ZYXEL
Your Networking Ally

User's Guide

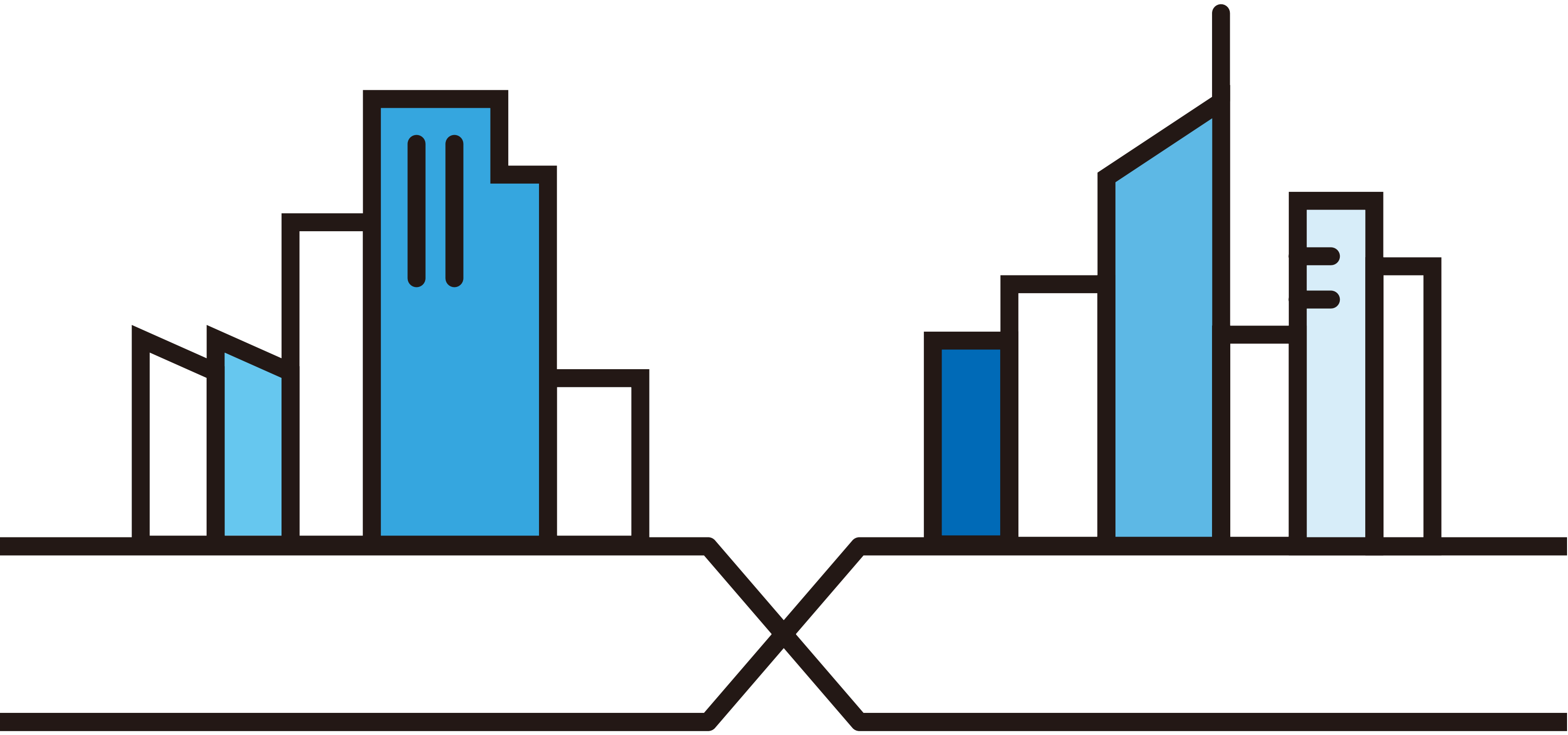
EMG6726-B10A

Dual-Band Wireless AC/N Gigabit Ethernet Gateway

Default Login Details	
LAN IP Address	http://192.168.1.1
Login	admin
Password	See the device label

Version 5.13 Edition 3, 05/2019

DRAFT



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. 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 EMG and access the Web Configurator.

- More Information

  Go to **support.zyxel.com** to find other information on the EMG.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this guide.

Warnings tell you about things that could harm you or your device.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The EMG6726-B10A may be referred to as the “EMG” in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Network Setting > Broadband** means you first click **Network Setting** in the navigation panel, then the **Broadband** sub menu to get to that screen.

Icons Used in Figures

Figures in this user guide may use the following generic icons. The EMG icon is not an exact representation of your device.

EMG 	Wireless Router / Access Point 	Switch
Firewall 	USB Storage Device 	Server

Telephone 	Cell Tower 	Printer
Telephone Jack 	Splitter 	

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Introducing the EMG

1.1 Overview

The EMG is an Ethernet gateway providing triple-play services with optimized HD IPTV services for the home or office. This model offers a Gigabit Ethernet (GbE) WAN port. The EMG offers 2.4G and 5G Wi-Fi networks that can operate simultaneously.

Only use firmware for your EMG's specific model.

1.1.1 Internet Access

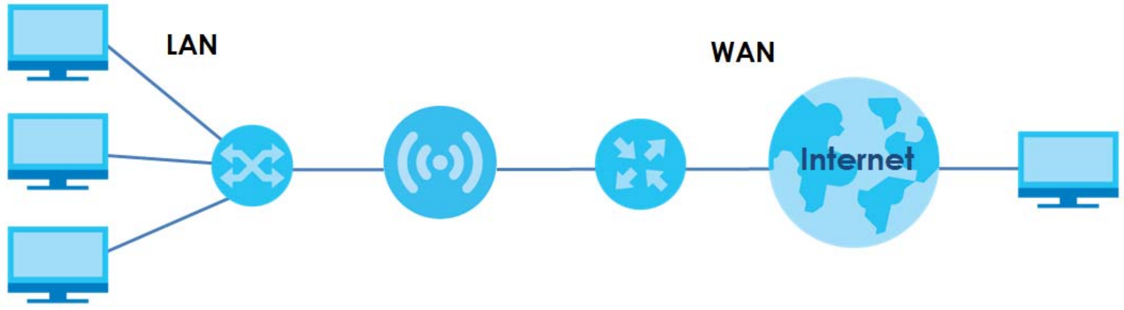
Your EMG has a Gigabit Ethernet port for super-fast Internet access. It provides Internet access by connecting the WAN port to your ISP. Computers can connect to the EMG's LAN ports (or wirelessly) and access the Internet simultaneously.

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.

1.1.2 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.

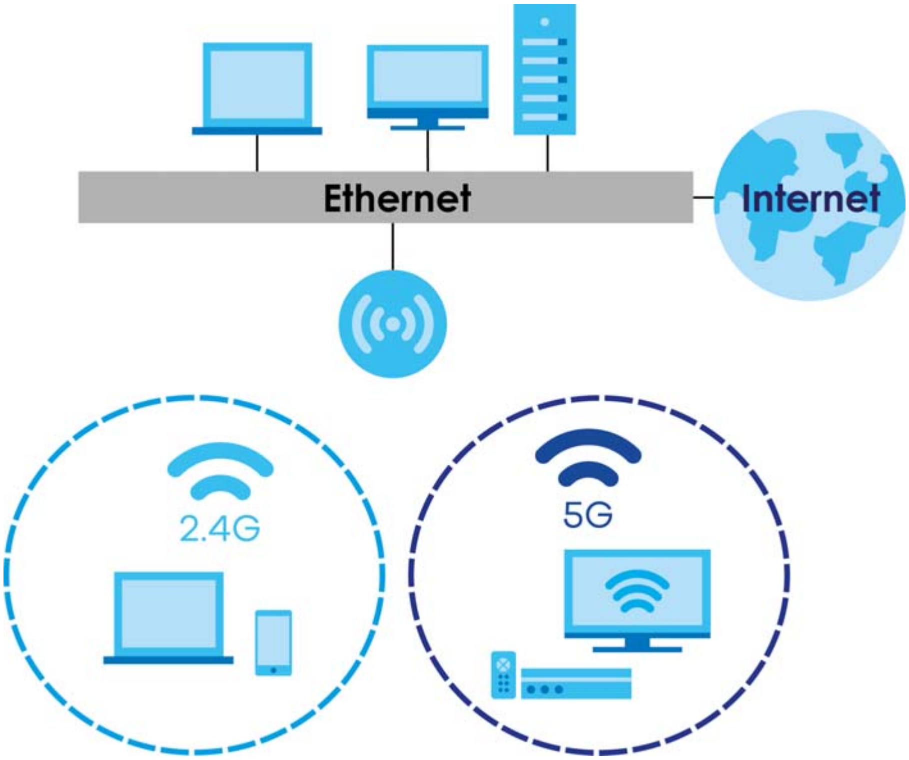
Figure 1 EMG's Internet Access Application: Ethernet WAN



1.1.3 Dual-Band

The EMG is a dual-band gateway that can use 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.

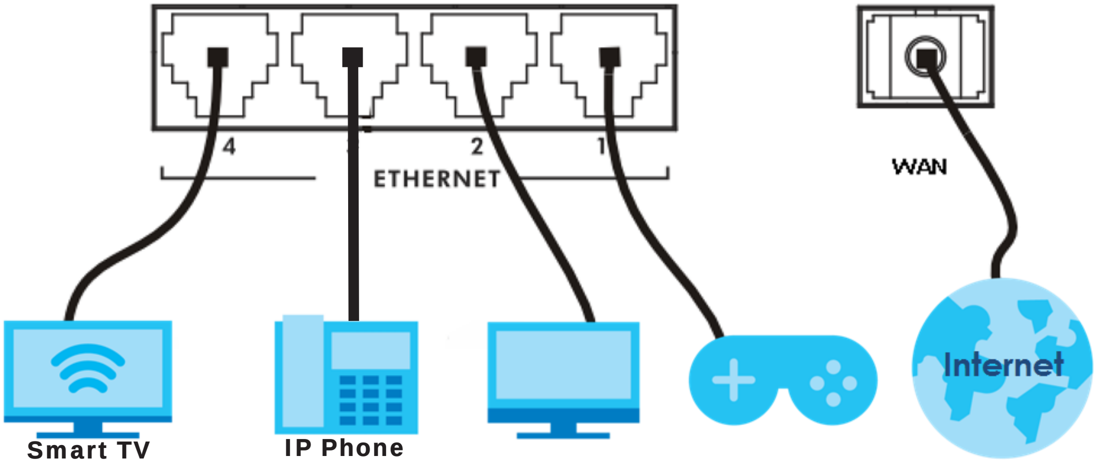
Figure 2 Dual-Band Application



1.1.4 Triple Play

Triple play means using broadband Internet access, VoIP and streaming video/audio media, all at the same time with no noticeable loss in bandwidth.

Figure 3 Triple Play Example



1.1.5 Wireless Access

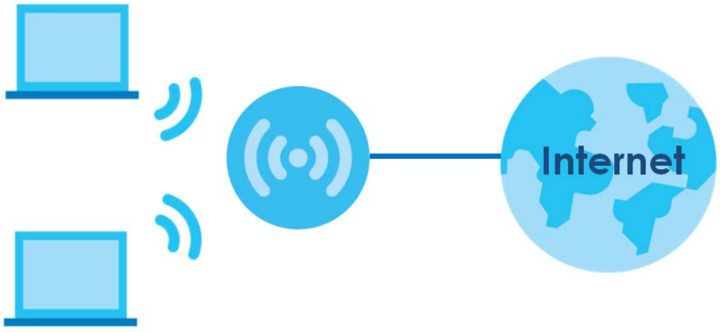
The EMG is a wireless Access Point (AP) for IEEE 802.11b/g/n/a/ac wireless clients, such as notebook computers, iPads, smartphones, etc. These devices can connect to the EMG to access network resources and the Internet.

Your EMG supports Wi-Fi Protected Setup (WPS), which allows you to quickly set up a wireless network with strong security.

You can configure your wireless network using the built-in Web Configurator.

See Section 4.3 on page 38 for more information about how to set up a wireless network.

Figure 4 Wireless Access Example



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 things regularly to make the EMG more secure and to manage the EMG more effectively.

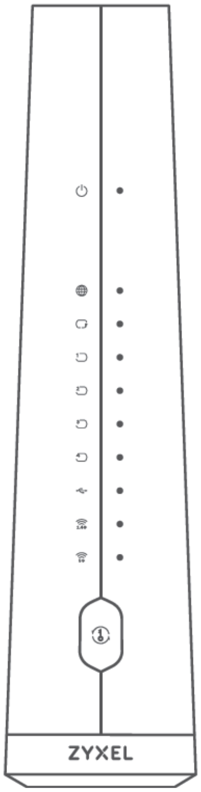
- Change the password. Use a password that’s not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the EMG to its factory default settings. 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 Hardware

1.4.1 Front Panel

The following graphic displays the front panel of the EMG.

Figure 5 LEDs on the EMG



1.4.2 LEDs (Lights)

The following table describes the LEDs.

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 uploading firmware.
		Off	The EMG is not receiving power.

Table 1 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
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.
LAN/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.
1 2 3 4 Ethernet 1~4	Green	On	The EMG has a successful 10/100/1000 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 10/100/1000 Mbps.
		Off	The EMG does not have an Ethernet connection with the LAN.
USB	Green	On	The EMG recognizes a USB connection through the USB slot.
		Blinking	The EMG is sending/receiving data to/from the USB device connected to it.
		Off	The EMG does not detect a USB connection through the USB slot.
Note: The **USB** LED is reserved for future development.			
2.4G 5G WiFi 2.4G WiFi 5G	Green	On	The 2.4 GHz or 5 GHz wireless network is activated.
		Blinking	The EMG is communicating with 2.4 GHz or 5 GHz wireless clients.
	Amber	Blinking	The EMG is setting up a WPS connection with a 2.4 GHz or 5 GHz wireless client.
		Off	The 2.4 GHz or 5GHz wireless network is not activated.
WPS	Amber	On	WPS is enabled.
		Off	WPS is disabled.

1.4.3 Using the WPS Button

Once the **WiFi** LED turns green, the wireless network is active. If the wireless network is turned off, see Section 7.2.1 on page 76 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 more than five seconds and release it.

3 Press the WPS button on another WPS-enabled device within range of the EMG. The **WiFi 2.4G** and **WiFi 5G** LEDs flash amber while the EMG sets up a WPS connection with the other wireless device.

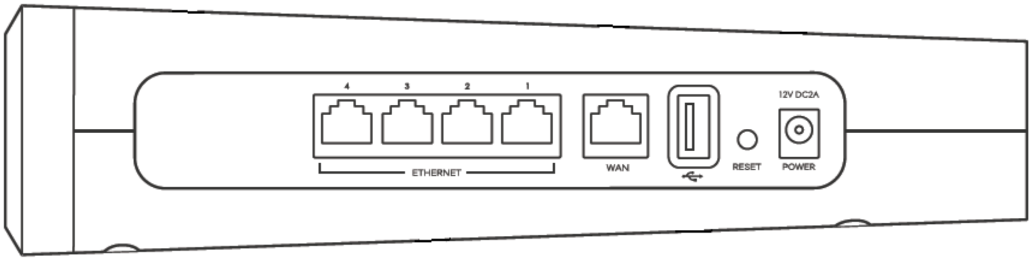
4 Once the connection is successfully made, the **WPS** LED shines green. Note that it depends on your client's configuration to have a 2.4GHz or 5GHz wireless network.

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

1.4.4 Rear Panel

The following graphic displays the rear panel of the EMG.

Figure 6 EMG6726-B10A's Rear Panel



The following table describes the items on the rear panel.

Rear Panel Ports

LABEL	DESCRIPTION
ETHERNET1 ~ ETHERNET4	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
WAN	Connect an Ethernet cable to the Ethernet WAN port for Internet access.
USB	The USB port is reserved for future development.
Reset	Press the button to return the EMG to the factory defaults.
Power	Connect the power cable and press the power button to start the EMG.

1.4.5 The RESET Button

If you forget your password or cannot access the Web Configurator, 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 and the password will be reset to the factory default (see the device label).

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 more than ten 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.

1.4.6 Wall Mounting

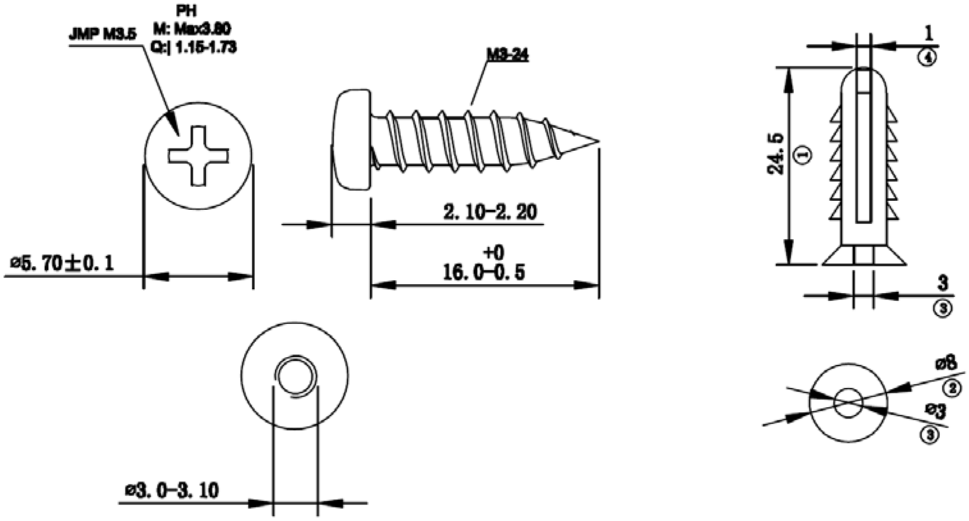
You may need screw anchors if mounting on a concrete or brick wall.

Table 2 Wall Mounting Information

Distance between holes	88 mm
Screws	Two
Screw anchors (optional)	Two

The following figure introduces the specifications of the screws and screws anchors for wall mounting.

Figure 7 Screws & Screw Anchors Specifications



1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.

2 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.

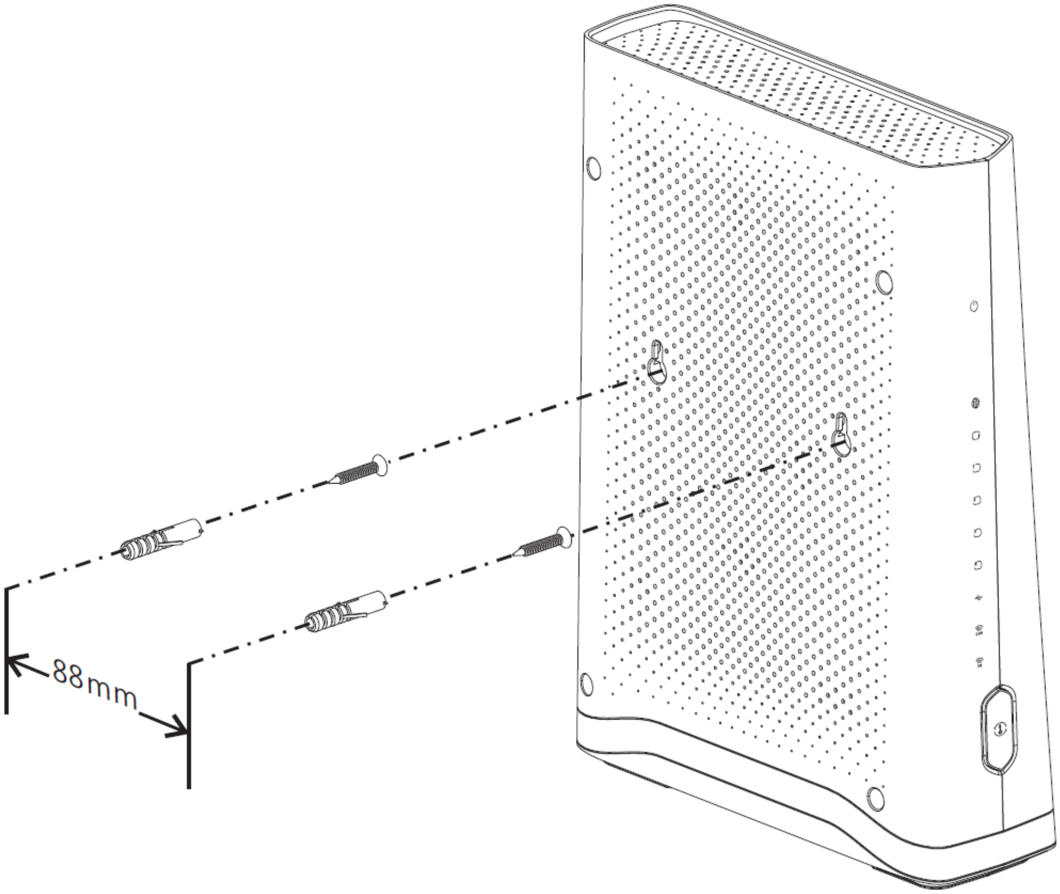
3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

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.

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

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

Figure 8 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).

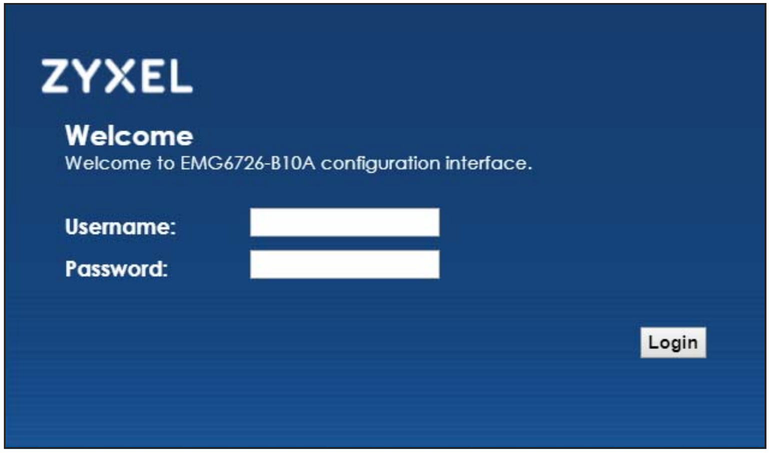
2.1.1 Accessing the Web Configurator

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://192.168.1.1.

