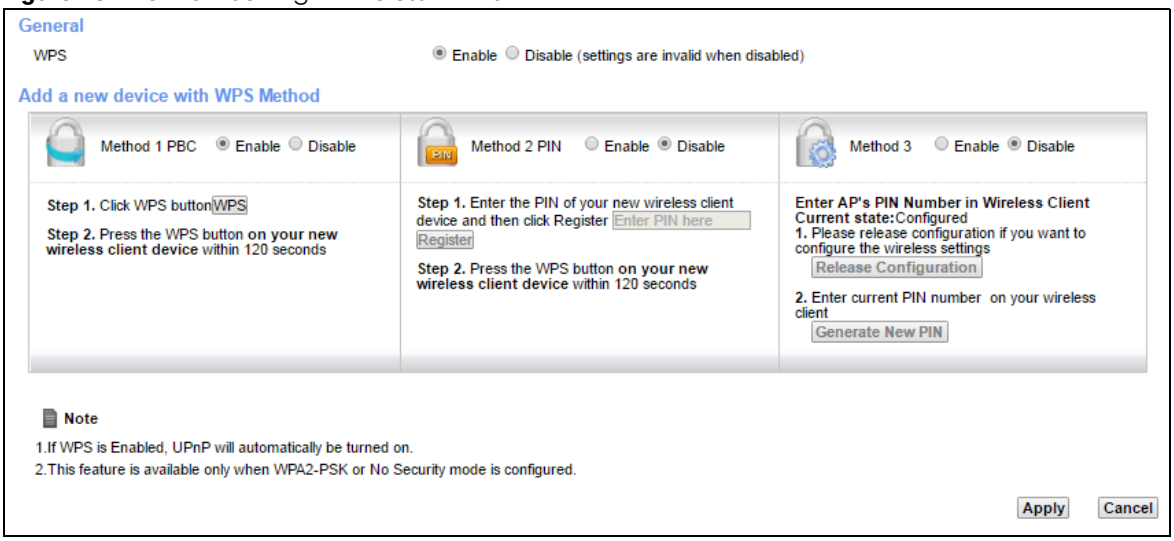
Use this screen to configure WiFi Protected Setup (WPS) on your EMG.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See Section 6.8.7.3 on page 83 for more information about WPS.

Note: The EMG applies the security settings of the **SSID1** profile (see Section 6.2 on page 65). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **WPA2-PSK** or **No Security**.

Click **Network Setting > Wireless > WPS**. The following screen displays. Select **Enable** and click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 25 Network Setting > Wireless > WPS



The following table describes the labels in this screen.

Table 16 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
General	
WPS	Select Enable to activate WPS on this EMG.
Add a new device with WPS Method	
Method 1	Use this section to set up a WPS wireless network using Push Button Configuration (PBC). Select **Enable** and click **Apply** to activate WPS method 1 on the EMG.
WPS	Click this button to add another WPS-enabled wireless device (within wireless range of the EMG) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **WPS** button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Method 2	Use this section to set up a WPS wireless network by entering the PIN of the client into the EMG. Select **Enable** and click **Apply** to activate WPS method 2 on the EMG.
Register	Enter the PIN of the device that you are setting up a WPS connection with and click **Register** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the EMG.

Table 16 Network Setting > Wireless > WPS (continued)

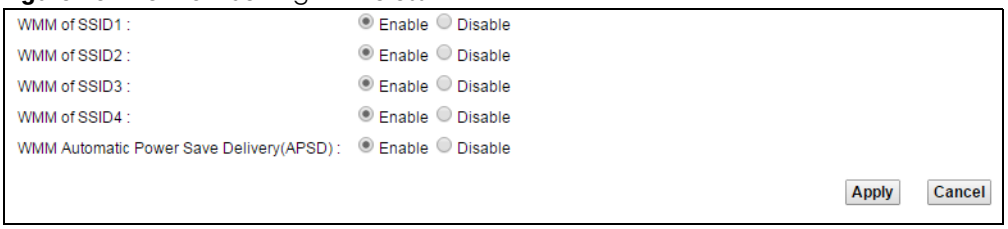
LABEL	DESCRIPTION
Method 3	Use this section to set up a WPS wireless network by entering the PIN of the EMG into the client. Select **Enable** and click **Apply** to activate WPS method 3 on the EMG.
Release Configuration	The default WPS status is configured. Click this button to remove all configured wireless and wireless security settings for WPS connections on the EMG.
Generate New PIN Number	If this method has been enabled, the PIN (Personal Identification Number) of the EMG is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method. Click the **Generate New PIN** button to have the EMG create a new PIN.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.5 The WMM Screen

Use this screen to enable Wi-Fi MultiMedia (WMM) and WMM Power Save in wireless networks for multimedia applications.

Click **Network Setting > Wireless > WMM**. The following screen displays.

Figure 26 Network Setting > Wireless > WMM



The following table describes the labels in this screen.

Table 17 Network Setting > Wireless > WMM

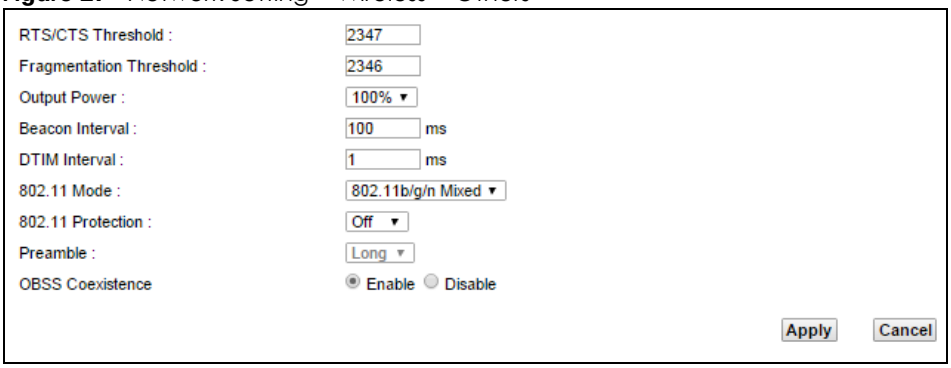
LABEL	DESCRIPTION
2.4GHz WMM Setup / 5GHz WMM Setup	
WMM of SSID1~4	Select **On** to have the EMG automatically give the wireless network (SSIDx) a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
WMM Automatic Power Save Delivery(APSD)	Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The EMG goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the EMG until the EMG "wakes up". The EMG wakes up periodically to check for incoming data. Note: This works only if the wireless device to which the EMG is connected also supports this feature.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.6 The Others Screen

Use this screen to configure advanced wireless settings. Click **Network Setting > Wireless > Others**. The screen appears as shown.

See Section 6.8.2 on page 77 for detailed definitions of the terms listed in this screen.

Figure 27 Network Setting > Wireless > Others



The following table describes the labels in this screen.

Table 18 Network Setting > Wireless > Others

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Output Power	Set the output power of the EMG. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: **20%**, **40%**, **60%**, **80%** or **100%**.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 50ms to 1000ms. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the EMG. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the EMG. Select **802.11n Only** to allow only IEEE 802.11n compliant WLAN devices to associate with the EMG. Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the EMG. The transmission rate of your EMG might be reduced. Select **802.11b/g/n Mixed** to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the EMG. The transmission rate of your EMG might be reduced.

Table 18 Network Setting > Wireless > Others (continued)

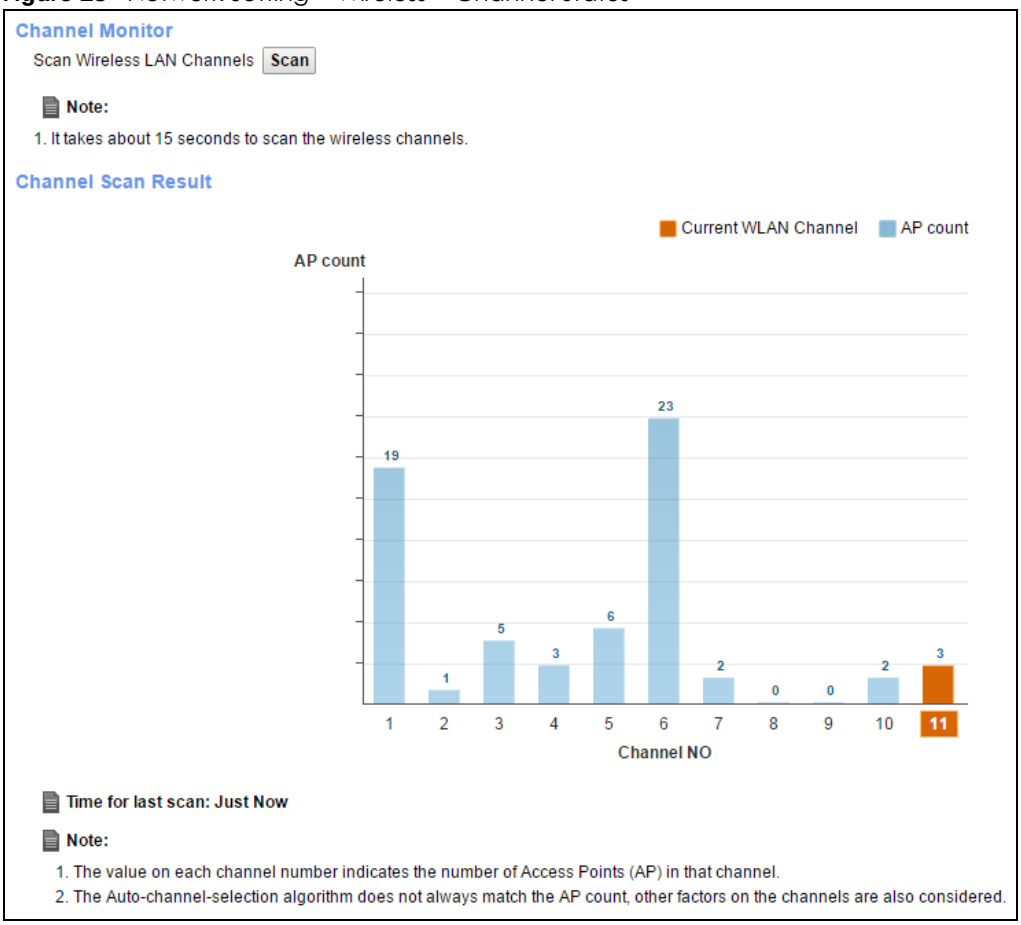
LABEL	DESCRIPTION
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select **Off** to disable 802.11 protection. The transmission rate of your EMG might be reduced in a mixed-mode network. This field displays **Off** and is not configurable when you set **802.11 Mode** to **802.11b Only**.
Preamble	Select a preamble type from the drop-down list box. Choices are **Long** or **Short**. See Section 6.8.6 on page 80 for more information. This field is configurable only when you set 802.11 Mode to **802.11b**.
OBSS Coexistence	Select **Enable** to allow the coexistence of 20 MHz and 40 MHz Overlapping Basic Service Sets (OBSS) in wireless local area networks. Select **Disabled** to disable this feature.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.7 The Channel Status Screen

Use the **Channel Status** screen to scan wireless LAN channel noises and view the results. Click **Network Setting > Wireless > Channel Status**. The screen appears as shown. Click **Scan** to scan the wireless LAN channels. You can view the results in the **Channel Scan Result** section.

Note: The **Scan** button only works when the EMG uses 20MHz for the wireless channel width. You can go to the **Network Setting > Wireless > General** screen, click the **more** link, and then change the channel width setting in the **Bandwidth** field.

Figure 28 Network Setting > Wireless > Channel Status



6.8 Technical Reference

This section discusses wireless LANs in depth. For more information, see Appendix B on page 222.

6.8.1 Wireless Network Overview

Wireless networks consist of wireless clients, access points and bridges.

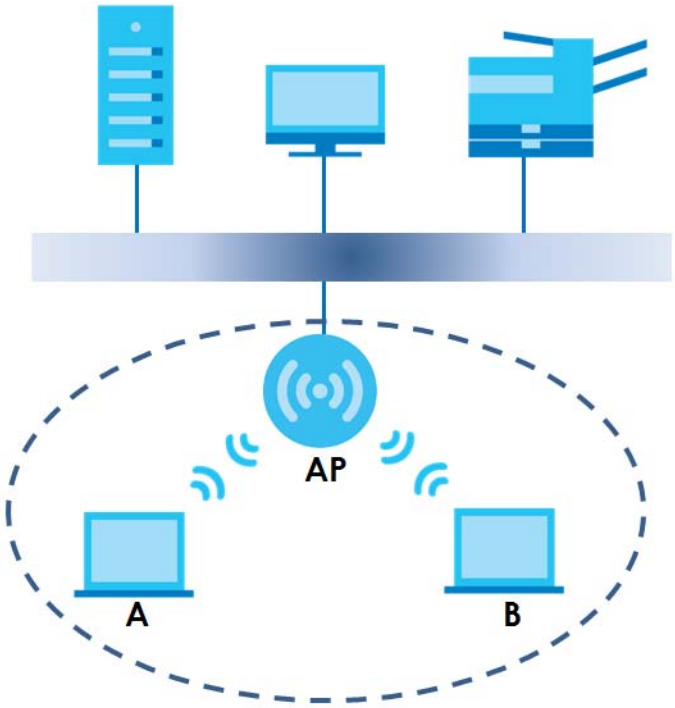
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 29 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your EMG is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentifier.
- If two wireless networks overlap, they should use a different channel.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

6.8.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the EMG's Web Configurator.

Table 19 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the EMG. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the EMG.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the EMG does, it cannot communicate with the EMG.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

6.8.3 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is

Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

6.8.3.1 SSID

Normally, the EMG acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the EMG does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

6.8.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the EMG which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

6.8.3.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

6.8.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See Section 6.8.3.3 on page 78 for information about this.)

Table 20 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
↕	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the EMG and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your EMG, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the EMG.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

6.8.4 Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

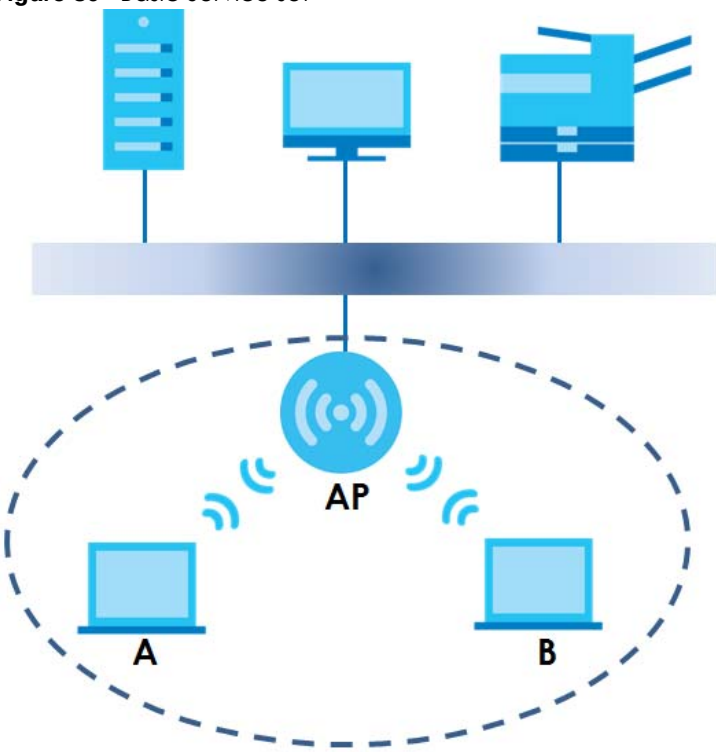
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

6.8.5 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 30 Basic Service set



6.8.6 Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the EMG uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

6.8.7 WiFi Protected Setup (WPS)

Your EMG supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

6.8.7.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the EMG, see Section 6.5 on page 72).
3. Press the button on one of the devices (it doesn't matter which). For the EMG you must press the WPS button for more than five seconds.
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

   If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

6.8.7.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

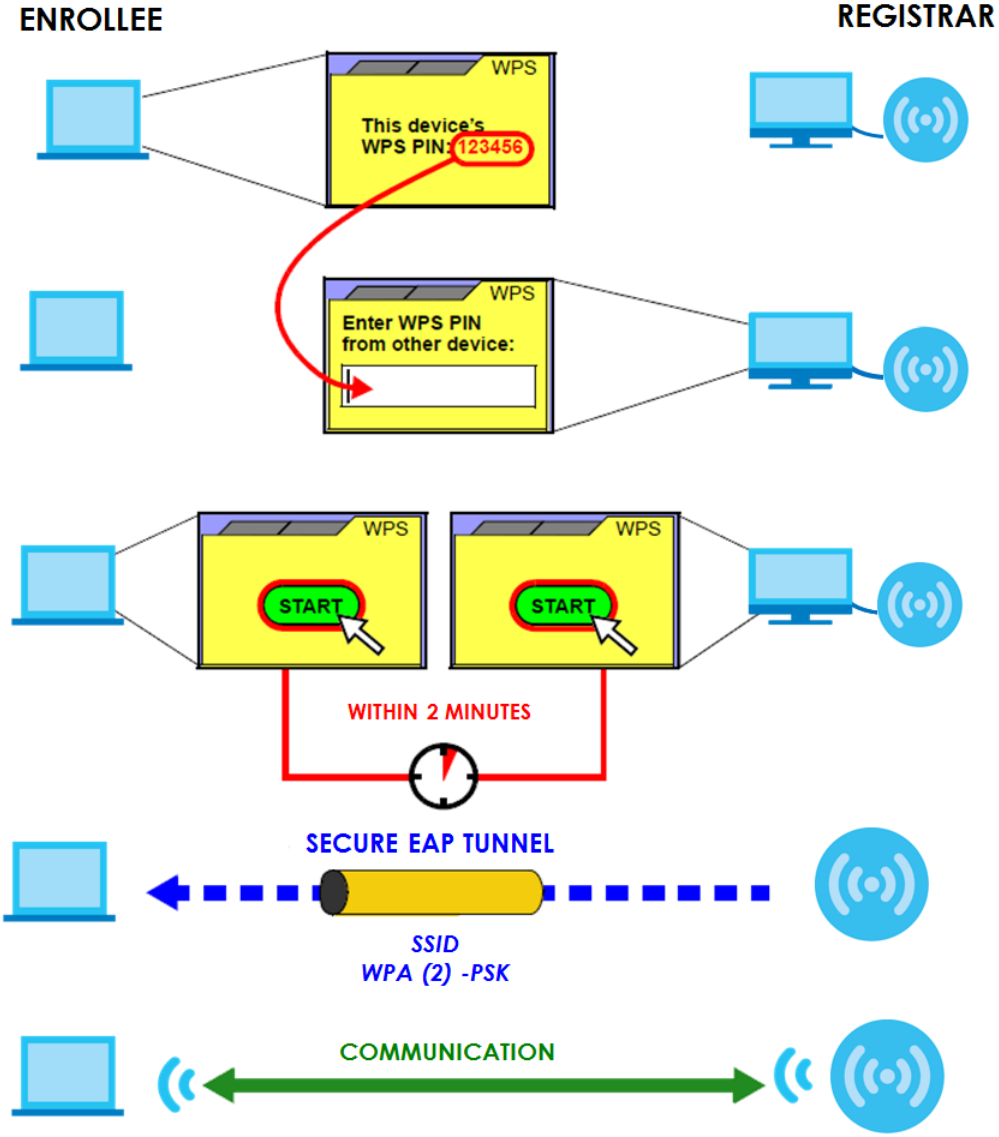
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

1. Ensure WPS is enabled on both devices.
2. Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
3. Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the EMG, see Section 6.4 on page 70).
4. Enter the client's PIN in the AP's configuration interface.
5. If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
6. Start WPS on both devices within two minutes.
7. Use the configuration utility to activate WPS, not the push-button on the device itself.
8. On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

   If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

   The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 31 Example WPS Process: PIN Method

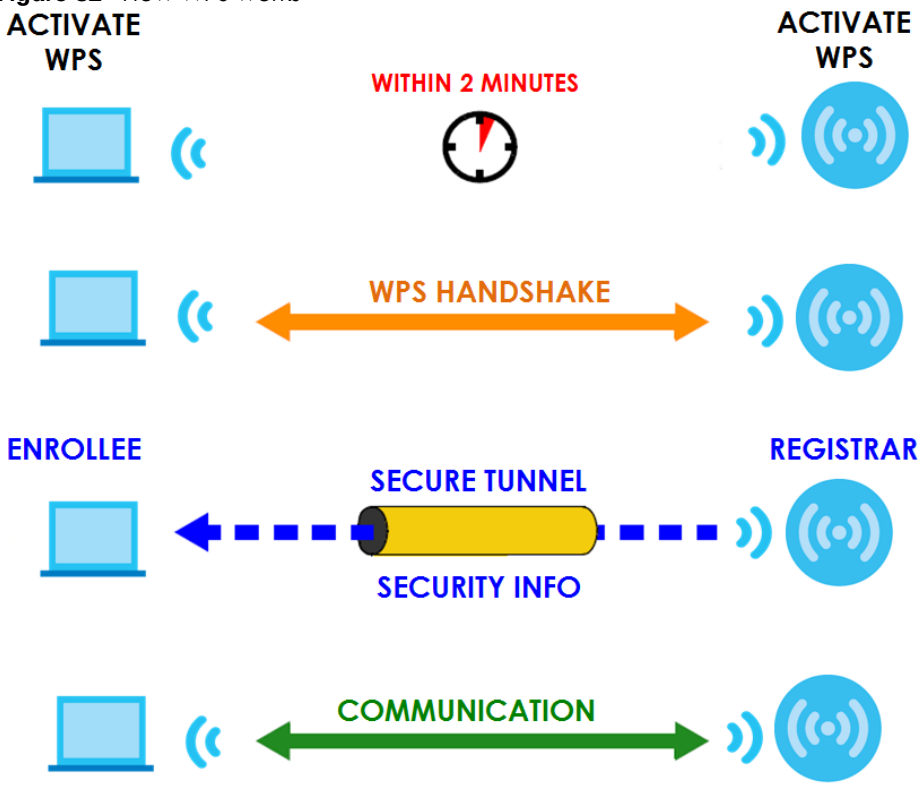


6.8.7.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 32 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

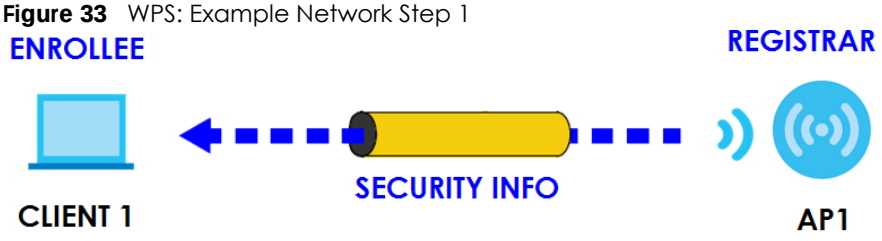
By default, a WPS devices is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes "configured". A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

6.8.7.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

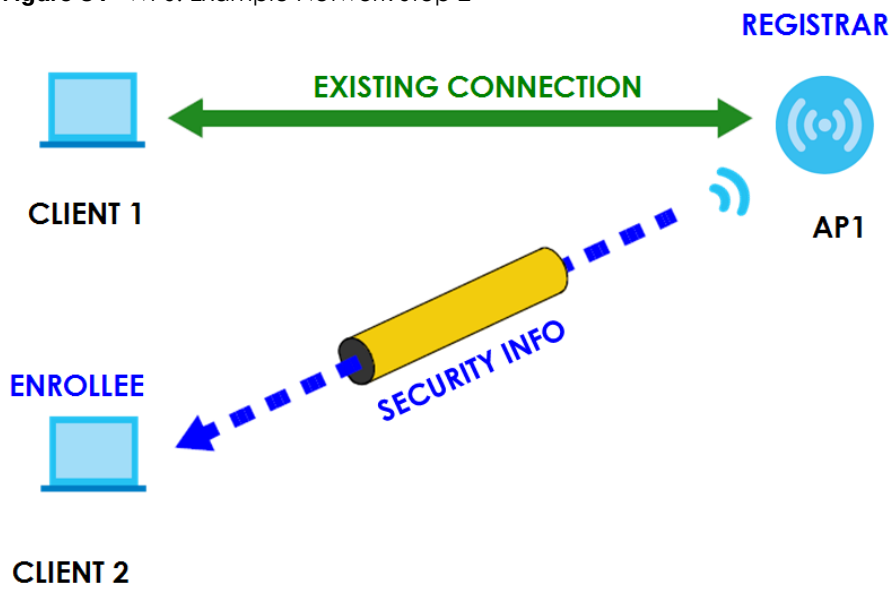
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 33 WPS: Example Network Step 1



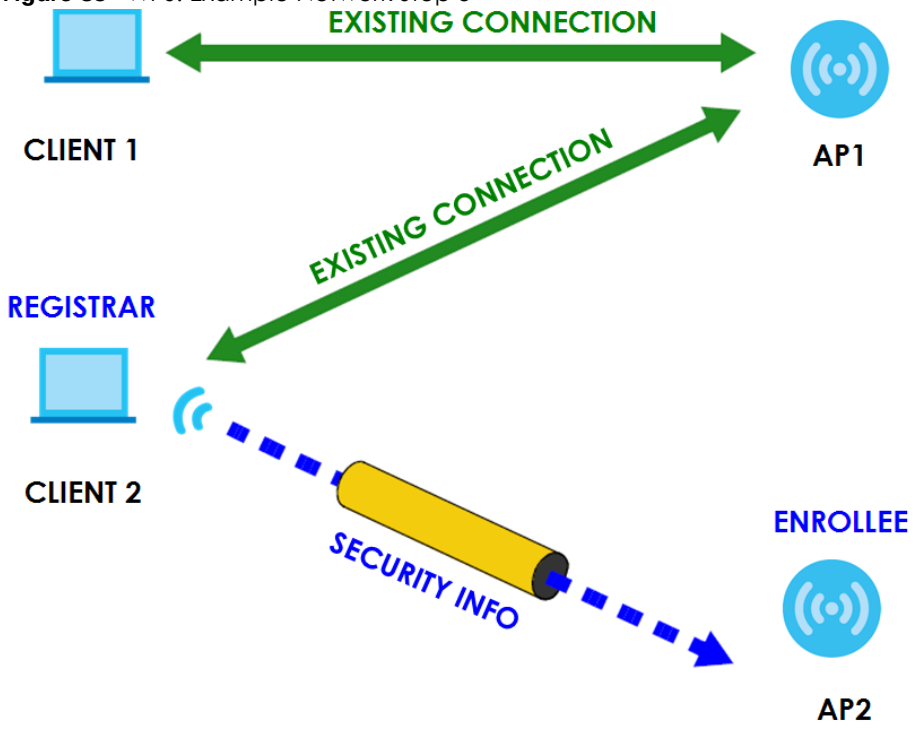
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 34 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 35 WPS: Example Network Step 3



6.8.7.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).
- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access

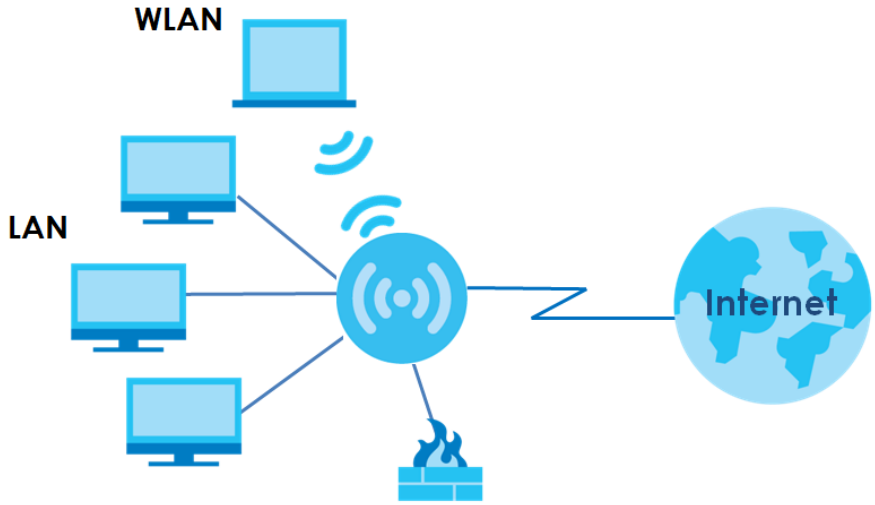
point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

CHAPTER 7
Home Networking

7.1 Overview

A Local Area Network (LAN) is a shared communication system to which many networking devices are connected. It is usually located in one immediate area such as a building or floor of a building.

Use the LAN screens to help you configure a LAN DHCP server and manage IP addresses.



7.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings of your EMG (Section 7.2 on page 90).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 7.3 on page 94).
- Use the **UPnP** screen to enable UPnP and UPnP NAT traversal on the EMG (Section 7.4 on page 95).
- Use the **Additional Subnet** screen to configure IP alias and public static IP (Section 7.5 on page 98).
- Use the **STB Vendor ID** screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the EMG automatically create static DHCP entries for the STB devices when they request IP addresses (Section 7.6 on page 99).
- Use the **Wake on LAN** screen to remotely turn on a device on the network. (Section 7.7 on page 99).
- Use the **TFTP Server Name** screen to set a TFTP server address which is passed to the clients using DHCP option 66. (Section 7.8 on page 100).

7.1.2 What You Need To Know

7.1.2.1 About LAN

IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet Mask

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your EMG an IP address, subnet mask, DNS and other routing information when it's turned on.

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a networking device before you can access it.

RADVD (Router Advertisement Daemon)

When an IPv6 host sends a Router Solicitation (RS) request to discover the available routers, RADVD with Router Advertisement (RA) messages in response to the request. It specifies the minimum and maximum intervals of RA broadcasts. RA messages containing the address prefix. IPv6 hosts can be generated with the IPv6 prefix an IPv6 address.

7.1.2.2 About UPnP

Identifying UPnP Devices

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses

- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the Chapter 10 on page 127 for more information on NAT.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the EMG allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and Zyxel

Zyxel has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). Zyxel's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See Section 7.4.1 on page 96 for examples of installing and using UPnP.

Finding Out More

See Section 7.9 on page 100 for technical background information on LANs.

7.1.3 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

7.2 The LAN Setup Screen

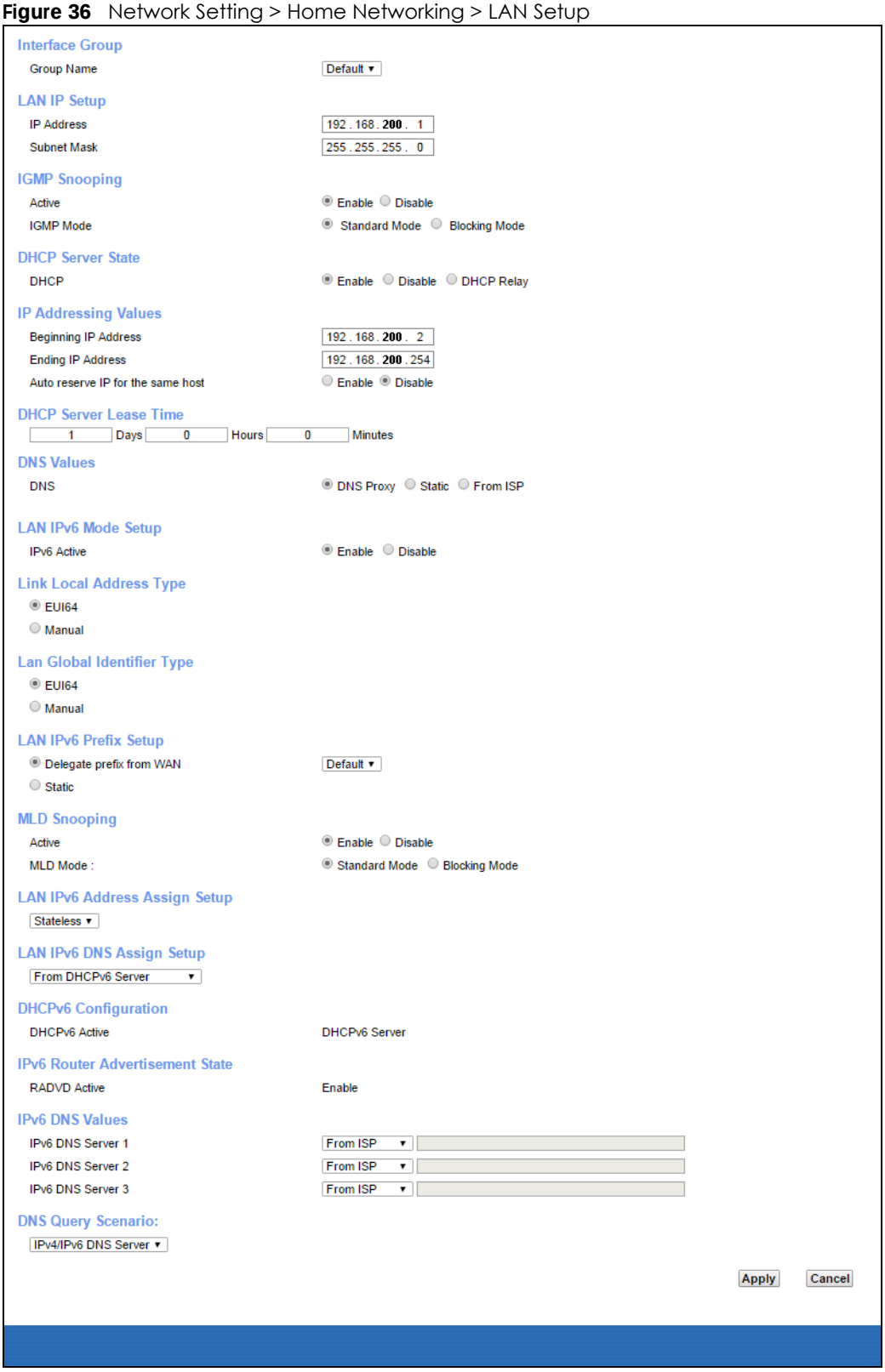
Use this screen to set the Local Area Network IP address and subnet mask of your EMG. Click **Network Setting > Home Networking** to open the **LAN Setup** screen.

Follow these steps to configure your LAN settings.

1. Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your EMG.
2. Enter the IP subnet mask into the **Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.

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

Figure 36 Network Setting > Home Networking > LAN Setup



The following table describes the fields in this screen.

Table 21 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group name for which you want to configure LAN settings. See Chapter 13 on page 149 for how to create a new interface group.
LAN IP Setup	
IP Address	Enter the LAN IPv4 address you want to assign to your EMG in dotted decimal notation, for example, 192.168.200.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your EMG automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
IGMP Snooping	
Active	Select **Enable** to allows the EMG to passively learn multicast group.
IGMP Mode	Select **Standard Mode** to allow the EMG to forward traffic only to ports that want to receive it. Select **Blocking Mode** to allow the EMG to block unknown muticast adresses.
DHCP Server State	
DHCP	Select **Enable** to have the EMG act as a DHCP server or DHCP relay agent. Select **Disable** to stop the DHCP server on the EMG. Select **DHCP Relay** to have the EMG forward DHCP request to the DHCP server.
DHCP Relay Server Address	This field is only available when you select **DHCP Relay** in the **DHCP** field.
IP Address	Enter the IPv4 address of the actual remote DHCP server in this field.
IP Addressing Values	This field is only available when you select **Enable** in the **DHCP** field.
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Select **Enable** to have the EMG record DHCP IP addresses with the MAC addresses the IP addresses are assigned to. The EMG assigns the same IP address to the same MAC address when the host requests an IP address again through DHCP.
DHCP Server Lease Time	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems. This field is only available when you select **Enable** in the **DHCP** field.
Days/Hours/ Minutes	Enter the lease time of the DHCP server.
DNS Values	This field is only available when you select **Enable** in the **DHCP** field.
DNS	Select **From ISP** if your ISP dynamically assigns DNS server information. Select **DNS Proxy** if you have the DNS proxy service. The EMG redirects clients' DNS queries to a DNS server for resolving domain names. Select **Static** if you have the IP address of a DNS server.
DNS Server 1/2	This field is only available when you select **Static** in the **DNS** field. Enter the first and second DNS (Domain Name System) server IP addresses the EMG passes to the DHCP clients.

Table 21 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
LAN IPv6 Mode Setup	
IPv6 Active	Select **Enable** to activate the IPv6 mode and configure IPv6 settings on the EMG.
Link Local Address Type	
EUI64	Select this to have the EMG generate an interface ID for the LAN interface's link-local address using the EUI-64 format.
Manual	Select this to manually enter an interface ID for the LAN interface's link-local address.
Lan Global Identifier Type	
EUI64	Select this to have the EMG generate an interface ID using the EUI-64 format for its global address .
Manual	Select this to manually enter an interface ID for the LAN interface's global IPv6 address.
LAN IPv6 Prefix Setup	
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 address for the EMG's LAN IPv6 address.
MLD Snooping	Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.
Active	Select **Enable** to activate MLD Snooping on the EMG. This allows the EMG to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.
MLD Mode	Select **Standard Mode** to allow the EMG to forward MLD packets only to ports that want to receive it. Select **MLD Mode** to allow the EMG to block MLD packets for a specific multicast group.
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: • **Stateless**: The EMG uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the EMG send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. • **Stateful**: The EMG uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the EMG act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.
LAN IPv6 DNS Assign Setup	Select how the EMG provide DNS server and domain name information to the clients: • **From Router Advertisement**: The EMG provides DNS information through router advertisements. • **From DHCPv6 Server**: The EMG provides DNS information through DHCPv6. • **From RA & DHCPv6 Server**: The EMG provides DNS information through both router advertisements and DHCPv6.
DHCPv6 Configuration	
DHCPv6 Active	This shows the status of the DHCPv6. **DHCPv6 Server** displays if you configured the EMG to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients.
IPv6 Router Advertisement State	
RADVD Active	This shows whether RADVD is enabled or not.
IPv6 DNS Values	
IPv6 DNS Server 1-3	Select **From ISP** if your ISP dynamically assigns IPv6 DNS server information. Select **User-Defined** if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the EMG passes to the DHCP clients. Select **None** if you do not want to configure IPv6 DNS servers.

Table 21 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DNS Query Scenario	Select how the EMG handles clients' DNS information requests. • **IPv4/IPv6 DNS Server**: The EMG forwards the requests to both the IPv4 and IPv6 DNS servers and sends clients the first DNS information it receives. • **IPv6 DNS Server Only**: The EMG forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives. • **IPv4 DNS Server Only**: The EMG forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives. • **IPv6 DNS Server First**: The EMG forwards the requests to the IPv6 DNS server first and then the IPv4 DNS server. Then it sends clients the first DNS information it receives. • **IPv4 DNS Server First**: The EMG forwards the requests to the IPv4 DNS server first and then the IPv6 DNS server. Then it sends clients the first DNS information it receives.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

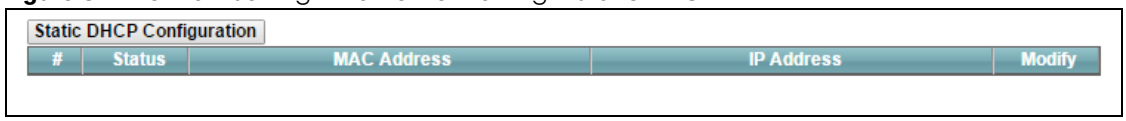
7.3 The Static DHCP Screen

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Use this screen to change your EMG's static DHCP settings. Click **Network Setting > Home Networking > Static DHCP** to open the following screen.

Figure 37 Network Setting > Home Networking > Static DHCP



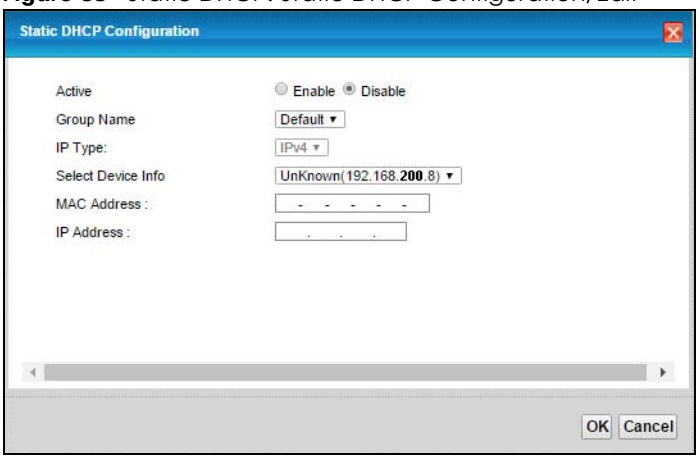
The following table describes the labels in this screen.

Table 22 Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Static DHCP Configuration	Click this to add a new static DHCP entry.
#	This is the index number of the entry.
Status	This field displays whether the client is connected to the EMG.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address relative to the # field listed above.
Modify	Click the **Edit** icon to have the IP address field editable and change it. Click the **Delete** icon to delete a static DHCP entry. A window displays asking you to confirm that you want to delete the selected entry.

If you click **Static DHCP Configuration** in the **Static DHCP** screen or the Edit icon next to a static DHCP entry, the following screen displays.

Figure 38 Static DHCP: Static DHCP Configuration/Edit



The following table describes the labels in this screen.

Table 23 Static DHCP: Static DHCP Configuration/Edit

LABEL	DESCRIPTION
Active	Select **Enable** to activate the connection between the client and the EMG.
Group Name	Select the interface group name for which you want to configure static DHCP settings. See Chapter 13 on page 149 for how to create a new interface group.
IP Type	This field displays **IPv4** for the type of the DHCP IP address. At the time of writing, it is not allowed to select other type.
Select Device Info	Select a device or computer from the drop-down list or select **Manual Input** to manually enter a device's MAC address and IP address in the following fields.
MAC Address	If you select **Manual Input**, enter the MAC address of a computer on your LAN.
IP Address	If you select **Manual Input**, enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

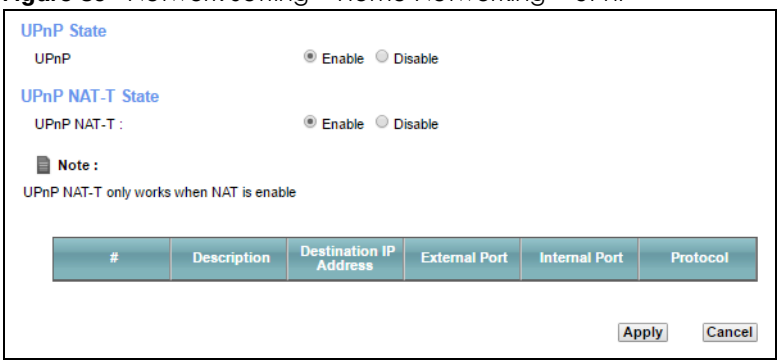
7.4 The UPnP Screen

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

See page 89 for more information on UPnP.

Use the following screen to configure the UPnP settings on your EMG. Click **Network Setting > Home Networking > UPnP** to display the screen shown next.

Figure 39 Network Setting > Home Networking > UPnP



The following table describes the labels in this screen.

Table 24 Network Setting > Home Networking > UPnP

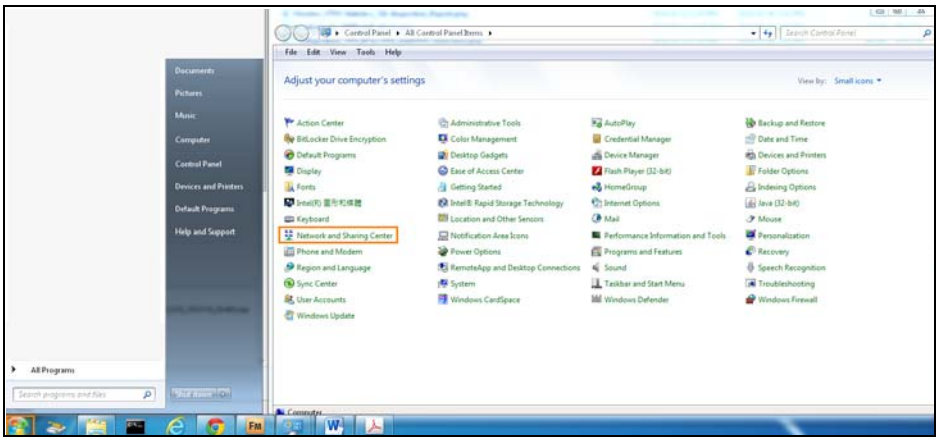
LABEL	DESCRIPTION
UPnP State	
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the EMG's IP address.
UPnP NAT-T State	
UPnP NAT-T	Select **Enable** to allow UPnP-enabled applications to automatically configure the EMG so that they can communicate through the EMG by using NAT traversal. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application. The table below displays the NAT port forwarding rules added automatically by UPnP NAT-T.
#	This is the index number of the UPnP NAT-T connection.
Description	This is the description of the UPnP NAT-T connection.
Destination IP Address	This is the IP address of the other connected UPnP-enabled device.
External Port	This is the external port number that identifies the service.
Internal Port	This is the internal port number that identifies the service.
Protocol	This is the transport layer protocol used for the service.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

7.4.1 Turning On UPnP in Windows 7 Example

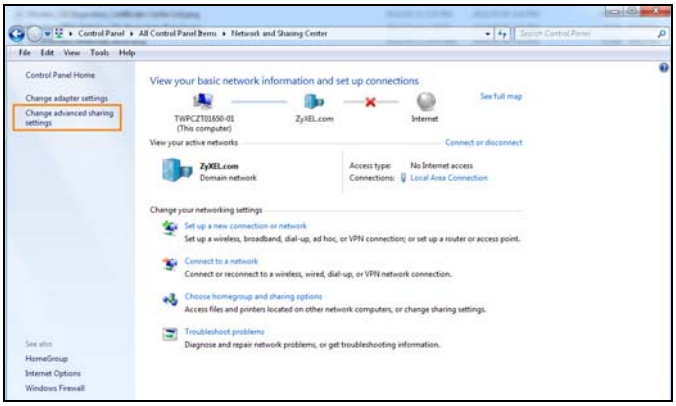
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the EMG.

Make sure the computer is connected to a LAN port of the EMG. Turn on your computer and the EMG.

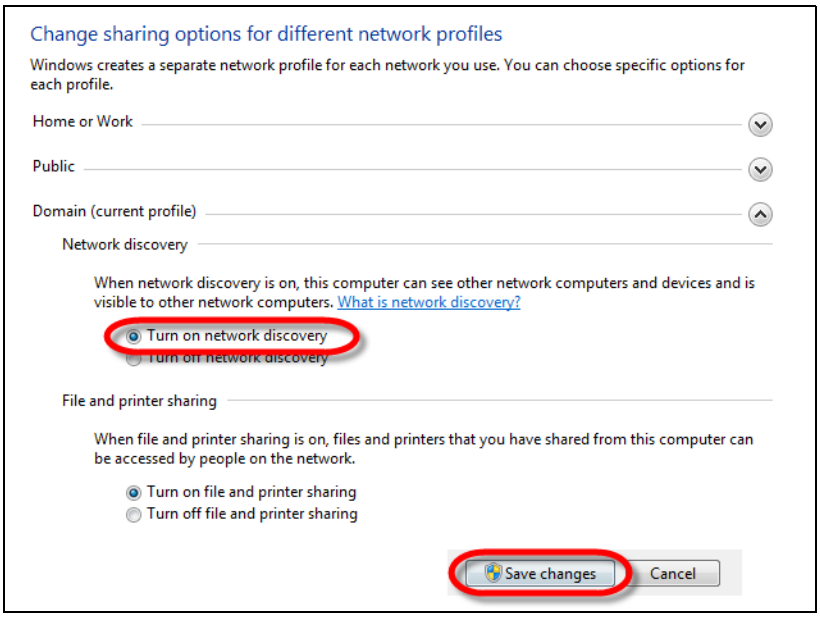
1 Click the start icon, **Control Panel** and then the **Network and Sharing Center.**



2 Click **Change Advanced Sharing Settings**.



3 Select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.



7.5 The Additional Subnet Screen

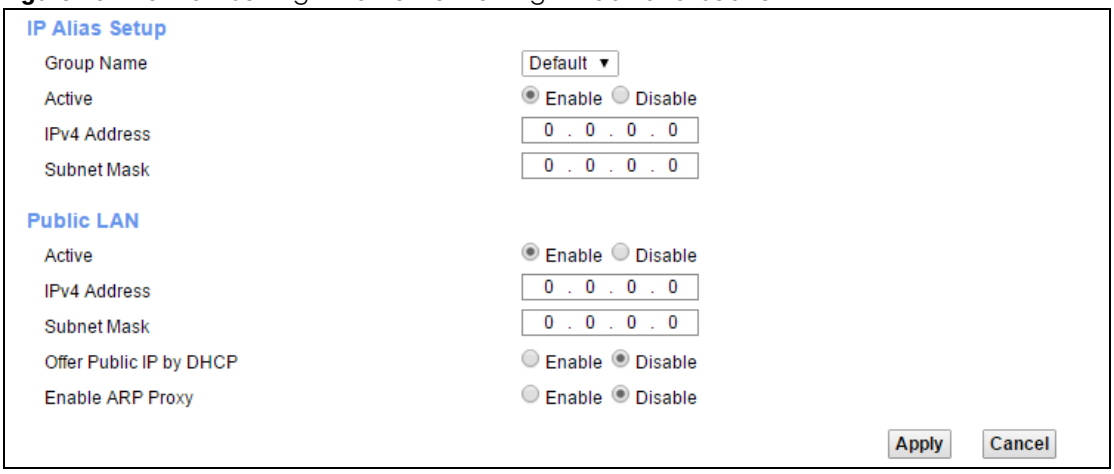
Use the **Additional Subnet** screen to configure IP alias and public static IP.

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The EMG supports multiple logical LAN interfaces via its physical Ethernet interface with the EMG itself as the gateway for the LAN network. When you use IP alias, you can also configure firewall rules to control access to the LAN's logical network (subnet).

If your ISP provides the Public LAN service, the EMG may use an LAN IP address that can be accessed from the WAN.

Click **Network Setting > Home Networking > Additional Subnet** to display the screen shown next.

Figure 40 Network Setting > Home Networking > Additional Subnet



The following table describes the labels in this screen.

Table 25 Network Setting > Home Networking > Additional Subnet

LABEL	DESCRIPTION
IP Alias Setup	
Group Name	Select the interface group name for which you want to configure the IP alias settings. See Chapter 13 on page 149 for how to create a new interface group.
Active	Select **Enable** to configure a LAN network for the EMG.
IPv4 Address	Enter the IP address of your EMG in dotted decimal notation.
Subnet Mask	Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default).
Public LAN	
Active	Select **Enable** to enable the Public LAN feature. Your ISP must support Public LAN and Static IP.
IPv4 Address	Enter the public IP address provided by your ISP.
Subnet Mask	Enter the public IPv4 subnet mask provided by your ISP.
Offer Public IP by DHCP	Select **Enable** to enable the EMG to provide public IP addresses by DHCP server.
Enable ARP Proxy	Select **Enable** to enable the ARP (Address Resolution Protocol) proxy.

Table 25 Network Setting > Home Networking > Additional Subnet (continued)

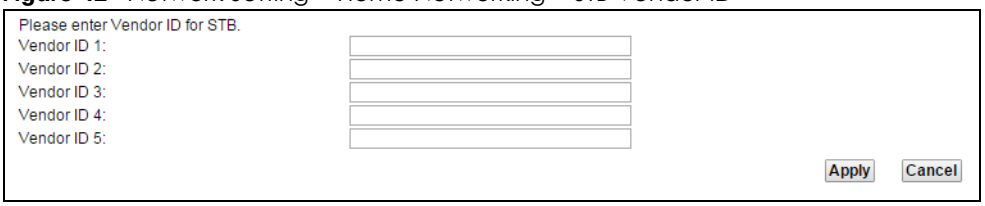
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

7.6 The STB Vendor ID Screen

Set Top Box (STB) devices with dynamic IP addresses sometimes don't renew their IP addresses before the lease time expires. This could lead to IP address conflicts if the STB continues to use an IP address that gets assigned to another device. Use this screen to configure the Vendor IDs of connected STBs, which have the EMG automatically created static DHCP entries for them when they request IP addresses.

Click **Network Setting** > **Home Networking** > **STB Vendor ID** to open this screen.

Figure 41 Network Setting > Home Networking > STB Vendor ID



The following table describes the labels in this screen.

Table 26 Network Setting > Home Networking > STB Vendor ID

LABEL	DESCRIPTION
Vendor ID 1~5	These are STB's Vendor Class Identifiers (DHCP option 60). A Vendor Class Identifier is usually used to inform the DHCP server a DHCP client's vendor and functionality.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

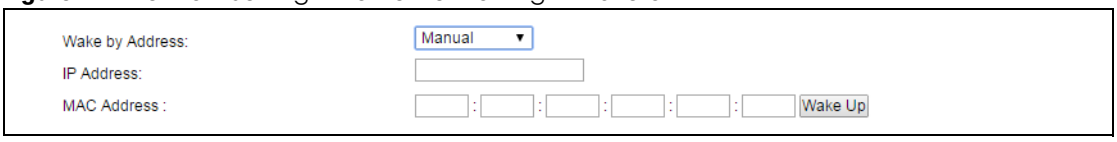
7.7 The Wake on LAN Screen

Use this screen to turn on a device on the LAN network. To use this feature, the remote device must also support Wake On LAN.

You need to know the MAC address of the LAN device. It may be on a label on the device or in its documentation.

Click **Network Setting** > **Home Networking** > **Wake on LAN** to open this screen.

Figure 42 Network Setting > Home Networking > Wake on LAN



The following table describes the labels in this screen.

Table 27 Network Setting > Home Networking > Wake on LAN

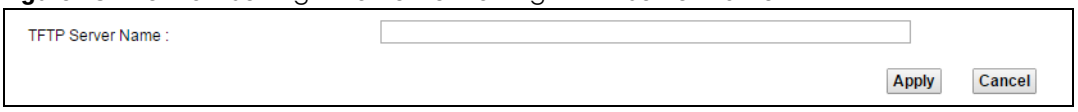
LABEL	DESCRIPTION
Wake by Address	Select **Manual** and enter the IP address or MAC address of the device to turn it on remotely. The drop-down list also lists the IP addresses that can be found in the EMG's ARP table. Select an IP address and it will then automatically update the IP address and MAC address in the following fields.
IP Address	Enter the IPv4 IP address of the device to turn it on.
MAC Address	Enter the MAC address of the device to turn it on. A MAC address consists of six hexadecimal character pairs.
Wake up	Click this to send a wake up packet to wake up the specified device.

7.8 The TFTP Server Name Screen

Use the **TFTP Server Name** screen to set the TFTP server address which is passed to the clients using DHCP option 66. The DHCP clients in the EMG local network, such as STB devices that support the TFTP booting mechanism, can then use the TFTP server address or domain name for initial system settings download. RFC 2132 defines the option 66 open standard. DHCP option 66 carries the IP address or the domain name of a single TFTP server.

Click **Network Setting** > **Home Networking** > **TFTP Server Name** to open this screen.

Figure 43 Network Setting > Home Networking > TFTP Server Name



The following table describes the labels in this screen.

Table 28 Network Setting > Home Networking > TFTP Server Name

LABEL	DESCRIPTION
TFTP Server Name	Enter the IP address or the domain name of a single TFTP server.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

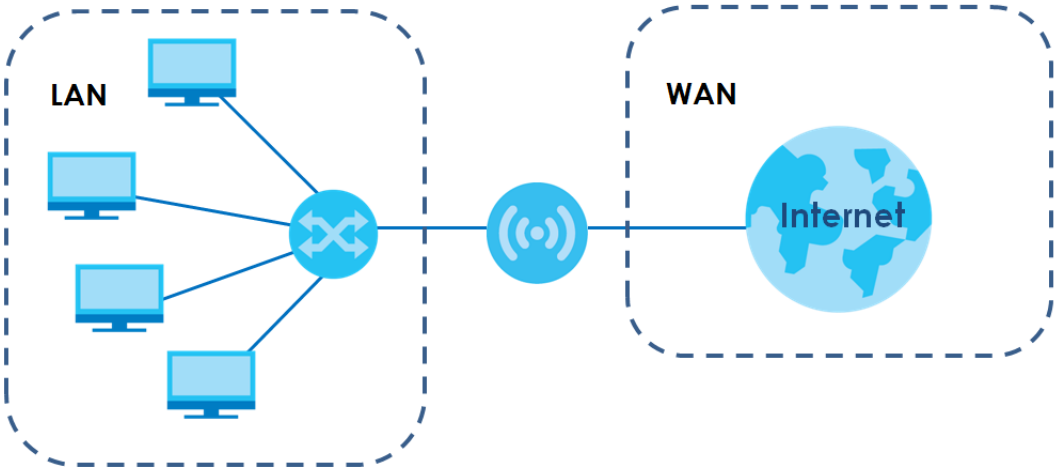
7.9 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

7.9.1 LANs, WANs and the EMG

The actual physical connection determines whether the EMG ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 44 LAN and WAN IP Addresses



7.9.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the EMG as a DHCP server or disable it. When configured as a server, the EMG provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The EMG is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

7.9.3 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The EMG supports the IPCP DNS server extensions through the DNS proxy feature.

  Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

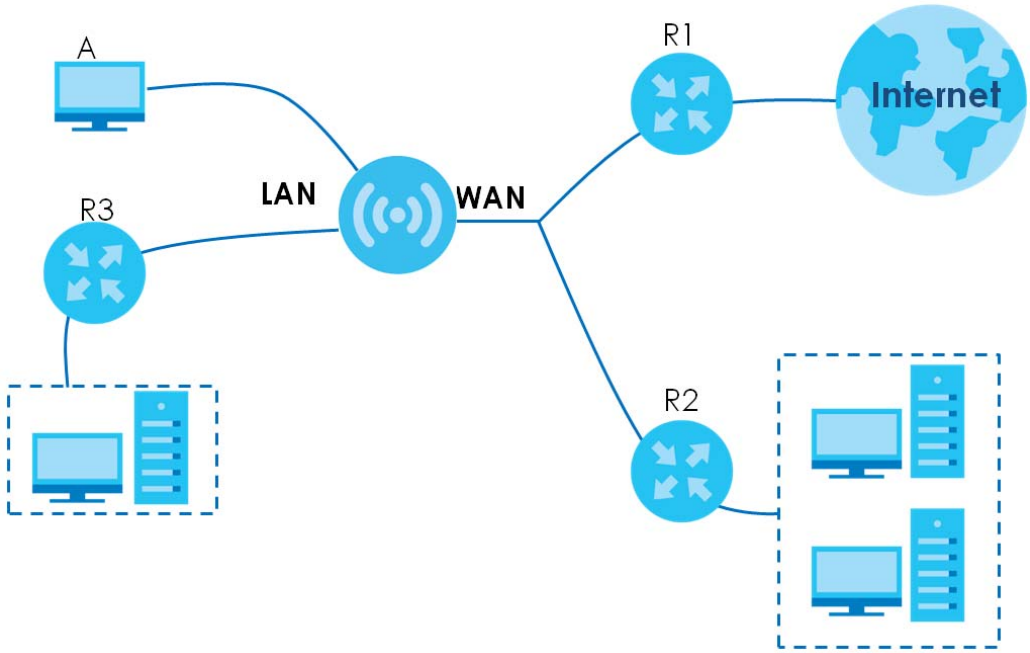
CHAPTER 8
Routing

8.1 Overview

The EMG usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the EMG send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the EMG's LAN interface. The EMG routes most traffic from **A** to the Internet through the EMG's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

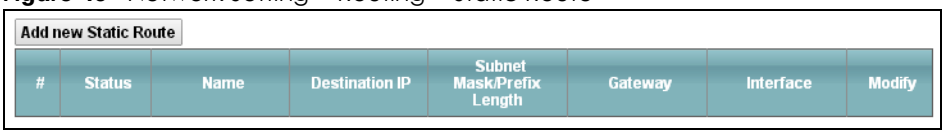
Figure 45 Example of Routing Topology



8.2 The Routing Screen

Use this screen to view and configure the static route rules on the EMG. Click **Network Setting > Routing > Static Route** to open the following screen.