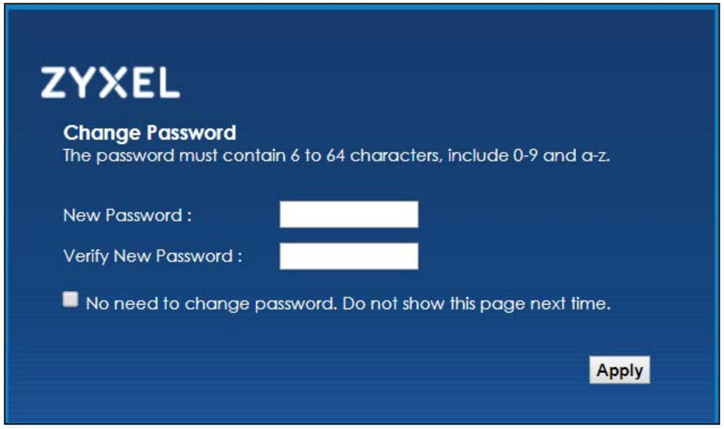
3 A password screen displays. To access the administrative web configurator and manage the EMG, type the default username **admin** and password **(see the back label on your** EMG) in the password screen and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 9 Password Screen



4 The following screen displays if you have not yet changed your password. Enter a new password, retype it to confirm and click **Apply**.

Figure 10 Change Password Screen



Change Password

The password must contain 6 to 64 characters, include 0-9 and a-z.

New Password :

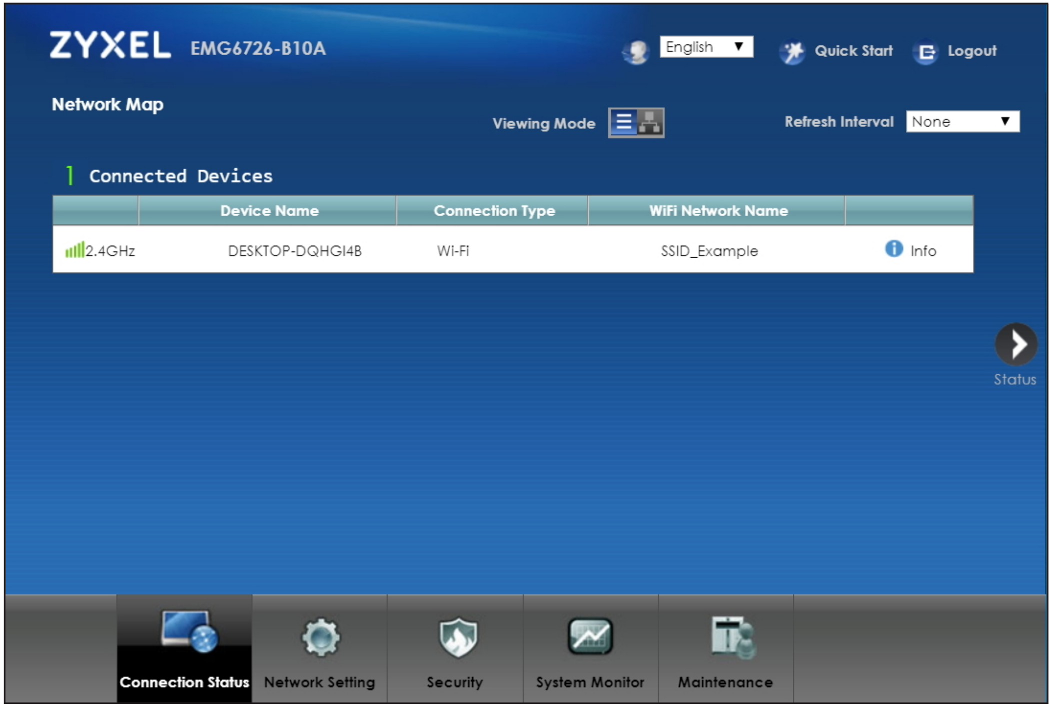
Verify New Password :

□ No need to change password. Do not show this page next time.

5 The **Quick Start Wizard** screen appears. You can configure basic Internet access, and wireless settings. See Chapter 3 on page 32 for more information.

6 After you finished or closed the **Quick Start Wizard** screen, the **Network Map** page appears.

Figure 11 Network Map: List View Mode



Network Map

Viewing Mode

Refresh Interval: None

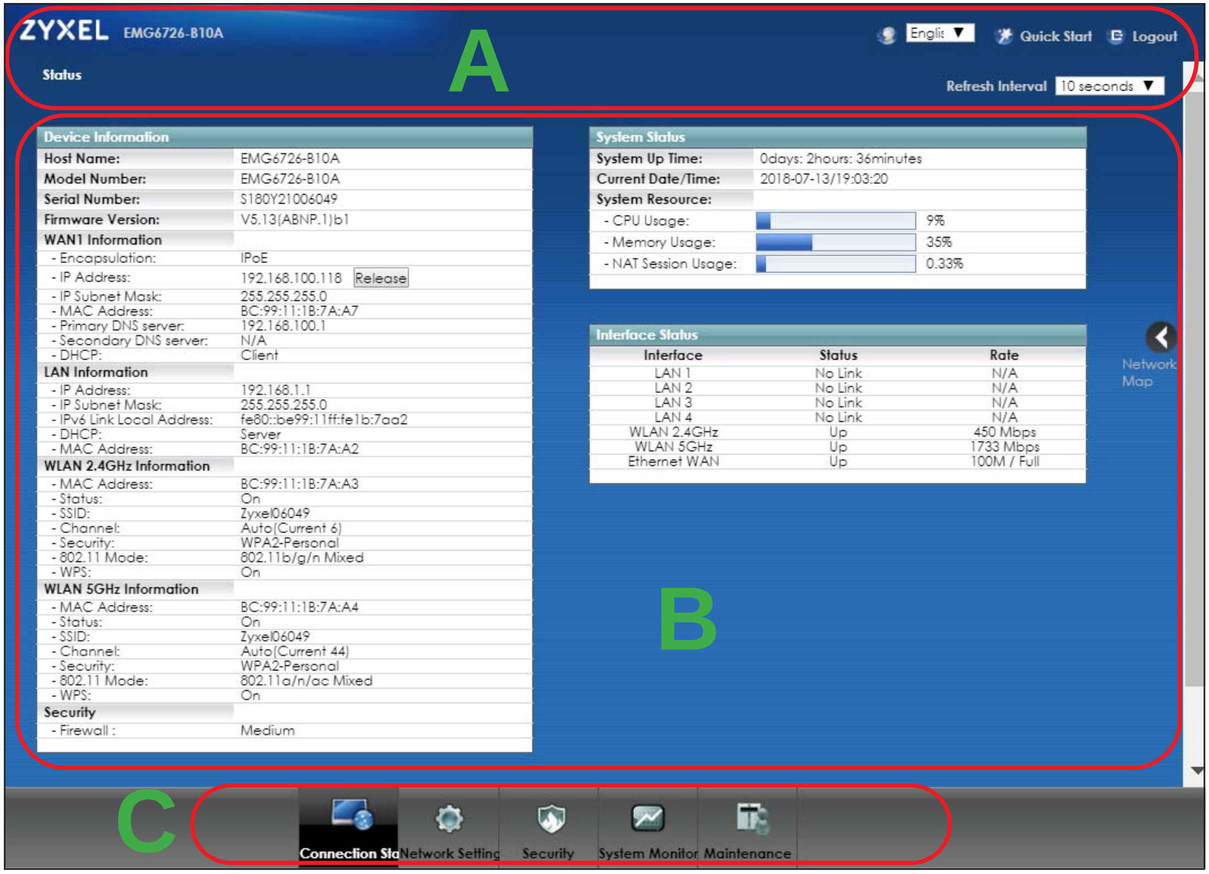
Connected Devices

	Device Name	Connection Type	WiFi Network Name	
2.4GHz	DESKTOP-DQHGI4B	Wi-Fi	SSID_Example	Info

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

2.2 Web Configurator Layout

Figure 12 Screen Layout



Device Information	
Host Name:	EMG6726-B10A
Model Number:	EMG6726-B10A
Serial Number:	S180Y21006049
Firmware Version:	V5.13(ABNP.1)b1
WAN1 Information	
- Encapsulation:	IPoE
- IP Address:	192.168.100.118
- IP Subnet Mask:	255.255.255.0
- MAC Address:	BC:99:11:1B:7A:A7
- Primary DNS server:	192.168.100.1
- Secondary DNS server:	N/A
- DHCP:	Client
LAN Information	
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- IPv6 Link Local Address:	fe80::be99:11ff:fe1b:7aa2
- DHCP:	Server
- MAC Address:	BC:99:11:1B:7A:A2
WLAN 2.4GHz Information	
- MAC Address:	BC:99:11:1B:7A:A3
- Status:	On
- SSID:	Zyxel06049
- Channel:	Auto(Current 6)
- Security:	WPA2-Personal
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	On
WLAN 5GHz Information	
- MAC Address:	BC:99:11:1B:7A:A4
- Status:	On
- SSID:	Zyxel06049
- Channel:	Auto(Current 44)
- Security:	WPA2-Personal
- 802.11 Mode:	802.11a/n/ac Mixed
- WPS:	On
Security	
- Firewall :	Medium

System Status		
System Up Time:	0days: 2hours: 36minutes	
Current Date/Time:	2018-07-13/19:03:20	
System Resource:		
- CPU Usage:		9%
- Memory Usage:		35%
- NAT Session Usage:		0.33%

Interface Status

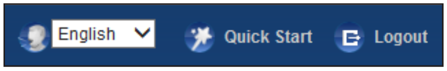
Interface	Status	Rate
LAN 1	No Link	N/A
LAN 2	No Link	N/A
LAN 3	No Link	N/A
LAN 4	No Link	N/A
WLAN 2.4GHz	Up	450 Mbps
WLAN 5GHz	Up	1733 Mbps
Ethernet WAN	Up	100M / Full

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

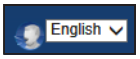
ICON	DESCRIPTION
	**Language**: Select the language you prefer.

Table 3 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
Quick Start	**Quick Start**: Click this icon to open screens where you can configure the EMG's time zone Internet access, and wireless settings.
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 Ethernet WAN connections. You can also add new WAN connections.
Wireless	WiFi	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	Guest WiFi	Use this screen to configure multiple wireless networks on the EMG.
	WPS	Use this screen to view your WPS (Wi-Fi Protected Setup) settings. You can use the screen to add a wireless client to your wireless network.
	Advanced	Use this screen to configure advanced wireless settings.
	Channel Status	Use this screen to scan the number of devices which are using 2.4G and/or 5G wireless channels and view the results.
	MESH	Use this screen to enable MESH which combines the 2.4GHz and 5GHz wireless network name, password, security type together for eliminating configuration hassles.
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.

Table 4 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
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.
	Monitor	Use this screen to view statistics of QoS on WAN/LAN interface and the status of queues.
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.
IGMP/MLD	IGMP/MLD	Use this screen to configure multicast settings (IGMP for IPv4 and MLD for IPv6 multicast groups) on the WAN.
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.
Home Connectivity	ONE Connect	Use this screen to enable the one connect function on the EMG.
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 Rule	Scheduler Rule	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.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your EMG's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the EMG without turning the power off.

Table 4 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
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.
	802.1ag	Use this screen to configure CFM (Connectivity Fault Management) MD (maintenance domain) and MA (maintenance association), perform connectivity tests and view test reports.
	802.3ah	Use this screen to configure link OAM port parameters.

CHAPTER 3 Quick Start

3.1 Overview

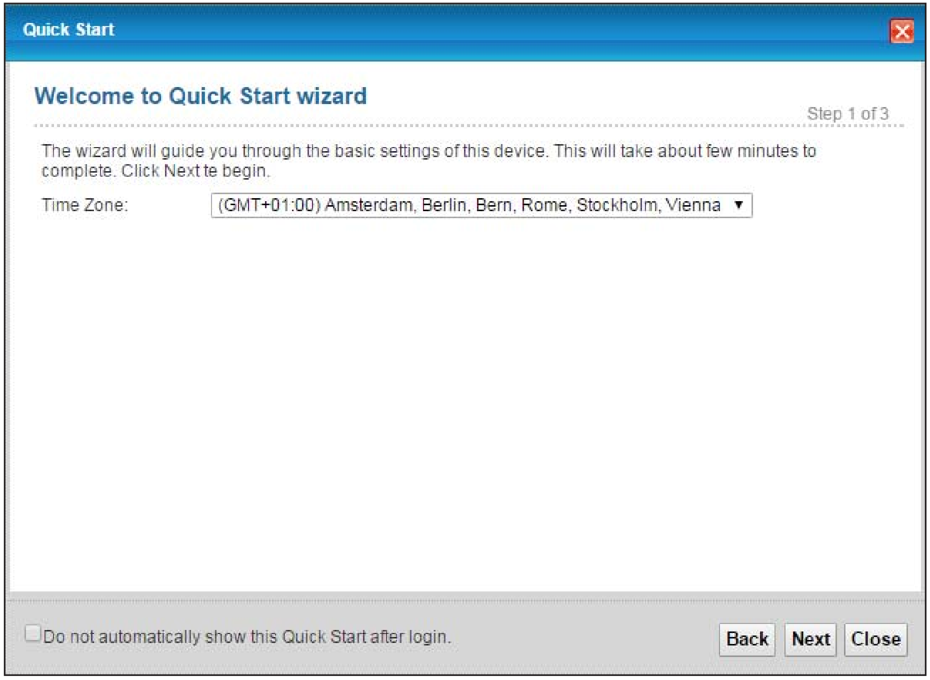
Use the Quick Start screens to configure the EMG's time zone, basic Internet access, and wireless settings.

Note: See the technical reference chapters (starting on Chapter 4 on page 35) for background information on the features in this chapter.

3.2 Quick Start Setup

1 The Quick Start Wizard appears automatically after login. Or you can click the **Quick Start** icon in the top right corner of the web configurator to open the quick start screens. Select the time zone of your location. Click **Next**.

Figure 13 Quick Start - Welcome



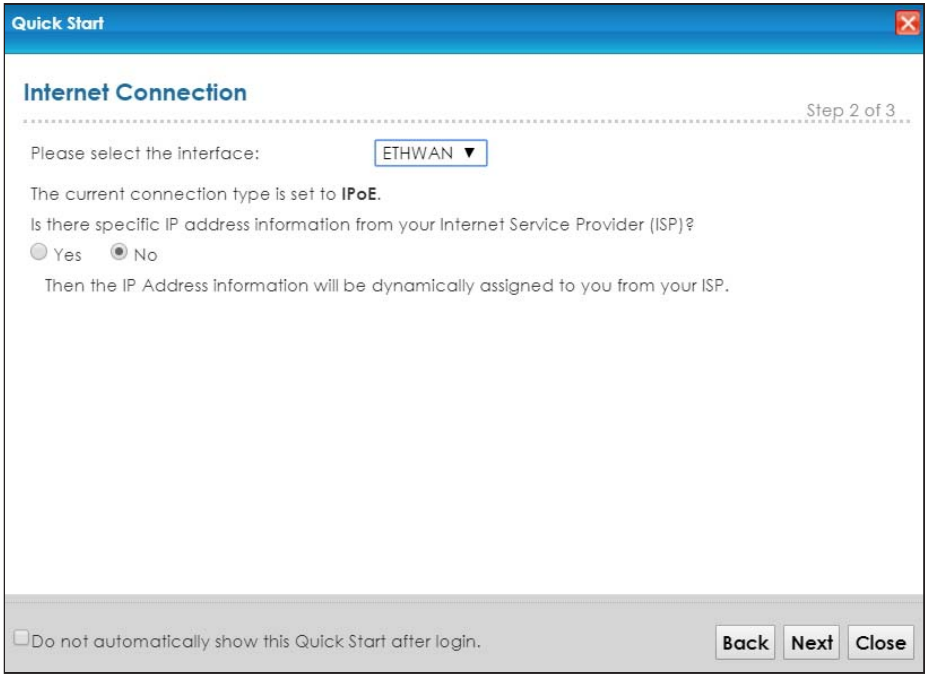
The wizard will guide you through the basic settings of this device. This will take about few minutes to complete. Click Next te begin.

Time Zone: (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna ▼

□ Do not automatically show this Quick Start after login.

2 Enter your Internet connection information in this screen. The screen and fields to enter may vary depending on your current connection type. Click **Next**.

Figure 14 Quick Start - Internet Connection



Internet Connection

Step 2 of 3

Please select the interface: ETHWAN ▼

The current connection type is set to **IPoE**.

Is there specific IP address information from your Internet Service Provider (ISP)?

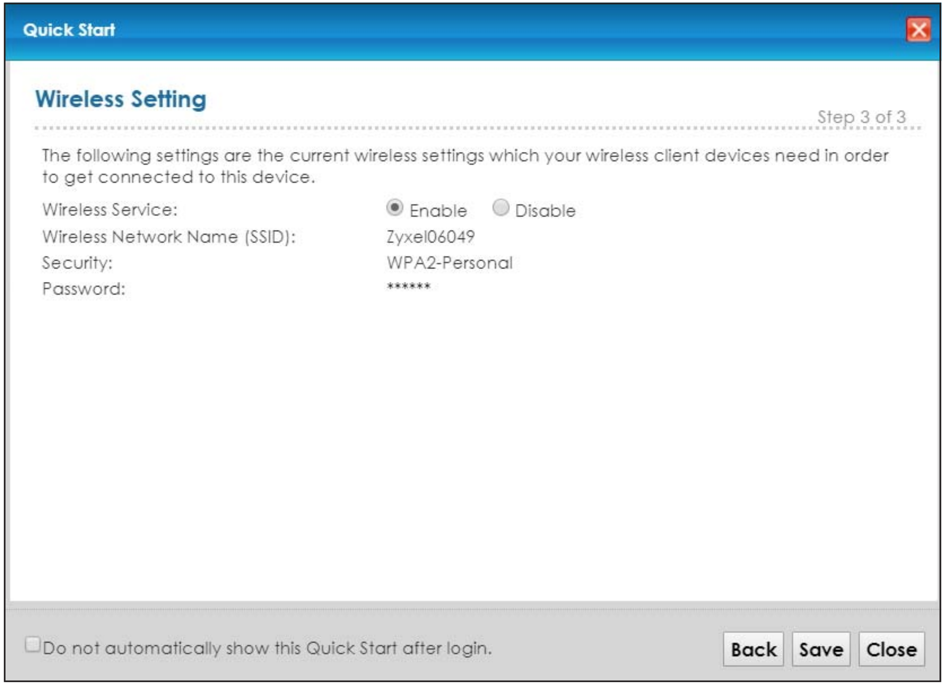
○ Yes ● No

Then the IP Address information will be dynamically assigned to you from your ISP.

□ Do not automatically show this Quick Start after login.

3 Turn the wireless LAN on or off. If you keep it on, record the security settings so you can configure your wireless clients to connect to the EMG. Click **Save**.

Figure 15 Quick Start - Wireless Setting



Wireless Setting

Step 3 of 3

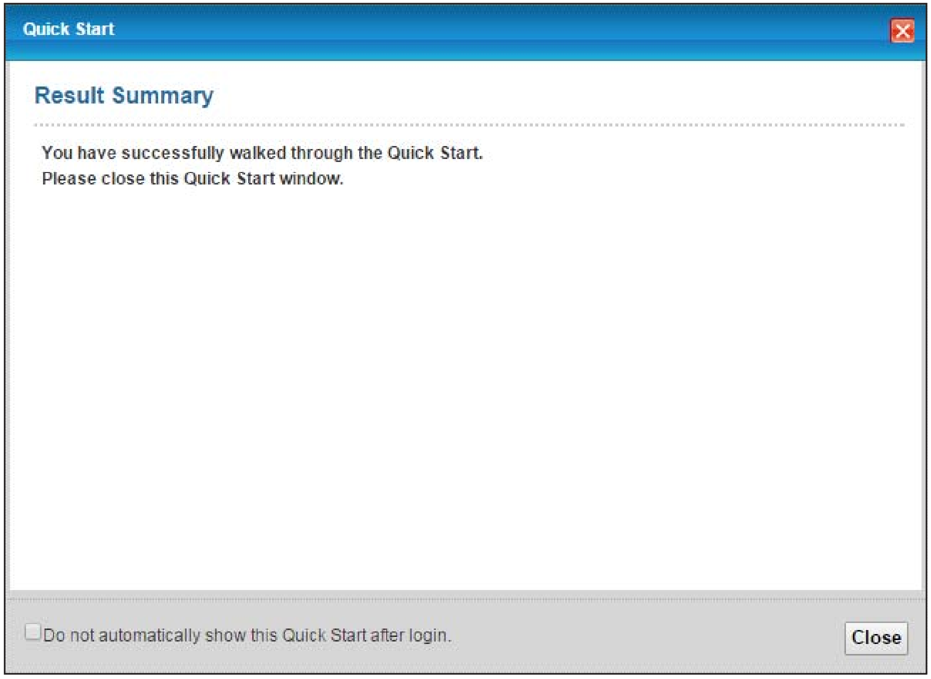
The following settings are the current wireless settings which your wireless client devices need in order to get connected to this device.

Wireless Service:	● Enable ○ Disable
Wireless Network Name (SSID):	Zyxel06049
Security:	WPA2-Personal
Password:	******

□ Do not automatically show this Quick Start after login.

4 Your EMG saves your settings and attempts to connect to the Internet. Click **Close** to complete the setup.

Figure 16 Quick Start - Result Summary



You have successfully walked through the Quick Start.
Please close this Quick Start window.

CHAPTER 4
Tutorials

4.1 Overview

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

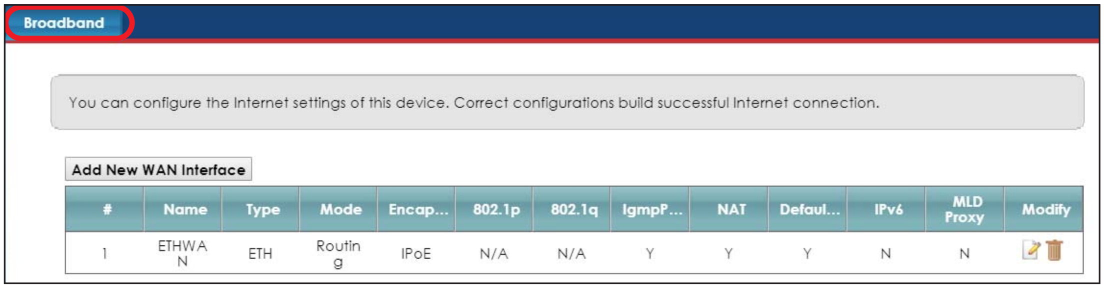
- Setting Up a New WAN Connection, see page 35
- Setting Up a Secure Wireless Network, see page 38
- Setting Up Multiple Wireless Groups, see page 46
- Configuring Static Route for Routing to Another Network, see page 49
- Configuring QoS Queue and Class Setup, see page 51
- Access the EMG Using DDNS, see page 54
- Configuring the MAC Address Filter, see page 55

4.2 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**.



You can configure the Internet settings of this device. Correct configurations build successful Internet connection.

#	Name	Type	Mode	Encap...	802.1p	802.1q	IgmpP...	NAT	Defaul...	IPv6	MLD Proxy	Modify
1	ETHWAN	ETH	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	

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

General	
Active	Enable
Name	MyWANConnection
Type	Ethernet
Mode	Routing

Encapsulation	PPPoE
IPv6/IPv4 Mode	IPv4 Only
Account Information	
PPP User Name	1234@WAN-Ex.com
PPP Password	ABCDEF!
Static IP Address	192.168.1.32
Others	PPP Connection Trigger: Auto Connect PPPoE Passthrough: Disable NAT Enable: Enable IGMP Proxy Enable: Enable Apply as Default Gateway: Enable VLAN Active: Disable

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.

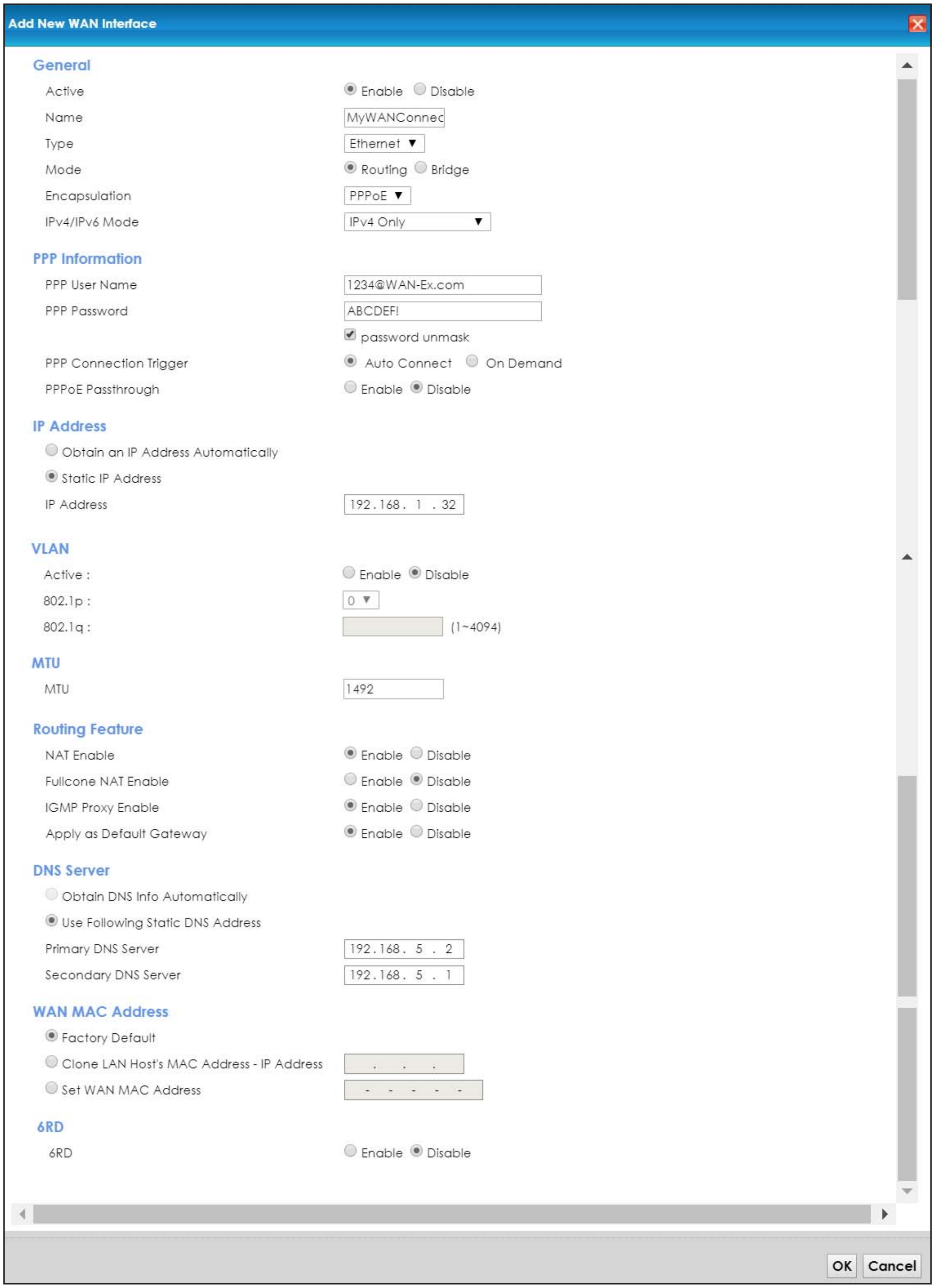
Set the **IPv6/IPv4 Mode** to **IPv4 Only**.

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.



Add New WAN Interface

General

Active	● Enable ○ Disable
Name	MyWANConnec
Type	Ethernet ▼
Mode	● Routing ○ Bridge
Encapsulation	PPPoE ▼
IPv4/IPv6 Mode	IPv4 Only ▼

PPP Information

PPP User Name	1234@WAN-Ex.com
PPP Password	ABCDEF!
	☑ password unmask
PPP Connection Trigger	● Auto Connect ○ On Demand
PPPoE Passthrough	○ Enable ● Disable

IP Address

○ Obtain an IP Address Automatically

● Static IP Address

IP Address	192 . 168 . 1 . 32

VLAN

Active :	○ Enable ● Disable
802.1p :	0 ▼
802.1q :	(1~4094)

MTU

MTU	1492

Routing Feature

NAT Enable	● Enable ○ Disable
Fullcone NAT Enable	○ Enable ● Disable
IGMP Proxy Enable	● Enable ○ Disable
Apply as Default Gateway	● Enable ○ Disable

DNS Server

○ Obtain DNS Info Automatically

● Use Following Static DNS Address

Primary DNS Server	192 . 168 . 5 . 2
Secondary DNS Server	192 . 168 . 5 . 1

WAN MAC Address

● Factory Default

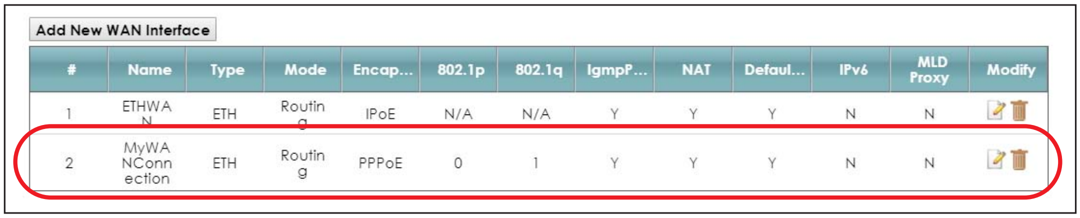
○ Clone LAN Host's MAC Address - IP Address . . .

○ Set WAN MAC Address - - - - -

6RD

6RD	○ Enable ● Disable

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



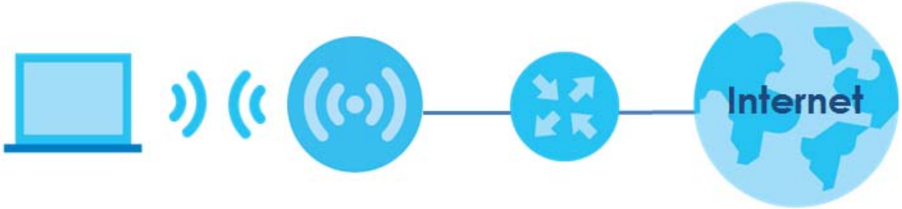
Add New WAN Interface

#	Name	Type	Mode	Encap...	802.1p	802.1q	IgmpP...	NAT	Defaul...	IPv6	MLD Proxy	Modify
1	ETHWAN	ETH	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	
2	MyWANConnection	ETH	Routing	PPPoE	0	1	Y	Y	Y	N	N	

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

4.3 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.



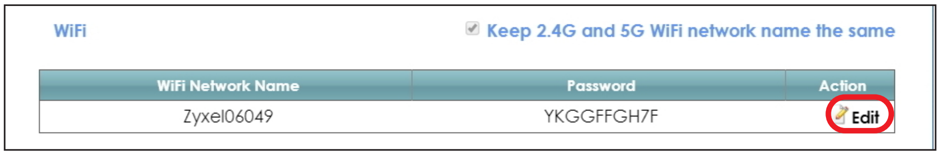
Thomas has to configure the wireless network settings on the EMG. Then he can set up a wireless network using WPS (Section 4.3.2 on page 40) or manual configuration (Section 4.3.3 on page 42).

4.3.1 Configuring the Wireless Network Settings

This example uses the following parameters to set up a 2.4G wireless network.

WiFi Network Name	Example
WiFi	Enable
WiFi Security Type	WPA2-PSK
WiFi Password	DoNotStealMyWirelessNetwork
802.11 Mode	802.11b/g/n Mixed

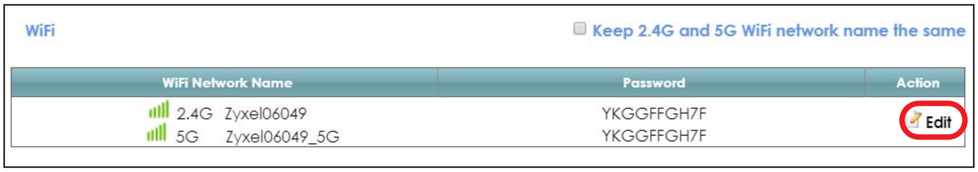
1 Click **Network Setting** > **Wireless** > **WiFi** and click the **Edit** button. Note that you may see one or two network name(s) displayed on this screen depending on whether you have selected **Keep 2.4G and 5G WiFi network name the same**.



WiFi ☑ Keep 2.4G and 5G WiFi network name the same

WiFi Network Name	Password	Action
Zyxel06049	YKGGFFGH7F	Edit

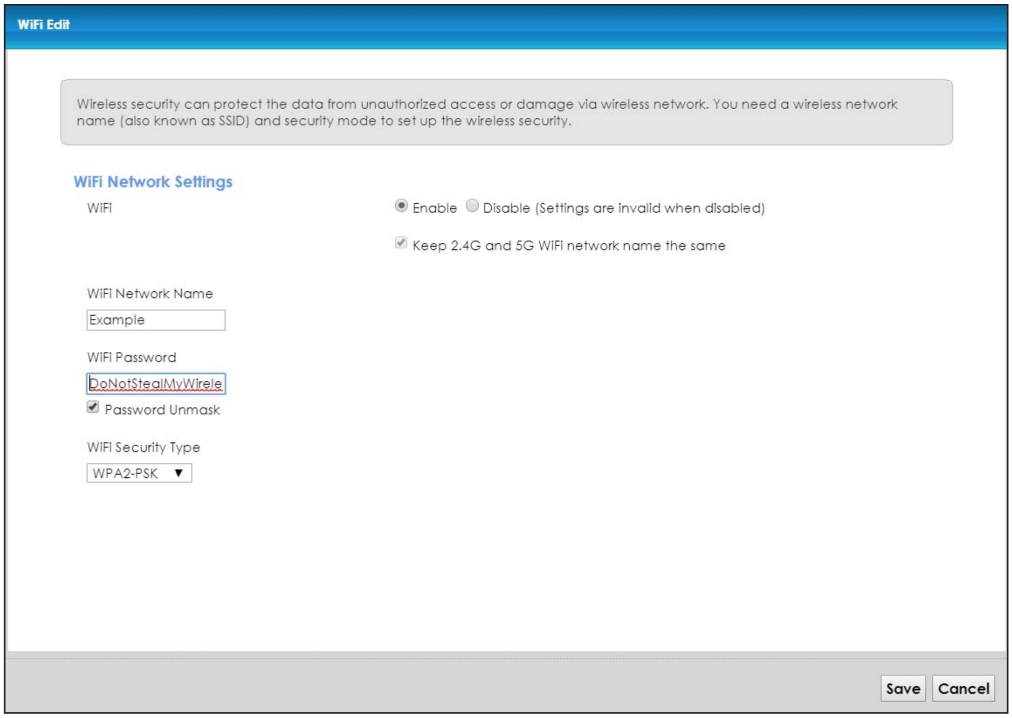
or



WiFi □ Keep 2.4G and 5G WiFi network name the same

WiFi Network Name	Password	Action
2.4G Zyxel06049 5G Zyxel06049_5G	YKGGFFGH7F YKGGFFGH7F	Edit

2 The **WiFi Edit** screen displays. Select **WPA2-PSK** as the security type. Configure the screen using the provided parameters (see page 38). Click **Save**.



WiFi Edit

Wireless security can protect the data from unauthorized access or damage via wireless network. You need a wireless network name (also known as SSID) and security mode to set up the wireless security.

WiFi Network Settings

WiFi ● Enable ○ Disable (Settings are invalid when disabled)

☑ Keep 2.4G and 5G WiFi network name the same

WiFi Network Name

Example

WiFi Password

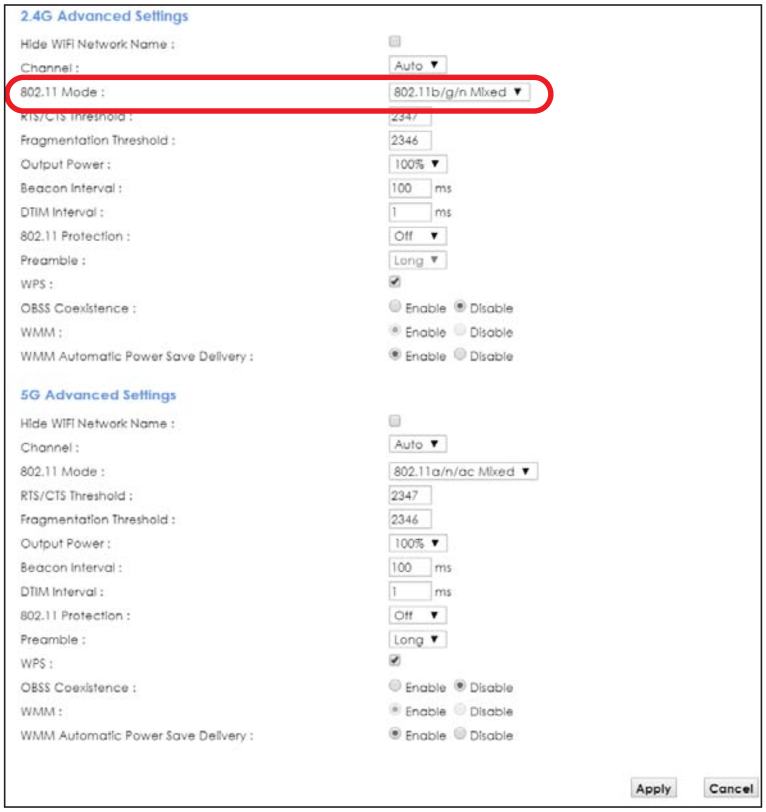
DoNotStealMyWirele

☑ Password Unmask

WiFi Security Type

WPA2-PSK ▼

3 Go to the **Wireless > Advanced** screen and select **802.11b/g/n Mixed** in the **802.11 Mode** field in the **2.4G Advanced Settings** section. Click **Apply**.



2.4G Advanced Settings

Hide WIFI Network Name :	□
Channel :	Auto ▼
802.11 Mode :	802.11b/g/n Mixed ▼
RTS/CTS Threshold :	2347
Fragmentation Threshold :	2346
Output Power :	100% ▼
Beacon Interval :	100 ms
DTIM Interval :	1 ms
802.11 Protection :	Off ▼
Preamble :	Long ▼
WPS :	☑
OBSS Coexistence :	○ Enable ● Disable
WMM :	● Enable ○ Disable
WMM Automatic Power Save Delivery :	● Enable ○ Disable

5G Advanced Settings

Hide WIFI Network Name :	□
Channel :	Auto ▼
802.11 Mode :	802.11a/n/ac Mixed ▼
RTS/CTS Threshold :	2347
Fragmentation Threshold :	2346
Output Power :	100% ▼
Beacon Interval :	100 ms
DTIM Interval :	1 ms
802.11 Protection :	Off ▼
Preamble :	Long ▼
WPS :	☑
OBSS Coexistence :	○ Enable ● Disable
WMM :	● Enable ○ Disable
WMM Automatic Power Save Delivery :	● Enable ○ Disable

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the EMG (see Section 4.3.2 on page 40). He can also use the notebook's wireless client to search for the EMG (see Section 4.3.3 on page 42).

4.3.2 Using WPS

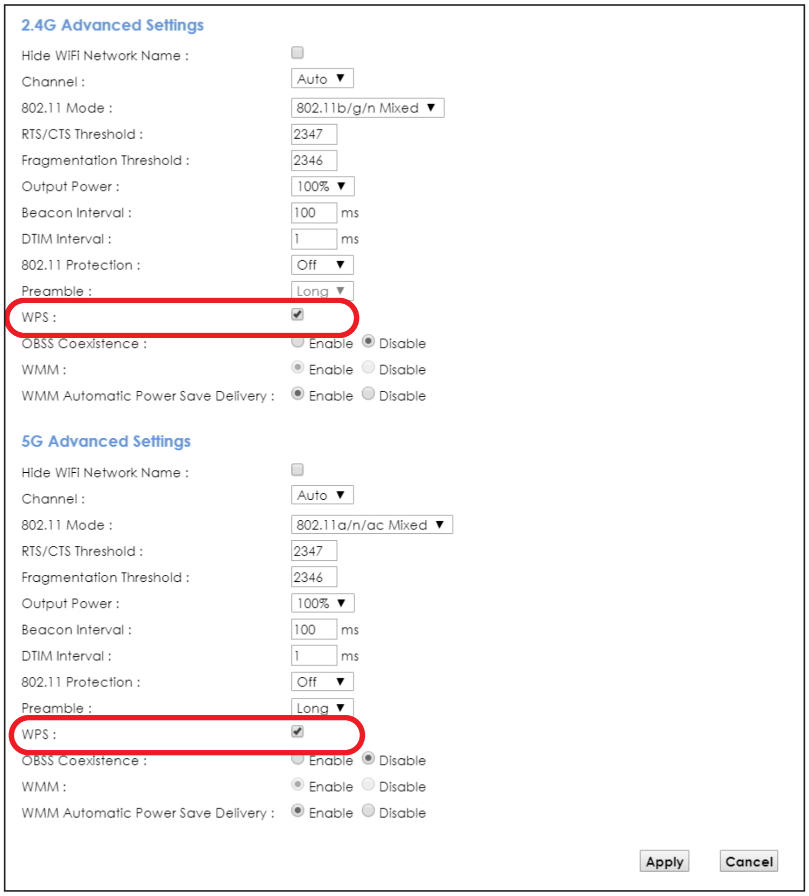
This section shows you how to set up a wireless network using WPS. It uses the EMG as the AP and a WPS-enabled Android 4.4.2 smartphone as the wireless client.

to set up the wireless client settings:

1. Make sure that your EMG is turned on and your Android 4.42 smartphone is within the cover range of the wireless signal.

2. Make sure WPS is enabled on the EMG. You can check it by logging into the EMG's Web Configurator and see if it is enabled in the **Network Setting > Wireless > Advanced** screen. If not, select the **WPS** checkbox for the 2.4G or 5G wireless network and then click **Apply**.

   Note: When the MESH function is enabled (see Section 7.7 on page 85), the EMG automatically enables WPS and grays the field out on this **Network Setting > Wireless > Advanced** screen.



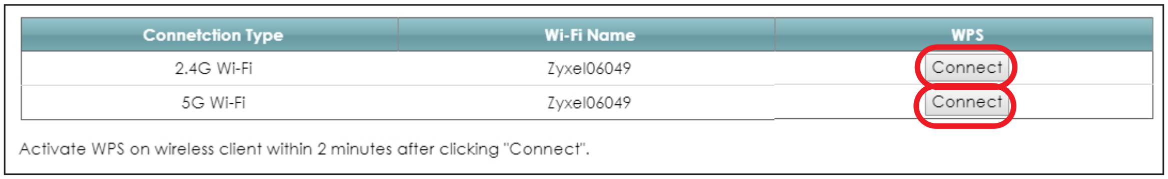
2.4G Advanced Settings

Hide WiFi Network Name :	☐
Channel :	Auto ▼
802.11 Mode :	802.11b/g/n Mixed ▼
RTS/CTS Threshold :	2347
Fragmentation Threshold :	2346
Output Power :	100% ▼
Beacon Interval :	100 ms
DTIM Interval :	1 ms
802.11 Protection :	Off ▼
Preamble :	Long ▼
WPS :	☑
OBSS Coexistence :	○ Enable ● Disable
WMM :	● Enable ○ Disable
WMM Automatic Power Save Delivery :	● Enable ○ Disable

5G Advanced Settings

Hide WiFi Network Name :	☐
Channel :	Auto ▼
802.11 Mode :	802.11a/n/ac Mixed ▼
RTS/CTS Threshold :	2347
Fragmentation Threshold :	2346
Output Power :	100% ▼
Beacon Interval :	100 ms
DTIM Interval :	1 ms
802.11 Protection :	Off ▼
Preamble :	Long ▼
WPS :	☑
OBSS Coexistence :	○ Enable ● Disable
WMM :	● Enable ○ Disable
WMM Automatic Power Save Delivery :	● Enable ○ Disable

3 You can either press the **WPS** button on the EMG's panel or click the **Connect** button for the corresponding 2.4G or 5G wireless band in the **Network Setting > Wireless > WPS** screen.