Figure 46 Network Setting > Routing > Static Route



The following table describes the labels in this screen.

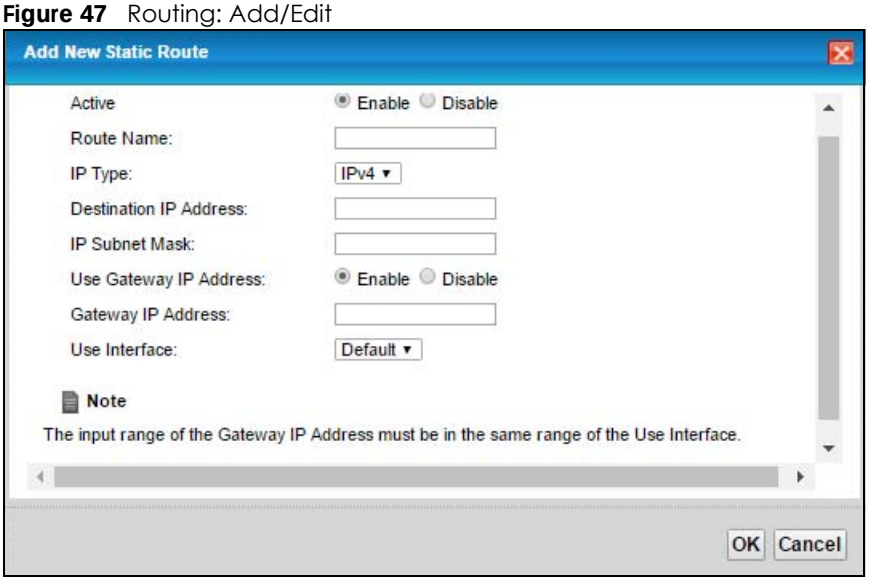
Table 29 Network Setting > Routing > Static Route

LABEL	DESCRIPTION
Add new static route	Click this to configure a new static route.
#	This is the index number of the entry.
Status	This field displays whether the static route is active or not. A yellow bulb signifies that this route is active. A gray bulb signifies that this route is not active.
Name	This is the name that describes or identifies this route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask/ Prefix Length	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the WAN interface used for this static route.
Modify	Click the **Edit** icon to edit the static route on the EMG. Click the **Delete** icon to remove a static route from the EMG. A window displays asking you to confirm that you want to delete the route.

8.2.1 Add/Edit Static Route

Use this screen to add or edit a static route. Click **Add new static route** in the **Routing** screen or the **Edit** icon next to the static route you want to edit. The screen shown next appears.

Figure 47 Routing: Add/Edit



The following table describes the labels in this screen.

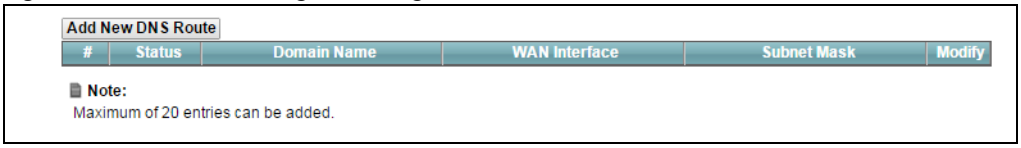
Table 30 Routing: Add/Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route. Select **Enable** to activate the static route. Select **Disable** to deactivate this static route without having to delete the entry.
Route Name	Enter a descriptive name for the static route.
IP Type	Select whether your IP type is **IPv4** or **IPv6**.
Destination IP Address	Enter the IPv4 or IPv6 network address of the final destination.
IP Subnet Mask	If you are using IPv4 and need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. Enter the IP subnet mask here.
Use Gateway IP Address	The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. If you want to use the gateway IP address, select **Enable**.
Gateway IP Address	Enter the IP address of the gateway.
Use Interface	Select the WAN interface you want to use for this static route.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

8.3 The DNS Route Screen

Use this screen to view and configure DNS routes on the EMG. Click **Network Setting > Routing > DNS Route** to open the following screen.

Figure 48 Network Setting > Routing > DNS Route



The following table describes the labels in this screen.

Table 31 Network Setting > Routing > DNS Route

LABEL	DESCRIPTION
Add New DNS Route	Click this to add a new DNS route.
#	This is the index number of a DNS route.
Status	This field displays whether the DNS route is active or not. A yellow bulb signifies that this DNS route is active. A gray bulb signifies that this DNS route is not active.
Domain Name	This is the host name or domain name of the DNS route entry.
WAN Interface	This is the WAN connection through which the EMG forwards DNS requests for this domain name.

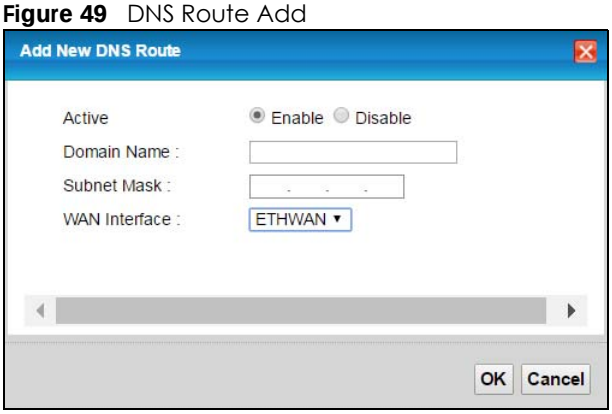
Table 31 Network Setting > Routing > DNS Route (continued)

LABEL	DESCRIPTION
Subnet Mask	This is the subnet mask of the DNS route entry.
Modify	Click the **Edit** icon to modify the DNS route. Click the **Delete** icon to delete the DNS route.

8.3.1 The DNS Route Add Screen

You can manually add the EMG's DNS route entry. Click **Add New DNS Route** in the **Network Setting > Routing > DNS Route** screen. The screen shown next appears.

Figure 49 DNS Route Add



The following table describes the labels in this screen.

Table 32 DNS Route Add

LABEL	DESCRIPTION
Active	Select to enable or disable this DNS route.
Domain Name	Enter the domain name of the DNS route entry.
Subnet Mask	Enter the subnet mask of the DNS route entry.
WAN Interface	Select the WAN connection through which the EMG forwards DNS requests for this domain name.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving any changes.

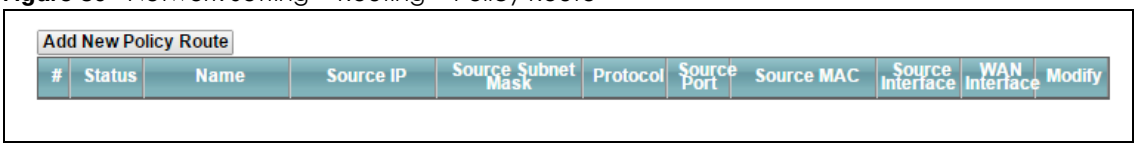
8.4 The Policy Route Screen

Traditionally, routing is based on the destination address only and the EMG takes the shortest path to forward a packet. Policy route allows the EMG to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing.

You can use source-based policy forwarding to direct traffic from different users through different connections or distribute traffic among multiple paths for load sharing.

The **Policy Route** screen let you view and configure routing policies on the EMG. Click **Network Setting > Routing > Policy Route** to open the following screen.

Figure 50 Network Setting > Routing > Policy Route



The following table describes the labels in this screen.

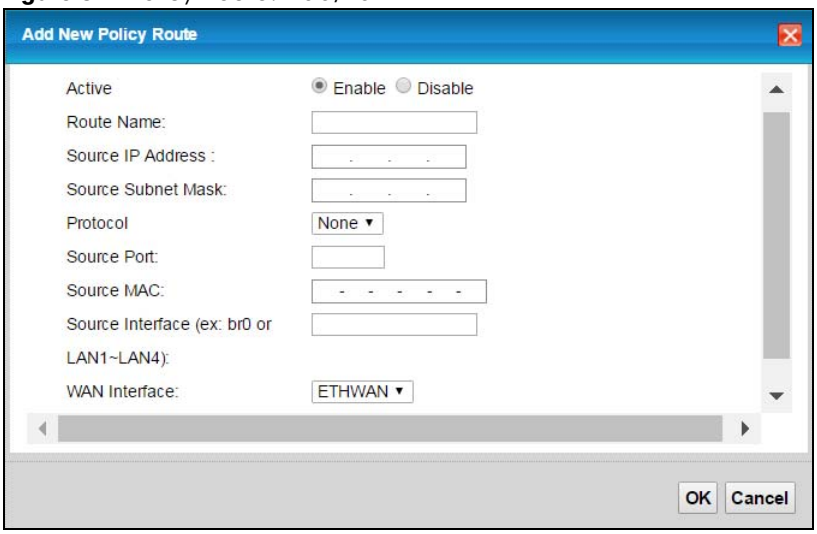
Table 33 Network Setting > Routing >Policy Route

LABEL	DESCRIPTION
Add New Policy Route	Click this to create a new policy forwarding rule.
#	This is the index number of the entry.
Status	This field displays whether the DNS route is active or not. A yellow bulb signifies that this DNS route is active. A gray bulb signifies that this DNS route is not active.
Name	This is the name of the rule.
Source IP	This is the source IP address.
Source Subnet Mask	his is the source subnet mask address.
Protocol	This is the transport layer protocol.
Source Port	This is the source port number.
Source MAC	This is the source MAC address.
Source Interface	This is the interface from which the matched traffic is sent.
WAN Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the **Edit** icon to edit this policy. Click the **Delete** icon to remove a policy from the EMG. A window displays asking you to confirm that you want to delete the policy.

8.4.1 Add/Edit Policy Route

Click **Add New Policy Route** in the **Policy Route** screen or click the **Edit** icon next to a policy. Use this screen to configure the required information for a policy route.

Figure 51 Policy Route: Add/Edit



The following table describes the labels in this screen.

Table 34 Policy Route: Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this policy route.
Route Name	Enter a descriptive name of up to 8 printable English keyboard characters, not including spaces.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (**TCP** or **UDP**).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Source Interface	Type the name of the interface from which the matched traffic is sent.
WAN Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **Broadband** screens.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

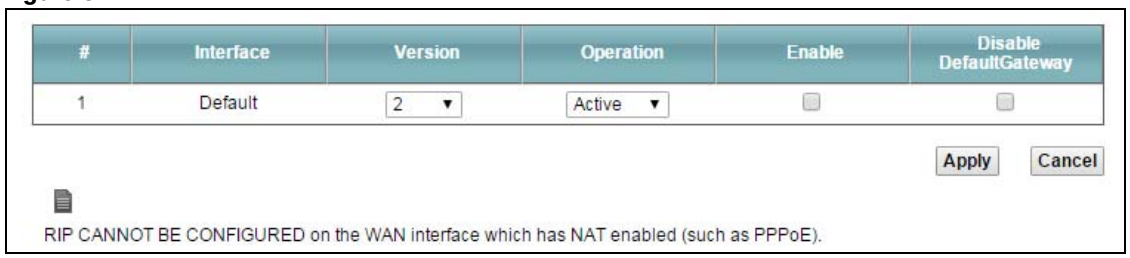
8.5 RIP

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers.

8.5.1 The RIP Screen

Click **Network Setting > Routing > RIP** to open the **RIP** screen.

Figure 52 RIP



The following table describes the labels in this screen.

Table 35 RIP

LABEL	DESCRIPTION
#	This is the index of the interface in which the RIP setting is used.
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the EMG sends (it recognizes both formats when receiving). RIP version **1** is universally supported but RIP version **2** carries more information. RIP version **1** is probably adequate for most networks, unless you have an unusual network topology.
Operation	Select **Passive** to have the EMG update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select **Active** to have the EMG advertise its route information and also listen for routing updates from neighboring routers.
Enable	Select the check box to activate the settings.
Disable Default Gateway	Select the check box to set the XMG to not send the route information to the default gateway.
Apply	Click **Apply** to save your changes back to the EMG.
Cancel	Click **Cancel** to restore your previously saved settings.

CHAPTER 9
Quality of Service (QoS)

9.1 Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

Configure QoS on the EMG to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

1. Configure classifiers to sort traffic into different flows.
2. Assign priority and define actions to be performed for a classified traffic flow.

The EMG assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

This chapter contains information about configuring QoS and editing classifiers.

9.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable or disable QoS and set the upstream bandwidth (Section 9.3 on page 111).
- Use the **Queue Setup** screen to configure QoS queue assignment (Section 9.4 on page 112).
- Use the **Classification Setup** screen to add, edit or delete QoS classifiers (Section 9.5 on page 115).
- Use the **Shaper Setup** screen to limit outgoing traffic transmission rate on the selected interface (Section 9.6 on page 119).
- Use the **Policer Setup** screen to control incoming traffic transmission rate and bursts (Section 9.7 on page 120).

9.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

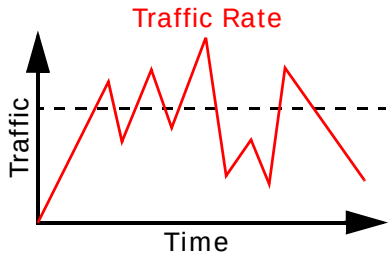
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

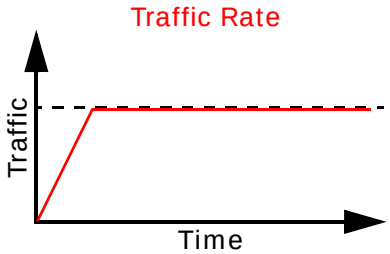
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or queues). Your EMG uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



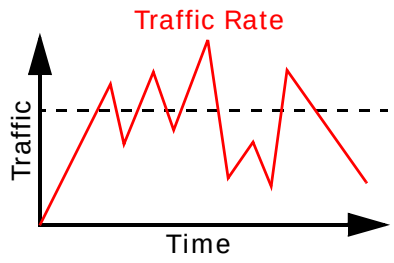
(Before Traffic Shaping)



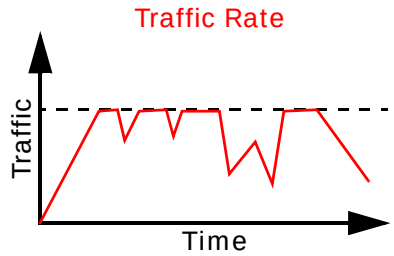
(After Traffic Shaping)

Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.



(Before Traffic Policing)



(After Traffic Policing)

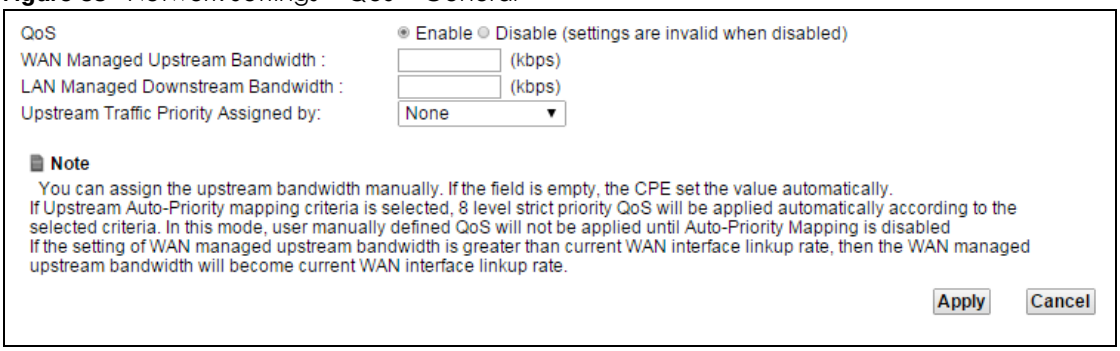
The EMG supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Maker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See Section 9.8 on page 122 for more information on each metering algorithm.

9.3 The Quality of Service General Screen

Click **Network Setting > QoS > General** to open the screen as shown next.

Use this screen to enable or disable QoS and set the upstream bandwidth. See Section 9.1 on page 109 for more information.

Figure 53 Network Settings > QoS > General



The following table describes the labels in this screen.

Table 36 Network Setting > QoS > General

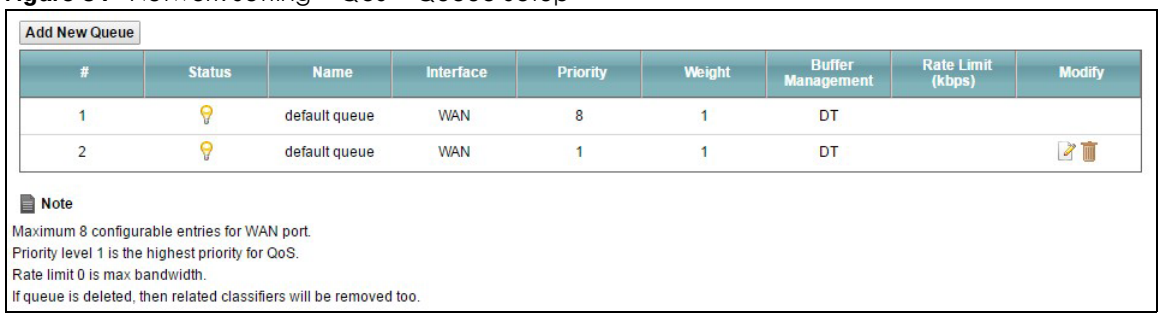
LABEL	DESCRIPTION
QoS	Select the **Enable** check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS. The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. You can also set this number lower than the interfaces' actual transmission speed. This will cause the EMG to not use some of the interfaces' available bandwidth. If you leave this field blank, the EMG automatically sets this number to be 95% of the WAN interfaces' actual upstream transmission speed.
LAN Managed Downstream Bandwidth	Enter the amount of downstream bandwidth for the LAN interfaces (including WLAN) that you want to allocate using QoS. The recommendation is to set this speed to match the WAN interfaces' actual transmission speed. For example, set the LAN managed downstream bandwidth to 100000 kbps if you use a 100 Mbps wired Ethernet WAN connection. You can also set this number lower than the WAN interfaces' actual transmission speed. This will cause the EMG to not use some of the interfaces' available bandwidth. If you leave this field blank, the EMG automatically sets this to the LAN interfaces' maximum supported connection speed.
Upstream Traffic Priority Assigned by	Select how the EMG assigns priorities to various upstream traffic flows. • **None:** Disables auto priority mapping and has the EMG put packets into the queues according to your classification rules. Traffic which does not match any of the classification rules is mapped into the default queue with the lowest priority. • **Ethernet Priority:** Automatically assign priority based on the IEEE 802.1p priority level. • **IP Precedence:** Automatically assign priority based on the first three bits of the TOS field in the IP header. • **Packet Length:** Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, internet gaming, or other real-time packets are usually small while larger packets are usually best effort data packets like file transfers.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

9.4 The Queue Setup Screen

Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

Use this screen to configure QoS queue assignment.

Figure 54 Network Setting > QoS > Queue Setup



The following table describes the labels in this screen.

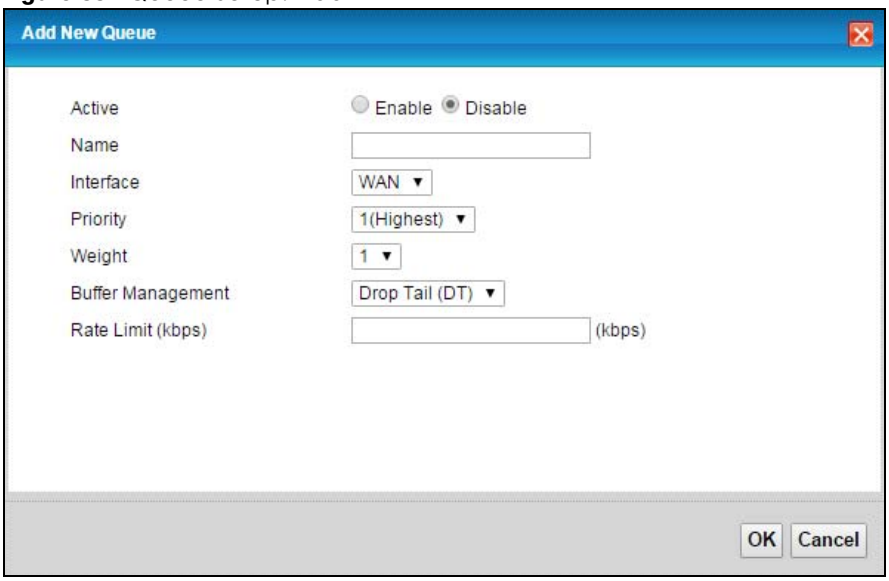
Table 37 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add New Queue	Click this button to create a new queue entry.
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the EMG's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used for this queue. Queue management algorithms determine how the EMG should handle packets when it receives too many (network congestion).
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the **Edit** icon to edit the queue. Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

9.4.1 Adding a QoS Queue

Click **Add New Queue** or the edit icon in the **Queue Setup** screen to configure a queue.

Figure 55 Queue Setup: Add



The following table describes the labels in this screen.

Table 38 Queue Setup: Add

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 7) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the EMG divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Buffer Management	This field displays **Drop Tail (DT)**. **Drop Tail (DT)** is a simple queue management algorithm that allows the EMG buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it).
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

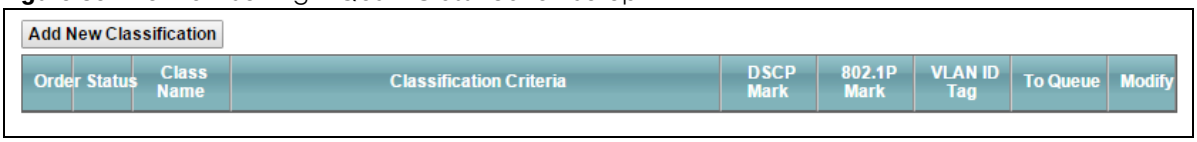
9.5 The Classification Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the EMG forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting > QoS > Classification Setup** to open the following screen.

Figure 56 Network Setting > QoS > Classification Setup



The following table describes the labels in this screen.

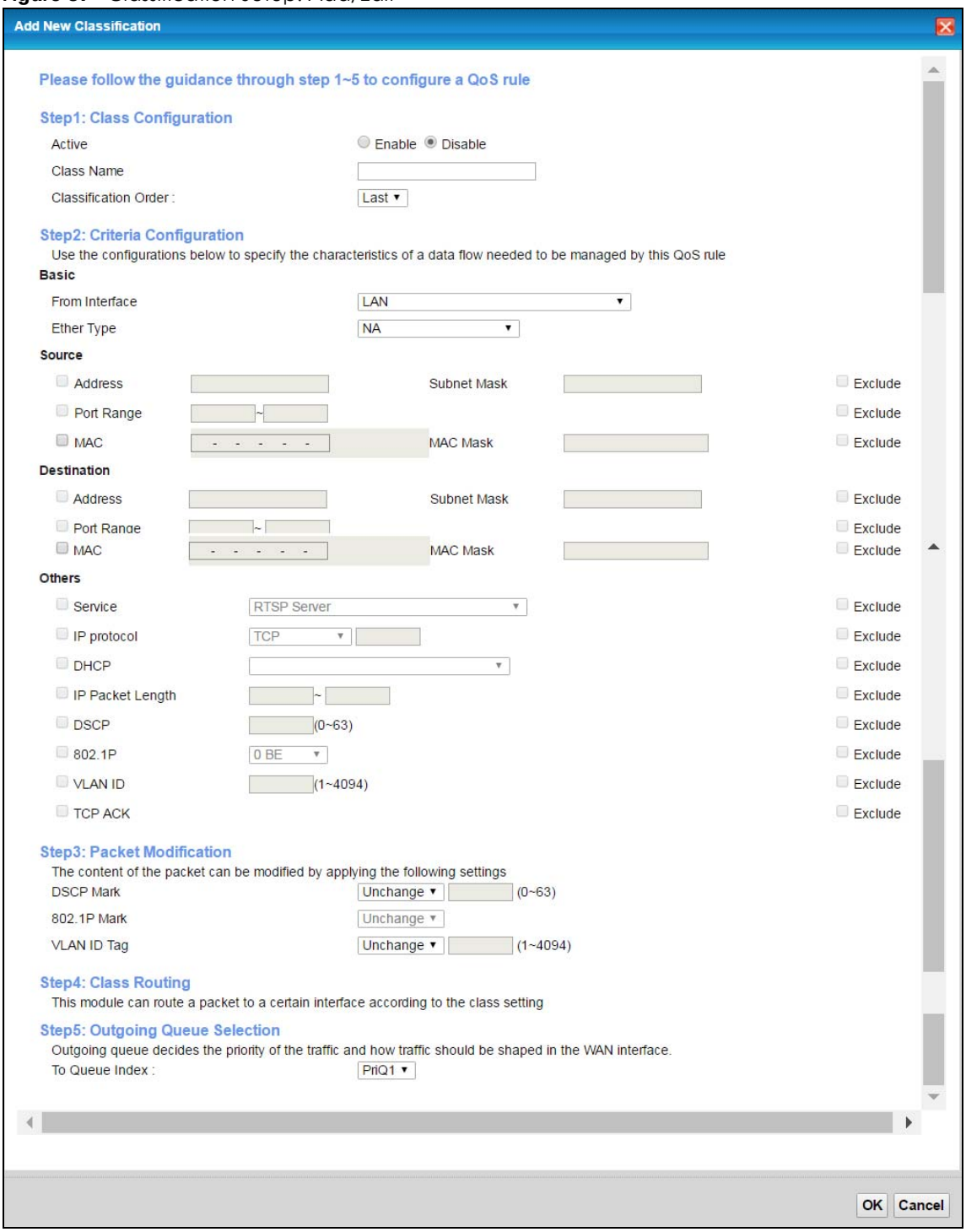
Table 39 Network Setting > QoS > Classification Setup

LABEL	DESCRIPTION
Add New Classification	Click this to create a new classifier.
Order	This is the index number of the entry. The classifiers are applied in order of their numbering.
Status	This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the **Edit** icon to edit the classifier. Click the **Delete** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

9.5.1 Add/Edit QoS Class

Click **Add New Classification** in the **Classification Setup** screen or the **Edit** icon next to a classifier to open the following screen.

Figure 57 Classification Setup: Add/Edit



The following table describes the labels in this screen.

Table 40 Classification Setup: Add/Edit

LABEL	DESCRIPTION
Step1: Class Configuration	
Active	Select to enable or disable this classifier.

Table 40 Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Class Name	Enter a descriptive name of up to 15 printable English keyboard characters, not including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**. Select **Last** to put this rule in the back of the classifier list.
Step2: Criteria Configuration	
From Interface	If you want to classify the traffic by an ingress interface, select an interface from the **From Interface** drop-down list box.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select **802.1Q**, you can configure an 802.1p priority level.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Mask	Enter the source subnet mask.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Mask	Enter the destination subnet mask.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the destination.
MAC	Select the check box and enter the destination MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified destination MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
Service	This field is available only when you select **IP** in the **Ether Type** field. This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields.

Table 40 Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
IP Protocol	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select the protocol (service type) from **TCP**, **UDP**, **ICMP** or **IGMP**. If you select **User defined**, enter the protocol (service type) number.
DHCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select a DHCP option. If you select **Vendor Class ID (DHCP Option 60)**, enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware. If you select **Client ID (DHCP Option 61)**, enter the Identity Association IDentifier (IAD Option 61) of the matched traffic, such as the MAC address of the device. If you select **User Class ID (DHCP Option 77)**, enter a string that identifies the user's category or application type in the matched DHCP packets. If you select **Vendor Specific Info (DHCP Option 125)**, enter the vendor specific information of the matched traffic, such as the product class, model name, and serial number of the device.
IP Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.
DSCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
802.1P	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and select a priority level (between 0 and 7) from the drop-down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and specify a VLAN ID number.
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Step3: Packet Modification	
DSCP Mark	This field is available only when you select **IP** in the **Ether Type** field. If you select **Remark**, enter a DSCP value with which the EMG replaces the DSCP field in the packets. If you select **Unchange**, the EMG keep the DSCP field in the packets.
802.1P Mark	Select a priority level with which the EMG replaces the IEEE 802.1p priority field in the packets. If you select **Unchange**, the EMG keep the 802.1p priority field in the packets.
VLAN ID Tag	If you select **Remark**, enter a VLAN ID number with which the EMG replaces the VLAN ID of the frames. If you select **Remove**, the EMG deletes the VLAN ID of the frames before forwarding them out. If you select **Add**, the EMG treat all matched traffic untagged and add a second VLAN ID. If you select **Unchange**, the EMG keep the VLAN ID in the packets.
Step4: Class Routing	
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the EMG forward traffic of this class according to the default routing table.

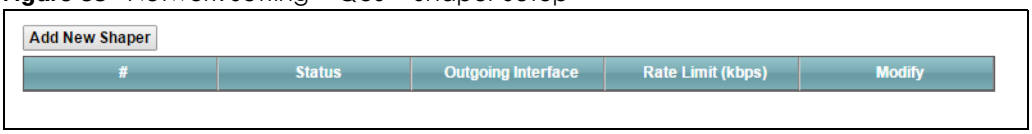
Table 40 Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Step5: Outgoing Queue Selection	
To Queue Index	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

9.6 The QoS Shaper Setup Screen

This screen shows that you can use the token bucket algorithm to allow a certain amount of large bursts while keeping a limit for processing outgoing traffic at the average rate. Click **Network Setting > QoS > Shaper Setup**. The screen appears as shown.

Figure 58 Network Setting > QoS > Shaper Setup



The following table describes the labels in this screen.