Connetction Type	Wi-Fi Name	WPS
2.4G Wi-Fi	Zyxel06049	Connect
5G Wi-Fi	Zyxel06049	Connect

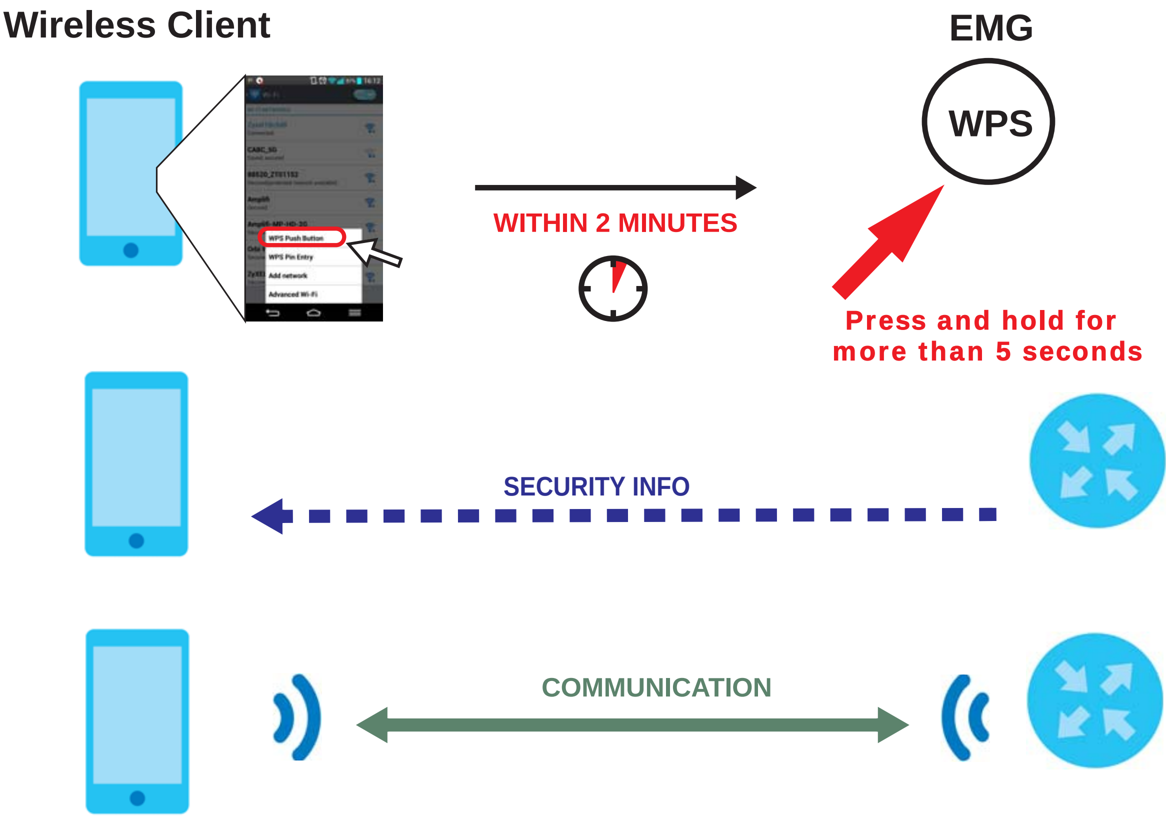
Activate WPS on wireless client within 2 minutes after clicking "Connect".

4 Go to your phone settings and turn on Wi-Fi. Open the Wi-Fi networks list and tap **WPS Push Button** or the WPS icon (⟳).

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 (the Android 4.4.2 phone in this example).



4.3.3 Connecting to the EMG's Wi-Fi Network Manually (No WPS)

In this example, we change the EMG's wireless settings, and then manually select the EMG's new SSID and enter the Wi-Fi key to connect a wireless client to the EMG.

4.3.4 Configuring Wireless Security on the EMG

This section shows you how to configure wireless security settings with the following parameters on your EMG.

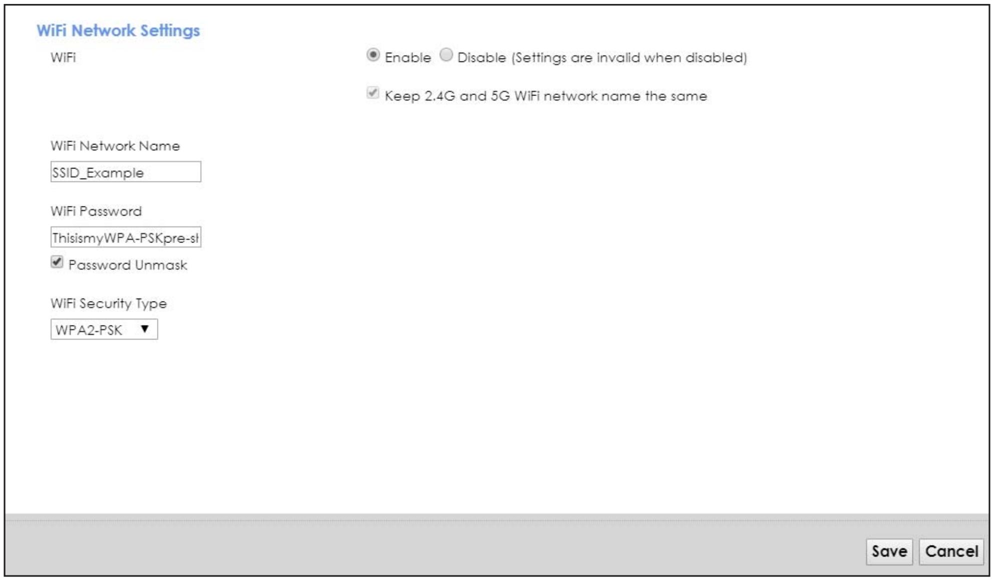
Frequency Band	2.4 GHz
SSID	SSID_Example
Channel	Auto
Security	WPA2-PSK (Wireless Password: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your EMG.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see Section 2.2 on page 27).

1 Go to the **Network Setting** > **Wireless** > **WiFi** > **Edit** screen to enable the 2.4 GHz wireless network.

2 Enter **SSID_Example** as the wireless name. Set WiFi security type to **WPA2-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Save**.



WiFi Network Settings

WiFi ● Enable ○ Disable (Settings are invalid when disabled)

☑ Keep 2.4G and 5G WiFi network name the same

WiFi Network Name: SSID_Example

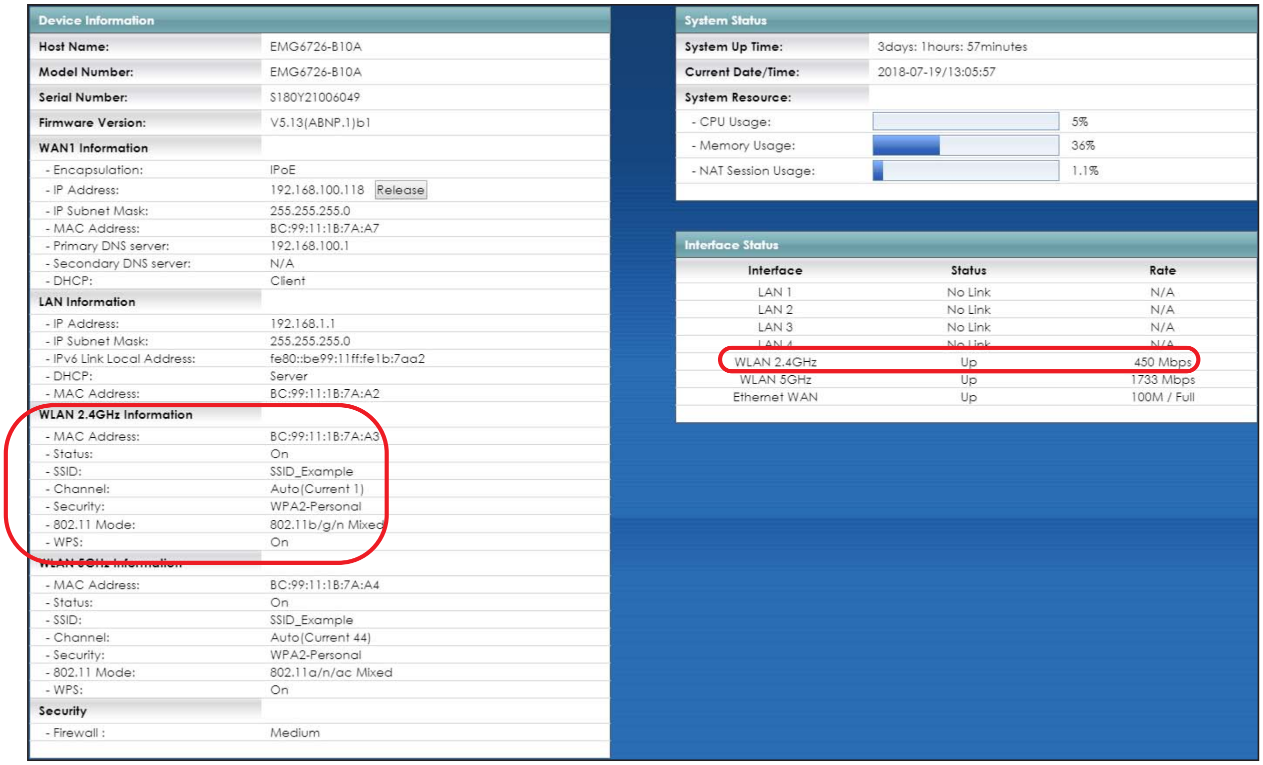
WiFi Password: ThisismyWPA-PSKpre-sł

☑ Password Unmask

WiFi Security Type: WPA2-PSK ▼

3 Go to the **Network Setting** > **Wireless** > **Advanced** screen and select **Auto** in the **Channel** field to have the EMG scan for and select an available channel automatically.

4 Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.



Device Information	
Host Name:	EMG6726-B10A
Model Number:	EMG6726-B10A
Serial Number:	S180Y21006049
Firmware Version:	V5.13(ABNP.1)b1
WAN1 Information	
- Encapsulation:	IPoE
- IP Address:	192.168.100.118 Release
- IP Subnet Mask:	255.255.255.0
- MAC Address:	BC:99:11:1B:7A:A7
- Primary DNS server:	192.168.100.1
- Secondary DNS server:	N/A
- DHCP:	Client
LAN Information	
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- IPv6 Link Local Address:	fe80::be99:11ff:fe1b:7aa2
- DHCP:	Server
- MAC Address:	BC:99:11:1B:7A:A2
WLAN 2.4GHz Information	
- MAC Address:	BC:99:11:1B:7A:A3
- Status:	On
- SSID:	SSID_Example
- Channel:	Auto(Current 1)
- Security:	WPA2-Personal
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	On
WLAN 5GHz Information	
- MAC Address:	BC:99:11:1B:7A:A4
- Status:	On
- SSID:	SSID_Example
- Channel:	Auto(Current 44)
- Security:	WPA2-Personal
- 802.11 Mode:	802.11a/n/ac Mixed
- WPS:	On
Security	
- Firewall :	Medium

System Status		
System Up Time:	3days: 1hours: 57minutes	
Current Date/Time:	2018-07-19/13:05:57	
System Resource:		
- CPU Usage:		5%
- Memory Usage:		36%
- NAT Session Usage:		1.1%

Interface Status

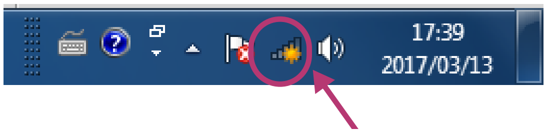
Interface	Status	Rate
LAN 1	No Link	N/A
LAN 2	No Link	N/A
LAN 3	No Link	N/A
LAN 4	No Link	N/A
WLAN 2.4GHz	Up	450 Mbps
WLAN 5GHz	Up	1733 Mbps
Ethernet WAN	Up	100M / Full

4.3.5 Configure Your Notebook

Note: In this example, we use a Windows 7 laptop that has a built-in wireless adapter as the wireless client.

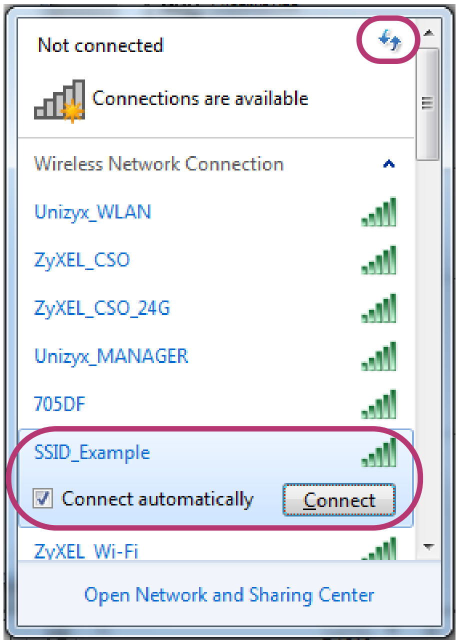
1 The EMG supports IEEE 802.11a/g/n/b/ac wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

2 Click the Wi-Fi icon in your computer's system tray



3 The **Wireless Network Connection** screen displays. Click the refresh button to update the list of available wireless APs within range.

4 Select **SSID_Example** and click **Connect**.


Not connected

Connections are available

Wireless Network Connection

Unizyx_WLAN

ZyXEL_CSO

ZyXEL_CSO_24G

Unizyx_MANAGER

705DF

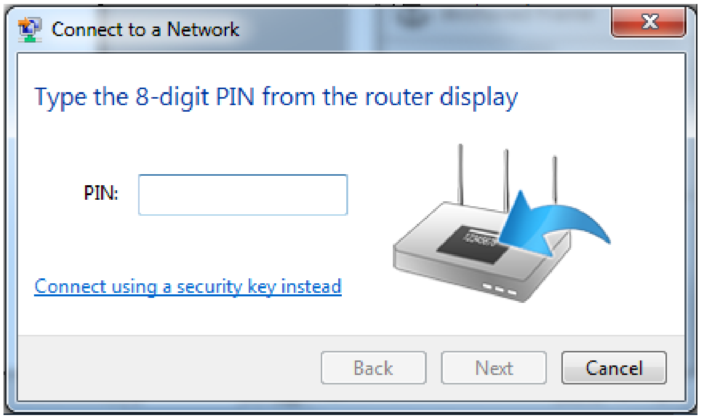
SSID_Example

☑ Connect automatically Connect

ZyXEL_Wi-Fi

Open Network and Sharing Center

5 The following screen displays if WPS is enabled on the EMG but you didn't press the WPS button. Click **Connect using as security key instead**.

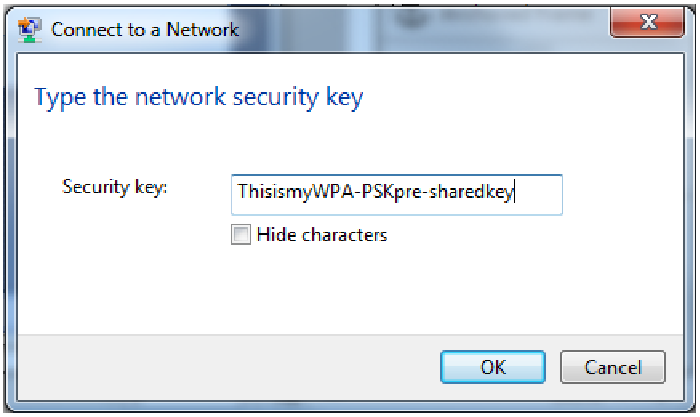


Type the 8-digit PIN from the router display

PIN:

Connect using a security key instead

6 Type the security key in the following screen. Click **OK**.

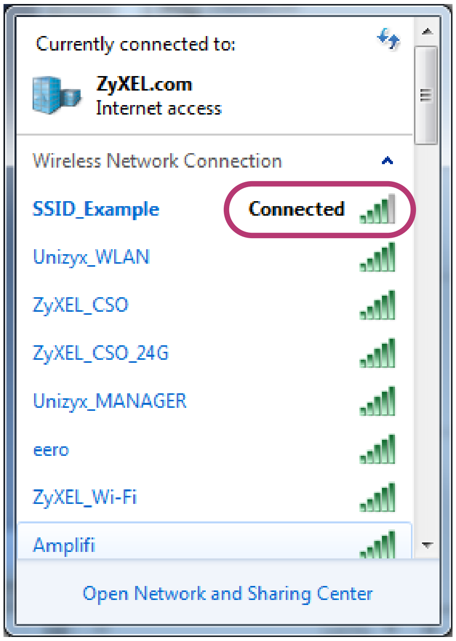


Type the network security key

Security key: ThisismyWPA-PSKpre-sharedkey

□ Hide characters

7 Check the status of your wireless connection in the screen below.



Currently connected to:

ZyXEL.com
Internet access

Wireless Network Connection

SSID_Example Connected

Unizyx_WLAN

ZyXEL_CSO

ZyXEL_CSO_24G

Unizyx_MANAGER

eero

ZyXEL_Wi-Fi

Amplifi

Open Network and Sharing Center

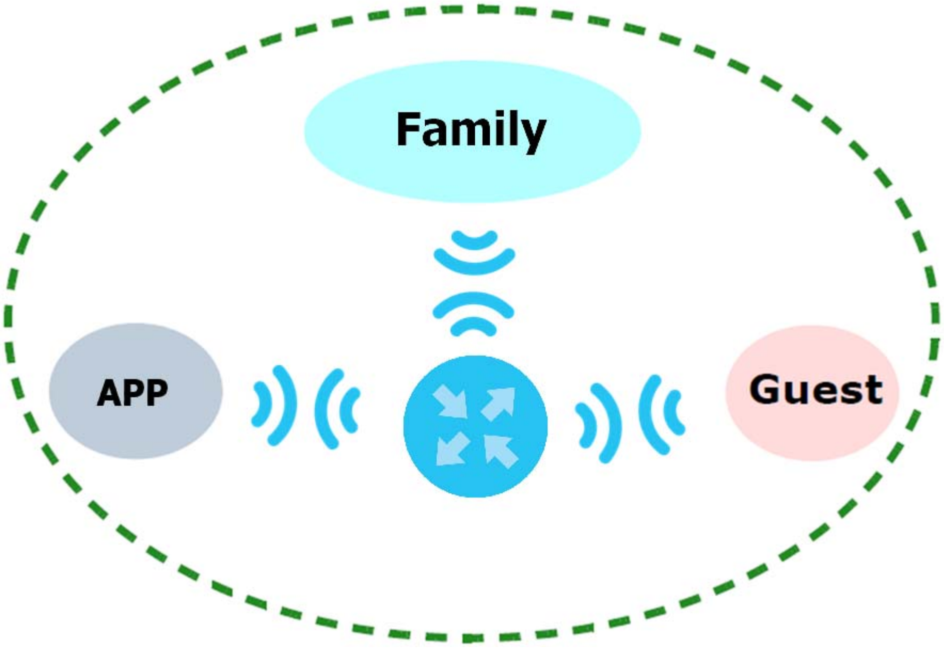
8 If the wireless client keeps trying to connect to or acquiring an IP address from the EMG, make sure you entered the correct security key.

If the connection has limited or no connectivity, make sure the EMG is connected to a router with the DHCP server enabled.

If your connection is successful, open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

4.4 Setting Up Multiple Wireless Groups

A family wants to create different wireless network groups for different types of users as shown in the following figure. Each group has its own wireless network name (SSID) and security type.

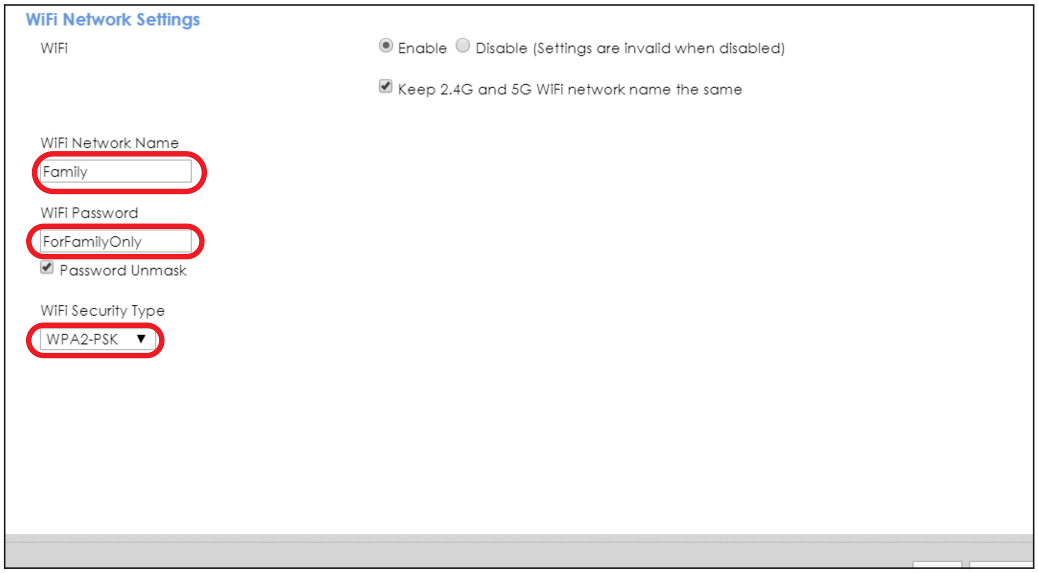


- The family members will use the general **Family** wireless network group.
- Visiting guests will use the **Guest** group with the restriction of the Internet access for the following 48 hours (in this example) after the setting is applied.
- The **APP** group will be dedicated to some home applications that require the Internet or an internal network, such as playing PS4 games.

The family will use the following parameters to set up the wireless network groups.

	FAMILY	GUEST	APP
SSID	Family	Guest	APP
Security Type	WPA2-PSK		
Wireless Password	ForFamilyOnly	guest123	123456789
Available Time	N/A	48 hours	N/A

1 Click **Network Setting > Wireless > WiFi > Edit** to open the **WiFi Edit** screen. Use this screen to set up the family's general wireless network group. Configure the screen using the provided parameters and click **Save**.



WiFi Network Settings

WiFi ● Enable ○ Disable (Settings are invalid when disabled)

☑ Keep 2.4G and 5G WiFi network name the same

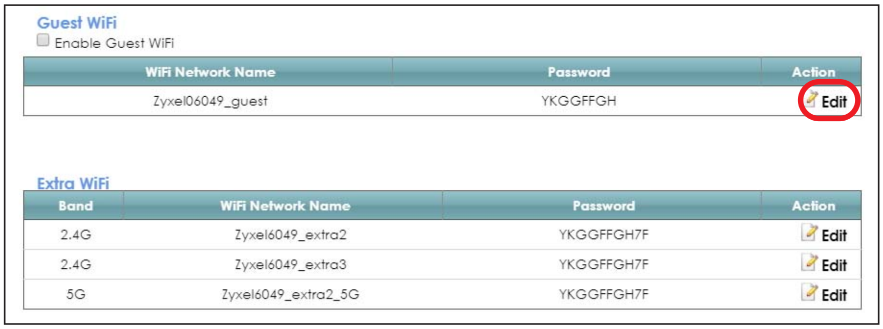
WiFi Network Name: Family

WiFi Password: ForFamilyOnly

☑ Password Unmask

WiFi Security Type: WPA2-PSK

2 Click **Network Setting > Wireless > Guest WiFi** to open the following screen. Click the **Edit** icon in the **Guest WiFi** section to configure the second wireless network group.



Guest WiFi

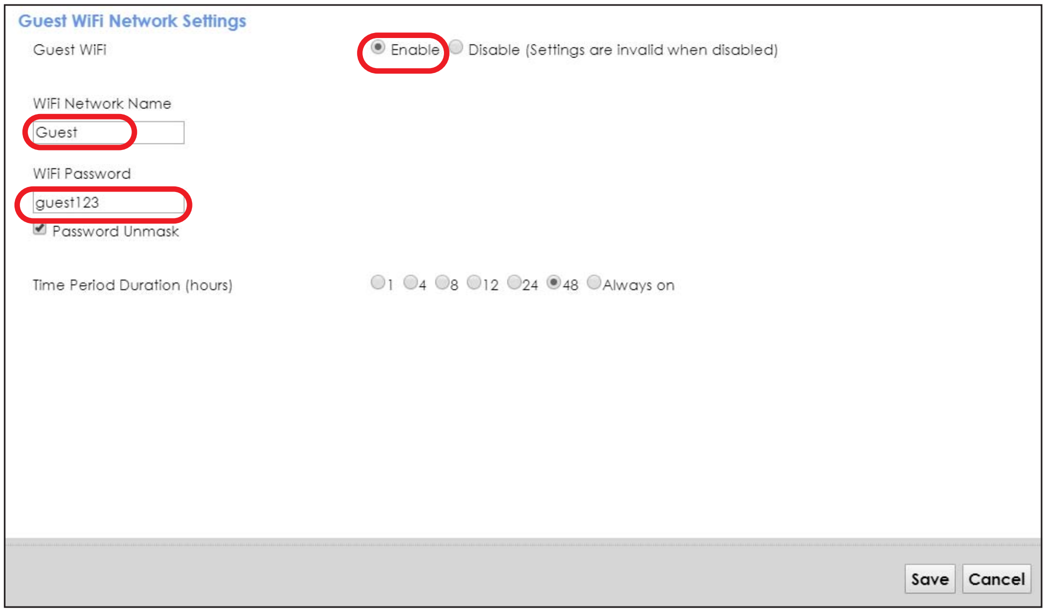
□ Enable Guest WiFi

WiFi Network Name	Password	Action
Zyxel06049_guest	YKGGFFGH	Edit

Extra WiFi

Band	WiFi Network Name	Password	Action
2.4G	Zyxel6049_extra2	YKGGFFGH7F	Edit
2.4G	Zyxel6049_extra3	YKGGFFGH7F	Edit
5G	Zyxel6049_extra2_5G	YKGGFFGH7F	Edit

3 Configure the screen using the provided parameters and click **Save**.



Guest WiFi Network Settings

Guest WiFi ● Enable ○ Disable (Settings are invalid when disabled)

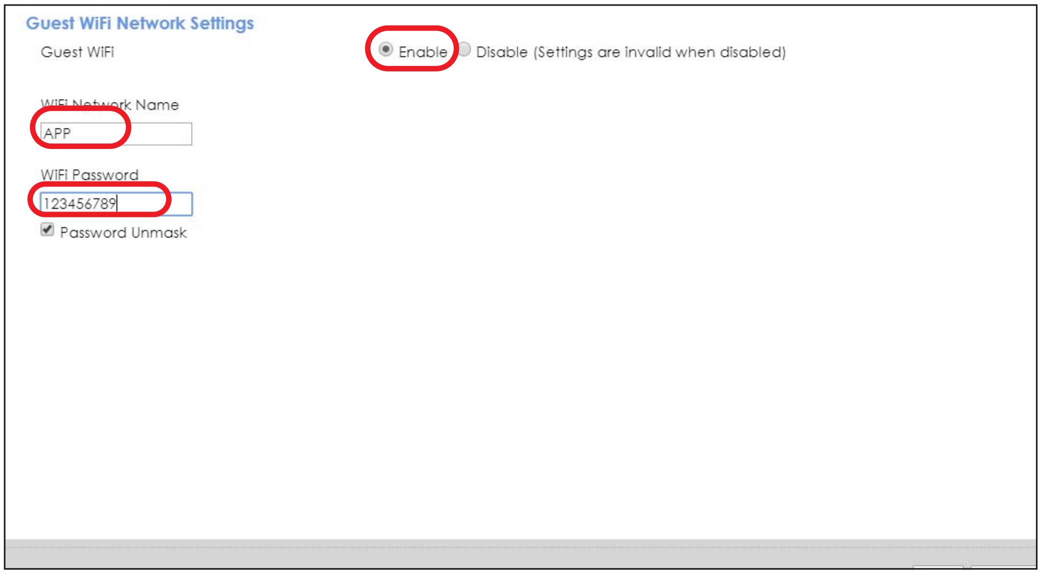
WiFi Network Name: Guest

WiFi Password: guest123

☑ Password Unmask

Time Period Duration (hours) ○1 ○4 ○8 ○12 ○24 ●48 ○Always on

4 In the **Guest WiFi** screen, click an **Edit** icon next to a 2.4G “extra WiFi” network to configure the third wireless network group. Configure the screen using the provided parameters and click **Save**.



Guest WiFi Network Settings

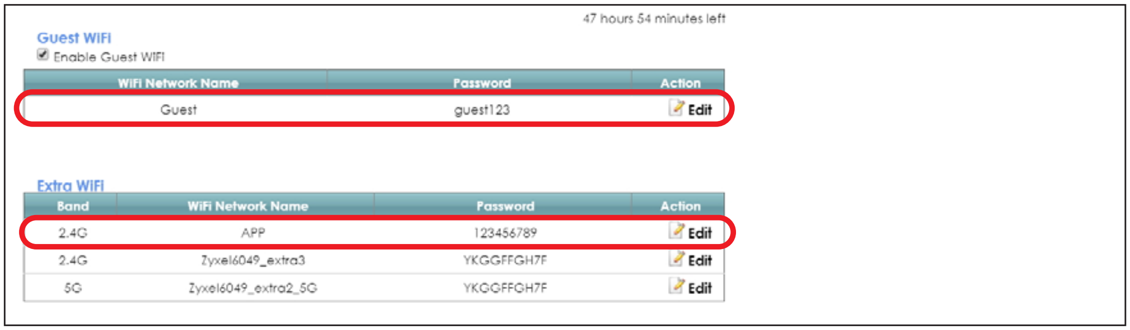
Guest WiFi ● Enable ○ Disable (Settings are invalid when disabled)

WiFi Network Name: APP

WiFi Password: 123456789

☑ Password Unmask

5 Check the status of **Guest** and **APP** in the **Guest WiFi** screen. The screen also displays the remaining available time for using the **Guest** WiFi network at the upper right corner.



47 hours 54 minutes left

Guest WiFi

☑ Enable Guest WiFi

WiFi Network Name	Password	Action
Guest	guest123	Edit

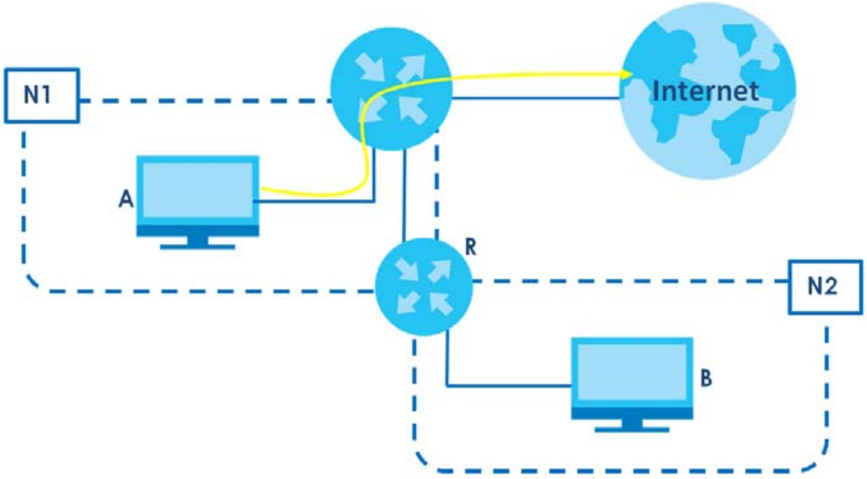
Extra WiFi

Band	WiFi Network Name	Password	Action
2.4G	APP	123456789	Edit
2.4G	Zyxel6049_extra3	YKGGFFGH7F	Edit
5G	Zyxel6049_extra2_5G	YKGGFFGH7F	Edit

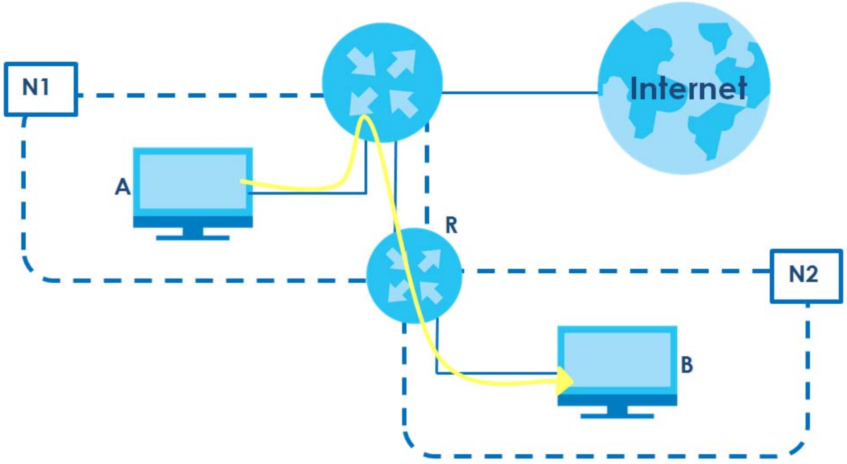
4.5 Configuring Static Route for Routing to Another Network

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

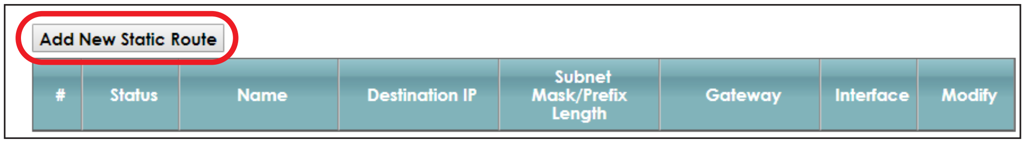
DEVICE / COMPUTER	IP ADDRESS
The EMG's WAN	172.16.1.1
The EMG's LAN	192.168.1.1
IP Type	IPv4
Use Interface	ETHWAN
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

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

1 Log into the EMG's Web Configurator in advanced mode.

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

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



Add New Static Route

#	Status	Name	Destination IP	Subnet Mask/Prefix Length	Gateway	Interface	Modify

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

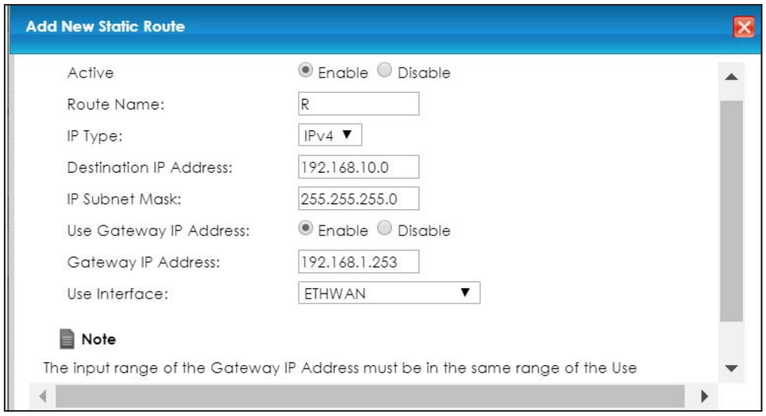
4a Select the **Active** check box. Enter the **Route Name** as **R**.

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**.



Add New Static Route

Active	● Enable ○ Disable
Route Name:	R
IP Type:	IPv4 ▼
Destination IP Address:	192.168.10.0
IP Subnet Mask:	255.255.255.0
Use Gateway IP Address:	● Enable ○ Disable
Gateway IP Address:	192.168.1.253
Use Interface:	ETHWAN ▼

Note

The input range of the Gateway IP Address must be in the same range of the Use

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.

4.6 Configuring QoS Queue and Class Setup

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

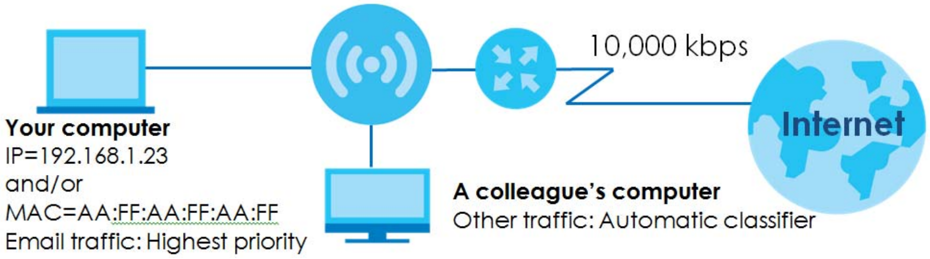
Let’s say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues 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:

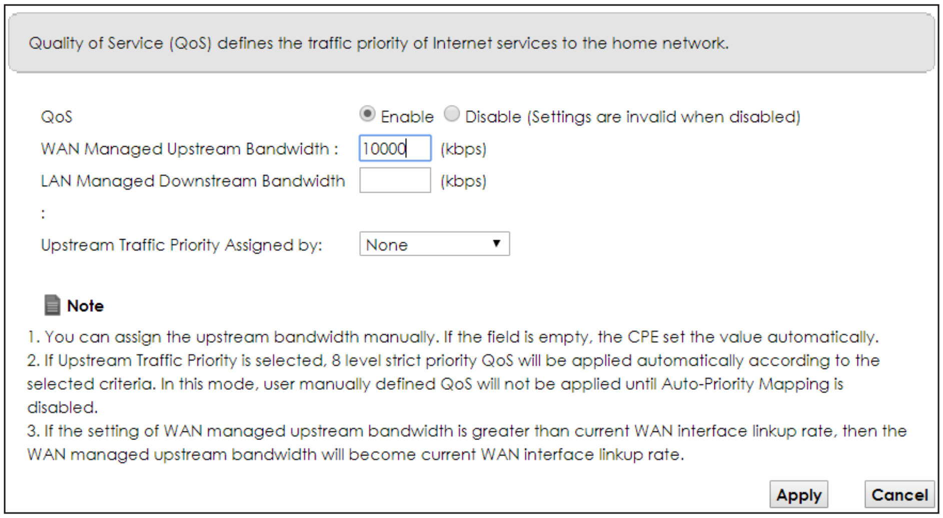
- Configure a queue to assign the highest priority queue (1) to e-mail traffic going to the WAN interface, so that e-mail traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer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



Quality of Service (QoS) defines the traffic priority of Internet services to the home network.

QoS ● Enable ○ Disable (Settings are invalid when disabled)

WAN Managed Upstream Bandwidth : 10000 (kbps)

LAN Managed Downstream Bandwidth : (kbps)

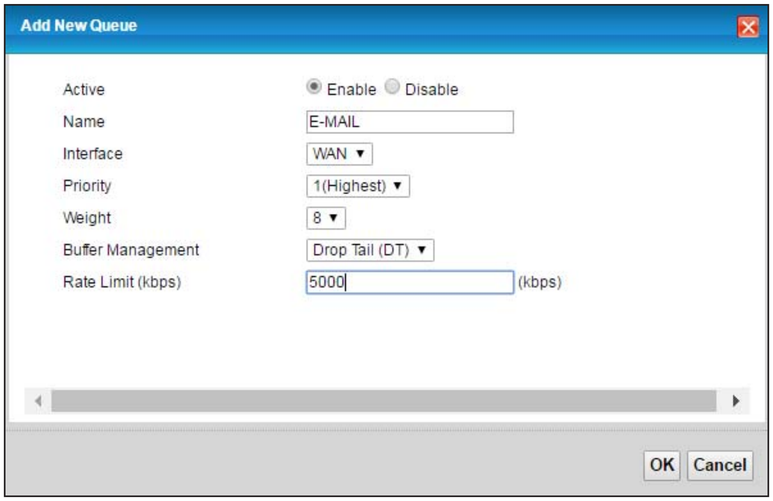
Upstream Traffic Priority Assigned by: None

Note

1. You can assign the upstream bandwidth manually. If the field is empty, the CPE set the value automatically.
2. If Upstream Traffic Priority is selected, 8 level strict priority QoS will be applied automatically according to the selected criteria. In this mode, user manually defined QoS will not be applied until Auto-Priority Mapping is disabled.
3. If the setting of WAN managed upstream bandwidth is greater than current WAN interface linkup rate, then the WAN managed upstream bandwidth will become current WAN interface linkup rate.

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

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



Active ● Enable ○ Disable

Name E-MAIL

Interface WAN

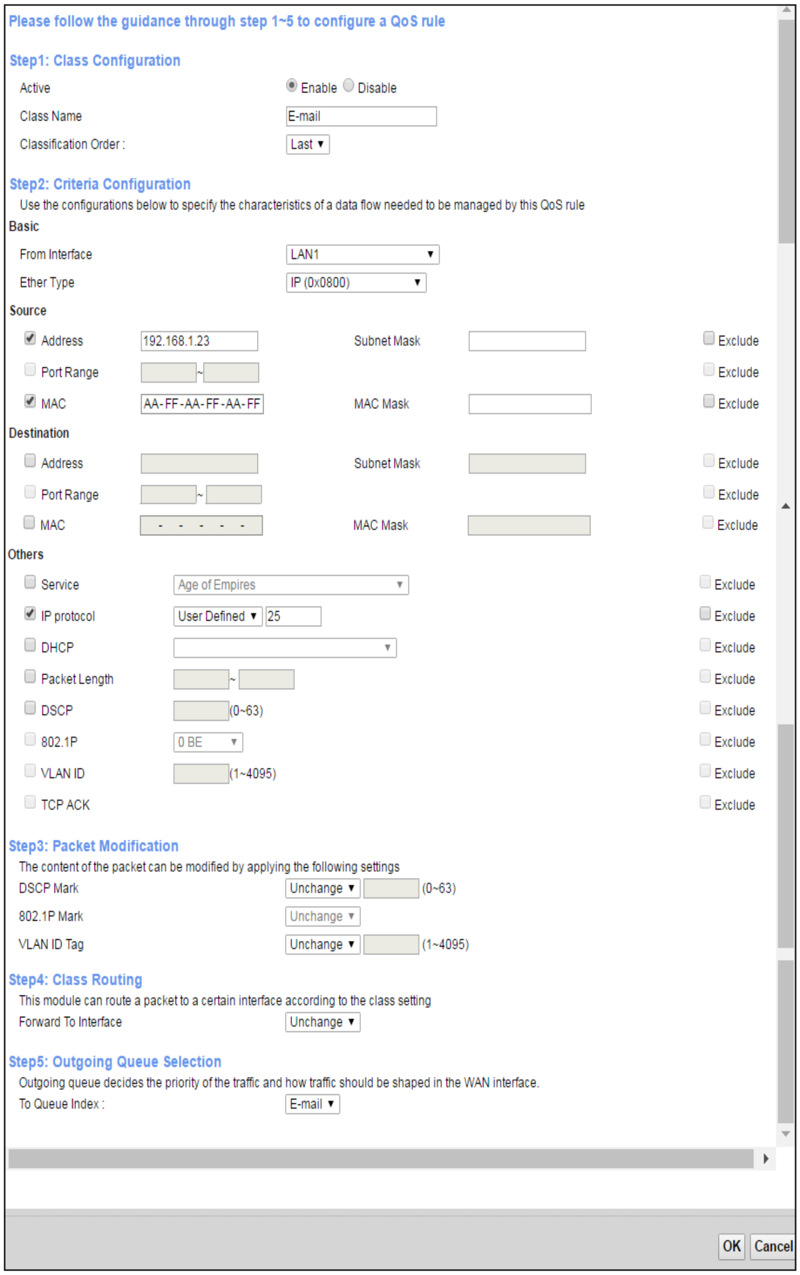
Priority 1(Highest)

Weight 8

Buffer Management Drop Tail (DT)

Rate Limit (kbps) 5000 (kbps)

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



Please follow the guidance through step 1~5 to configure a QoS rule

Step1: Class Configuration

Active	● Enable ○ Disable
Class Name	E-mail
Classification Order :	Last ▾

Step2: Criteria Configuration

Use the configurations below to specify the characteristics of a data flow needed to be managed by this QoS rule

Basic

From Interface	LAN1 ▾
Ether Type	IP (0x0800) ▾

Source

☑ Address	192.168.1.23	Subnet Mask		□ Exclude
□ Port Range	~			□ Exclude
☑ MAC	AA-FF-AA-FF-AA-FF	MAC Mask		□ Exclude

Destination

□ Address		Subnet Mask		□ Exclude
□ Port Range	~			□ Exclude
□ MAC	- - - - -	MAC Mask		□ Exclude

Others

□ Service	Age of Empires ▾	□ Exclude
☑ IP protocol	User Defined ▾ 25	□ Exclude
□ DHCP	▾	□ Exclude
□ Packet Length	~	□ Exclude
□ DSCP	(0~63)	□ Exclude
□ 802.1P	0 BE ▾	□ Exclude
□ VLAN ID	(1~4095)	□ Exclude
□ TCP ACK		□ Exclude

Step3: Packet Modification

The content of the packet can be modified by applying the following settings

DSCP Mark	Unchange ▾ (0~63)
802.1P Mark	Unchange ▾
VLAN ID Tag	Unchange ▾ (1~4095)

Step4: Class Routing

This module can route a packet to a certain interface according to the class setting

Forward To Interface	Unchange ▾

Step5: Outgoing Queue Selection

Outgoing queue decides the priority of the traffic and how traffic should be shaped in the WAN interface.

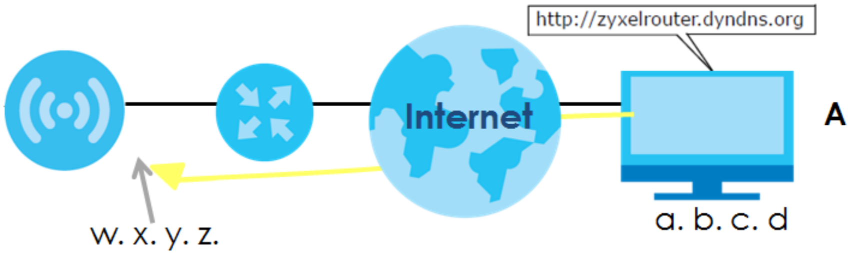
To Queue Index :	E-mail ▾

FIELD TO CONFIGURE	HOW TO CONFIGURE
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).

4.7 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.

4.7.1 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.

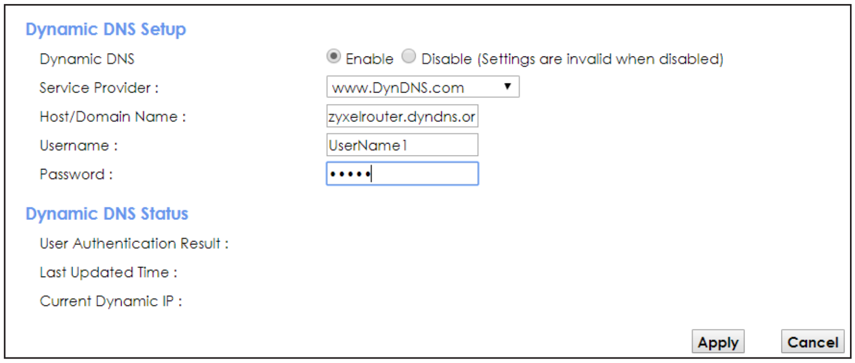
- Hostname: **zyxelrouter.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your EMG is currently using. You can find the IP address on the EMG's Web Configurator **Status** page.