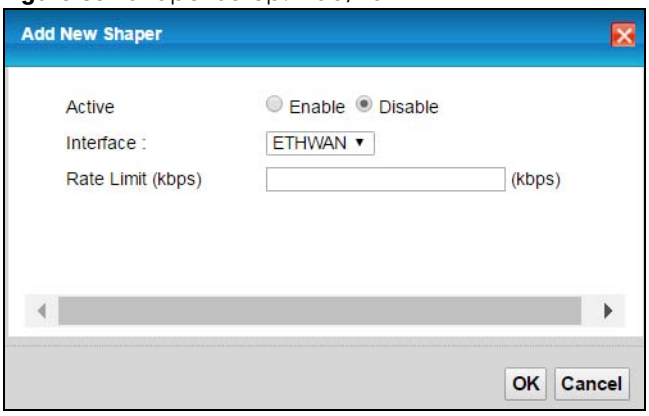
Table 41 Network Setting > QoS > Shaper Setup

LABEL	DESCRIPTION
Add New Shaper	Click this to create a new entry.
#	This is the index number of the entry.
Status	This field displays whether the shaper is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this shaper is not active.
Outgoing Interface	This shows the name of the EMG's interface through which traffic in this shaper applies.
Rate Limit (kbps)	This shows the average rate limit of traffic bursts for this shaper.
Modify	Click the **Edit** icon to edit the shaper. Click the **Delete** icon to delete an existing shaper. Note that subsequent rules move up by one when you take this action.

9.6.1 Add/Edit a QoS Shaper

Click **Add New Shaper** in the **Shaper Setup** screen or the **Edit** icon next to a shaper to show the following screen.

Figure 59 Shaper Setup: Add/Edit



The following table describes the labels in this screen.

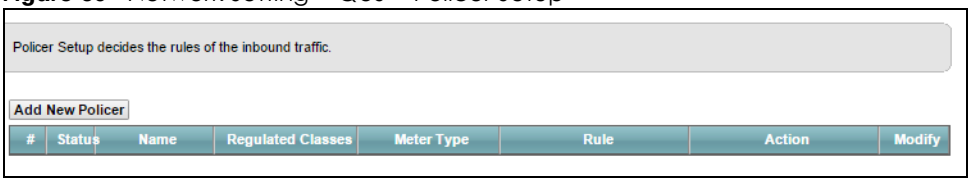
Table 42 Shaper Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this shaper.
Interface	Select the EMG's interface through which traffic in this shaper applies
Rate Limit	Enter the average rate limit of traffic bursts for this shaper.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

9.7 The QoS Policer Setup Screen

Use this screen to view QoS policers that allow you to limit the transmission rate of incoming traffic and apply actions, such as drop, pass, or modify the DSCP value for matched traffic. Click **Network Setting > QoS > Policer Setup**. The screen appears as shown.

Figure 60 Network Setting > QoS > Policer Setup



The following table describes the labels in this screen.

Table 43 Network Setting > QoS > Policer Setup

LABEL	DESCRIPTION
Add new Policer	Click this to create a new entry.
#	This is the index number of the entry.

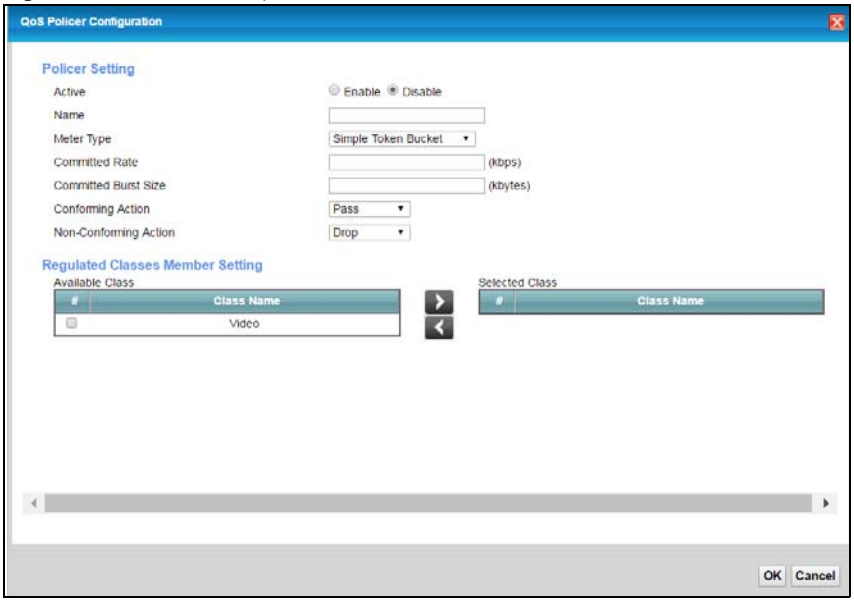
Table 43 Network Setting > QoS > Policer Setup (continued)

LABEL	DESCRIPTION
Status	This field displays whether the policer is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this policer is not active.
Name	This field displays the descriptive name of this policer.
Regulated Classes	This field displays the name of a QoS classifier
Meter Type	This field displays the type of QoS metering algorithm used in this policer.
Rule	These are the rates and burst sizes against which the policer checks the traffic of the member QoS classes.
Action	This shows the how the policer has the EMG treat different types of traffic belonging to the policer's member QoS classes.
Modify	Click the **Edit** icon to edit the policer. Click the **Delete** icon to delete an existing policer. Note that subsequent rules move up by one when you take this action.

9.7.1 Add/Edit a QoS Policer

Click **Add New Policer** in the **Policer Setup** screen or the **Edit** icon next to a policer to show the following screen.

Figure 61 Policer Setup: Add/Edit



The following table describes the labels in this screen.

Table 44 Policer Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this policer.
Name	Enter the descriptive name of this policer.

Table 44 Policer Setup: Add/Edit

LABEL	DESCRIPTION
Meter Type	This shows the traffic metering algorithm used in this policer. The **Simple Token Bucket** algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size. The **Single Rate Three Color Marker** (srTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR), the Committed Burst Size (CBS) and the Excess Burst Size (EBS). The **Two Rate Three Color Marker** (trTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR) and the Peak Information Rate (PIR).
Committed Rate	Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic.
Committed Burst Size	Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured. This is the maximum size of the (first) token bucket in a traffic metering algorithm.
Conforming Action	Specify what the EMG does for packets within the committed rate and burst size (green-marked packets). • **Pass:** Send the packets without modification. • **DSCP Mark:** Change the DSCP mark value of the packets. Enter the DSCP mark value to use.
Non-Conforming Action	Specify what the EMG does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets). • **Drop:** Discard the packets. • **DSCP Mark:** Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network.
Available Class Selected Class	Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier. Highlight a QoS classifier in the **Available Class** box and use the **>** button to move it to the **Selected Class** box. To remove a QoS classifier from the **Selected Class** box, select it and use the **<** button.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

9.8 Technical Reference

The following section contains additional technical information about the EMG features described in this chapter.

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 45 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new Differentiated Services (DS) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

Automatic Priority Queue Assignment

If you enable QoS on the EMG, the EMG can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the EMG. On the EMG, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 46 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size, so the bucket can hold up to *b* tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.
- If there are no tokens in the bucket, the EMG stops transmitting until enough tokens are generated.
- If not enough tokens are available, the EMG treats the packet in either one of the following ways:

  In traffic shaping:

  - Holds it in the queue until enough tokens are available in the bucket.

  In traffic policing:

  - Drops it.
  - Transmits it but adds a DSCP mark. The EMG may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface's capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

Single Rate Three Color Marker

The Single Rate Three Color Marker (srTCM, defined in RFC 2697) is a type of traffic policing that identifies packets by comparing them to one user-defined rate, the Committed Information Rate (CIR), and two burst sizes: the Committed Burst Size (CBS) and Excess Burst Size (EBS).

The srTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The srTCM is based on the token bucket filter and has two token buckets (CBS and EBS). Tokens are generated and added into the bucket at a constant rate, called Committed Information Rate (CIR). When the first bucket (CBS) is full, new tokens overflow into the second bucket (EBS).

All packets are evaluated against the CBS. If a packet does not exceed the CBS it is marked green. Otherwise it is evaluated against the EBS. If it is below the EBS then it is marked yellow. If it exceeds the EBS then it is marked red.

The following shows how tokens work with incoming packets in srTCM:

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.

- If there are not enough tokens in the CBS bucket, the EMG checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

Two Rate Three Color Marker

The Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

The trTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

The following shows how tokens work with incoming packets in trTCM:

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.
- If the PBS bucket has enough tokens, the EMG checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

CHAPTER 10
Network Address Translation (NAT)

10.1 Overview

This chapter discusses how to configure NAT on the EMG. NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

10.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network (Section 10.2 on page 128).
- Use the **Applications** screen to forward incoming service requests to the server(s) on your local network (Section 10.3 on page 131).
- Use the **Port Triggering** screen to add and configure the EMG's trigger port settings (Section 10.4 on page 133).
- Use the **DMZ** screen to configure a default server (Section 10.5 on page 135).
- Use the **ALG** screen to enable and disable the NAT and SIP (VoIP) ALG in the EMG (Section 10.6 on page 136).
- Use the **Address Mapping** screen to configure the EMG's address mapping settings (Section 10.7 on page 137).
- Use the **Sessions** screen to configure the EMG's maximum number of NAT sessions (Section 10.8 on page 139).

10.1.2 What You Need To Know

Inside/Outside

Inside/outside denotes where a host is located relative to the EMG, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Finding Out More

See Section 10.9 on page 139 for advanced technical information on NAT.

10.2 The Port Forwarding Screen

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

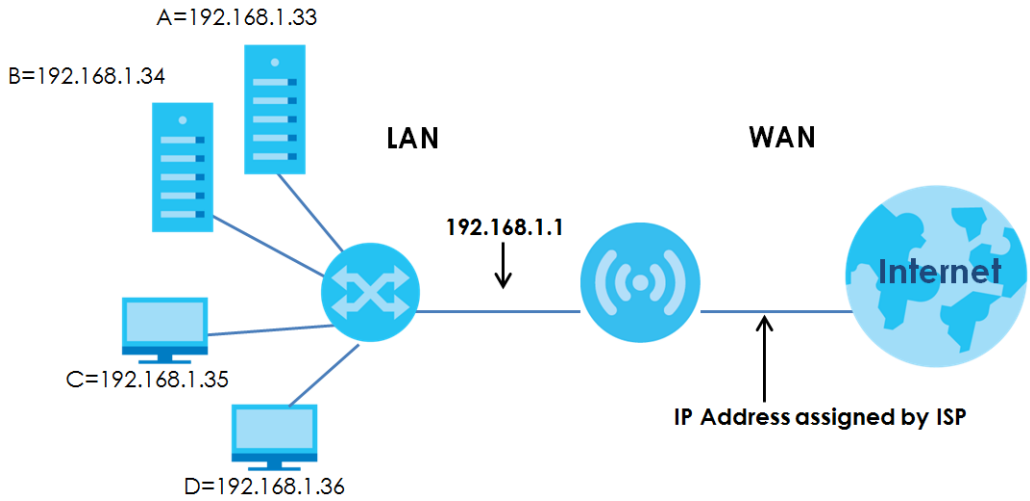
The most often used port numbers and services are shown in Appendix D on page 242. Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

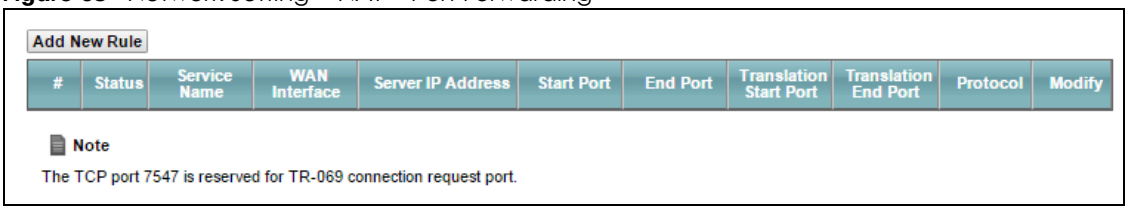
Figure 62 Multiple Servers Behind NAT Example



Click **Network Setting > NAT > Port Forwarding** to open the following screen.

See Appendix D on page 242 for port numbers commonly used for particular services.

Figure 63 Network Setting > NAT > Port Forwarding



The following table describes the fields in this screen.

Table 47 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add New Rule	Click this to add a new rule.
#	This is the index number of the entry.
Status	This field displays whether the NAT rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This shows the service's name.
WAN Interface	This shows the WAN interface through which the service is forwarded.
Server IP Address	This is the server's IP address.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.

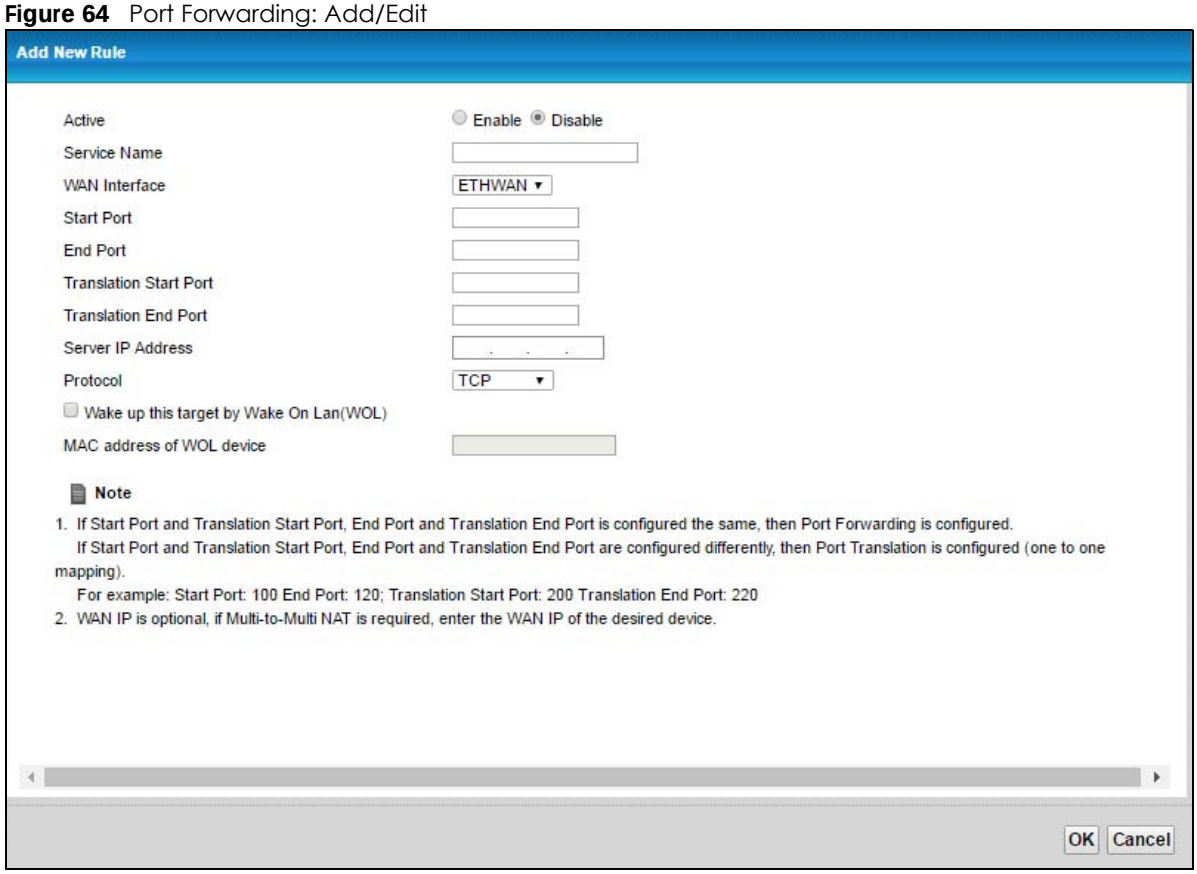
Table 47 Network Setting > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
Protocol	This shows the IP protocol supported by this virtual server, whether it is **TCP**, **UDP**, or **TCP/UDP**.
Modify	Click the **Edit** icon to edit this rule. Click the **Delete** icon to delete an existing rule.

10.2.1 Add/Edit Port Forwarding

Click **Add New Rule** in the **Port Forwarding** screen or click the **Edit** icon next to an existing rule to open the following screen.

Figure 64 Port Forwarding: Add/Edit



The following table describes the labels in this screen.

Table 48 Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable the rule.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.

Table 48 Port Forwarding: Add/Edit (continued)

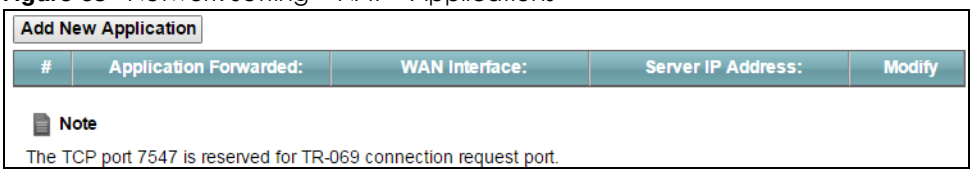
LABEL	DESCRIPTION
Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port** field.
End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port** field above.
Translation Start Port	This shows the port number to which you want the EMG to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
Wake up this target by Wake On Lan (WOL)	Select this to allow the EMG's network to remotely turn on a device in the network.
MAC address of WOL device	Enter the MAC address of the device that will be turned on by an EMG's network message. A MAC address consists of six hexadecimal character pairs.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

10.3 The Applications Screen

This screen provides a summary of all NAT applications and their configuration. In addition, this screen allows you to create new applications and/or remove existing ones.

To access this screen, click **Network Setting > NAT > Applications**. The following screen appears.

Figure 65 Network Setting > NAT > Applications



The following table describes the labels in this screen.

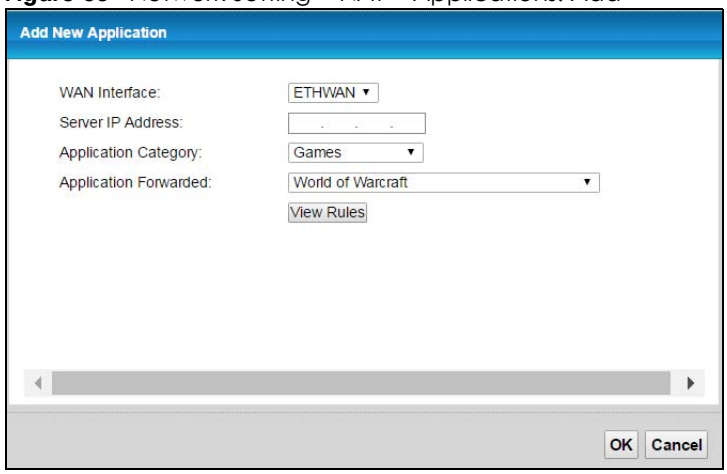
Table 49 Network Setting > NAT > Applications

LABEL	DESCRIPTION
Add New Application	Click this to add a new NAT application rule.
#	This is the index number of the entry.
Application Forwarded	This field shows the type of application that the service forwards.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Server IP Address	This field displays the destination IP address for the service.
Modify	Click the **Delete** icon to delete the rule.

10.3.1 Add New Application

This screen lets you create new NAT application rules. Click **Add New Application** in the **Applications** screen to open the following screen.

Figure 66 Network Setting > NAT > Applications: Add



The following table describes the labels in this screen.

Table 50 Network Setting > NAT > Applications: Add

LABEL	DESCRIPTION
WAN Interface	Select the WAN interface that you want to apply this NAT rule to.
Server IP Address	Enter the inside IP address of the application here.
Application Category	Select the category of the application from the drop-down list box.
Application Forwarded	Select a service from the drop-down list box and the EMG automatically configures the protocol, start, end, and map port number that define the service.
View Rules	Click this to display the configuration of the service that you have chosen in **Application Fowarded**.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

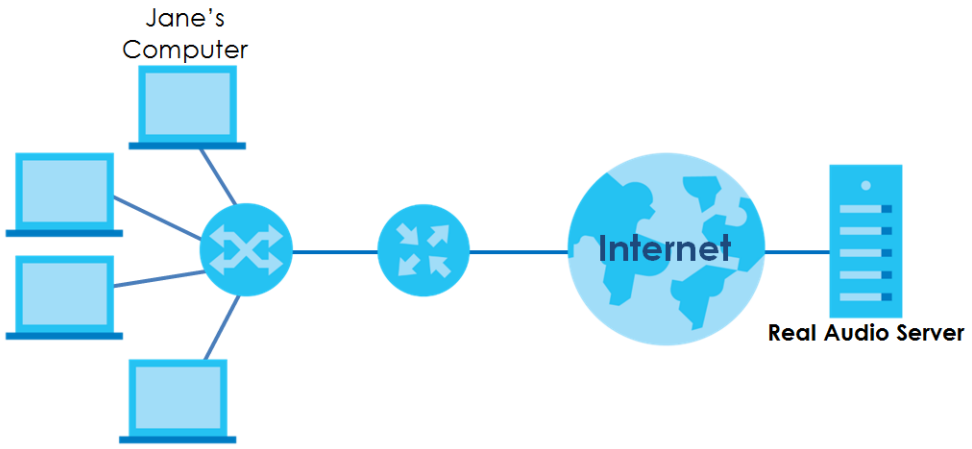
10.4 The Port Triggering Screen

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The EMG records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the EMG's WAN port receives a response with a specific port number and protocol ("open" port), the EMG forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

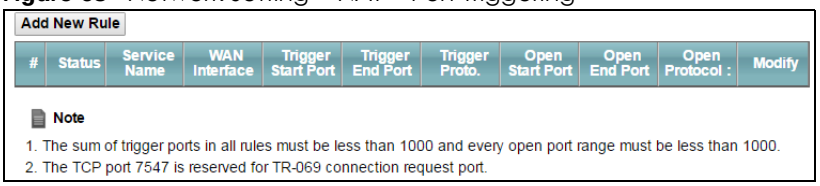
Figure 67 Trigger Port Forwarding Process: Example



1. Jane requests a file from the Real Audio server (port 7070).
2. Port 7070 is a "trigger" port and causes the EMG to record Jane's computer IP address. The EMG associates Jane's computer IP address with the "open" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The EMG forwards the traffic to Jane's computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The EMG times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Network Setting > NAT > Port Triggering** to open the following screen. Use this screen to view your EMG's trigger port settings.

Figure 68 Network Setting > NAT > Port Triggering



The following table describes the labels in this screen.

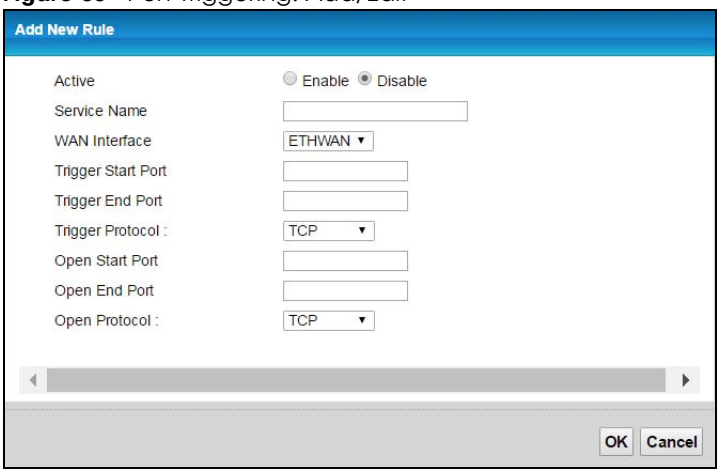
Table 51 Network Setting > NAT > Port Triggering

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This field displays the name of the service used by this rule.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the EMG to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service.
Trigger End Port	This is the last port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The EMG forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service.
Open End Port	This is the last port number that identifies a service.
Open Proto.	This is the open transport layer protocol.
Modify	Click the **Edit** icon to edit this rule. Click the **Delete** icon to remove an existing rule.

10.4.1 Add/Edit Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add new rule** in the **Port Triggering** screen or click a rule's **Edit** icon to open the following screen.

Figure 69 Port Triggering: Add/Edit



The following table describes the labels in this screen.

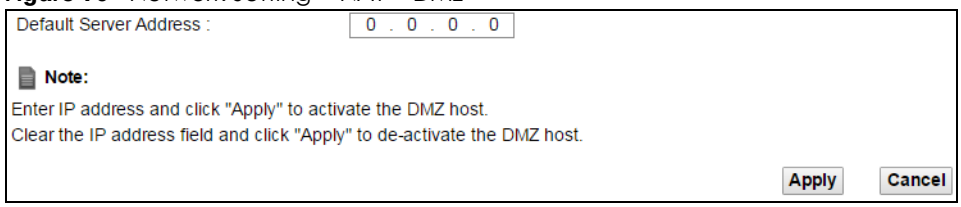
Table 52 Port Triggering: Configuration Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this rule.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the EMG to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.
Trigger End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The EMG forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

10.5 The DMZ Screen

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in the **NAT Port Forwarding Setup** screen.

Figure 70 Network Setting > NAT > DMZ



The following table describes the fields in this screen.

Table 53 Network Setting > NAT > DMZ

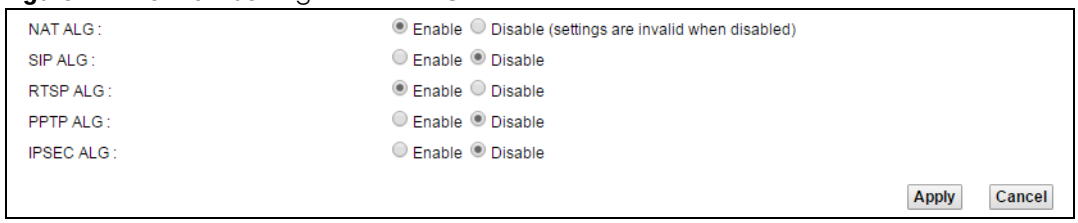
LABEL	DESCRIPTION
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the **NAT Port Forwarding** screen. Note: If you do not assign a **Default Server Address**, the EMG discards all packets received for ports that are not specified in the **NAT Port Forwarding** screen.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.6 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the EMG registers with the SIP register server, the SIP ALG translates the EMG's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your EMG is behind a SIP ALG.

Use this screen to enable and disable the ALGs in the EMG. To access this screen, click **Network Setting > NAT > ALG**.

Figure 71 Network Setting > NAT > ALG



The following table describes the fields in this screen.

Table 54 Network Setting > NAT > ALG

LABEL	DESCRIPTION
NAT ALG	Enable this to make sure applications such as FTP and file transfer in IM applications work correctly with port-forwarding and address-mapping rules.
SIP ALG	Enable this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
RTSP ALG	Enable this to have the EMG detect RTSP traffic and help build RTSP sessions through its NAT. The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.

Table 54 Network Setting > NAT > ALG (continued)

LABEL	DESCRIPTION
PPTP ALG	Enable this to turn on the PPTP ALG on the EMG to detect PPTP traffic and help build PPTP sessions through the EMG's NAT.
IPSEC ALG	Enable this to turn on the IPsec ALG on the EMG to detect IPsec traffic and help build IPsec sessions through the EMG's NAT.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.7 The Address Mapping Screen

Ordering your rules is important because the EMG applies the rules in the order that you specify. When a rule matches the current packet, the EMG takes the corresponding action and the remaining rules are ignored.

Click **Network Setting > NAT > Address Mapping** to display the following screen.

Figure 72 Network Setting > NAT > Address Mapping

The following table describes the fields in this screen.

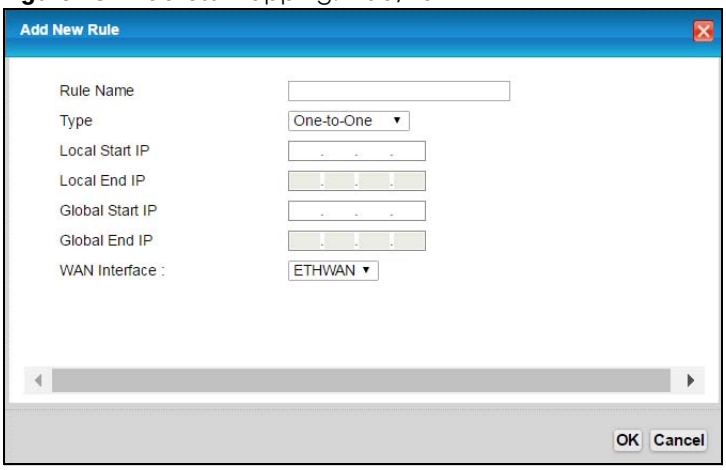
Table 55 Network Setting > NAT > Address Mapping

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
Rule Name	This show the name of the rule.
Local Start IP	This is the starting Inside Local IP Address (ILA).
Local End IP	This is the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for **One-to-One** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the **Many-to-One** mapping type.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types.
Type	This is the address mapping type. **One-to-One**: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the EMG's Single User Account feature that previous routers supported only. **Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses.
Wan Interface Name	This is the WAN interface to which the address mapping rule applies.
Modify	Click the **Edit** icon to go to the screen where you can edit the address mapping rule. Click the **Delete** icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

10.7.1 Add/Edit Address Mapping Rule

To add or edit an address mapping rule, click **Add new rule** or the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

Figure 73 Address Mapping: Add/Edit



The following table describes the fields in this screen.

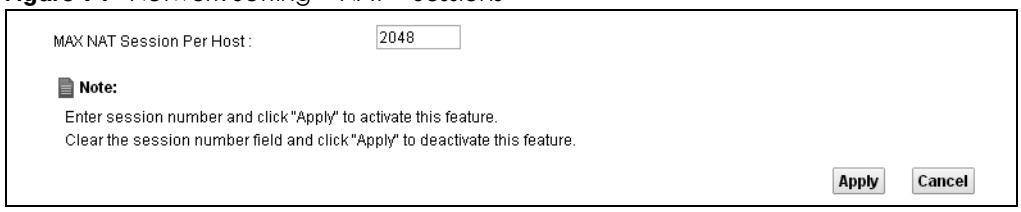
Table 56 Address Mapping: Add/Edit

LABEL	DESCRIPTION
Rule Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
Type	Choose the IP/port mapping type from one of the following. **One-to-One**: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the EMG's Single User Account feature that previous routers supported only. **Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses.
Local Start IP	Enter the starting Inside Local IP Address (ILA).
Local End IP	Enter the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for **One-to-One** mapping types.
Global Start IP	Enter the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the **Many-to-One** mapping type.
Global End IP	Enter the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types.
WAN Interface	Select a WAN interface to which the address mapping rule applies.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

10.8 The Sessions Screen

Use this screen to limit the number of concurrent NAT sessions a client can use. Click **Network Setting > NAT > Sessions** to display the following screen.