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

4.7.2 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**).



Dynamic DNS Setup

Dynamic DNS ● Enable ○ Disable (Settings are invalid when disabled)

Service Provider : www.DynDNS.com ▼

Host/Domain Name : zyxelrouter.dyndns.or

Username : UserName1

Password : •••••

Dynamic DNS Status

User Authentication Result :

Last Updated Time :

Current Dynamic IP :

Click **Apply**.

4.7.3 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.

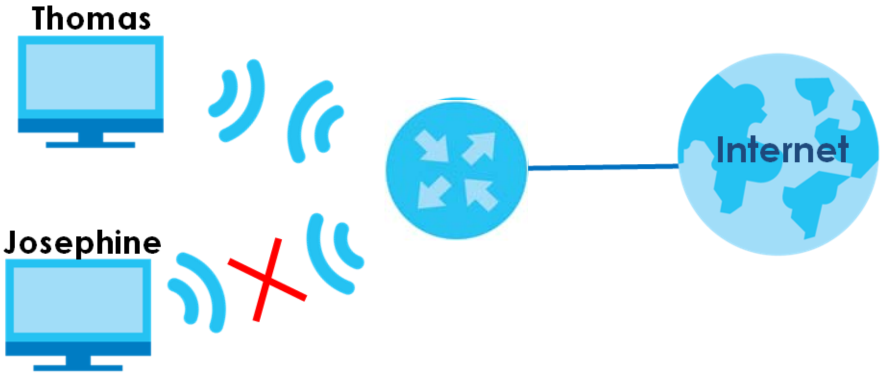
2 Type **http://zyxelrouter.dyndns.org** and press [Enter].

3 The EMG's login page should appear. You can then log into the EMG and manage it.

4.8 Configuring the MAC Address Filter

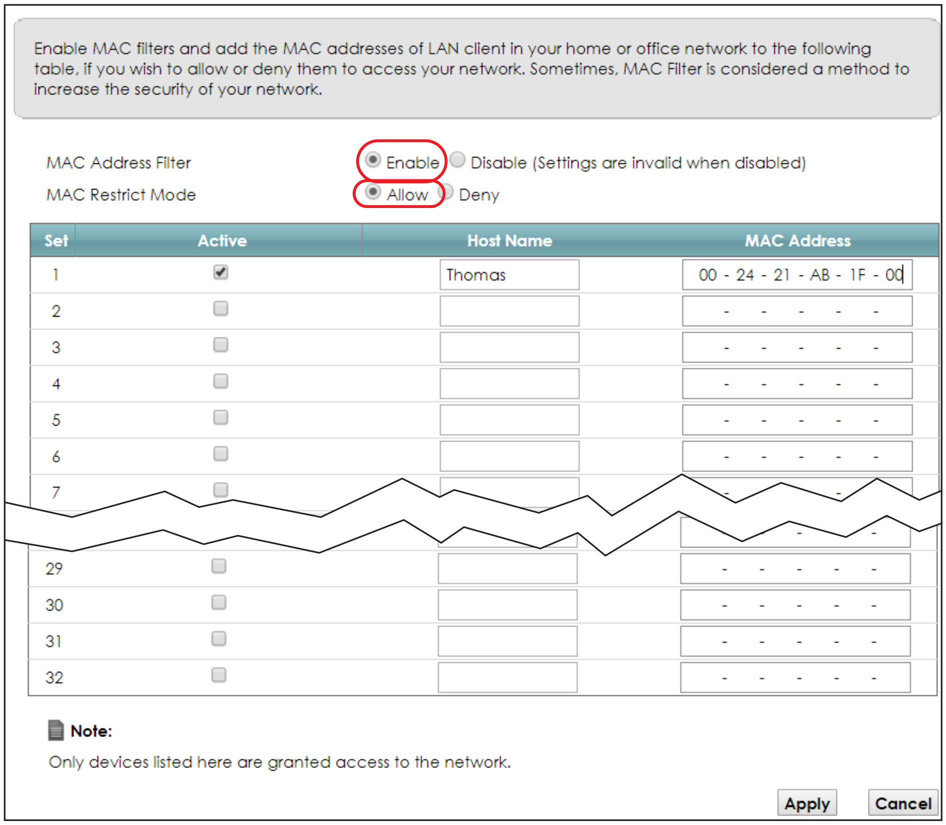
Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

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**.



Enable MAC filters and add the MAC addresses of LAN client in your home or office network to the following table, if you wish to allow or deny them to access your network. Sometimes, MAC Filter is considered a method to increase the security of your network.

MAC Address Filter ● Enable ○ Disable (Settings are invalid when disabled)

MAC Restrict Mode ● Allow ○ Deny

Set	Active	Host Name	MAC Address
1	☑	Thomas	00 - 24 - 21 - AB - 1F - 00
2	□		- - - - -
3	□		- - - - -
4	□		- - - - -
5	□		- - - - -
6	□		- - - - -
7	□		- - - - -
29	□		- - - - -
30	□		- - - - -
31	□		- - - - -
32	□		- - - - -

Note:

Only devices listed here are granted access to the network.

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 5
Network Map and Status Screens

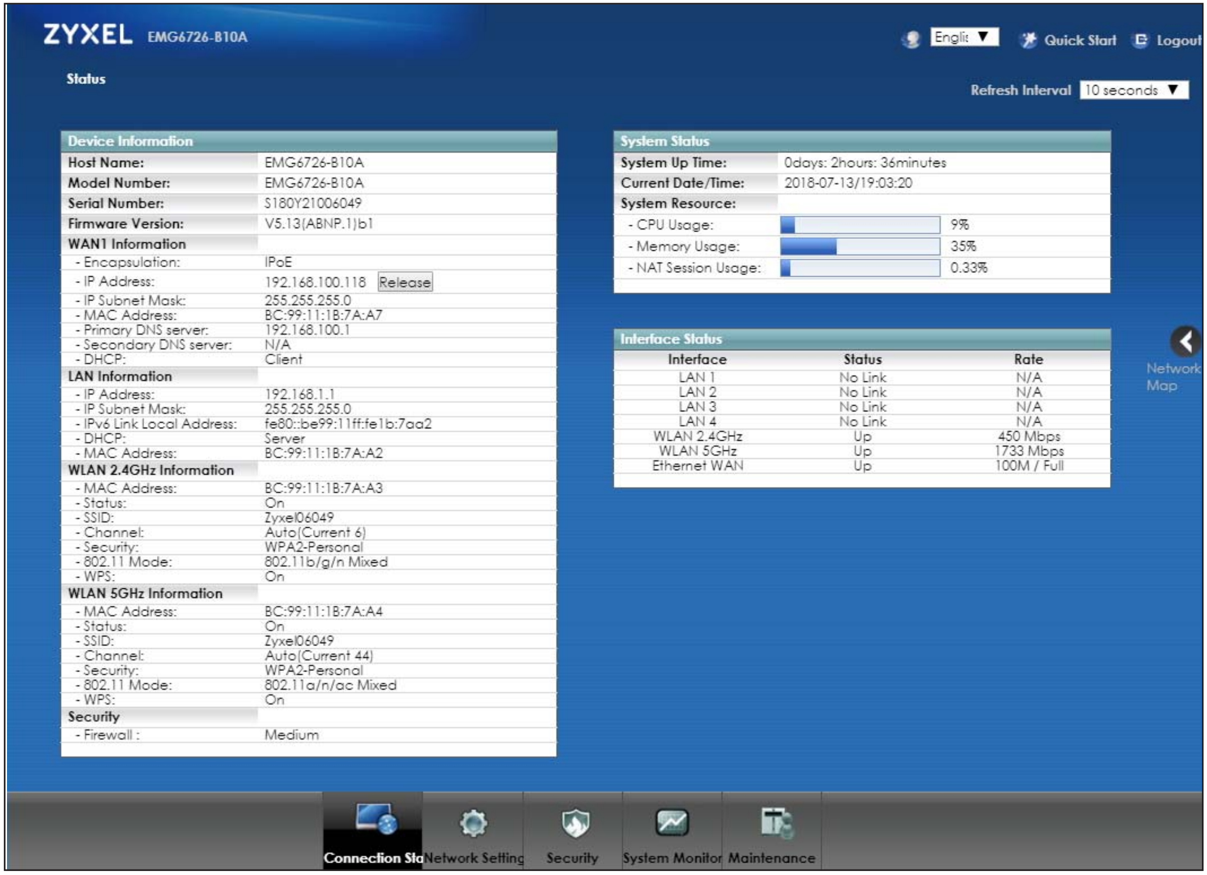
5.1 Overview

After you log into the Web Configurator, the **Status** screen appears. You can use the **Status** screen to look at the current status of the EMG, system resources, and interfaces (LAN, WAN, and WLAN).

5.2 The Status Screen

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

Figure 17 Status Screen



Refresh Interval: 10 seconds

Device Information	
Host Name:	EMG6726-B10A
Model Number:	EMG6726-B10A
Serial Number:	S180Y21006049
Firmware Version:	V5.13(ABNP.1)b1
WAN1 Information	
- Encapsulation:	IPoE
- IP Address:	192.168.100.118 Release
- IP Subnet Mask:	255.255.255.0
- MAC Address:	BC:99:11:1B:7A:A7
- Primary DNS server:	192.168.100.1
- Secondary DNS server:	N/A
- DHCP:	Client
LAN Information	
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- IPv6 Link Local Address:	fe80::be99:11ff:fe1b:7aa2
- DHCP:	Server
- MAC Address:	BC:99:11:1B:7A:A2
WLAN 2.4GHz Information	
- MAC Address:	BC:99:11:1B:7A:A3
- Status:	On
- SSID:	Zyxel06049
- Channel:	Auto(Current 6)
- Security:	WPA2-Personal
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	On
WLAN 5GHz Information	
- MAC Address:	BC:99:11:1B:7A:A4
- Status:	On
- SSID:	Zyxel06049
- Channel:	Auto(Current 44)
- Security:	WPA2-Personal
- 802.11 Mode:	802.11a/n/ac Mixed
- WPS:	On
Security	
- Firewall :	Medium

System Status	
System Up Time:	0days: 2hours: 36minutes
Current Date/Time:	2018-07-13/19:03:20
System Resource:	
- CPU Usage:	9%
- Memory Usage:	35%
- NAT Session Usage:	0.33%

Interface Status

Interface	Status	Rate
LAN 1	No Link	N/A
LAN 2	No Link	N/A
LAN 3	No Link	N/A
LAN 4	No Link	N/A
WLAN 2.4GHz	Up	450 Mbps
WLAN 5GHz	Up	1733 Mbps
Ethernet WAN	Up	100M / Full

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. Click **Release** to release the current IP address settings. Click **Renew** to obtain an IP address from the ISP.
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.
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.

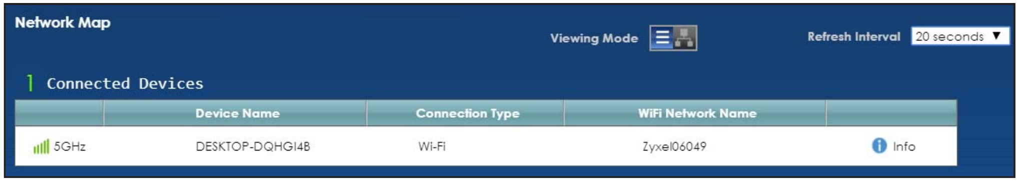
Table 6   Status Screen (continued)

LABEL	DESCRIPTION
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 10 on page 121).
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 35.2 on page 225, 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	
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.

5.3 The Network Map Screen

Use this screen to view the network connection status of the device and its clients in a list. You can configure how often you want the EMG to update this screen in **Refresh interval**.

Figure 18   Network Map: List View Mode



Network Map

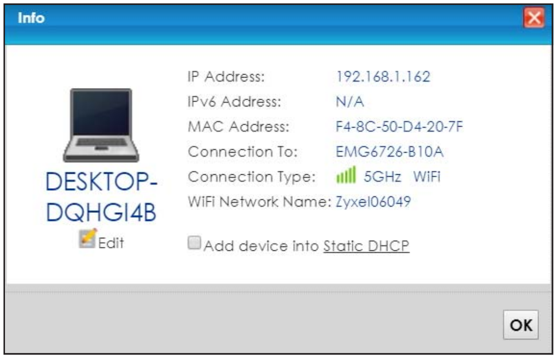
Viewing Mode

Refresh Interval: 20 seconds

Connected Devices

	Device Name	Connection Type	WiFi Network Name	
5GHz	DESKTOP-DQHGI4B	Wi-Fi	Zyxel06049	Info

If you want to view information about a client, click **Info** of the entry and the following screen displays.



Info

DESKTOP-DQHGI4B

Edit

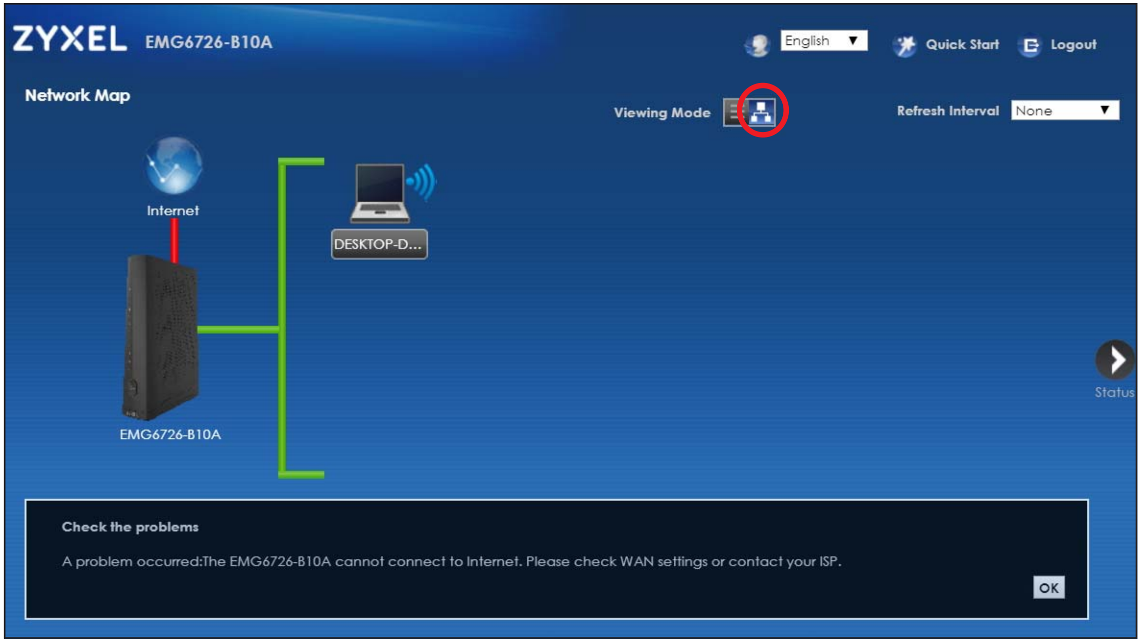
IP Address: 192.168.1.162
IPv6 Address: N/A
MAC Address: F4-8C-50-D4-20-7F
Connection To: EMG6726-B10A
Connection Type: 5GHz WiFi
WiFi Network Name: Zyxel06049

□ Add device into Static DHCP

OK

If you prefer to view the layout of the device and its client icons, click **Icon View** in the **Viewing Mode** selection box. A warning message appears if there is a connection problem.

Figure 19 Network Map: Icon View Mode

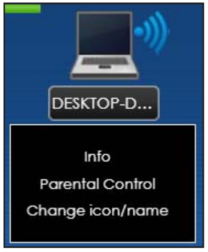


Check the problems

A problem occurred:The EMG6726-B10A cannot connect to Internet. Please check WAN settings or contact your ISP.

OK

If you want to view information about a client in this icon mode, click the client's name and **Info**. If you want to change the name or icon of the client, click **Change icon/name**.



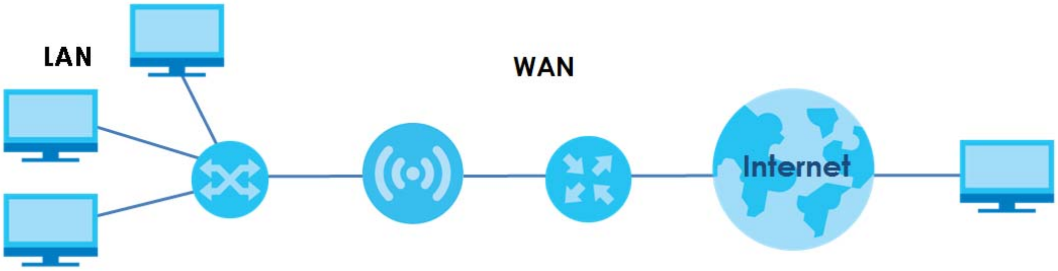
CHAPTER 6 Broadband

6.1 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 20 LAN and WAN



6.1.1 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 6.2 on page 65).

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

6.1.2 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

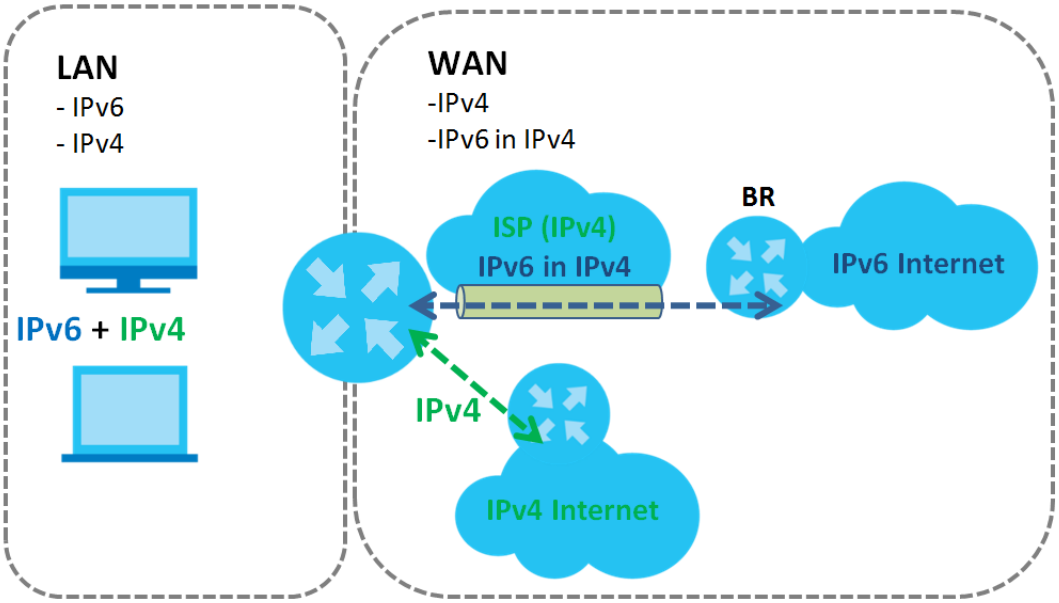
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, 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 21 IPv6 Rapid Deployment

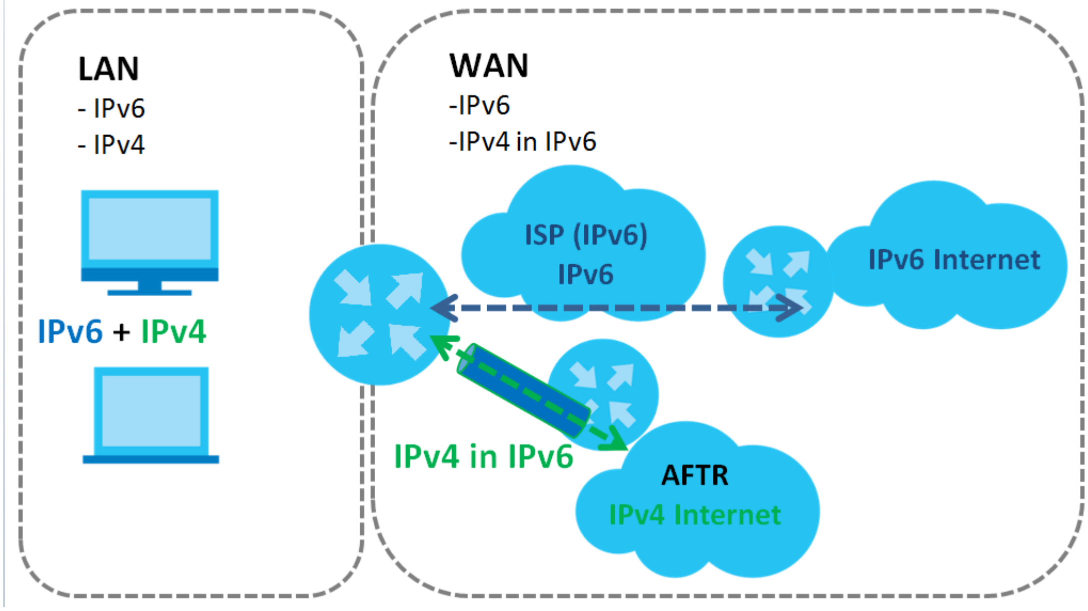


Dual Stack Lite

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 22 Dual Stack Lite



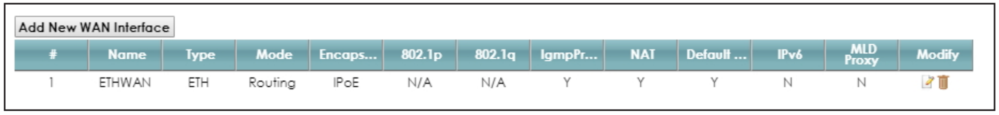
6.1.3 Before You Begin

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

6.2 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 23 Network Setting > Broadband



Add New WAN Interface

#	Name	Type	Mode	Encaps...	802.1p	802.1q	IgmpPr...	NAT	Default ...	IPv6	MLD Proxy	Modify
1	ETHWAN	ETH	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	📝🗑

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 it is an Ethernet connection.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.
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.

Table 8 Network Setting > Broadband (continued)

LABEL	DESCRIPTION
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.