Figure 74 Network Setting > NAT > Sessions



The following table describes the fields in this screen.

Table 57 Network Setting > NAT > Sessions

LABEL	DESCRIPTION
MAX NAT Session Per Host	Use this field to set a limit to the number of concurrent NAT sessions each client host can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer-to-peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Apply	Click this to save your changes on this screen.
Cancel	Click this to exit this screen without saving any changes.

10.9 Technical Reference

This part contains more information regarding NAT.

10.9.1 NAT Definitions

Inside/outside denotes where a host is located relative to the EMG, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 58 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

10.9.2 What NAT Does

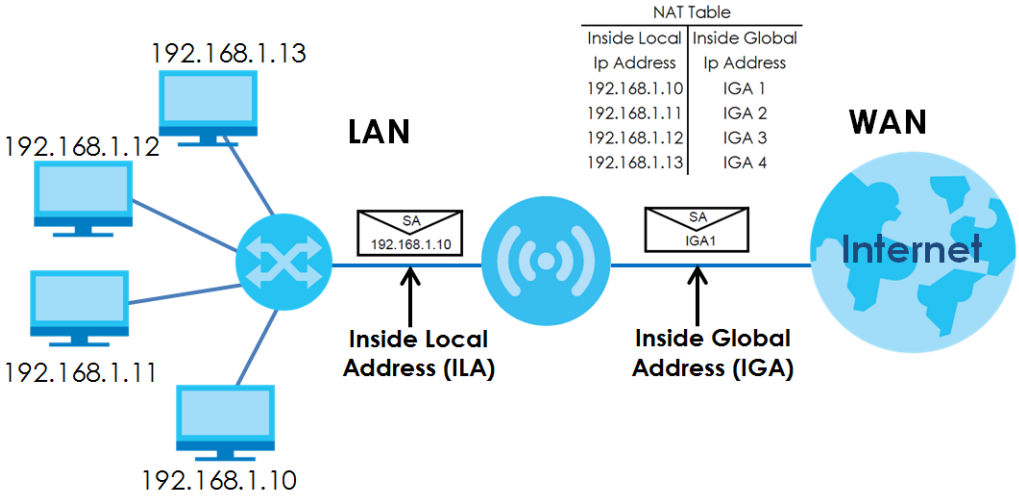
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your EMG filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

10.9.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The EMG keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

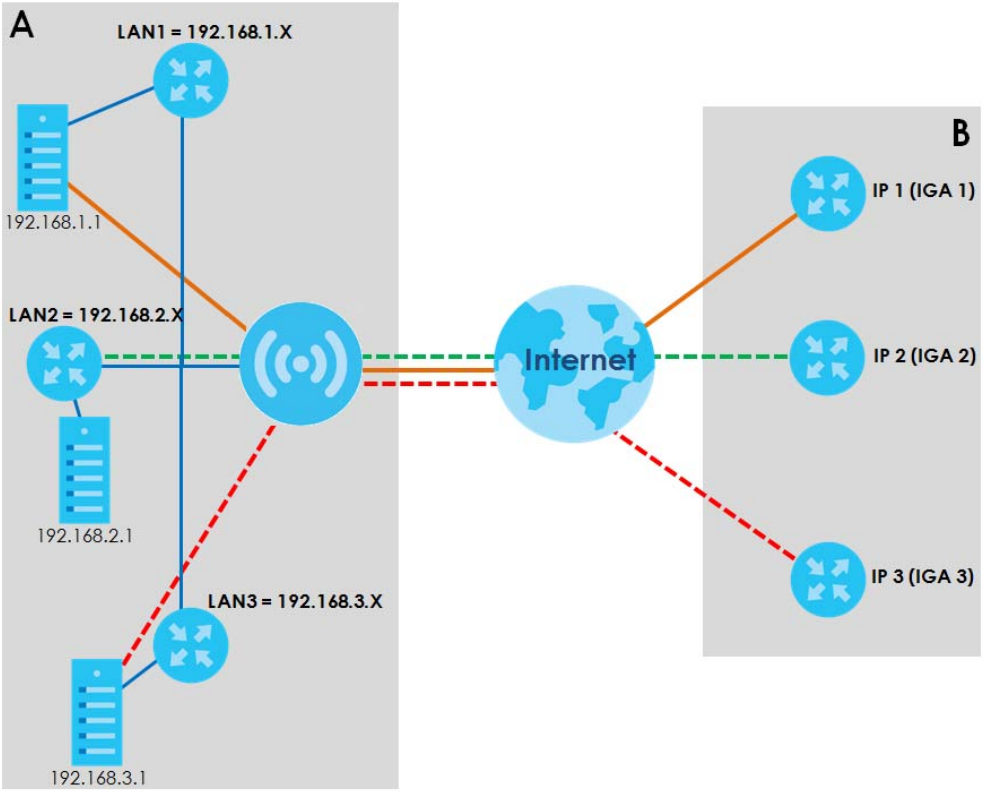
Figure 75 How NAT Works



10.9.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the EMG can communicate with three distinct WAN networks.

Figure 76 NAT Application With IP Alias



Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

Table 59 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161

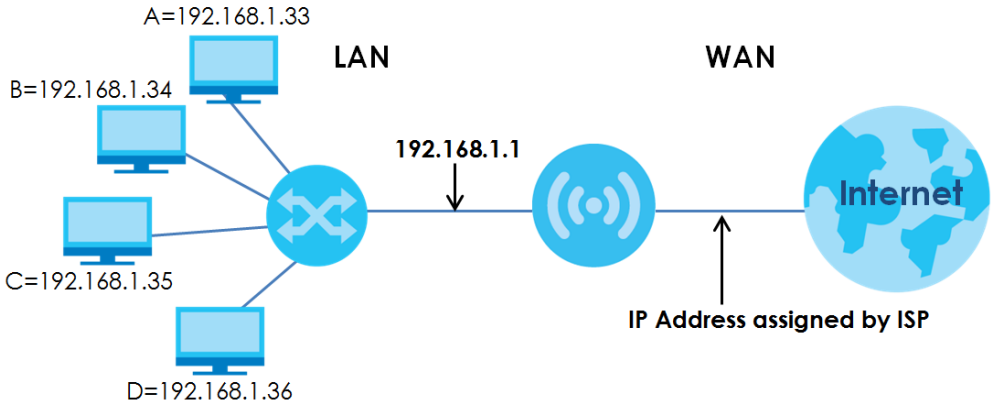
Table 59 Services and Port Numbers

SERVICES	PORT NUMBER
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 77 Multiple Servers Behind NAT Example



CHAPTER 11
DNS

11.1 Overview

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

In addition to the system DNS server(s), each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s). The EMG uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the EMG receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

11.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes (Section 11.2 on page 144).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the EMG (Section 11.3 on page 145).

11.1.2 What You Need To Know

DYNDNS Wildcard

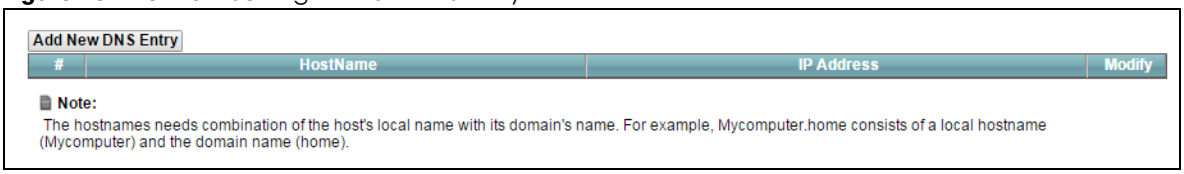
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

11.2 The DNS Entry Screen

Use this screen to view and configure DNS routes on the EMG. Click **Network Setting > DNS** to open the **DNS Entry** screen.

Figure 78 Network Setting > DNS > DNS Entry



The following table describes the fields in this screen.

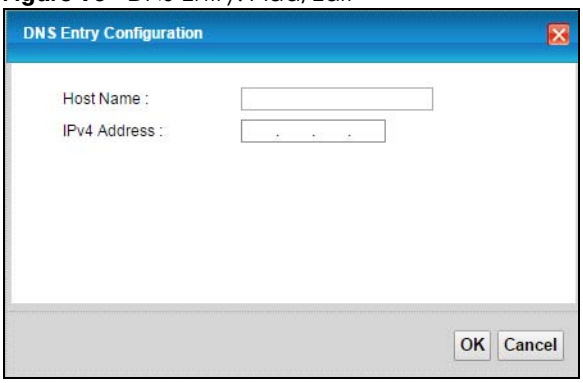
Table 60 Network Setting > DNS > DNS Entry

LABEL	DESCRIPTION
Add New DNS Entry	Click this to create a new DNS entry.
#	This is the index number of the entry.
Hostname	This indicates the host name or domain name.
IP Address	This indicates the IP address assigned to this computer.
Modify	Click the **Edit** icon to edit the rule. Click the **Delete** icon to delete an existing rule.

11.2.1 Add/Edit DNS Entry

You can manually add or edit the EMG's DNS name and IP address entry. Click **Add New DNS Entry** in the **DNS Entry** screen or the **Edit** icon next to the entry you want to edit. The screen shown next appears.

Figure 79 DNS Entry: Add/Edit



The following table describes the labels in this screen.

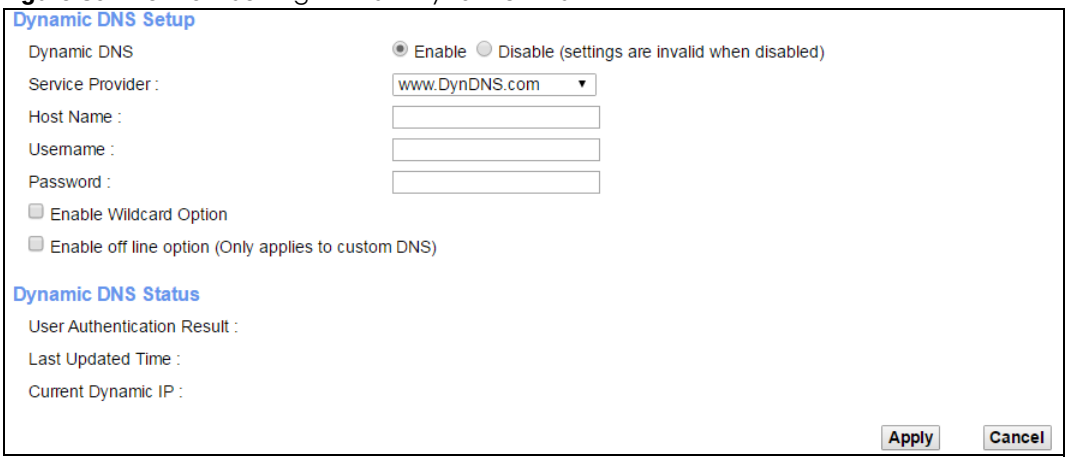
Table 61 DNS Entry: Add/Edit

LABEL	DESCRIPTION
Host Name	Enter the host name of the DNS entry.
IPv4 Address	Enter the IPv4 address of the DNS entry.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

11.3 The Dynamic DNS Screen

Use this screen to change your EMG's DDNS. Click **Network Setting > DNS > Dynamic DNS**. The screen appears as shown.

Figure 80 Network Setting > DNS > Dynamic DNS



The following table describes the fields in this screen.

Table 62 Network Setting > DNS > > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select **Enable** to use dynamic DNS.
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Host Name	Type the domain name assigned to your EMG by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Username	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable Offline Option (Only applies to custom DNS)	Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Dynamic DNS Status	

Table 62 Network Setting > DNS > > Dynamic DNS (continued)

LABEL	DESCRIPTION
User Authentication Result	This shows **Success** if the account is correctly set up with the Dynamic DNS provider account.
Last Updated Time	This shows the last time the IP address the Dynamic DNS provider has associated with the hostname was updated.
Current Dynamic IP	This shows the IP address your Dynamic DNS provider has currently associated with the hostname.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

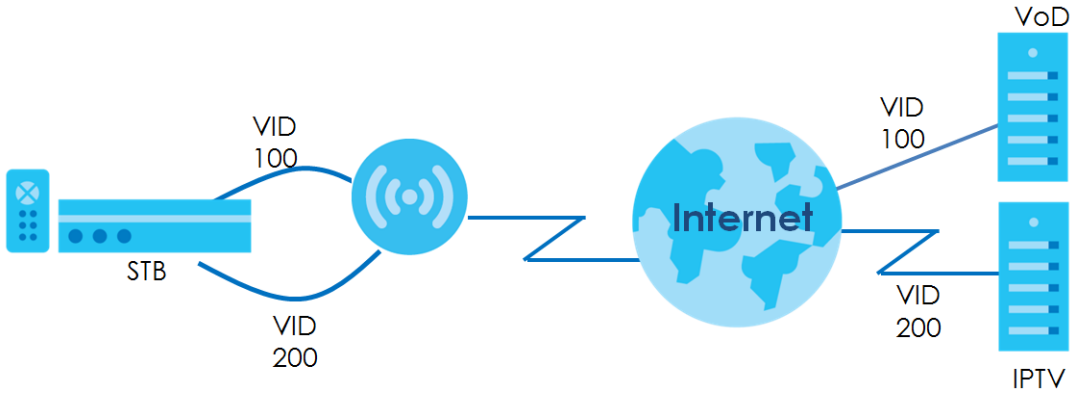
CHAPTER 12
VLAN Group

12.1 Overview

Virtual LAN IDs are used to identify different traffic types over the same physical link.

In the following example, the EMG (DSL) can use VLAN IDs (VID) 100 and 200 to identify Video-on-Demand and IPTV traffic respectively coming from the two VoD and IPTV multicast servers. The EMG (DSL) can also tag outgoing requests to these servers with these VLAN IDs.

Figure 81 VLAN Group Example



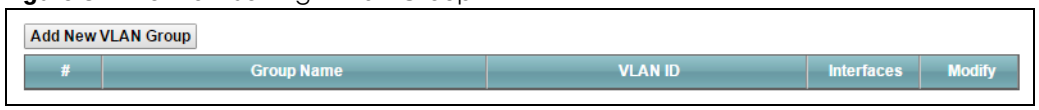
12.1.1 What You Can Do in this Chapter

Use these screens to group separate VLAN groups together to be treated as one VLAN group.

12.2 The VLAN Group Screen

Click **Network Setting > Vlan Group** to open the following screen.

Figure 82 Network Setting > Vlan Group



The following table describes the fields in this screen.

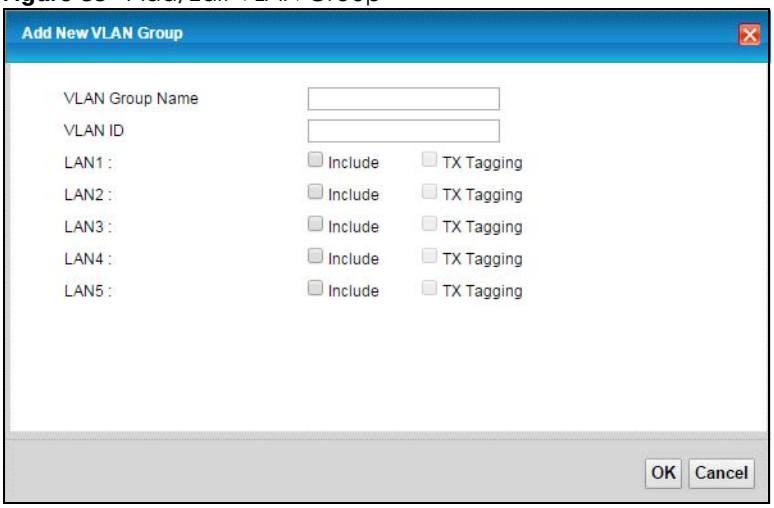
Table 63 Network Setting > Vlan Group

LABEL	DESCRIPTION
Add New Vlan Group	Click this button to create a new VLAN group.
#	This is the index number of the VLAN group.
Group Name	This shows the descriptive name of the VLAN group.
VLAN ID	This shows the unique ID number that identifies the VLAN group.
Interfaces	This shows the LAN ports included in the VLAN group and if traffic leaving the port will be tagged with the VLAN ID.
Modify	Click the **Edit** icon to change an existing VLAN group setting or click the **Delete** icon to remove the VLAN group.

12.2.1 Add/Edit a VLAN Group

Click the **Add New VLAN Group** button in the **Vlan Group** screen to open the following screen. Use this screen to create a new VLAN group.

Figure 83 Add/Edit VLAN Group



The following table describes the fields in this screen.

Table 64 Add/Edit VLAN Group

LABEL	DESCRIPTION
VLAN Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
VLAN ID	Enter a unique ID number, from 1 to 4,094, to identify this VLAN group. Outgoing traffic is tagged with this ID if **Tx Tagging** is selected below.
LAN	Select **Include** to add the associated LAN interface to this VLAN group. Select **Tx Tagging** to tag outgoing traffic from the associated LAN port with the **VLAN ID** number entered above.
OK	Click **OK** to save your changes back to the EMG.
Cancel	Click **Cancel** to exit this screen without saving.

CHAPTER 13
Interface Grouping

13.1 Overview

By default, all LAN and WAN interfaces on the EMG are in the same group and can communicate with each other. Create interface groups to have the EMG assign the IP addresses in different domains to different groups. Each group acts as an independent network on the EMG. This lets devices connected to an interface group's LAN interfaces communicate through the interface group's WAN or LAN interfaces but not other WAN or LAN interfaces.

13.1.1 What You Can Do in this Chapter

The **Interface Grouping** screens let you create multiple networks on the EMG (Section 13.2 on page 149).

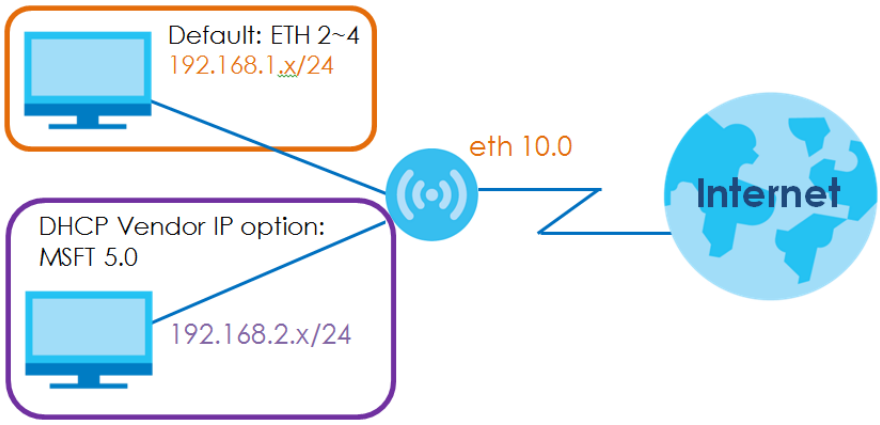
13.2 The Interface Grouping Screen

You can manually add a LAN interface to a new group. Alternatively, you can have the EMG automatically add the incoming traffic and the LAN interface on which traffic is received to an interface group when its DHCP Vendor ID option information matches one listed for the interface group.

Use the **LAN** screen to configure the private IP addresses the DHCP server on the EMG assigns to the clients in the default and/or user-defined groups. If you set the EMG to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See Chapter 7 on page 88 for more information.

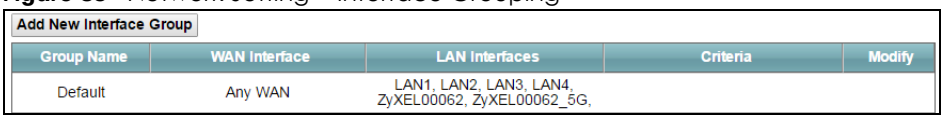
In the following example, the client that sends packets with the DHCP Vendor ID option set to MSFT 5.0 (meaning it is a Windows 2000 DHCP client) is assigned the IP address 192.168.2.2 and uses the WAN VDSL_PoE/ppp0.1 interface.

Figure 84 Interface Grouping Application



Click **Network Setting > Interface Grouping** to open the following screen.

Figure 85 Network Setting > Interface Grouping



The following table describes the fields in this screen.

Table 65 Network Setting > Interface Grouping

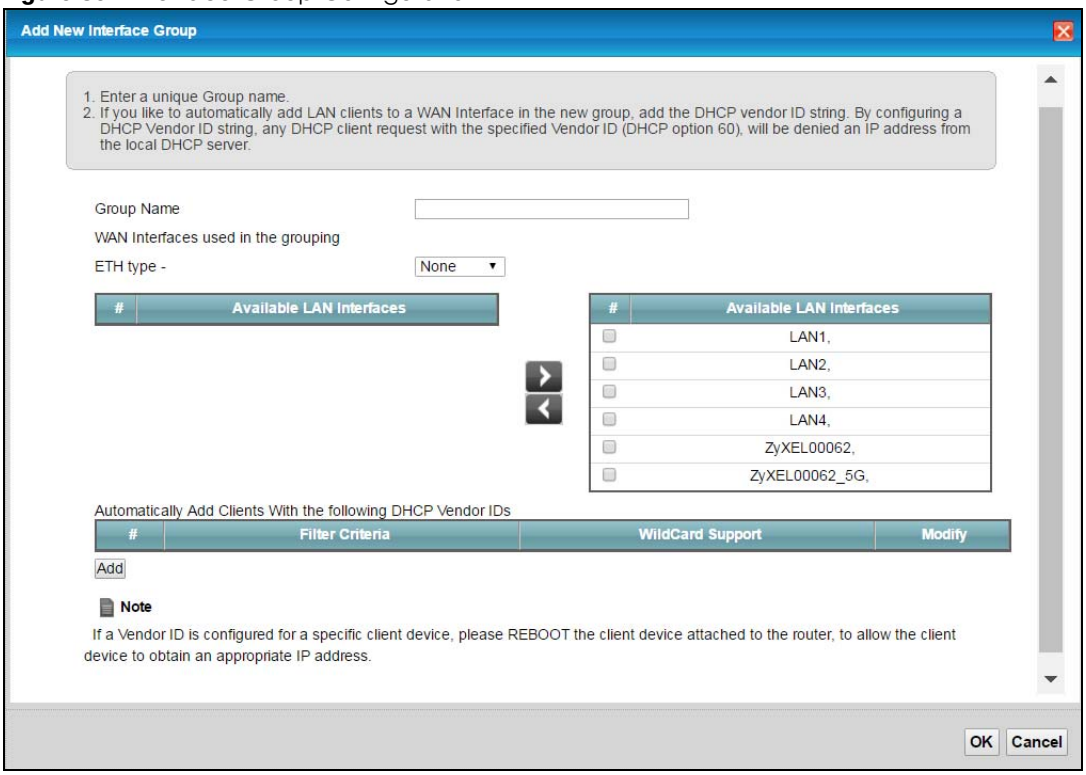
LABEL	DESCRIPTION
Add New Interface Group	Click this button to create a new interface group.
Group Name	This shows the descriptive name of the group.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN interfaces in the group.
Criteria	This shows the filtering criteria for the group.
Modify	Click the **Delete** icon to remove the group.

13.2.1 Interface Group Configuration

Click the **Add New Interface Group** button in the **Interface Grouping** screen to open the following screen. Use this screen to create a new interface group.

Note: An interface can belong to only one group at a time.

Figure 86 Interface Group Configuration



The following table describes the fields in this screen.

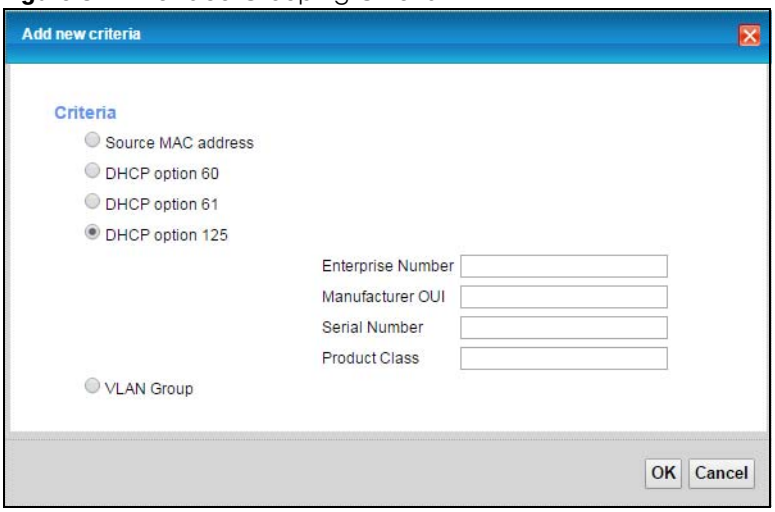
Table 66 Interface Group Configuration

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
WAN Interfaces used in the grouping	Select the WAN interface this group uses. The group can have up to one ETH interface. Select **None** to not add a WAN interface to this group.
Available LAN Interfaces	Select one or more LAN interfaces (Ethernet LAN, HPNA or wireless LAN) on the right interface list and use the left arrow to move them to the interface list on the left to add the interfaces to this group. To remove a LAN or wireless LAN interface from the interface list on the left, use the rightfacing arrow.
Automatically Add Clients With the following DHCP Vendor IDs	Click **Add** to identify LAN hosts to add to the interface group by criteria such as the type of the hardware or firmware. See Section 13.2.2 on page 151 for more information.
#	This shows the index number of the rule.
Filter Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.
WildCard Support	This shows if wildcard on DHCP option 60 is enabled.
Modify	Click the **Modify** icon to edit this rule from the EMG.
OK	Click **OK** to save your changes back to the EMG.
Cancel	Click **Cancel** to exit this screen without saving.

13.2.2 Interface Grouping Criteria

Click the **Add** button in the **Interface Grouping Configuration** screen to open the following screen.

Figure 87 Interface Grouping Criteria



The following table describes the fields in this screen.

Table 67 Interface Grouping Criteria

LABEL	DESCRIPTION
Source MAC Address	Select this option and enter the source MAC address of the packet.
DHCP Option 60	Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
Enable wildcard	Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60.
DHCP Option 61	Select this and enter the device identity of the matched traffic.
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.
Enterprise Number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address.
Serial Number	Enter the serial number of the device.
Product Class	Enter the product class of the device.
VLAN Group	Select this and the VLAN group of the matched traffic from the drop-down list box.
OK	Click **OK** to save your changes back to the EMG.
Cancel	Click **Cancel** to exit this screen without saving.

CHAPTER 14
Firewall

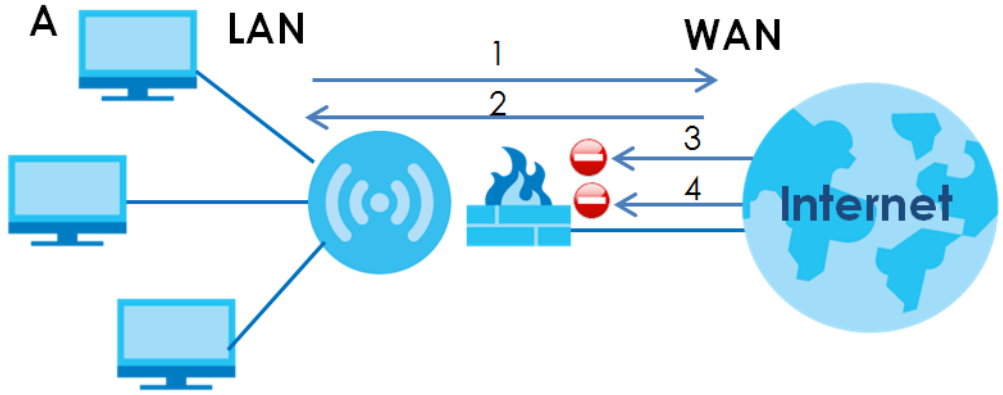
14.1 Overview

This chapter shows you how to enable and configure the EMG's security settings. Use the firewall to protect your EMG and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 88 Default Firewall Action



14.1.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the EMG (Section 14.2 on page 154).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 14.3 on page 155).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules (Section 14.4 on page 157).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (.Section 14.5 on page 159).

14.1.2 What You Need to Know

SYN Attack

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The EMG is pre-configured to automatically detect and thwart all known DoS attacks.

DDoS

A DDoS attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

Ping of Death

Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

SPI

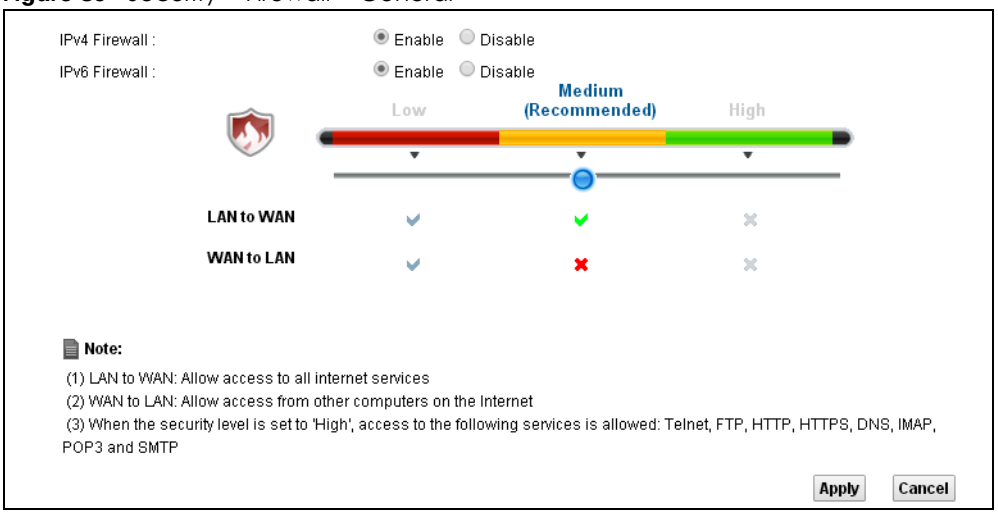
Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

14.2 The Firewall Screen

Use this screen to set the security level of the firewall on the EMG. Firewall rules are grouped based on the direction of travel of packets to which they apply.