6.2.1 Add/Edit Internet Connection

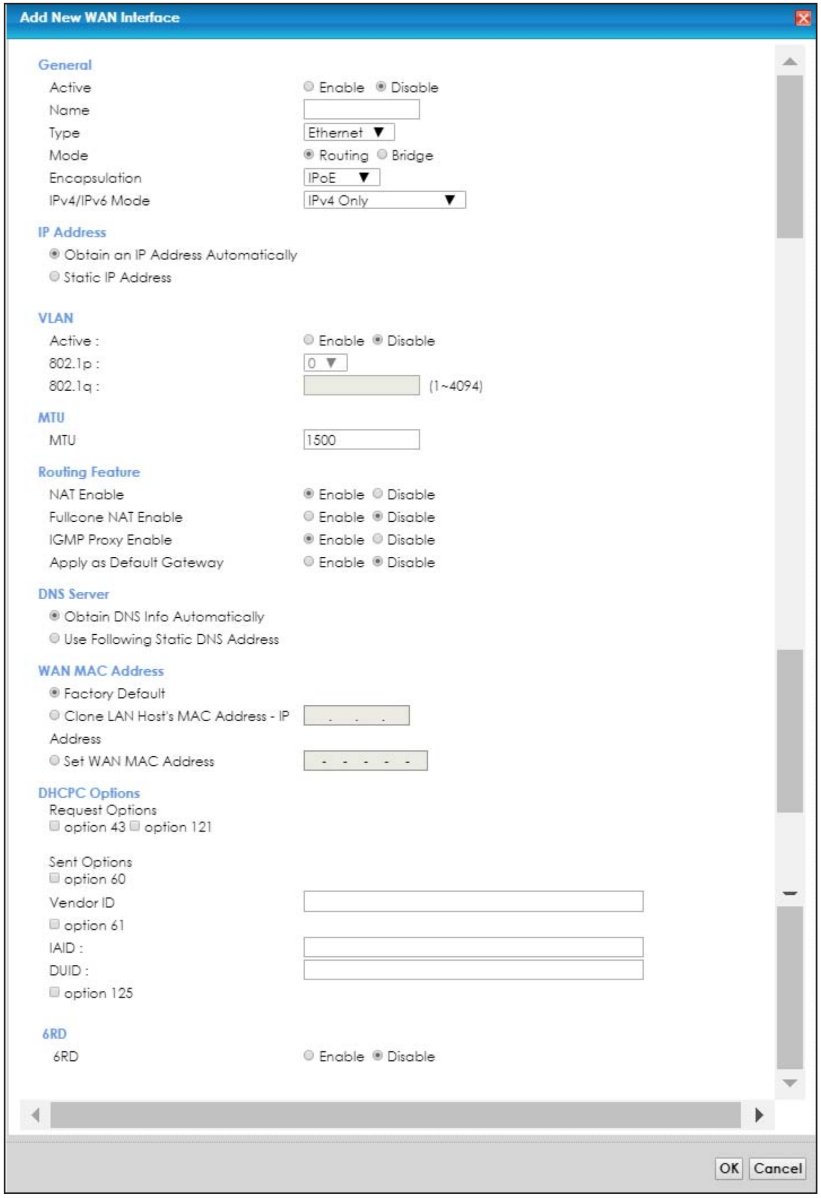
Click **Add New WAN Interface** in the **Broadband** screen or the **Edit** icon next to an existing WAN interface to configure a WAN connection. The screen varies depending on the interface type, mode, encapsulation, and IPv6/IPv4 mode you select.

6.2.1.1 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 24 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode)



Add New WAN Interface

General

Active ○ Enable ● Disable

Name

Type Ethernet

Mode ● Routing ○ Bridge

Encapsulation IPoE

IPv4/IPv6 Mode IPv4 Only

IP Address

● Obtain an IP Address Automatically

○ Static IP Address

VLAN

Active : ○ Enable ● Disable

802.1p : 0

802.1q : (1~4094)

MTU

MTU 1500

Routing Feature

NAT Enable ● Enable ○ Disable

Fullcone NAT Enable ○ Enable ● Disable

IGMP Proxy Enable ● Enable ○ Disable

Apply as Default Gateway ○ Enable ● Disable

DNS Server

● Obtain DNS Info Automatically

○ Use Following Static DNS Address

WAN MAC Address

● Factory Default

○ Clone LAN Host's MAC Address - IP Address . . .

○ Set WAN MAC Address - - - - -

DHCPC Options

Request Options

□ option 43 □ option 121

Sent Options

□ option 60

Vendor ID

□ option 61

IAID :

DUID :

□ option 125

6RD

6RD ○ Enable ● Disable

The following table describes the labels in this screen.

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

LABEL	DESCRIPTION
General	
Active	Select **Enable** to activate this WAN interface.
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**.

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

LABEL	DESCRIPTION
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.
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 **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 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 **Enable** to activate NAT on this connection.

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

LABEL	DESCRIPTION
Fullcone NAT Enable	Select **Enable** 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.
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 **Enable** 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 **Enable** 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.
WAN MAC Address You can see the default MAC address on the EMG's bottom label. This is also the MAC address the EMG reports to the ACS (Auto Configuration Server) server.	
Factory Default	Select this option to have the EMG use the default MAC address for the WAN interface that came along with this EMG when it was produced.
Clone LAN Host's MAC Address - IP Address	Select this option and enter a LAN host's MAC address this WAN interface will use. In this way, the WAN interface pretends to be that LAN host to the ISP.
Set WAN MAC Address	Select this option and enter a MAC address that you want the WAN interface to use.
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 64 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 64 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**.

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

LABEL	DESCRIPTION
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 **IPoE** for the encapsulation and **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.
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.

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

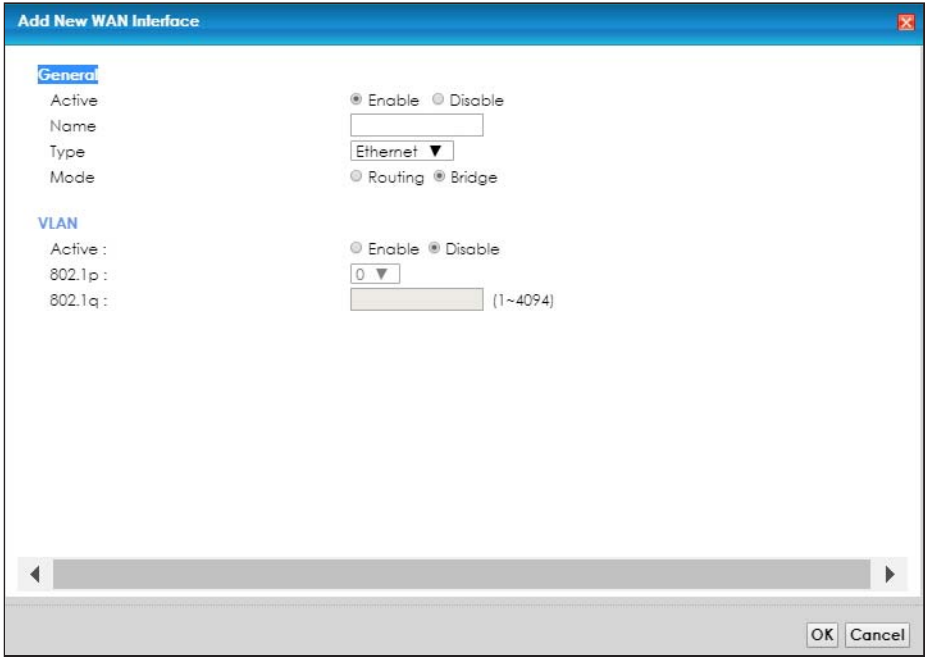
LABEL	DESCRIPTION
Primary DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.
OK	Click **OK** to save your changes back to the EMG.
Cancel	Click **Cancel** to exit this screen without saving.

6.2.1.2 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 25 Network Setting > Broadband > Add New WAN Interface/Edit (Ethernet-Bridge Mode)



Add New WAN Interface

General

Active: ● Enable ○ Disable

Name:

Type: Ethernet

Mode: ○ Routing ● Bridge

VLAN

Active : ○ Enable ● Disable

802.1p : 0

802.1q : (1~4094)

The following table describes the fields in this screen.

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

LABEL	DESCRIPTION
General	
Active	Select **Enable** to enable this WAN interface.
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	

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

LABEL	DESCRIPTION
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.

6.3 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.

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 7 Wireless

7.1 Overview

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

7.1.1 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 **WiFi** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode (Section 7.2 on page 76).
- Use the **Guest WiFi** screen to set up multiple wireless networks on your EMG (Section 7.3 on page 78).
- Use the **WPS** screen to add another WPS-enabled wireless device (within wireless range of the EMG) to the EMG's 2.4G or 5G wireless network(Section 7.4 on page 80).
- Use the **Advanced** screen to configure advanced settings for the EMG's 2.4G and 5G wireless network (Section 7.5 on page 80).
- Use the **Channel Status** screen to scan the number of devices which are using 2.4G and/or 5G wireless channels and view the results (Section 7.6 on page 83).
- Use the **MESH** screen to enable or disable wireless roaming between the EMG and an wireless AP extender device (Section 7.7 on page 85).

7.1.2 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

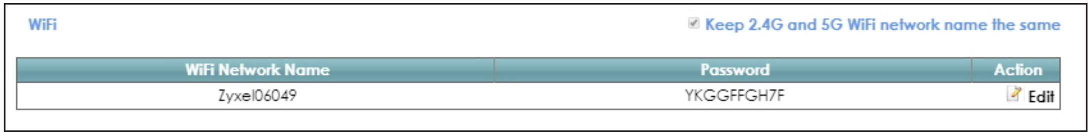
See Section 7.8 on page 87 for advanced technical information on wireless networks.

7.2 The WiFi Screen

Use this screen to view the wireless network name and password. You can also click the **Edit** icon to configure the settings.

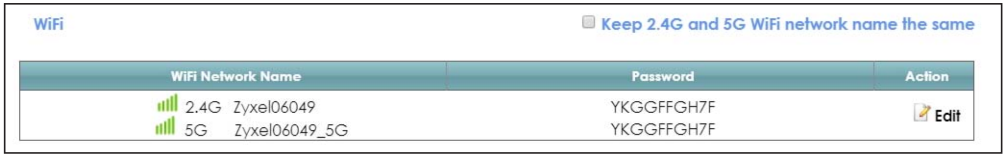
Click **Network Setting** > **Wireless** to open the **WiFi** screen.

Figure 26 Network Setting > Wireless > WiFi



WiFi Network Name	Password	Action
Zyxel06049	YKGGFFGH7F	Edit

Figure 27 Network Setting > Wireless > WiFi (Without Keeping 2.4G and 5G WiFi Network Name The Same)



WiFi Network Name	Password	Action
2.4G Zyxel06049 5G Zyxel06049_5G	YKGGFFGH7F YKGGFFGH7F	Edit

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

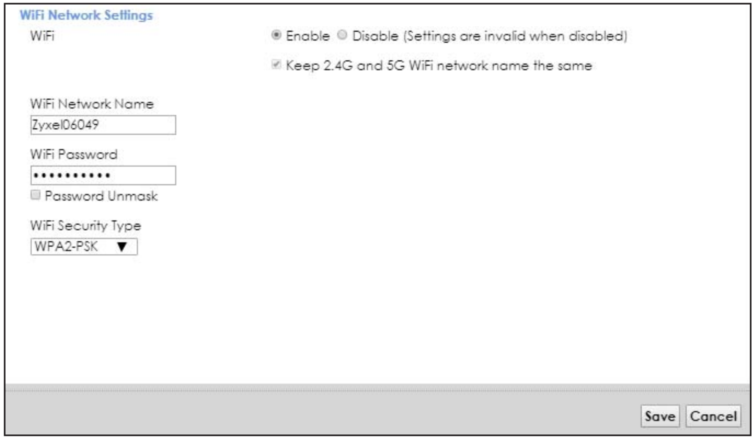
Table 11 Network Setting > Wireless > WiFi

LABEL	DESCRIPTION
Keep 2.4G and 5G WiFi network name the same	Select this if you want the EMG use the same wireless network name, password, and security type for both the 2.4GHz and 5GHz band networks. Clear this to have the screen display the corresponding information for the 2.4GHz and 5GHz band networks. 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. Note: This setting is configurable only when the MESH function is disabled in the **Network Setting > Wireless > MESH** screen.
WiFi Network Name	This is the wireless network name.
Password	This is the password of the wireless network.
Action	Click the **Edit** icon to configure the wireless network settings.

7.2.1 The WiFi Edit Screen

Use this screen to view and configure the wireless network name, password and security type. Click the **Edit** icon on the **Network Setting** > **Wireless** > **WiFi** screen to open the **WiFi Edit** screen.

Figure 28 Network Setting > Wireless > WiFi > Edit



WiFi Network Settings

WiFi ● Enable ○ Disable (Settings are invalid when disabled)

☑ Keep 2.4G and 5G WiFi network name the same

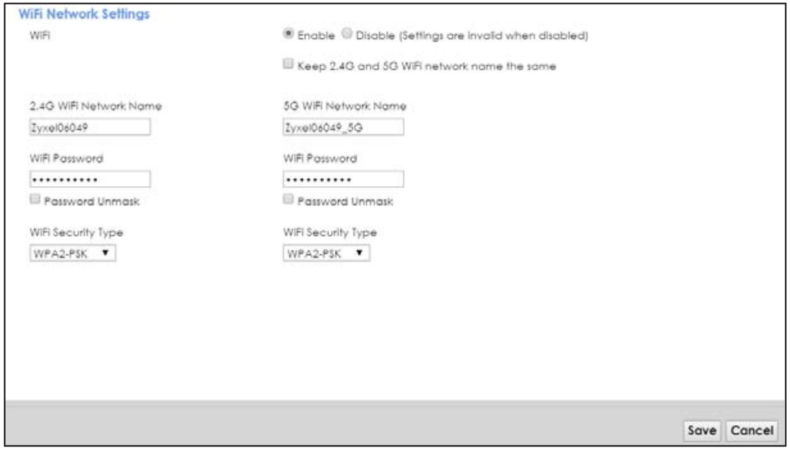
WiFi Network Name: Zyxel06049

WiFi Password: ••••••••••

□ Password Unmask

WiFi Security Type: WPA2-PSK ▼

Figure 29 Network Setting > Wireless > WiFi > Edit (Without Keeping 2.4G and 5G WiFi Network Name The Same)



WiFi Network Settings

WiFi ● Enable ○ Disable (Settings are invalid when disabled)

□ Keep 2.4G and 5G WiFi network name the same

2.4G WiFi Network Name: Zyxel06049

WiFi Password: ••••••••••

□ Password Unmask

WiFi Security Type: WPA2-PSK ▼

5G WiFi Network Name: Zyxel06049_5G

WiFi Password: ••••••••••

□ Password Unmask

WiFi Security Type: WPA2-PSK ▼

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

Table 12 Network Setting > Wireless > WiFi > Edit

LABEL	DESCRIPTION
WiFi	You can **Enable** or **Disable** the wireless LAN in this field.
Keep 2.4G and 5G WiFi network name the same	Select this if you want the EMG use the same wireless network name, password, and security type for both the 2.4G and 5G networks. Clear this to have the screen display the corresponding information for the 2.4GHz and 5GHz band networks. Note: This setting is configurable only when the MESH function is disabled in the **Network Setting > Wireless > MESH** screen.
WiFi Network Name	This is the wireless network name.
WiFi Password	This is the password of the wireless network. Select **Password Unmask** to display the entered password in plain text. Clear it to hide the password to avoid shoulder surfing.

Table 12 Network Setting > Wireless > WiFi > Edit (continued)

LABEL	DESCRIPTION
WiFi Security Type	Select **WPA2-PSK** to add security on this wireless network. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers wireless clients a better and secure connection. The wireless clients which want to associate to this network must have same wireless security settings as the EMG. Or you can select **No Security** to allow any client to associate this network and the guest wireless network of the same wireless band (see Section 7.3) without any data encryption or authentication.
Save	Click **Save** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

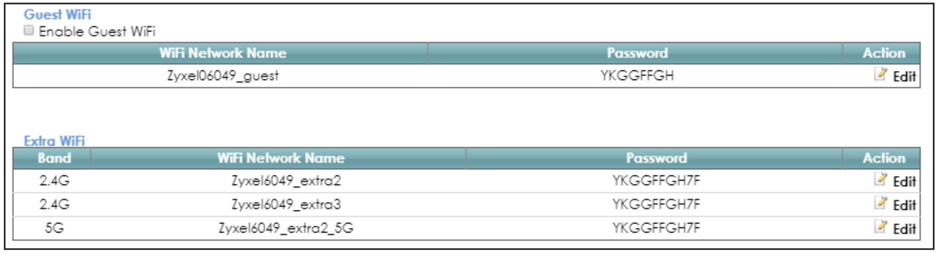
7.3 The Guest WiFi Screen

This screen allows you to enable and configure multiple wireless networks for guests on the EMG.

You can view/configure one guest WiFi network and three extra WiFi networks on this screen. The extra WiFi networks include two extra 2.4GHz WiFi networks and one extra 5GHz WiFi network. The only difference between guest WiFi and extra WiFi is that you can configure the number of hours to keep the guest WiFi network on before the EMG turns it off.

Click **Network Setting** > **Wireless** > **Guest WiFi**. The following screen displays.

Figure 30 Network Setting > Wireless > Guest WiFi



Guest WiFi

□ Enable Guest WiFi

WiFi Network Name	Password	Action
Zyxel06049_guest	YKGGFFGH	Edit

Extra WiFi

Band	WiFi Network Name	Password	Action
2.4G	Zyxel6049_extra2	YKGGFFGH7F	Edit
2.4G	Zyxel6049_extra3	YKGGFFGH7F	Edit
5G	Zyxel6049_extra2_5G	YKGGFFGH7F	Edit

The following table describes the labels in this screen.

Table 13 Network Setting > Wireless > Guest WiFi

LABEL	DESCRIPTION
Guest WiFi	
Enable Guest WiFi	Select this to enable the guest wireless network.
WiFi Network Name	This field displays the guest WiFi network name.
Password	This field displays the password used to connect to this guest wireless network.
Action	Click the **Edit** icon to configure the WiFi network profile.
Extra WiFi	
Band	This field indicates whether this extra WiFi network uses 2.4GHz or 5GHz band.
WiFi Network Name	This field displays the extra WiFi network name.

Table 13 Network Setting > Wireless > Guest WiFi (continued)

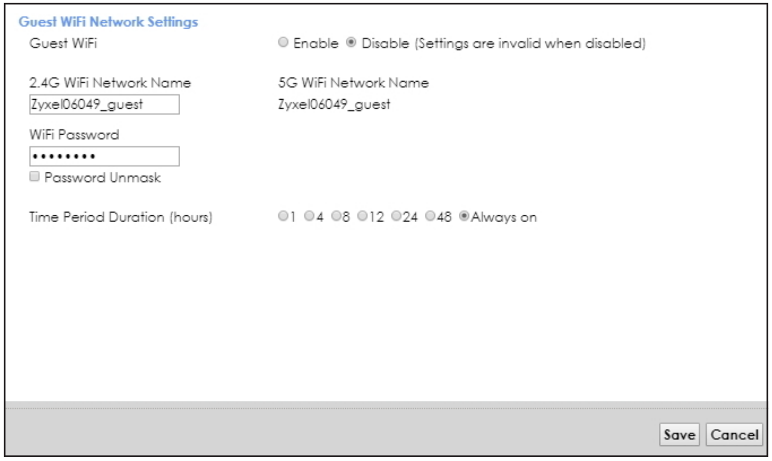
LABEL	DESCRIPTION
Password	This field displays the password used to connect to this extra wireless network.
Action	Click the **Edit** icon to configure the WiFi network profile.

7.3.1 Edit Guest WiFi

Use this screen to edit a guest WiFi or an extra WiFi settings. Click an **Edit** icon in the **Guest WiFi** screen. The following screen displays.

Note: Guest WiFi and Extra WiFi share the same security type with the main WiFi network setting configured in the **Network Setting > Wireless > WiFi > Edit** screen.

Figure 31 Network Setting > Wireless > Guest WiFi > Edit (For Guest WiFi)



Guest WiFi Network Settings

Guest WiFi ○ Enable ● Disable (Settings are invalid when disabled)

2.4G WiFi Network Name: Zyxel06049_guest

5G WiFi Network Name: Zyxel06049_guest

WiFi Password: •••••••••

□ Password Unmask

Time Period Duration (hours) ○1 ○4 ○8 ○12 ○24 ○48 ●Always on

The following table describes the fields in this screen.

Table 14 Network Setting > Wireless > Guest WiFi > Edit

LABEL	DESCRIPTION
Guest WiFi	You can **Enable** or **Disable** the wireless LAN in this field.
2.4G/5G WiFi Network Name	Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
WiFi Password	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.
Time Period Duration (hours)	This field is only available when you are editing for the guest WiFi network, rather than for an extra WiFi network. Select the number of hours that you want to keep this wireless network on right after you apply the setting. The EMG automatically turns it off when time is up. Select **Always on** to have the EMG never turn the wireless network off.
Save	Click **Save** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

7.4 The WPS Screen

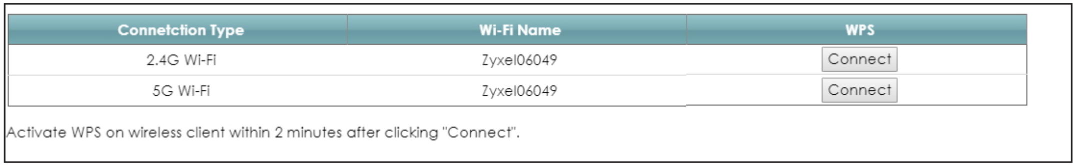
Use this screen to use the WiFi Protected Setup (WPS) function on your EMG.

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 7.8.8.2 on page 93 for more information about WPS.

Note: The EMG applies the security settings of the main 2.4G or 5G wireless profile (see Section 7.2.1 on page 76). If you want to use the WPS feature, make sure you have enabled **WPS** in the **Network Setting** > **Wireless** > **Advanced** screen.

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

Figure 32 Network Setting > Wireless > WPS



Connetction Type	Wi-Fi Name	WPS
2.4G Wi-Fi	Zyxel06049	Connect
5G Wi-Fi	Zyxel06049	Connect

Activate WPS on wireless client within 2 minutes after clicking "Connect".

The following table describes the labels in this screen.