Click **Security > Firewall** to display the **General** screen.

Figure 89 Security > Firewall > General



The following table describes the labels in this screen.

Table 68 Security > Firewall > General

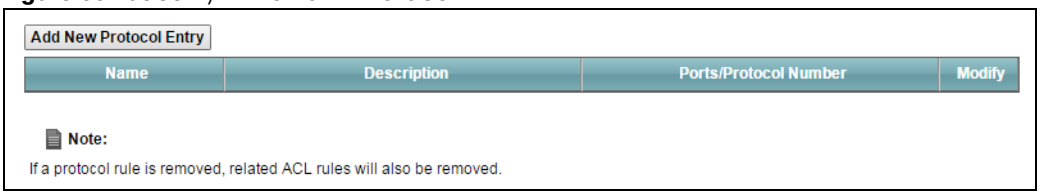
LABEL	DESCRIPTION
Firewall	Select **Enable** to activate the firewall feature on the EMG.
Low	Select **Low** to allow LAN to WAN and WAN to LAN packet directions.
Medium	Select **Medium** to allow LAN to WAN but deny WAN to LAN packet directions.
High	Select **High** to deny LAN to WAN and WAN to LAN packet directions.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

14.3 The Protocol Screen

You can configure customized services and port numbers in the **Protocol** screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See Appendix D on page 242 for some examples.

Click **Security > Firewall > Protocol** to display the following screen.

Figure 90 Security > Firewall > Protocol



The following table describes the labels in this screen.

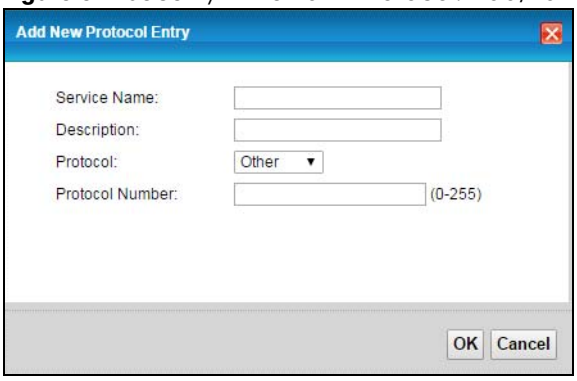
Table 69 Security > Firewall > Protocol

LABEL	DESCRIPTION
Add New Protocol Entry	Click this to add a new service.
Name	This is the name of your customized service.
Description	This is the description of your customized service.
Ports/Protocol Number	This shows the IP protocol (**TCP**, **UDP**, **ICMP**, or **TCP/UDP**) and the port number or range of ports that defines your customized service. **Other** and the protocol number displays if the service uses another IP protocol.
Modify	Click the **Edit** icon to edit the entry. Click the **Delete** icon to remove this entry.

14.3.1 Add/Edit a Service

Use this screen to add a customized service rule that you can use in the firewall's ACL rule configuration. Click **Add New Protocol Entry** or the edit icon next to an existing service rule in the **Protocol** screen to display the following screen.

Figure 91 Security > Firewall > Protocol: Add/Edit



The following table describes the labels in this screen.

Table 70 Security > Firewall > Protocol: Add/Edit

LABEL	DESCRIPTION
Service Name	Enter a unique name (up to 32 printable English keyboard characters, including spaces) for your customized port.
Description	Enter a description for your customized port.
Protocol	Choose the IP protocol (**TCP**, **UDP**, **ICMP**, **ICMPv6** or **Other**) that defines your customized port from the drop-down list box. Select **Other** to be able to enter a protocol number.
Source/ Destination Port	These fields are displayed if you select **TCP** or **UDP** as the IP port. Select **Single** to specify one port only or **Range** to specify a span of ports that define your customized service. If you select **Any**, the service is applied to all ports. Type a single port number or the range of port numbers that define your customized service.
Protocol Number	This field is displayed if you select **Other** as the protocol. Enter the protocol number of your customized port.

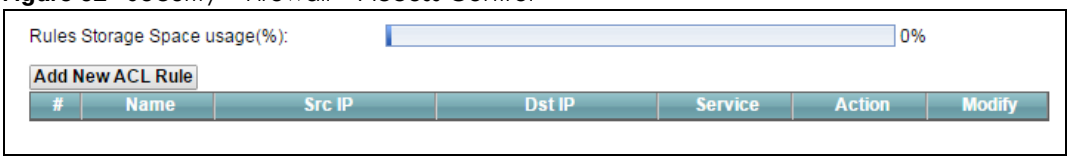
Table 70 Security > Firewall > Protocol: Add/Edit (continued)

LABEL	DESCRIPTION
ICMPv6 Type	This field is displayed if you select **ICMPv6** as the protocol. Enter the type value for the ICMPv6 messages.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

14.4 The Access Control Screen

Click **Security > Firewall > Access Control** to display the following screen. This screen displays a list of the configured incoming or outgoing filtering rules.

Figure 92 Security > Firewall > Access Control



The following table describes the labels in this screen.

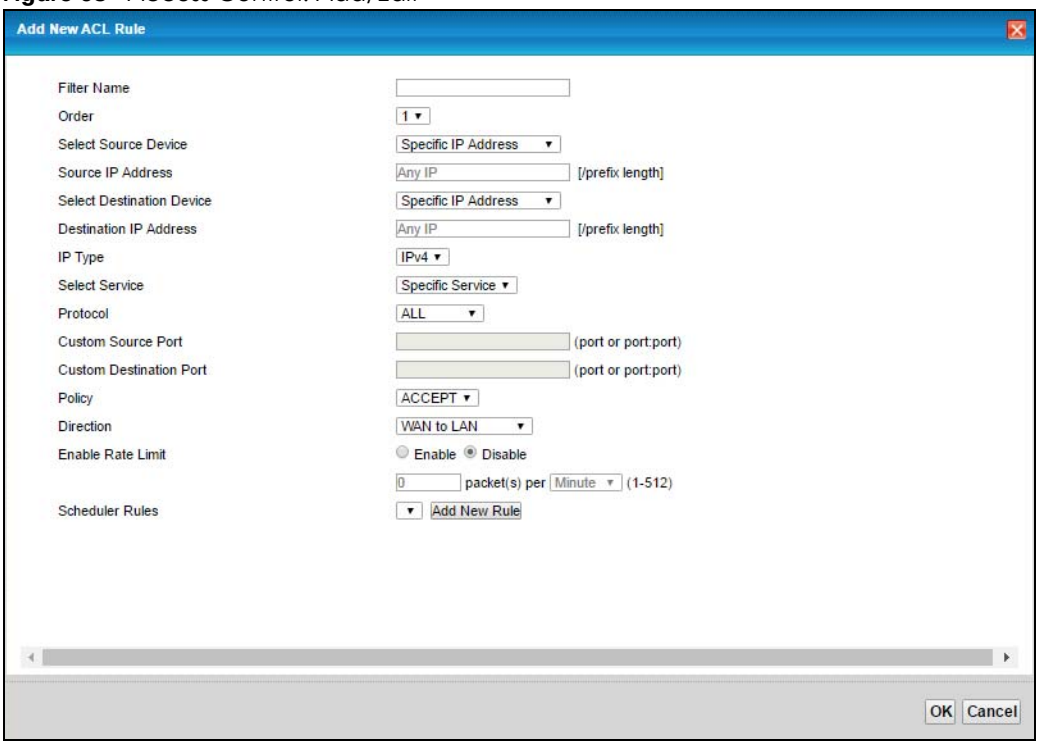
Table 71 Security > Firewall > Access Control

LABEL	DESCRIPTION
Add New ACL Rule	Click this to go to add a filter rule for incoming or outgoing IP traffic.
#	This is the index number of the entry.
Name	This displays the name of the rule.
Src IP	This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to **Any**.
Dst IP	This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to **Any**.
Service	This displays the transport layer protocol that defines the service and the direction of traffic to which this rule applies.
Action	This field displays whether the rule silently discards packets (**DROP**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**REJECT**) or allows the passage of packets (**ACCEPT**).
Modify	Click the **Edit** icon to edit the rule. Click the **Delete** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action. Click the **Move To** icon to change the order of the rule. Enter the number in the # field.

14.4.1 Add/Edit an ACL Rule

Click **Add new ACL rule** or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays.

Figure 93 Access Control: Add/Edit



The following table describes the labels in this screen.

Table 72 Access Control: Add/Edit

LABEL	DESCRIPTION
Filter Name	Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes. You must enter the filter name to add an ACL rule. This field is read-only if you are editing the ACL rule.
Order	Select the order of the ACL rule.
Select Source Device	Select the source device to which the ACL rule applies. If you select **Specific IP Address**, enter the source IP address in the field below.
Source IP Address	Enter the source IP address.
Select Destination Device	Select the destination device to which the ACL rule applies. If you select **Specific IP Address**, enter the destiniation IP address in the field below.
Destination IP Address	Enter the destination IP address.
IP Type	Select whether your IP type is **IPv4** or **IPv6**.
Select Service	Select the transport layer protocol that defines your customized port from the drop-down list box. The specific protocol rule sets you add in the **Security > Firewall > Service > Add** screen display in this list. If you want to configure a customized protocol, select **Specific Service**.
Protocol	This field is displayed only when you select **Specific Protocol** in **Select Protocol**. Choose the IP port (**TCP/UDP**, **TCP**, **UDP**, **ICMP**, or **ICMPv6**) that defines your customized port from the drop-down list box.

Table 72 Access Control: Add/Edit (continued)

LABEL	DESCRIPTION
Custom Source Port	This field is displayed only when you select **Specific Protocol** in **Select Protocol**. Enter a single port number or the range of port numbers of the source.
Custom Destination Port	This field is displayed only when you select **Specific Protocol** in **Select Protocol**. Enter a single port number or the range of port numbers of the destination.
Policy	Use the drop-down list box to select whether to discard (**DROP**), deny and send an ICMP destination-unreachable message to the sender of (**REJECT**) or allow the passage of (**ACCEPT**) packets that match this rule.
Direction	Use the drop-down list box to select the direction of traffic to which this rule applies.
Enable Rate Limit	Select **Enable** to set a limit on the upstream/downstream transmission rate for the specified protocol. Specify how many packets per minute or second the transmission rate is.
Scheduler Rules	Select a schedule rule for this ACL rule form the drop-down list box. You can configure a new schedule rule by click **Add New Rule**. This will bring you to the **Security > Scheduler Rules** screen.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

14.5 The DoS Screen

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable.

Use the **DoS** screen to activate protection against DoS attacks. Click **Security > Firewall > DoS** to display the following screen.

Figure 94 Security > Firewall > DoS

The following table describes the labels in this screen.

Table 73 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Select **Enable** to enable protection against DoS attacks.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

CHAPTER 15
MAC Filter

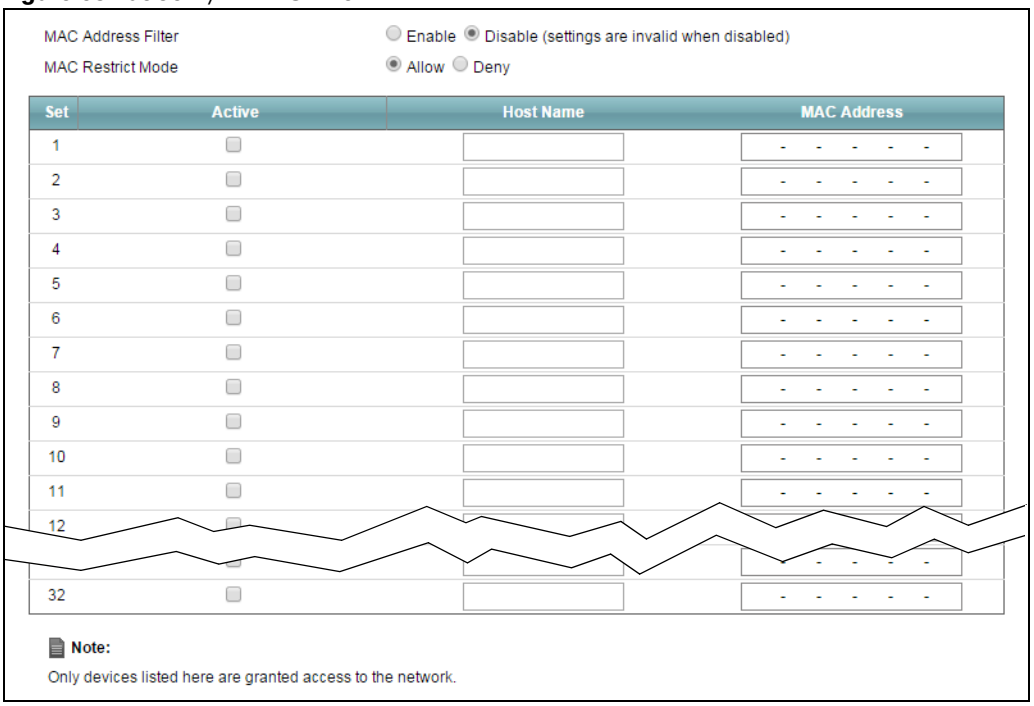
15.1 Overview

You can configure the EMG to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

15.2 The MAC Filter Screen

Use this screen to allow wireless and LAN clients access to the EMG. Click **Security** > **MAC Filter**. The screen appears as shown.

Figure 95 Security > MAC Filter



The following table describes the labels in this screen.

Table 74 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select **Enable** to activate the MAC filter function.
MAC Restrict Mode	Select **Allow** to only permit the listed MAC addresses access to the EMG. Select **Deny** to permit anyone access to the EMG except the listed MAC addresses.
Set	This is the index number of the MAC address.
Active	Select **Active** to enable the MAC filter rule. . The rule will not be applied if **Active** is not selected.
Host Name	Enter the host name of the wireless or LAN clients that are allowed access to the EMG.
MAC Address	Enter the MAC addresses of the wireless or LAN clients that are allowed access to the EMG in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

CHAPTER 16
Parental Control

16.1 Overview

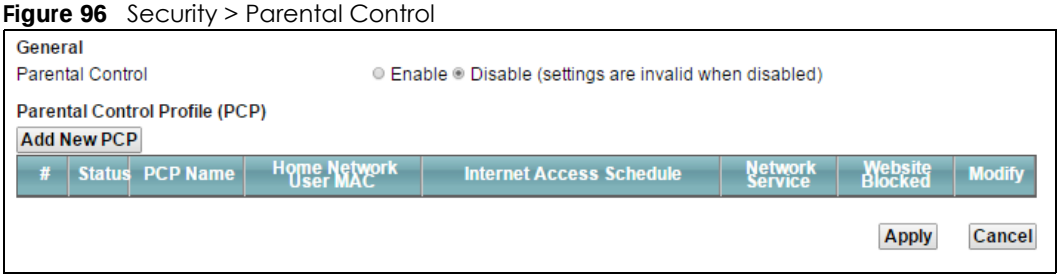
Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the EMG performs parental control on a specific user.

16.2 The Parental Control Screen

Use this screen to enable parental control, view the parental control rules and schedules.

Click **Security** > **Parental Control** to open the following screen.

Figure 96 Security > Parental Control



The following table describes the fields in this screen.

Table 75 Security > Parental Control

LABEL	DESCRIPTION
General	
Parental Control	Select **Enable** to activate parental control.
Parental Control Profile (PCP)	
Add New PCP	Click this if you want to configure a new Parental Control Profile.
#	This shows the index number of the rule.
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
PCP Name	This shows the name of the rule.
Home Network User MAC	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the day(s) and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, **None** will be shown.
Website Blocked	This shows whether the website block is configured. If not, **None** will be shown.

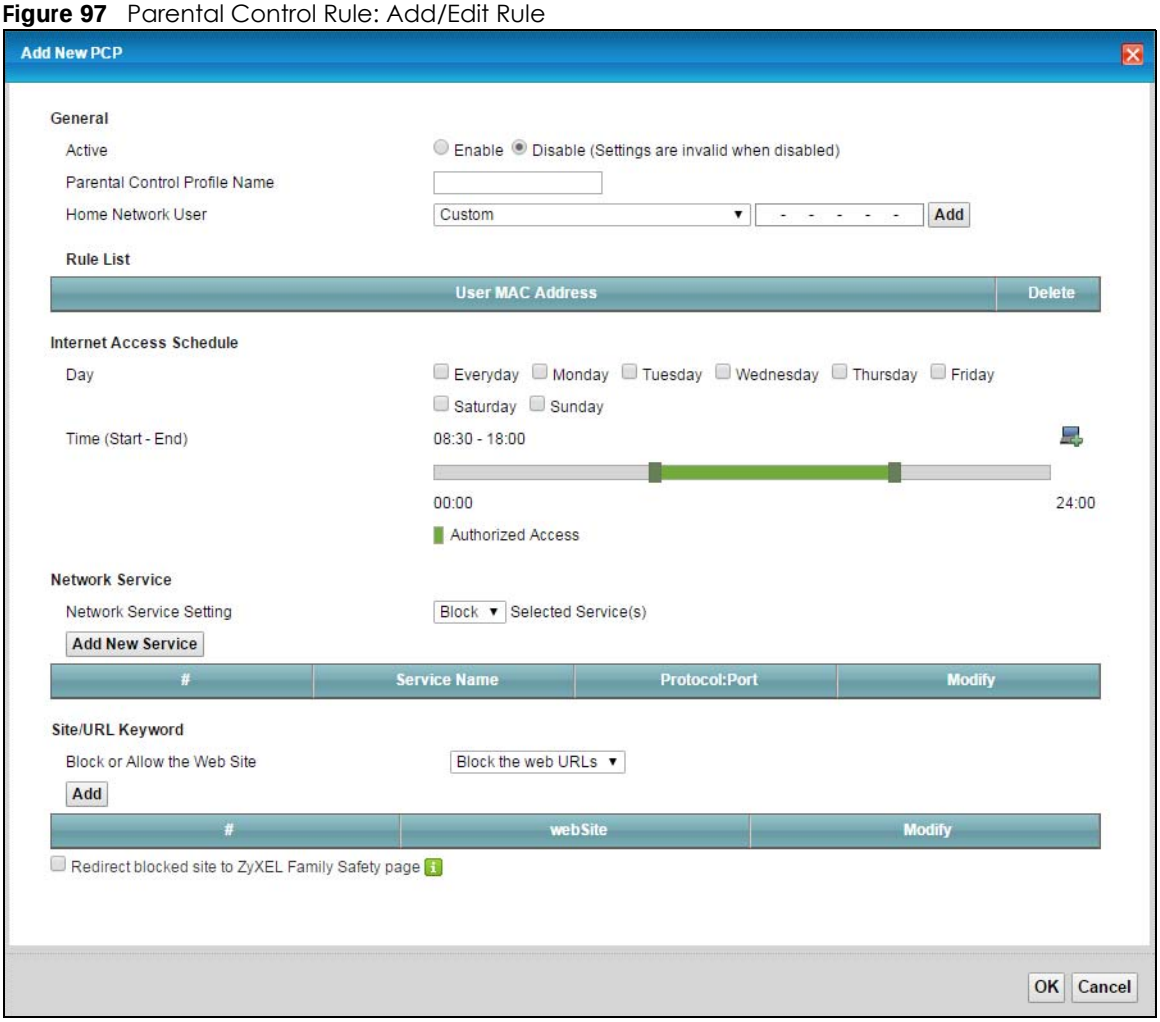
Table 75 Security > Parental Control (continued)

LABEL	DESCRIPTION
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

16.2.1 Add/Edit a Parental Control Profile

Click **Add New PCP** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 97 Parental Control Rule: Add/Edit Rule



The following table describes the fields in this screen.

Table 76 Parental Control Rule: Add/Edit

LABEL	DESCRIPTION
General	
Active	Select to enable or disable this parental control rule.
Parental Control Profile Name	Enter a descriptive name for the rule.
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select **Custom**, enter the LAN user's MAC address. If you select **All**, the rule applies to all LAN users.
Rule List	In **Home Network User**, select **Custom**, enter the LAN user's MAC address, then click the **Add** icon to enter a computer MAC address for this PCP. Up to five are allowed. Click the **Delete** icon to remove one.
Internet Access Schedule	
Day	Select check boxes for the days that you want the EMG to perform parental control.
Time	Drag the time bar to define the time that the LAN user is allowed access (**Authorized access**) or denied access (**No access**). Click the **Add** icon above the time bar to add a new time bar. Up to three are allowed.
Network Service	
Network Service Setting	If you select **Block**, the EMG prohibits the users from viewing the Web sites with the URLs listed below. If you select **Allow**, the EMG blocks access to all URLs except ones listed below.
Add New Service	Click this to show a screen in which you can add a new service rule. You can configure the **Service Name**, **Protocol**, and **Name** of the new rule.
#	This shows the index number of the rule.
Service Name	This shows the name of the rule.
Protocol:Port	This shows the protocol and the port of the rule.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Site/URL Keyword	
Block or Allow the Web Site	If you select **Block the Web URLs**, the EMG prohibits the users from viewing the Web sites with the URLs listed below. If you select **Allow the Web URLs**, the EMG blocks access to all URLs except ones listed below.
Add	Click **Add** to show a screen to enter the URL of web site or URL keyword to which the EMG blocks or allows access.
#	This shows the index number of the rule.
WebSite	This shows the URL of web site or URL keyword to which the EMG blocks or allows access.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.

Table 76 Parental Control Rule: Add/Edit (continued)

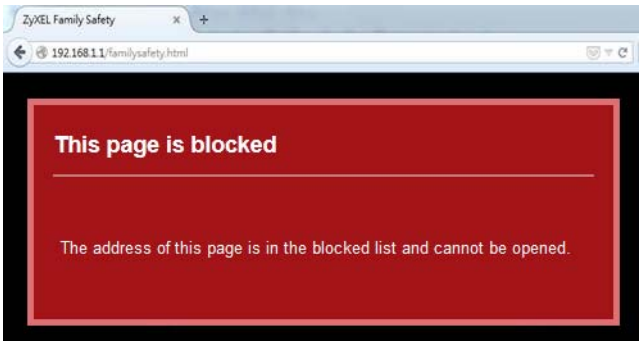
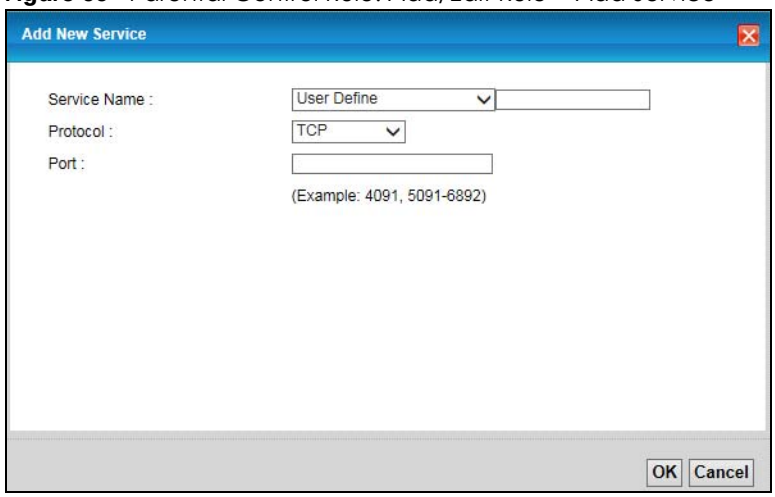
LABEL	DESCRIPTION
Redirect blocked site to Zyxel Family Safety page	Select this to redirect users who access any blocked websites listed above to the Zyxel Family Safety page as shown next. **Figure 98** Zyxel Family Safety Page Example 
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to to exit this screen without saving.

Figure 99 Parental Control Rule: Add/Edit Rule > Add Service



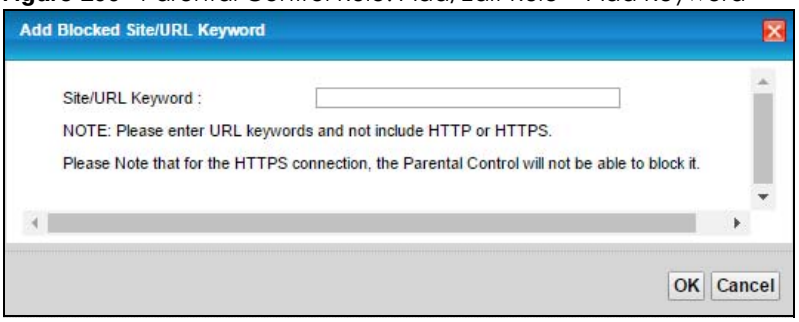
The following table describes the fields in this screen.

Table 77 Parental Control Rule: Add/Edit > Add New Service

LABEL	DESCRIPTION
Service Name	Select the name of the service. Otherwise, select **User Define** and manualy specify the protocol and the port of the service. If you have chosen a pre-defined service in the **Service Name** field, this field will not be configurable.
Protocol	Select the transport layer protocol used for the service. Choices are **TCP**, **UDP**, or **TCP & UDP**.
Port	Enter the port of the service. If you have chosen a pre-defined service in the **Service Name** field, this field will not be configurable.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

Click **Security** > **Parental Control** > **Add New PCP** > **Add** to open the following screen.

Figure 100 Parental Control Rule: Add/Edit Rule > Add Keyword



The following table describes the fields in this screen.

Table 78 Parental Control Rule: Add/Edit > Add Keyword

LABEL	DESCRIPTION
Site/URL Keyword	Enter a keyword and click **OK** to have the EMG block access to the website URLs that contain the keyword.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

CHAPTER 17
Scheduler Rule

17.1 Overview

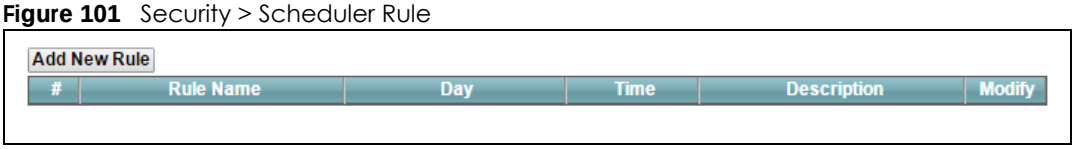
You can define time periods and days during which the EMG performs scheduled rules of certain features (such as Firewall Access Control) in the **Scheduler Rule** screen.

17.2 The Scheduler Rule Screen

Use this screen to view, add, or edit time schedule rules.

Click **Security > Scheduler Rule** to open the following screen.

Figure 101 Security > Scheduler Rule



The following table describes the fields in this screen.

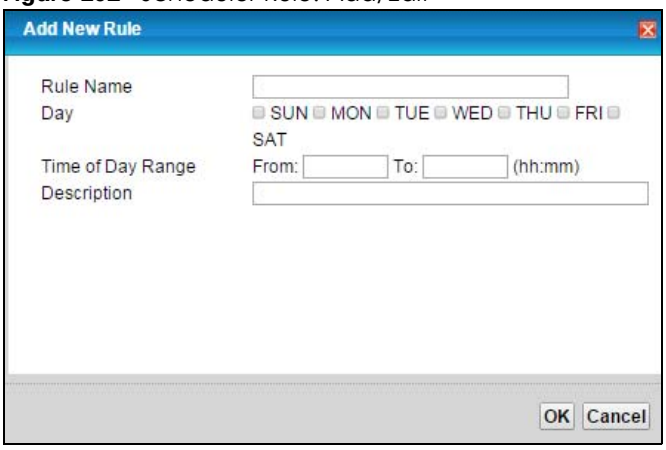
Table 79 Security > Scheduler Rule

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Rule Name	This shows the name of the rule.
Day	This shows the day(s) on which this rule is enabled.
Time	This shows the period of time on which this rule is enabled.
Description	This shows the description of this rule.
Modify	Click the **Edit** icon to edit the schedule. Click the **Delete** icon to delete a scheduler rule. Note: You cannot delete a scheduler rule once it is applied to a certain feature.

17.2.1 Add/Edit a Schedule

Click the **Add New Rule** button in the **Scheduler Rule** screen or click the **Edit** icon next to a schedule rule to open the following screen. Use this screen to configure a restricted access schedule.

Figure 102 Scheduler Rule: Add/Edit



The following table describes the fields in this screen.

Table 80 Scheduler Rule: Add/Edit

LABEL	DESCRIPTION
Rule Name	Enter a name (up to 31 printable English keyboard characters, not including spaces) for this schedule.
Day	Select check boxes for the days that you want the EMG to perform this scheduler rule.
Time of Day Range	Enter the time period of each day, in 24-hour format, during which the rule will be enforced.
Description	Enter a description for this scheduler rule.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

CHAPTER 18
Certificates

18.1 Overview

The EMG can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

18.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to generate certification requests and import the EMG's CA-signed certificates (Section 18.4 on page 172).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the EMG (Section 18.4 on page 172).

18.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the EMG to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

18.3 The Local Certificates Screen

Click **Security > Certificates** to open the **Local Certificates** screen. This is the EMG's summary list of certificates and certification requests.

Figure 103 Security > Certificates > Local Certificates

The following table describes the labels in this screen.

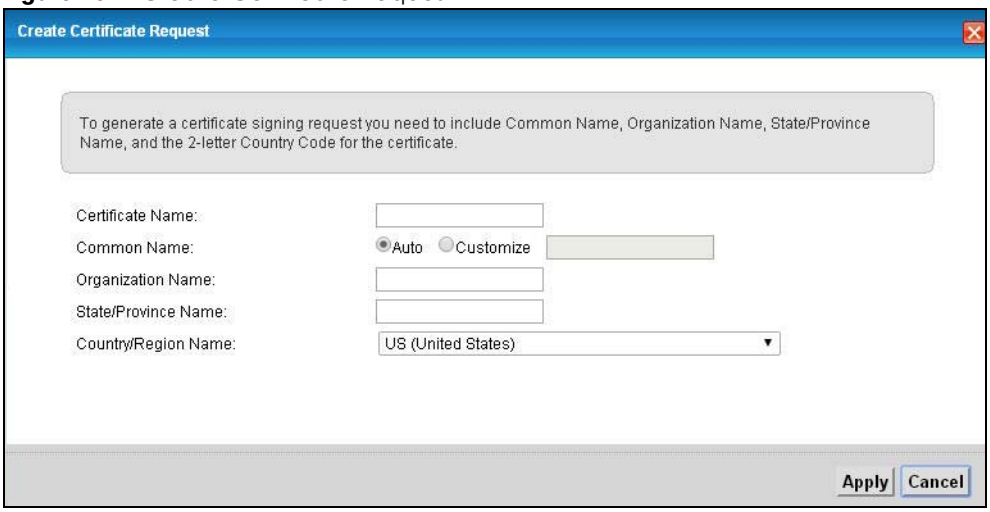
Table 81 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Private Key is protected by a password	Select the checkbox and enter the private key into the text box to store it on the EMG. The private key should not exceed 63 ASCII characters (not including spaces).
Choose File	Click this to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the EMG.
Create Certificate Request	Click this button to go to the screen where you can have the EMG generate a certification request.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). For a certification request, click **Load Signed** to import the signed certificate. Click the **Remove** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

18.3.1 Create Certificate Request

Click **Security** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the EMG generate a certification request.

Figure 104 Create Certificate Request



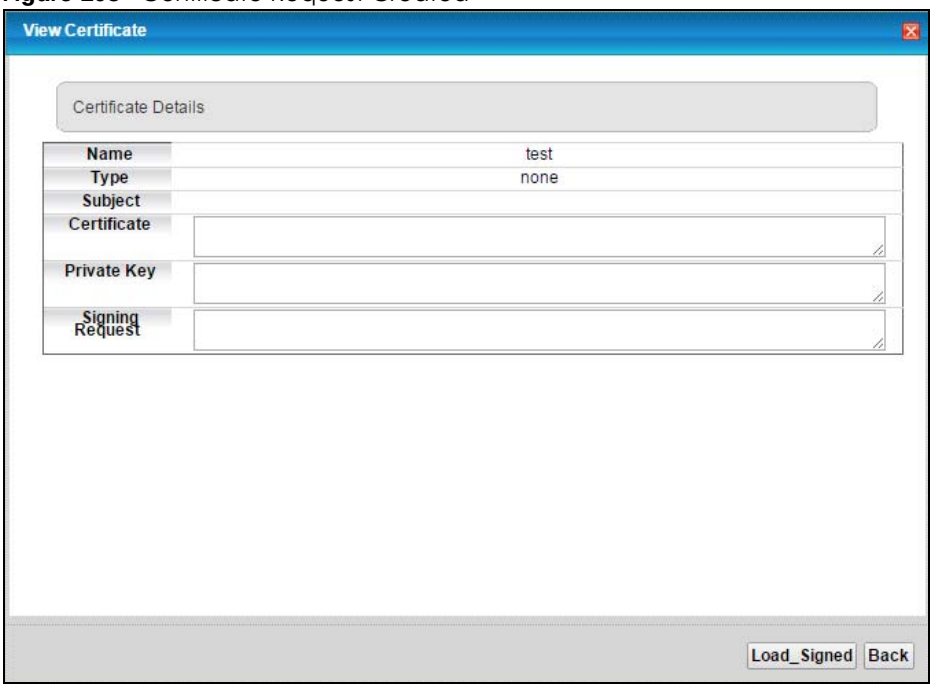
The following table describes the labels in this screen.

Table 82 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select **Auto** to have the EMG configure this field automatically. Or select **Customize** to enter it manually. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the EMG drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the EMG drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

After you click **Apply**, the following screen displays to notify you that you need to get the certificate request signed by a Certificate Authority. If you already have, click **Load_Signed** to import the signed certificate into the EMG. Otherwise click **Back** to return to the **Local Certificates** screen.

Figure 105 Certificate Request Created

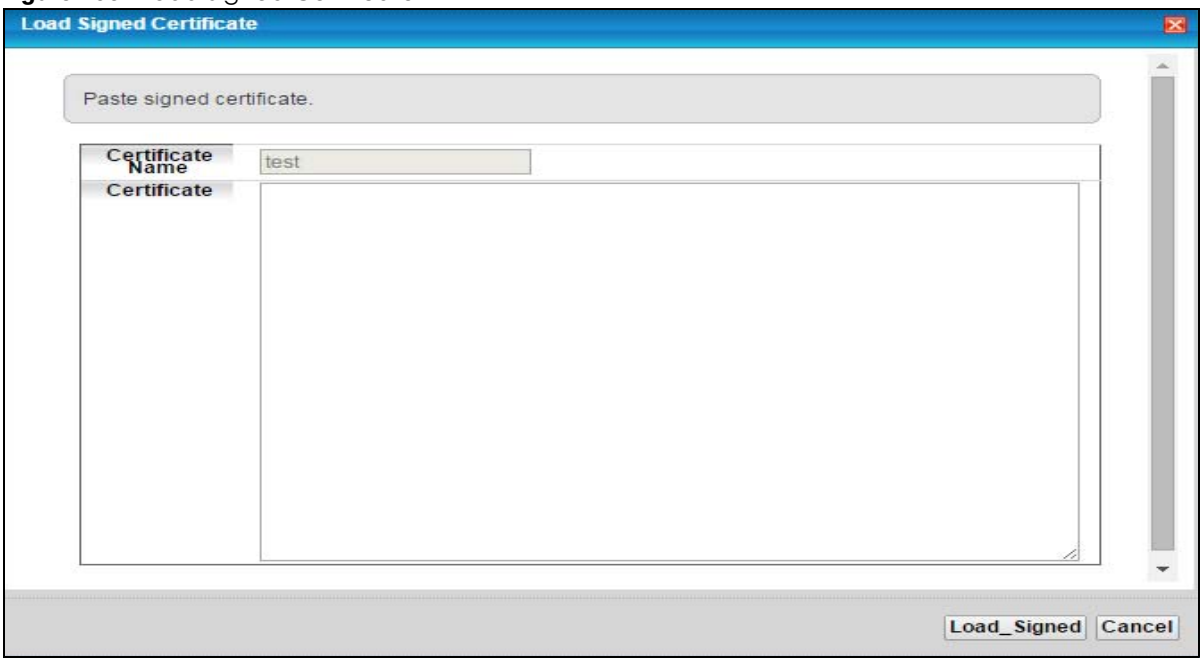


18.3.2 Load Signed Certificate

After you create a certificate request and have it signed by a Certificate Authority, in the **Local Certificates** screen click the certificate request's **Load Signed** icon to import the signed certificate into the EMG.

Note: You must remove any spaces from the certificate's filename before you can import it.

Figure 106 Load Signed Certificate



The following table describes the labels in this screen.

Table 83 Load Signed Certificate

LABEL	DESCRIPTION
Certificate Name	This is the name of the signed certificate.
Certificate	Copy and paste the signed certificate into the text box to store it on the EMG.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

18.4 The Trusted CA Screen

Click **Security > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the EMG to accept as trusted. The EMG accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 107 Security > Certificates > Trusted CA

The following table describes the fields in this screen.

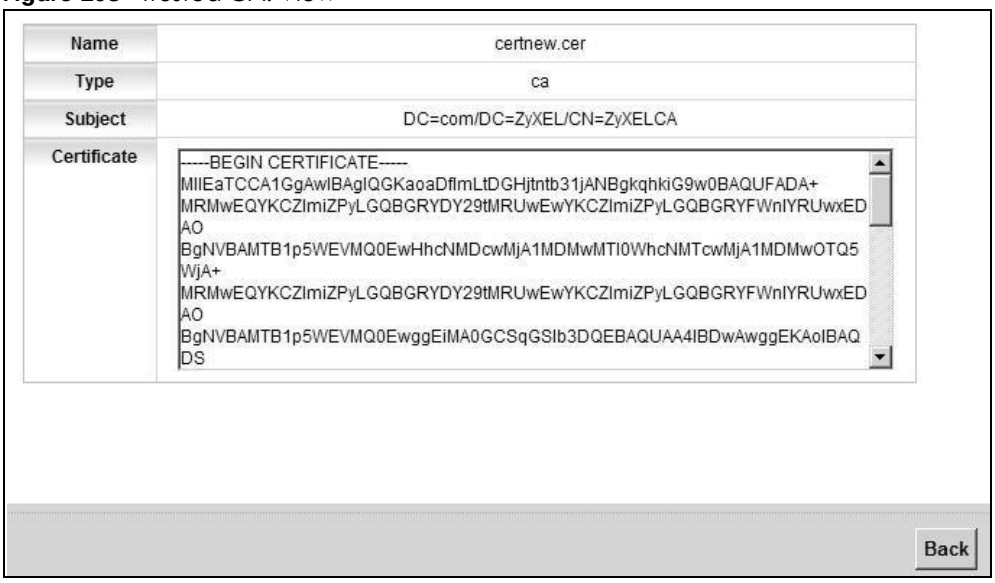
Table 84 Security > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the EMG.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

18.4.1 View Trusted CA Certificate

Click the **View** icon in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate.

Figure 108 Trusted CA: View



The following table describes the fields in this screen.

Table 85 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).

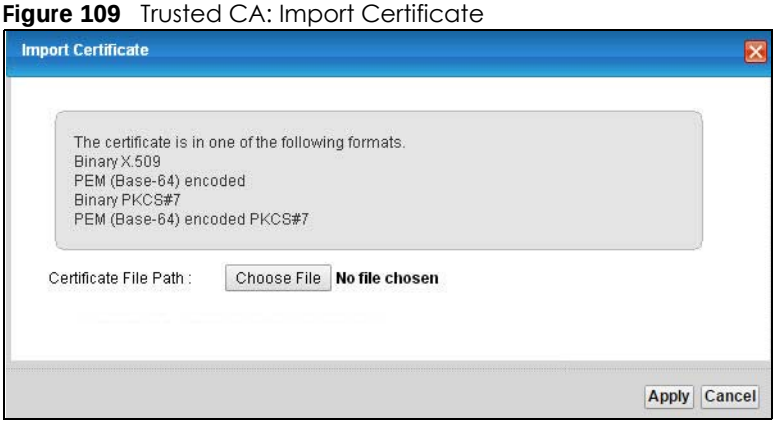
Table 85 Trusted CA: View (continued)

LABEL	DESCRIPTION
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click **Back** to return to the previous screen.

18.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The EMG trusts any valid certificate signed by any of the imported trusted CA certificates.

Figure 109 Trusted CA: Import Certificate



The following table describes the fields in this screen.

Table 86 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate File Path	Type in the location of the certificate you want to upload in this field or click **Choose File** to find it.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

CHAPTER 19
Log

19.1 Overview

The web configurator allows you to choose which categories of events and/or alerts to have the EMG log and then display the logs or have the EMG send them to an administrator (as e-mail) or to a syslog server.

19.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs (Section 19.2 on page 176).
- Use the **Security Log** screen to see the security-related logs for the categories that you select (Section 19.3 on page 176).

19.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 87 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.

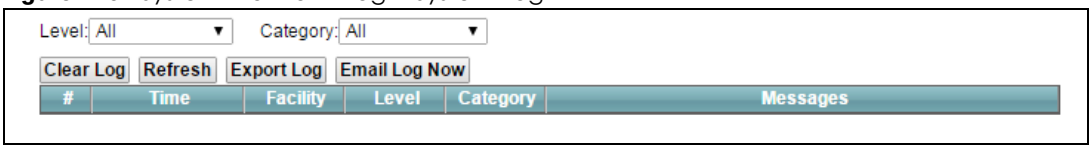
Table 87 Syslog Severity Levels

CODE	SEVERITY
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

19.2 The System Log Screen

Use the **System Log** screen to see the system logs. Click **System Monitor > Log** to open the **System Log** screen.

Figure 110 System Monitor > Log > System Log



The following table describes the fields in this screen.

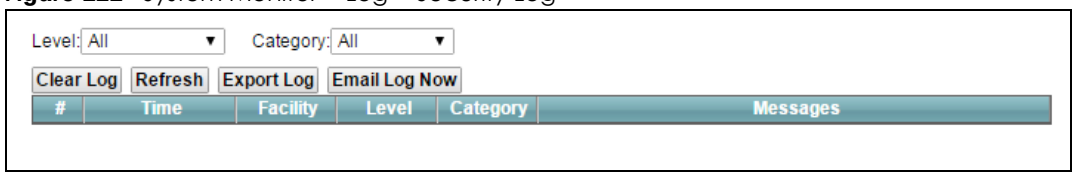
Table 88 System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the EMG searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s).
Email Log Now	Click this to send the log file(s) to the E-mail address you specify in the **Maintenance > Logs Setting** screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

19.3 The Security Log Screen

Use the **Security Log** screen to see the security-related logs for the categories that you select. Click **System Monitor > Log > Security Log** to open the following screen.

Figure 111 System Monitor > Log > Security Log



The following table describes the fields in this screen.

Table 89 System Monitor > Log > Security Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the EMG searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s).
E-mail Log Now	Click this to send the log file(s) to the E-mail address you specify in the **Maintenance > Logs Setting** screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

CHAPTER 20
Traffic Status

20.1 Overview

Use the **Traffic Status** screens to look at network traffic status and statistics of the WAN, LAN interfaces and NAT.

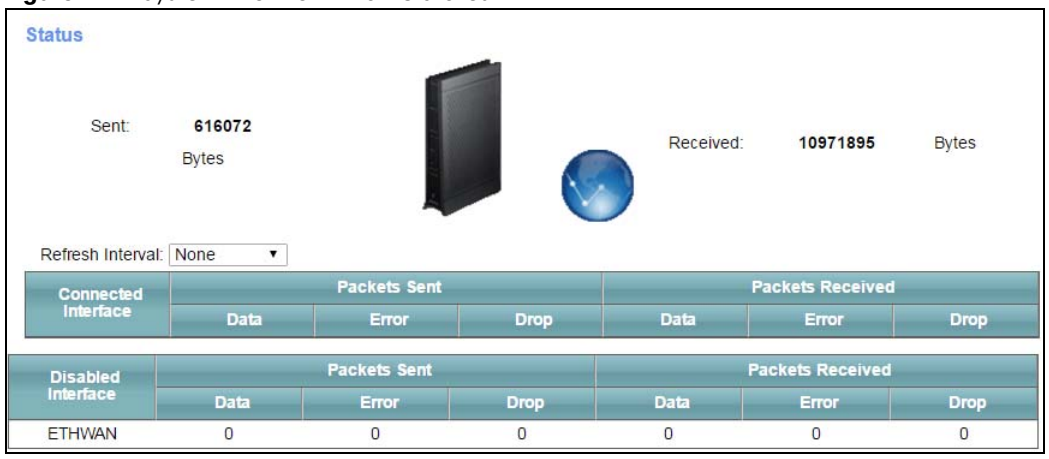
20.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 20.2 on page 178).
- Use the **LAN** screen to view the LAN traffic statistics (Section 20.3 on page 179).
- Use the **NAT** screen to view the NAT status of the EMG's client(s) (Section 20.4 on page 180)

20.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. The figure in this screen shows the number of bytes received and sent on the EMG.

Figure 112 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 90 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the EMG to update this screen.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	

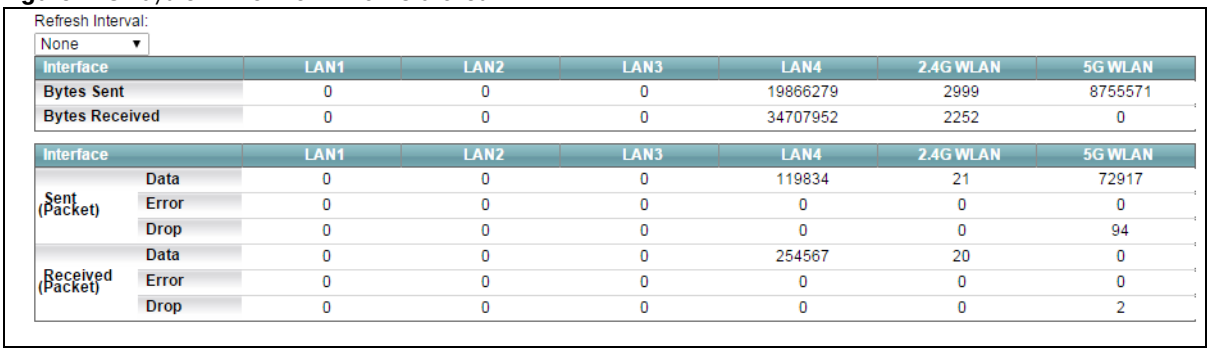
Table 90 System Monitor > Traffic Status > WAN (continued)

LABEL	DESCRIPTION
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.
Disabled Interface	This shows the name of the WAN interface that is currently disconnected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

20.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. The figure in this screen shows the interface that is currently connected on the EMG.

Figure 113 System Monitor > Traffic Status > LAN



Interface	LAN1	LAN2	LAN3	LAN4	2.4G WLAN	5G WLAN
Bytes Sent	0	0	0	19866279	2999	8755571
Bytes Received	0	0	0	34707952	2252	0

Interface		LAN1	LAN2	LAN3	LAN4	2.4G WLAN	5G WLAN
Sent (Packet)	Data	0	0	0	119834	21	72917
	Error	0	0	0	0	0	0
	Drop	0	0	0	0	0	94
Received (Packet)	Data	0	0	0	254567	20	0
	Error	0	0	0	0	0	0
	Drop	0	0	0	0	0	2

The following table describes the fields in this screen.

Table 91 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the EMG to update this screen.
Interface	This shows the LAN or WLAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.

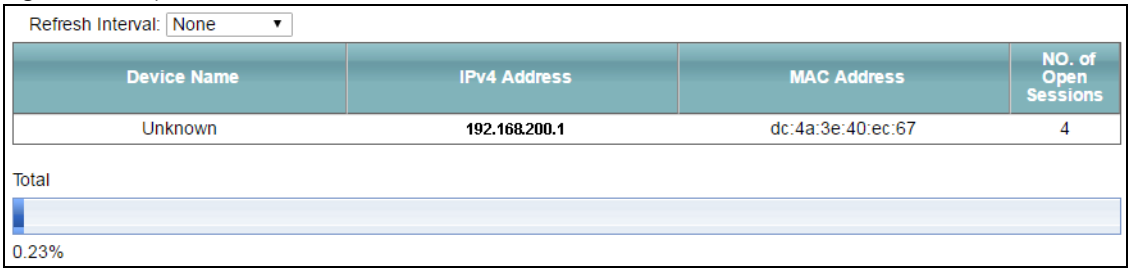
Table 91 System Monitor > Traffic Status > LAN (continued)

LABEL	DESCRIPTION
Interface	This shows the LAN or WLAN interfaces.
Sent (Packets)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packets)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

20.4 The NAT Status Screen

Click **System Monitor > Traffic Status > NAT** to open the following screen. The figure in this screen shows the NAT session statistics for hosts currently connected on the EMG.

Figure 114 System Monitor > Traffic Status > NAT



The following table describes the fields in this screen.

Table 92 System Monitor > Traffic Status > NAT

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the EMG to update this screen.
Device Name	This displays the name of the connected host.
IPv4 Address	This displays the IP address of the connected host.
MAC Address	This displays the MAC address of the connected host.
No. of Open Session	This displays the number of NAT sessions currently opened for the connected host.
Total	This displays what percentage of NAT sessions the EMG can support is currently being used by all connected hosts. You can also see the number of active NAT sessions and the maximum number of NAT sessions the EMG can support.

CHAPTER 21
ARP Table

21.1 Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

21.1.1 How ARP Works

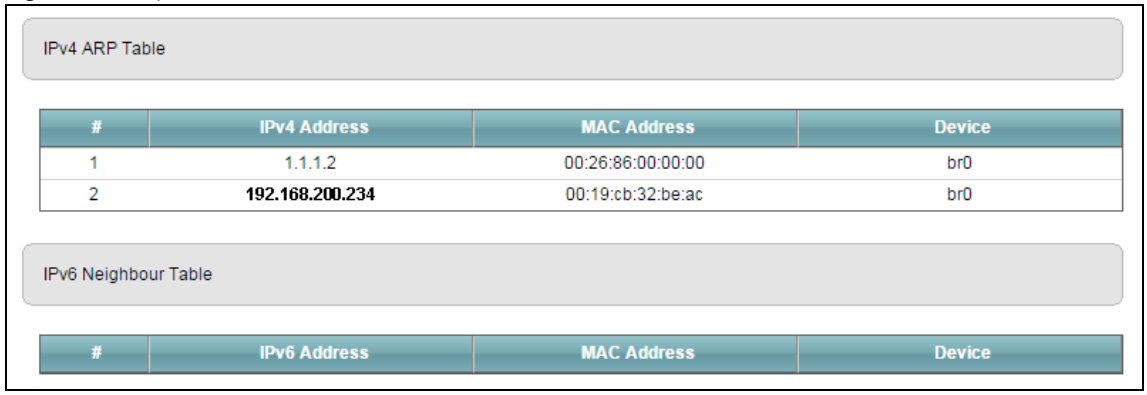
When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

21.2 ARP Table Screen

Use the ARP table to view IP-to-MAC address mapping(s). To open this screen, click **System Monitor** > **ARP Table**.

Figure 115 System Monitor > ARP Table



#	IPv4 Address	MAC Address	Device
1	1.1.1.2	00:26:86:00:00:00	br0
2	192.168.200.234	00:19:cb:32:be:ac	br0

#	IPv6 Address	MAC Address	Device

The following table describes the labels in this screen.

Table 93 System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the ARP table entry number.
IPv4/IPv6 Address	This is the learned IPv4 or IPv6 address of a device connected to a port.
MAC Address	This is the MAC address of the device with the listed IP address.
Device	This is the type of interface used by the device.

CHAPTER 22
Routing Table

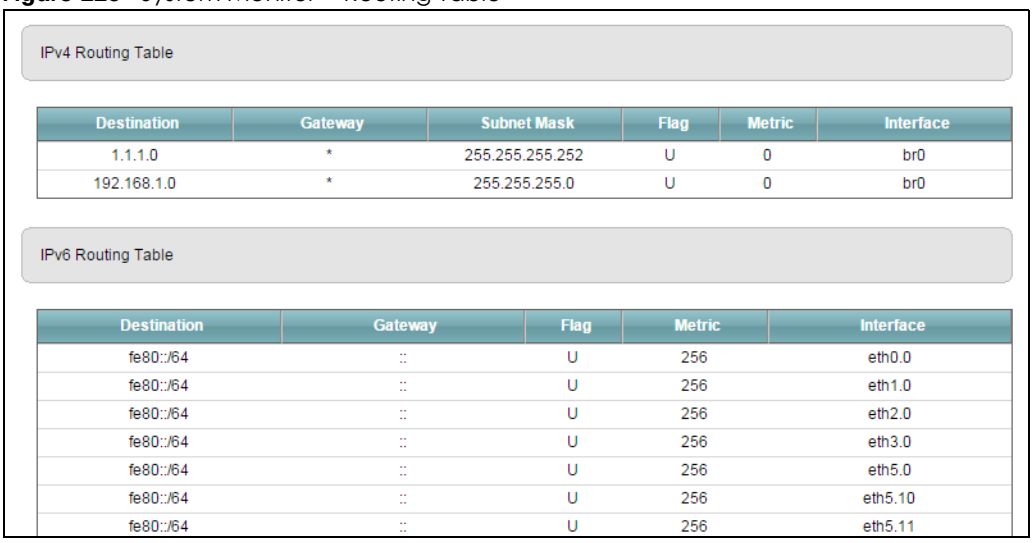
22.1 Overview

Routing is based on the destination address only and the EMG takes the shortest path to forward a packet.

22.2 The Routing Table Screen

Click **System Monitor** > **Routing Table** to open the following screen.

Figure 116 System Monitor > Routing Table



IPv4 Routing Table

Destination	Gateway	Subnet Mask	Flag	Metric	Interface
1.1.1.0	*	255.255.255.252	U	0	br0
192.168.1.0	*	255.255.255.0	U	0	br0

IPv6 Routing Table

Destination	Gateway	Flag	Metric	Interface
fe80::/64	::	U	256	eth0.0
fe80::/64	::	U	256	eth1.0
fe80::/64	::	U	256	eth2.0
fe80::/64	::	U	256	eth3.0
fe80::/64	::	U	256	eth5.0
fe80::/64	::	U	256	eth5.10
fe80::/64	::	U	256	eth5.11

The following table describes the labels in this screen.

Table 94 System Monitor > Routing Table

LABEL	DESCRIPTION
IPv4/IPv6 Routing Table	
Destination	This indicates the destination IPv4 address or IPv6 address and prefix of this route.
Gateway	This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of the IPv4 route.

Table 94 System Monitor > Routing Table (continued)

LABEL	DESCRIPTION
Flag	This indicates the route status. **U-Up:** The route is up. **!-Reject:** The route is blocked and will force a route lookup to fail. **G-Gateway:** The route uses a gateway to forward traffic. **H-Host:** The target of the route is a host. **R-Reinstate:** The route is reinstated for dynamic routing. **D-Dynamic (redirect):** The route is dynamically installed by a routing daemon or redirect. **M-Modified (redirect):** The route is modified from a routing daemon or redirect.
Metric	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".
Interface	This indicates the name of the interface through which the route is forwarded. **brx** indicates a LAN interface where x can be 0~3 to represent LAN1 to LAN4 respectively. **ptm0** indicates a DSL WAN interface using IPoE, IPoA or in bridge mode. **ethx** indicates an Ethernet WAN interface using IPoE or in bridge mode. **ppp0** indicates a WAN interface using PPPoE or PPPoA.

CHAPTER 23
Multicast Status

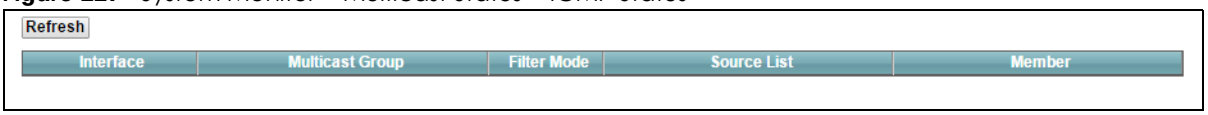
23.1 Overview

Use the **Multicast Status** screens to look at IGMP/MLD group status and traffic statistics.

23.2 The IGMP Status Screen

Use this screen to look at the current list of multicast groups the EMG has joined and which ports have joined it. To open this screen, click **System Monitor > Multicast Status > IGMP Status**.

Figure 117 System Monitor > Multicast Status > IGMP Status



The following table describes the labels in this screen.

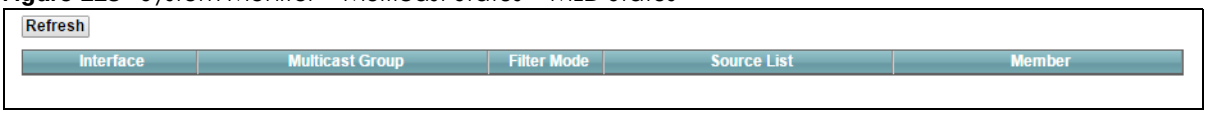
Table 95 System Monitor > Multicast Status > IGMP Status

LABEL	DESCRIPTION
Refresh	Click this button to update the information on this screen.
Interface	This field displays the name of an interface on the EMG that belongs to an IGMP multicast group.
Multicast Group	This field displays the name of the IGMP multicast group to which the interface belongs.
Filter Mode	**INCLUDE** means that only the IP addresses in the **Source List** get to receive the multicast group's traffic. **EXCLUDE** means that the IP addresses in the **Source List** are not allowed to receive the multicast group's traffic but other IP addresses can.
Source List	This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode.
Member	This is the list of the members of the multicast group.

23.3 The MLD Status Screen

Use this screen to look at the current list of multicast groups the EMG has joined and which ports have joined it. To open this screen, click **System Monitor > Multicast Status > MLD Status**.

Figure 118 System Monitor > Multicast Status > MLD Status



The following table describes the labels in this screen.

Table 96 System Monitor > Multicast Status > MLD Status

LABEL	DESCRIPTION
Refresh	Click this button to update the status on this screen.
Interface	This field displays the name of an interface on the EMG that belongs to an MLD multicast group.
Multicast Group	This field displays the name of the MLD multicast group to which the interface belongs.
Filter Mode	**INCLUDE** means that only the IP addresses in the **Source List** get to receive the multicast group's traffic. **EXCLUDE** means that the IP addresses in the **Source List** are not allowed to receive the multicast group's traffic but other IP addresses can.
Source List	This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode.
Member	This is the list of members in the multicast group.

CHAPTER 24
System

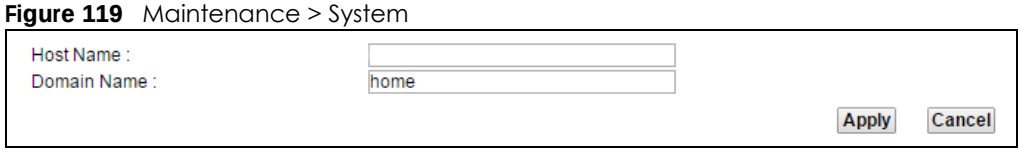
24.1 Overview

In the **System** screen, you can name your EMG (Host) and give it an associated domain name for identification purposes.

24.2 The System Screen

Click **Maintenance > System** to open the following screen.

Figure 119 Maintenance > System



The following table describes the labels in this screen.

Table 97 Maintenance > System

LABEL	DESCRIPTION
Host Name	Type a hostname for your EMG. Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes.
Domain Name	Type a Domain name for your host EMG.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to abandon this screen without saving.

CHAPTER 25
User Account

25.1 Overview

In the **User Account** screen, you can view the settings of the "admin" and other user accounts that you used to log in the EMG.

The "admin" account is a default account in the EMG. You can create other user accounts for temporary visits. Once a new user account is created, you'll be logged out by the EMG. Afterwards, you need to log in with the new user account you created. Also, you need to pay attention to the following details regarding the other user accounts.

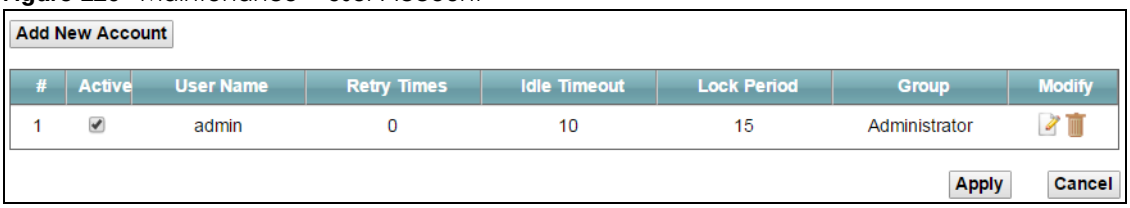
The other user accounts that you created will be deleted, and the configured timeout value will be reset to its default value by the EMG when one of the following scenarios happens:

- WAN remote access is disabled in **Maintenance > Remote Management > MGMT Services** screen;
- The EMG times out. To configure the timeout value, go to **Maintenance > Remote Management > MGMT Services** screen;
- You reboot the system. To reboot the EMG, go to **Maintenance > Reboot** screen.

25.2 The User Account Screen

Click **Maintenance > User Account** to open the following screen.

Figure 120 Maintenance > User Account



The following table describes the labels in this screen.

Table 98 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account.
#	This is the index number
Active	Select or deselect the check box to activate or deactivate the user name.
User Name	This field displays the name of the account used to log into the EMG web configurator.
Retry Times	This field displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.

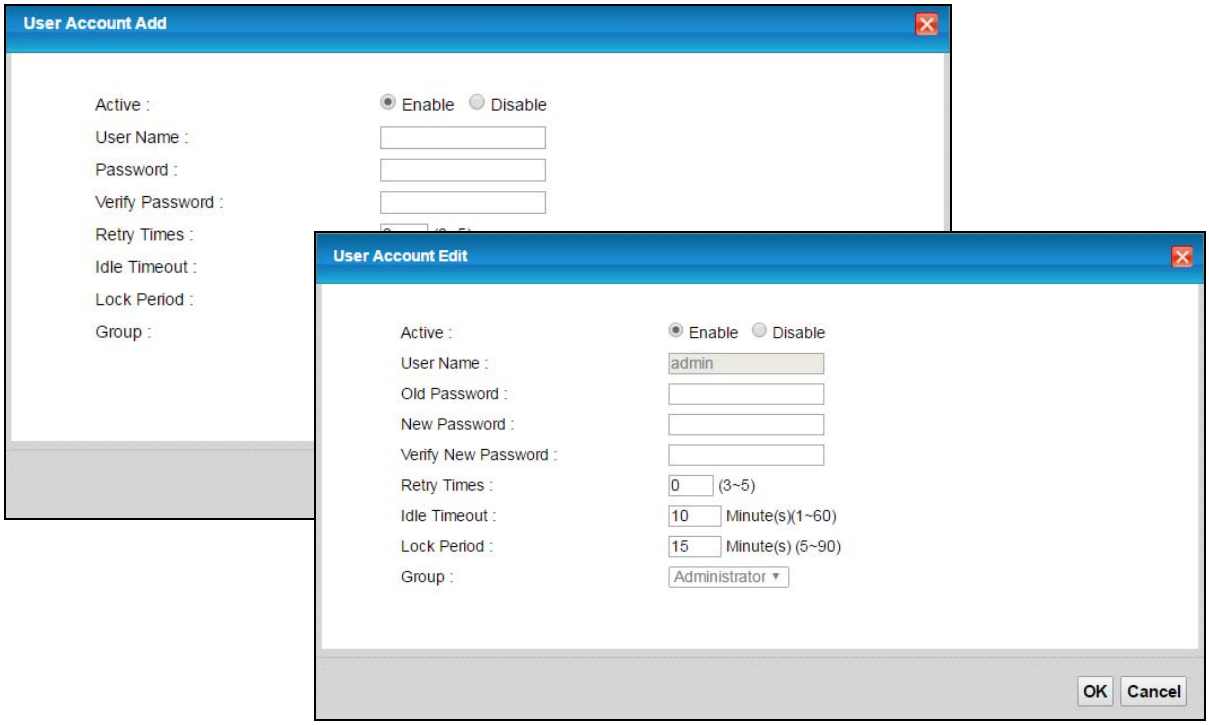
Table 98 Maintenance > User Account (continued) (continued)

LABEL	DESCRIPTION
Idle Timeout	This field displays the the length of inactive time before the EMG will automatically log the user out of the web configurator.
Lock Period	This field displays the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	This field displays whether this user has **Administrator** or **User** privleges.
Modify	Click the **Edit** icon to configure the entry. Click the **Delete** icon to remove the entry.
Apply	Click **Apply** to save your changes back to the EMG.
Cancel	Click **Cancel** to exit the screen without saving.

25.2.1 The User Account Add/Edit Screen

Click **Add New Account** or the **Edit** icon of an existing account in the **Maintenance > User Account** to open the following screen. Once you create a new account, you'll be logged out automatically by the EMG. This time, your username and password are required to log in the EMG.

Figure 121 Maintenance > User Account > Add/Edit



The following table describes the labels in this screen.

Table 99 Maintenance > User Account > Add/Edit

LABEL	DESCRIPTION
Active	Select **Enable** or **Disable** to activate or deactivate the user name.
User Name	Enter a new name for the account. This field displays the name of an existing account.
Old Password	Type the default password or the existing password used to access the EMG web configurator.

Table 99 Maintenance > User Account > Add/Edit (continued) (continued)

LABEL	DESCRIPTION
Password/New Password	Type your new system password (up to 256 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the EMG.
Verify Password/ Verify New Password	Type the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	Enter the length of inactive time before the EMG will automatically log the user out of the web configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number if consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	Specify whether this user will have **Administrator** or **User** privleges.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

CHAPTER 26
Remote Management

26.1 Overview

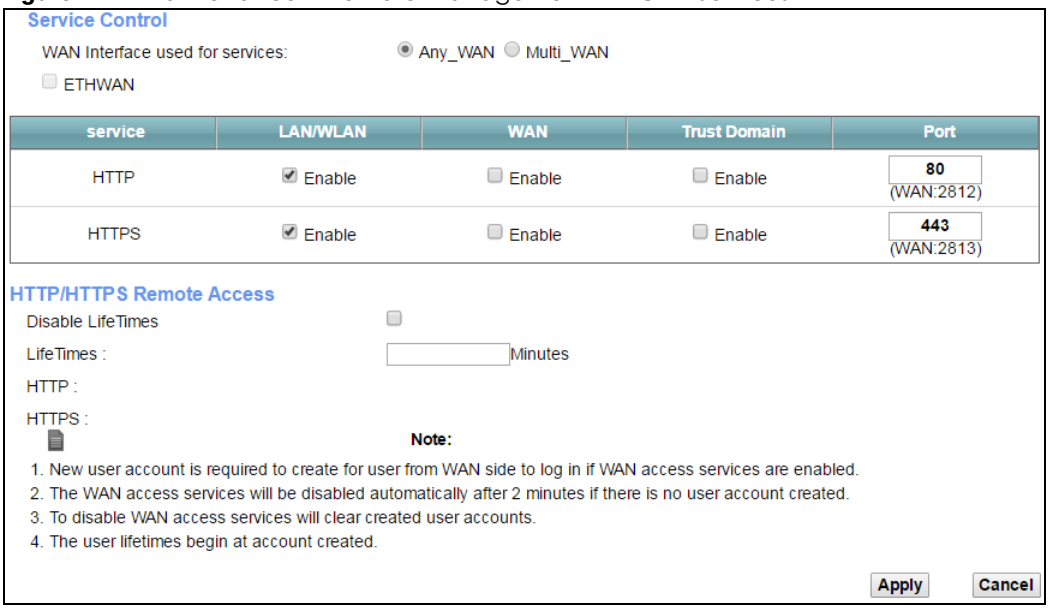
Remote management controls through which interface(s), which services can access the EMG.

Note: The EMG is managed using the Web Configurator.

26.2 The MGMT Services Screen

Use this screen to configure through which interface(s), which services can access the EMG. You can also specify the port numbers the services must use to connect to the EMG. Click **Maintenance > Remote Management > MGMT Services** to open the following screen.

Figure 122 Maintenance > Remote Management > MGMT Services



The following table describes the fields in this screen.

Table 100 Maintenance > Remote Management > MGMT Services

LABEL	DESCRIPTION
WAN Interface used for services	Select **Any_WAN** to have the EMG automatically activate the remote management service when any WAN connection is up. Select **Multi_WAN** and then select one or more WAN connections to have the EMG activate the remote management service when the selected WAN connections are up.
service	This is the service you may use to access the EMG.

Table 100 Maintenance > Remote Management > MGMT Services (continued)

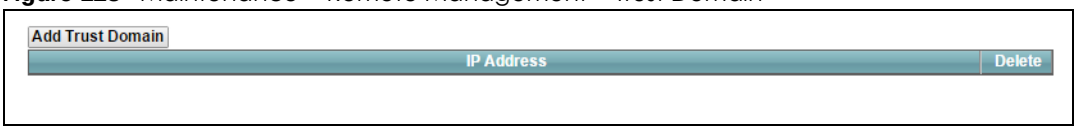
LABEL	DESCRIPTION
LAN/WLAN	Select the **Enable** check box for the corresponding services that you want to allow access to the EMG from the LAN/WLAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the EMG from all WAN connections.
Trust Domain	Select the **Enable** check box for the corresponding services that you want to allow access to the EMG from the trusted hosts configured in the **Maintenance > Remote MGMT > Trust Domain** screen. If you only want certain WAN connections to have access to the EMG using the corresponding services, then clear **WAN**, select **Trust Domain** and configure the allowed IP address(es) in the **Trust Domain** screen.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
HTTP/HTTPS Remote Access	
Disable LifeTimes	Click the check box to disable the HTTP/HTTPS WAN remote access service timeout. If this is checked, HTTP/HTTPS WAN remote access will not be disabled after the timeout.
LifeTimes	Enter a number of minutes that HTTP/HTTPS WAN remote access service will be disabled after the timeout.
HTTP/HTTPS	This field displays the URL with port to remote access CPE from WAN side.
Apply	Click **Apply** to save your changes back to the EMG.
Cancel	Click **Cancel** to restore your previously saved settings.

26.3 The Trust Domain Screen

Use this screen to view a list of public IP addresses which are allowed to access the EMG through the services configured in the **Maintenance > Remote Management** screen. Click **Maintenance > Remote Management > Trust Domain** to open the following screen.

Note: If this list is empty, all public IP addresses can access the EMG from the WAN through the specified services.

Figure 123 Maintenance > Remote Management > Trust Domain



The following table describes the fields in this screen.

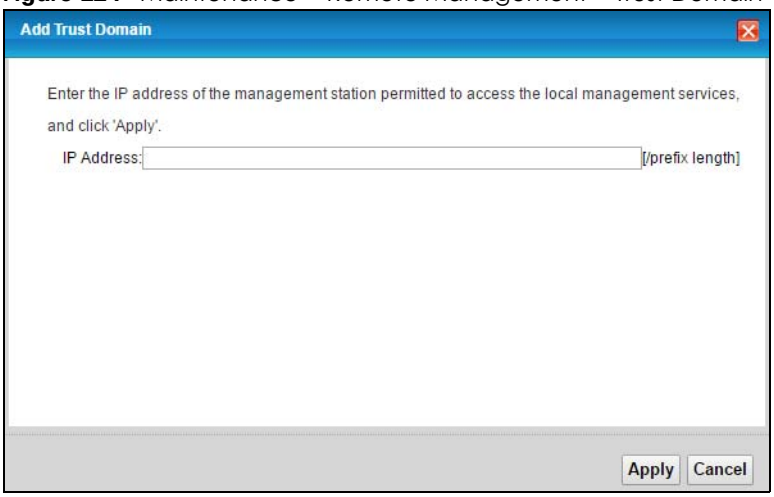
Table 101 Maintenance > Remote Management > Trust Domain

LABEL	DESCRIPTION
Add Trust Domain	Click this to add a trusted host IP address.
IP Address	This field shows a trusted host IP address.
Delete	Click the **Delete** icon to remove the trust IP address.

26.3.1 The Add Trust Domain Screen

Use this screen to configure a public IP address which is allowed to access the EMG. Click the **Add Trust Domain** button in the **Maintenance > Remote Management > Turst Domain** screen to open the following screen.

Figure 124 Maintenance > Remote Management > Trust Domain > Add Trust Domain



The following table describes the fields in this screen.

Table 102 Maintenance > Remote Management > Trust Domain > Add Trust Domain

LABEL	DESCRIPTION
IP Address	Enter a public IPv4 IP address which is allowed to access the service on the EMG from the WAN.
Apply	Click **Apply** to save your changes back to the EMG.
Cancel	Click **Cancel** to exit this screen without saving.

CHAPTER 27
SNMP

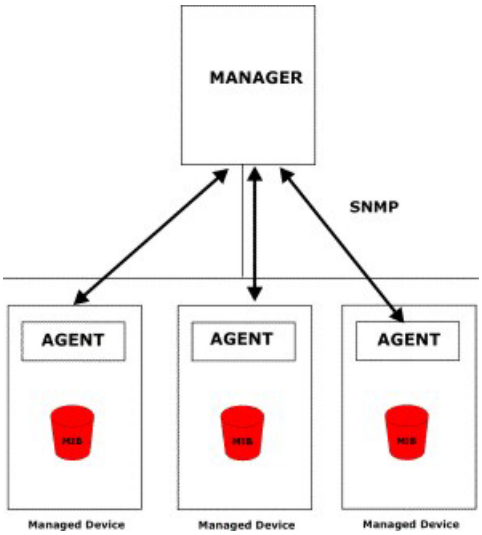
27.1 Overview

This chapter explains how to configure the SNMP settings on the EMG.

27.2 The SNMP Screen

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your EMG supports SNMP agent functionality, which allows a manager station to manage and monitor the EMG through the network. The EMG supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 125 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the EMG). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

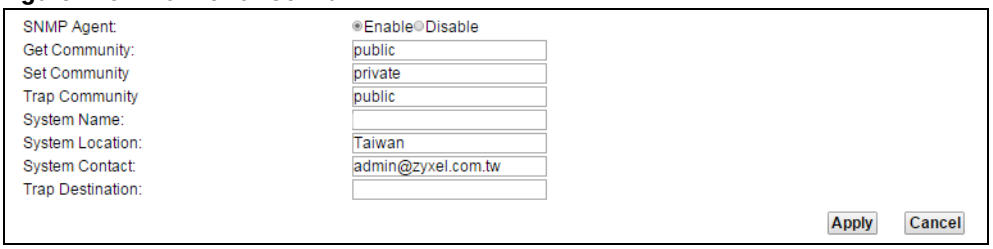
The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

Click **Maintenance > SNMP** to open the following screen. Use this screen to configure the EMG SNMP settings.

Figure 126 Maintenance > SNMP



The following table describes the fields in this screen.

Table 103 Maintenance > SNMP

LABEL	DESCRIPTION
SNMP Agent	Select **Enable** to let the EMG act as an SNMP agent, which allows a manager station to manage and monitor the EMG through the network. Select **Disable** to turn this feature off.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station.
Trap Community	Enter the **Trap Community**, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
System Name	Enter the SNMP system name.
System Location	Enter the SNMP system location.
System Contact	Enter the SNMP system contact.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click this to save your changes back to the EMG.
Cancel	Click this to restore your previously saved settings.

CHAPTER 28
Time Settings

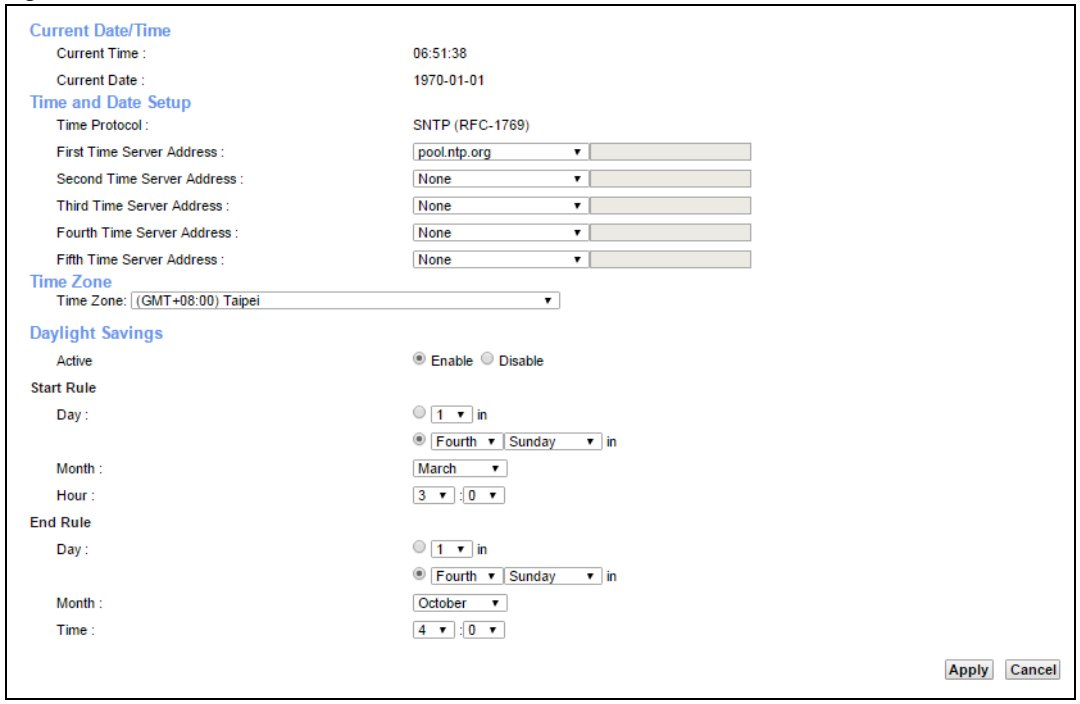
28.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

28.2 The Time Screen

To change your EMG's time and date, click **Maintenance > Time**. The screen appears as shown. Use this screen to configure the EMG's time based on your local time zone.

Figure 127 Maintenance > Time



The following table describes the fields in this screen.

Table 104 Maintenance > Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your EMG. Each time you reload this page, the EMG synchronizes the time with the time server.

Table 104 Maintenance > Time (continued)

LABEL	DESCRIPTION
Current Date	This field displays the date of your EMG. Each time you reload this page, the EMG synchronizes the date with the time server.
Time and Date Setup	
First ~ Fifth Time Server Address	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select **None** if you don't want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Active	Select **Enable** if you use Daylight Saving Time.
Start Rule	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Hour** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to **Second**, **Sunday**, the month to **March** and the time to **2** in the **Hour** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday** and the month to **March**. The time you select depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Rule	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Time** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would set the day to **First**, **Sunday**, the month to **November** and the time to **2** in the **Time** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday**, and the month to **October**. The time you select depends on your time zone. In Germany for instance, you would select **2** in the **Time** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

CHAPTER 29
E-mail Notification

29.1 Overview

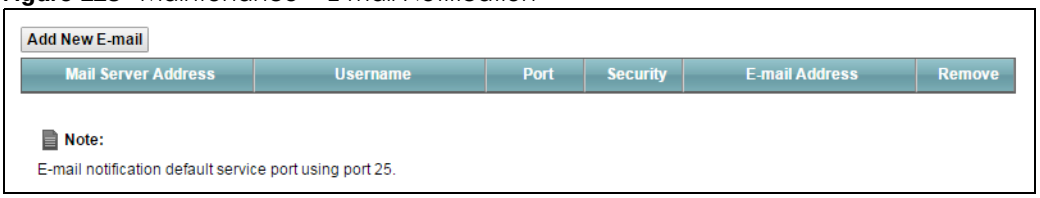
A mail server is an application or a computer that runs such an application to receive, forward and deliver e-mail messages.

To have the EMG send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

29.2 The E-mail Notification Screen

Click **Maintenance > E-mail Notification** to open the **E-mail Notification** screen. Use this screen to view, remove and add mail server information on the EMG.

Figure 128 Maintenance > E-mail Notification



The following table describes the labels in this screen.

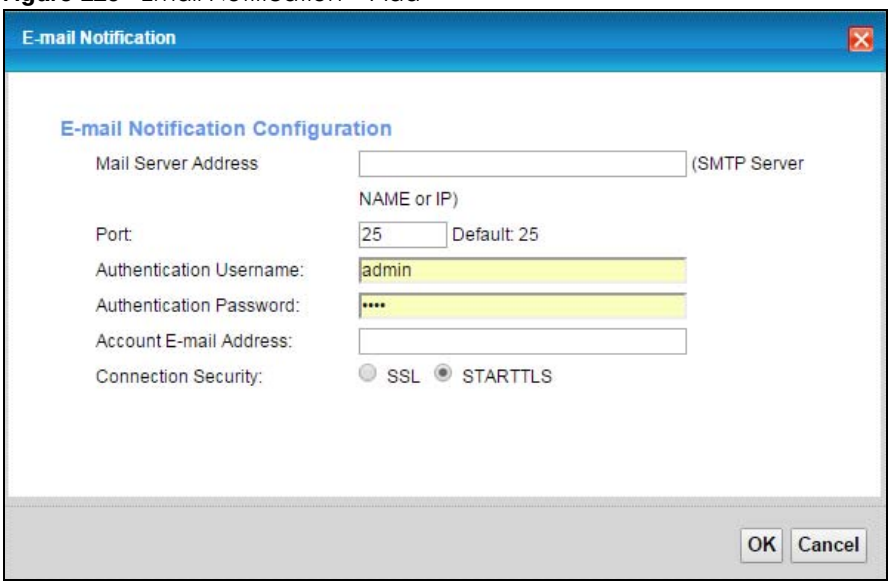
Table 105 Maintenance > E-mail Notification

LABEL	DESCRIPTION
Add New E-mail	Click this button to create a new entry.
Mail Server Address	This field displays the server name or the IP address of the mail server.
Username	This field displays the user name of the sender's mail account.
Port	This field displays the port number of the mail server.
Security	This field displays the protocol used for encryption.
E-mail Address	This field displays the e-mail address that you want to be in the from/sender line of the e-mail that the EMG sends.
Remove	Click this button to delete the selected entry(ies).

29.2.1 E-mail Notification Edit

Click the **Add** button in the **E-mail Notification** screen. Use this screen to configure the required information for sending e-mail via a mail server.

Figure 129 Email Notification > Add



The following table describes the labels in this screen.

Table 106 Email Notification > Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the **Account Email Address** field. If this field is left blank, reports, logs or notifications will not be sent via e-mail.
Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication Username	Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the **Account Email Address** field.
Authentication Password	Enter the password associated with the user name above.
Account E-mail Address	Enter the e-mail address that you want to be in the from/sender line of the e-mail notification that the EMG sends. If you activate SSL/TLS authentication, the e-mail address must be able to be authenticated by the mail server as well.
Connection Security	Select **SSL** to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the XMG. Select **STARTTLS** to upgrade a plain text connection to a secure connection using SSL/TLS.
OK	Click this button to save your changes and return to the previous screen.
Cancel	Click this button to exit this screen without saving.

CHAPTER 30
Log Setting

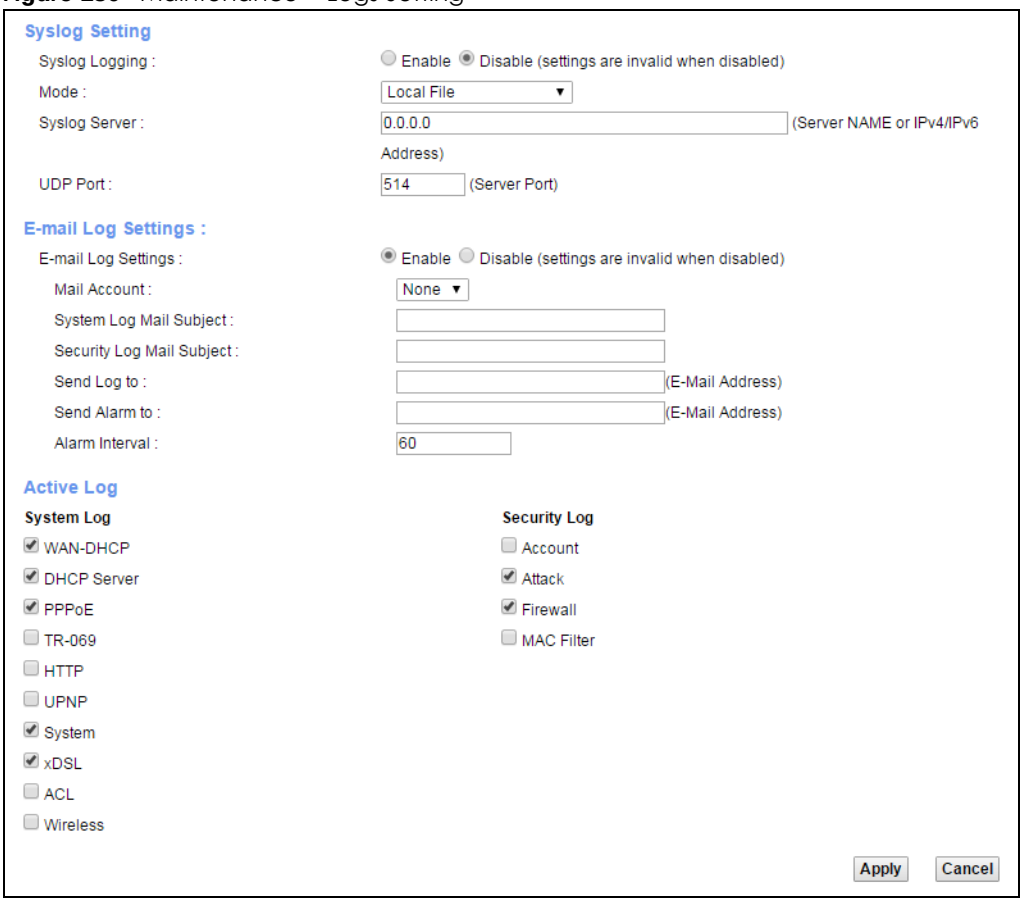
30.1 Overview

You can configure where the EMG sends logs and which logs and/or immediate alerts the EMG records in the **Logs Setting** screen.

30.2 The Log Settings Screen

To change your EMG's log settings, click **Maintenance > Logs Setting**. The screen appears as shown.

Figure 130 Maintenance > Logs Setting



The following table describes the fields in this screen.

Table 107 Maintenance > Logs Setting

LABEL	DESCRIPTION
Syslog Setting	
Syslog Logging	The EMG sends a log to an external syslog server. Select **Enable** to enable syslog logging.
Mode	Select the syslog destination from the drop-down list box. If you select **Remote**, the log(s) will be sent to a remote syslog server. If you select **Local File**, the log(s) will be saved in a local file. If you want to send the log(s) to a remote syslog server and save it in a local file, select **Local File and Remote**.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
E-mail Log Settings	
E-mail Log Settings	Select **Enable** to have the EMG send logs and alarm messages to the configured e-mail addresses.
Mail Account	This section is available only when you select **Enable** in the **E-mail Log Settings** field. Select a mail account from which you want to send logs. You can configure mail accounts in the **Maintenance > E-mail Notification** screen.
System Log Mail Subject	Type a title that you want to be in the subject line of the system log e-mail message that the EMG sends.
Security Log Mail Subject	Type a title that you want to be in the subject line of the security log e-mail message that the EMG sends.
Send Log to	The EMG sends logs to the e-mail address specified in this field. If this field is left blank, the EMG does not send logs via E-mail.
Send Alarm to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
Alarm Interval	Specify how often the alarm should be updated.
Active Log	
System Log	Select the categories of system logs that you want to record.
Security Log	Select the categories of security logs that you want to record.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

30.2.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- "`End of Log`" message shows that a complete log has been sent.

Figure 131 E-mail Log Example

```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10 |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……................{snip}……................
……................{snip}……................
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |

End of Firewall Log
```

CHAPTER 31
Firmware Upgrade

31.1 Overview

This chapter explains how to upload new firmware to your EMG. You can download new firmware releases from your nearest Zyxel FTP site (or www.zyxel.com) to use to upgrade your device's performance.

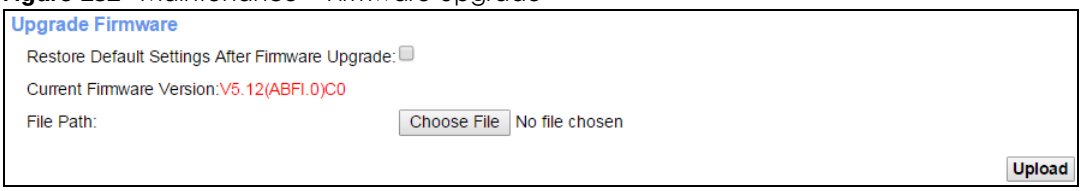
Only use firmware for your device's specific model. Refer to the label on the bottom of your EMG.

31.2 The Firmware Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the EMG while firmware upload is in progress!

Figure 132 Maintenance > Firmware Upgrade



The following table describes the labels in this screen. After you see the firmware updating screen, wait two minutes before logging into the EMG again.

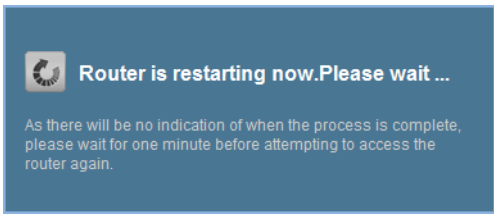
Table 108 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Click the check box to have the EMG automatically reset itself after the new firmware is uploaded.
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you wasnt to upload in this field or click **Choose File** to find it.

Table 108 Maintenance > Firmware Upgrade

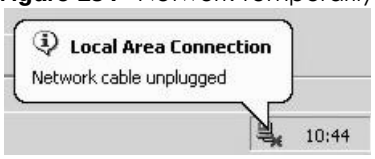
LABEL	DESCRIPTION
Choose File	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.

Figure 133 Firmware Uploading



The EMG automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 134 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.