Table 15 Network Setting > Wireless > WPS

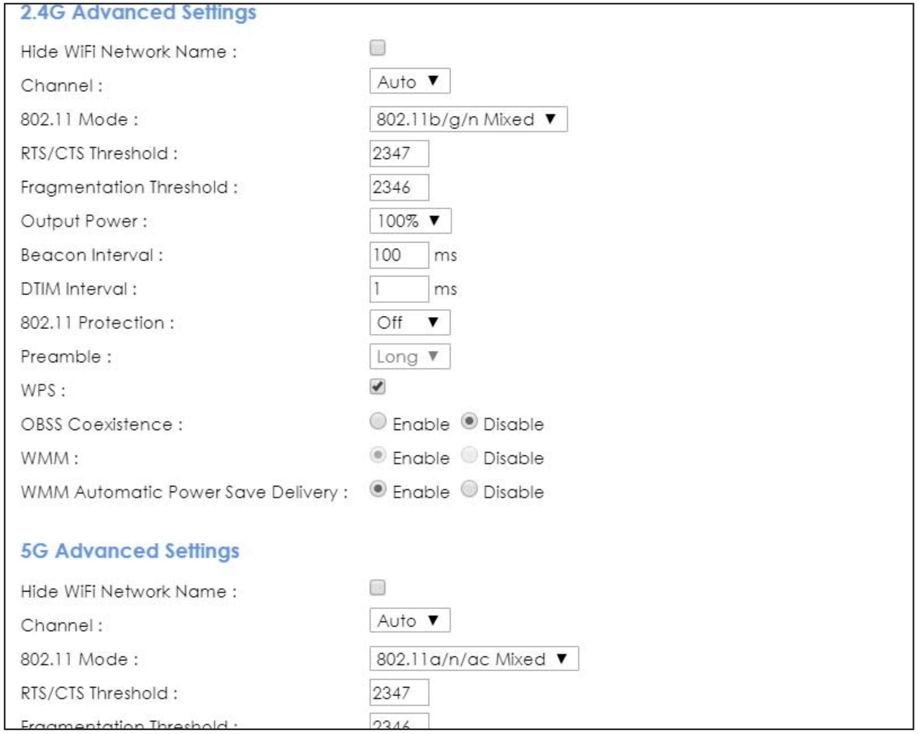
LABEL	DESCRIPTION
Connection Type	This field indicates whether you will apply WPS to the 2.4G or 5G wireless network.
Wi-Fi Name	This field displays the wireless network name.
WPS	Click the **Connect** button to add another WPS-enabled wireless device (within wireless range of the EMG) to the wireless 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.

7.5 The Advanced Screen

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

See Section 7.8.2 on page 89 for detailed definitions of the terms listed in this screen.

Figure 33 Network Setting > Wireless > Advanced



2.4G Advanced Settings

Hide WiFi Network Name :	□
Channel :	Auto ▼
802.11 Mode :	802.11b/g/n Mixed ▼
RTS/CTS Threshold :	2347
Fragmentation Threshold :	2346
Output Power :	100% ▼
Beacon Interval :	100 ms
DTIM Interval :	1 ms
802.11 Protection :	Off ▼
Preamble :	Long ▼
WPS :	☑
OBSS Coexistence :	○ Enable ● Disable
WMM :	● Enable ○ Disable
WMM Automatic Power Save Delivery :	● Enable ○ Disable

5G Advanced Settings

Hide WiFi Network Name :	□
Channel :	Auto ▼
802.11 Mode :	802.11a/n/ac Mixed ▼
RTS/CTS Threshold :	2347
Fragmentation Threshold :	2346

The following table describes the labels in this screen.

Table 16 Network Setting > Wireless > Advanced

LABEL	DESCRIPTION
2.4G Advanced Settings / 5G Advanced Settings	
Hide WiFi Network Name	Select this check box to hide the wireless band's network name (SSID) in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool or any wireless clients. Note: This setting only applies to the main 2.4G and 5G wireless networks. It does not apply to the guest and extra wireless networks configured in the **Network Setting > Wireless > Guest WiFi** screen.
Channel	Select a specific channel the EMG uses for the wireless band. Select **Auto** to have the EMG automatically determine a channel to use.
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.
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.

Table 16 Network Setting > Wireless > Advanced (continued)

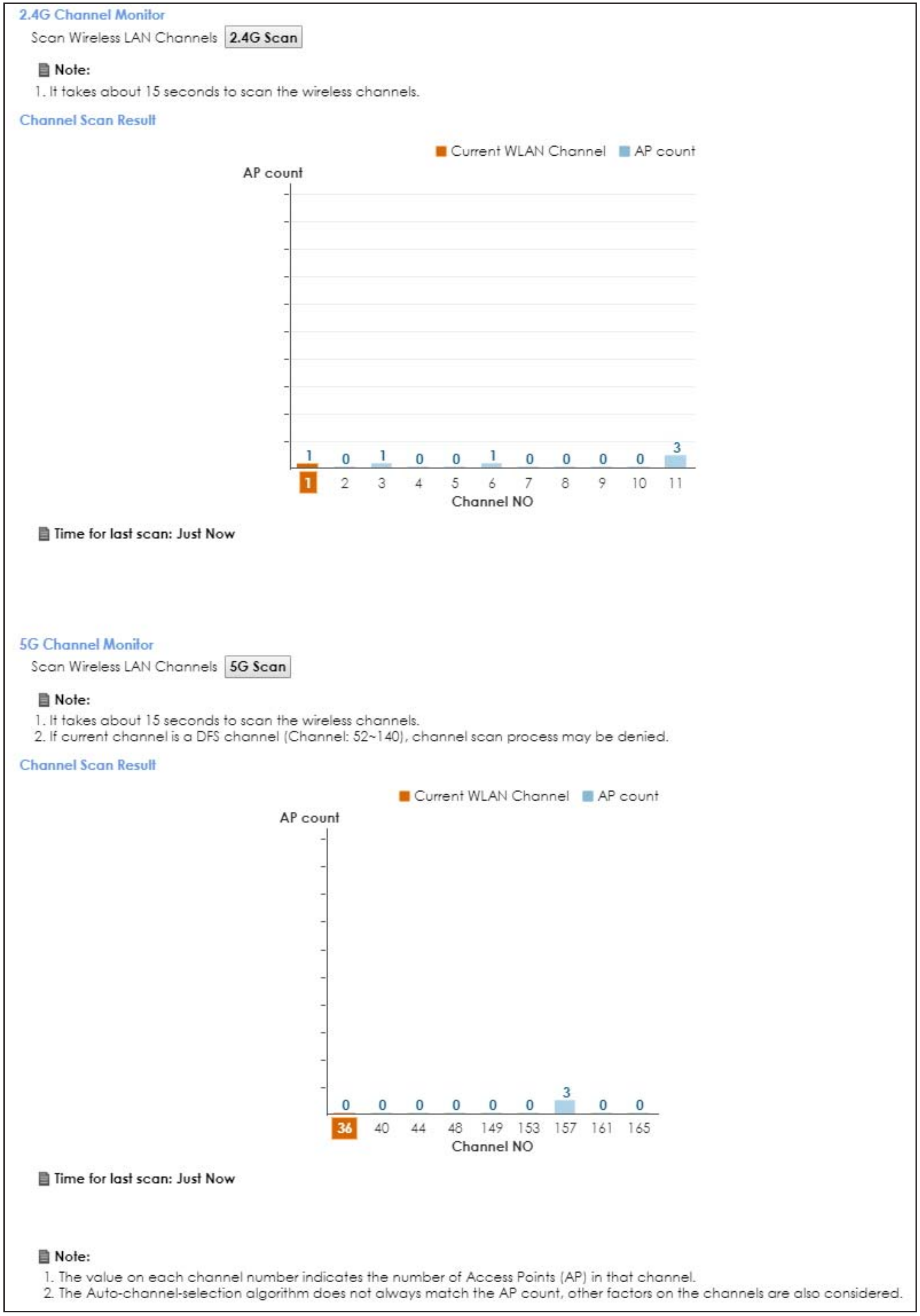
LABEL	DESCRIPTION
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Output Power	Set the output power of the EMG. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one 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 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 7.8.7 on page 92 for more information. This field is configurable only when you set 802.11 Mode to **802.11b**.
WPS	Select this to enable WPS function for the wireless network. Note: This setting only applies to the main 2.4G and 5G wireless networks. It does not apply to the guest and extra wireless networks configured in the **Network Setting > Wireless > Guest WiFi** screen. Note: This setting is configurable only when the MESH function is disabled in the **Network Setting > Wireless > MESH** screen.
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.
WMM	Select **Enable** to have the EMG automatically give the wireless network 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. Note: At the time of writing, WMM is enabled by default and it is not changeable.
WMM Automatic Power Save Delivery	Select **Enable** 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.

7.6 The Channel Status Screen

Use the **Channel Status** screen to scan the number of devices which are using 2.4G and/or 5G wireless LAN channels and view the results. Click **Network Setting > Wireless > Channel Status**. The screen appears as shown. Click **2.4G Scan** and/or **5G Scan** to scan the 2.4GHz and/or 5GHz wireless band channels. You can view the results in the corresponding **Channel Scan Result** section.

Note: The **2.4G Scan** or **5G 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 34 Network Setting > Wireless > Channel Status



2.4G Channel Monitor

Scan Wireless LAN Channels **2.4G Scan**

Note:

1. It takes about 15 seconds to scan the wireless channels.

Channel Scan Result

Time for last scan: Just Now

5G Channel Monitor

Scan Wireless LAN Channels **5G Scan**

Note:

1. It takes about 15 seconds to scan the wireless channels.
2. If current channel is a DFS channel (Channel: 52~140), channel scan process may be denied.

Channel Scan Result

Time for last scan: Just Now

Note:

1. The value on each channel number indicates the number of Access Points (AP) in that channel.
2. The Auto-channel-selection algorithm does not always match the AP count, other factors on the channels are also considered.

7.7 The MESH Screen

Use this screen to enable or disable Zyxel MESH (Multy Pro). It supports AP steering and Band steering. AP steering allows wireless clients to roam seamlessly between Multy-Pro-supported devices in your MESH network by using the same SSID and WiFi password. Also, AP steering helps monitor wireless clients and drop their connections to optimize the EMG bandwidth when the clients are idle or have a low signal.

When a wireless client is dropped, it has the opportunity to steer to a Multy-Pro-supported device with a strong signal. Band steering allows dual band wireless clients to steer from one band to another.

A MESH network consists of a controller, the EMG, and a maximum of three Multy-Pro-supported extenders.

When Multy Pro is enabled:

• One Connect will be enabled and grayed out automatically. It's used for the communication between the EMG and a Multy-Pro-supported extenders for the setup of a MESH network.

• The SSID and WiFi password of the main 2.4GHz wireless network will be copied to the main 5GHz wireless network.

See the steps below on how to set up a MESH network with the EMG. The setup could take you 30 minutes.

Configurations on a Multy-Pro-Supported Extender(s)

1 Prepare a Multy-Pro-supported extender(s) from Zyxel.

The following table lists the Multy-Pro-supported extenders from Zyxel at the time of writing.

Table 17 Multy-Pro-Supported Extenders from Zyxel

MODELS
WAP6804
WAP6906
WAP7205

2 If the Multy-Pro-supported extender is in repeater mode, enable the wireless LAN. See your Multy-Prosupported extender's UG for how to enable the wireless LAN.

3 If the Multy-Pro-supported extender is in AP mode, connect it to the EMG using an Ethernet cable.

4 Turn on the Multy-Pro-supported extender.

5 Enable Zyxel MESH in the Web Configurator. See your Multy-Pro-supported extender's UG for how to enable Zyxel MESH.

Configurations on the EMG

1 If the Multy-Pro-supported extender is in repeater mode, enable the wireless LAN. See Section 5.1.3 on page 74 or Section 1.4.4 on page 24 for more information on enabling the wireless LAN.

2 Enable Zyxel MESH in the **Network > Wireless > MESH** screen.

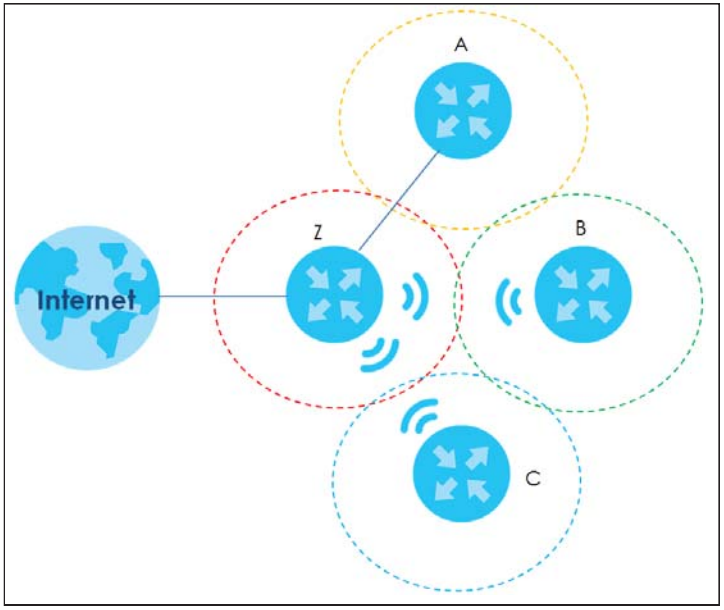
3 3 Press the **WPS** button for more than five seconds on the EMG.

Or

Click **Add Extender** in the Multy Pro App. Install from Google Play or the Apple App store.

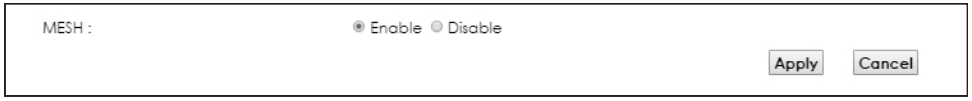
The following figure shows the Multy Pro application. Device Z is the EMG. Device A is a Multy-Prosupported extender in AP mode. Devices B and C are Multy-Pro-supported extenders in repeater Mode.

Figure 35 MESH Application



Click **Network > Wireless > MESH**. The following screen displays.

Figure 36 Network Setting > Wireless > MESH



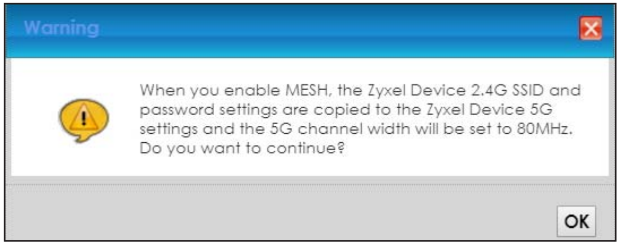
MESH : ● Enable ○ Disable

The following table describes the labels in this screen.

Table 18 Network Setting > Wireless > MESH

LABEL	DESCRIPTION
MESH	Select **Enable** to activate MESH and have the EMG apply the wireless name, password, and security type of the main 2.4G wireless network to the main 5G wireless network. A warning displays when you select **Enable** (see Figure 37 on page 87). Note: When MESH is enabled, the following settings become not configurable: • The **Keep 2.4G and 5G WiFi network name the same** setting in the **Network Setting > Wireless > WiFi** and **Network Setting > Wireless > WiFi > Edit** screens. • The **WPS** setting in the **Network Setting > Wireless > Advanced** screen. • The **ONE Connect** setting in the **Network Setting > Home Connectivity** screen.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

Figure 37 Network Setting > Wireless > MESH > A Warning When You Enable MESH



When you enable MESH, the Zyxel Device 2.4G SSID and password settings are copied to the Zyxel Device 5G settings and the 5G channel width will be set to 80MHz. Do you want to continue?

7.8 Technical Reference

This section discusses wireless LANs in depth. For more information, see Appendix B on page 245.

7.8.1 Wireless Network Overview

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

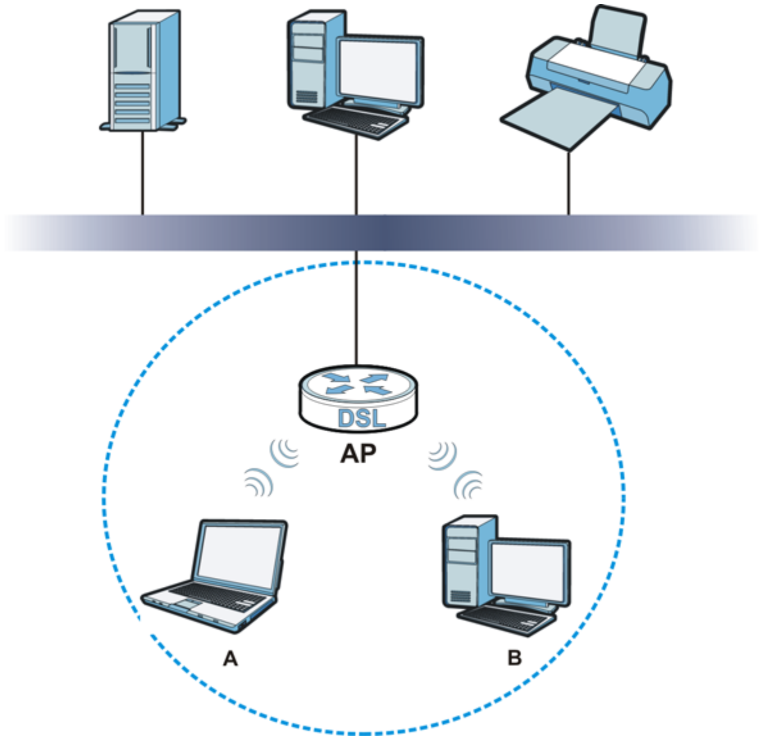
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, 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 38 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.

7.8.2 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.

7.8.3 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.

WPA2-PSK does two things. First, it authenticates. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, it encrypts. 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.

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.

7.8.3.1 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.

7.8.3.2 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.

7.8.3.3 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. 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.

7.8.3.4 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.

[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.

The types of encryption you can choose depend on the type of authentication. (See Section 7.8.3.3 on page 90 for information about this.)

Table 20 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION
Weakest	No Security
↕	
Strongest	WPA2-PSK

For example, If users do not log in to the wireless network, you can choose no encryption 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.

Note: It is recommended that wireless networks use **WPA2-PSK**.

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.

7.8.4 Signal Problems

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

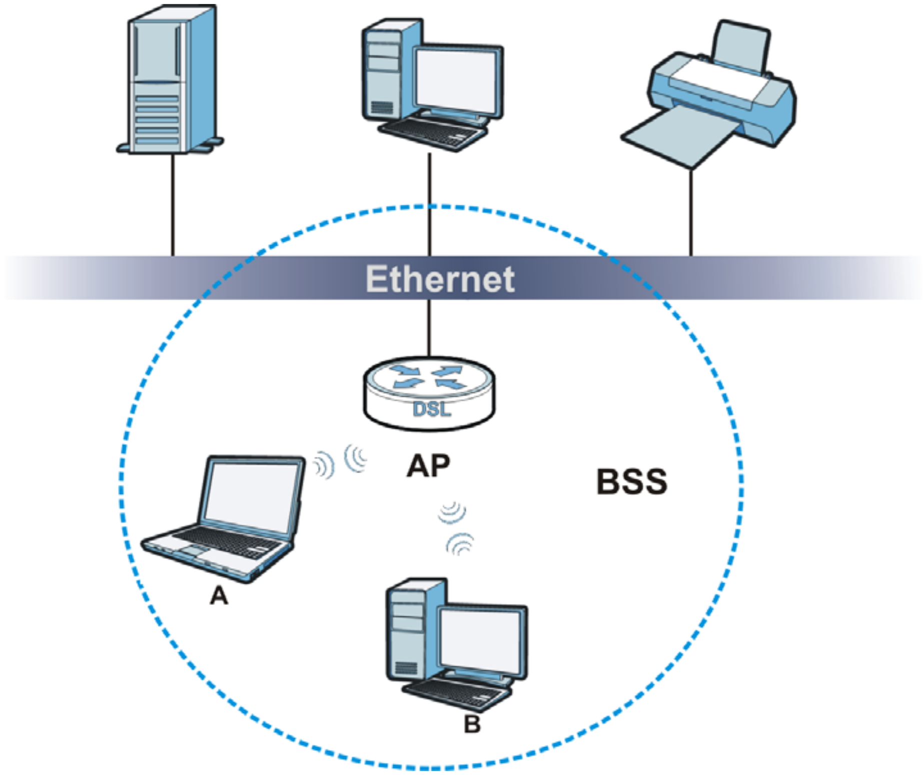
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters 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.

7.8.5 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 39 Basic Service set



7.8.6 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The EMG's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

7.8.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).

7.8.7 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.

7.8.8 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) 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.

7.8.8.1 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 7.5 on page 80).

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 three 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.

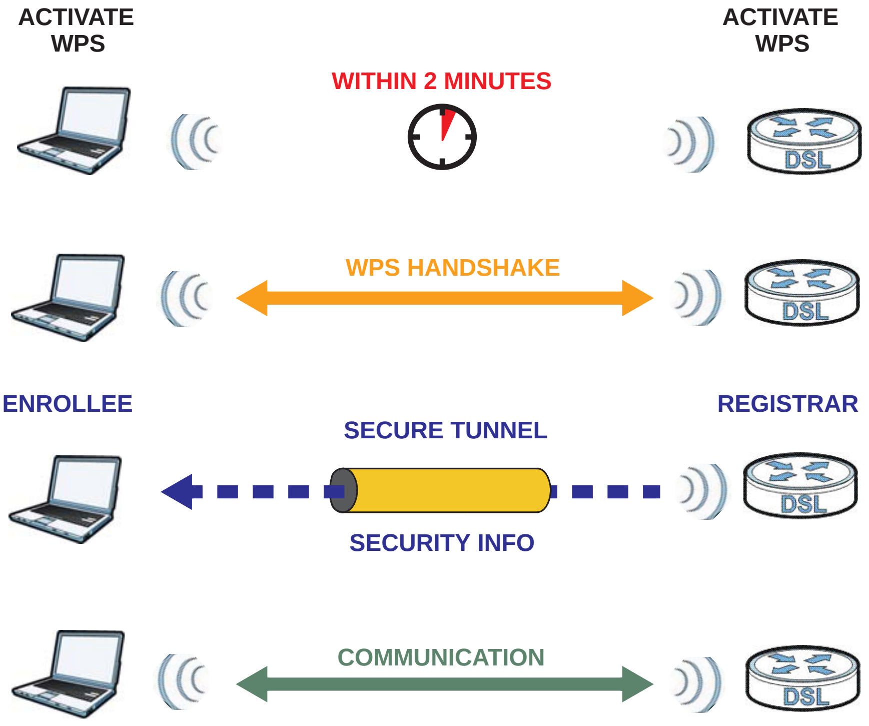
If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

7.8.8.2 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 WPA2-PSK pre-shared key to the enrollee. Whether 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 WPA2-PSK randomly.

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

Figure 40 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.

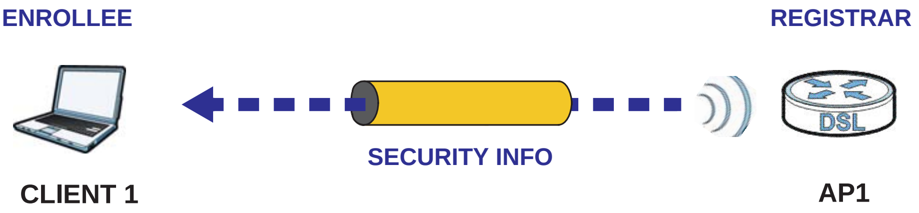
By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled 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.

7.8.8.3 Example WPS Network Setup

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

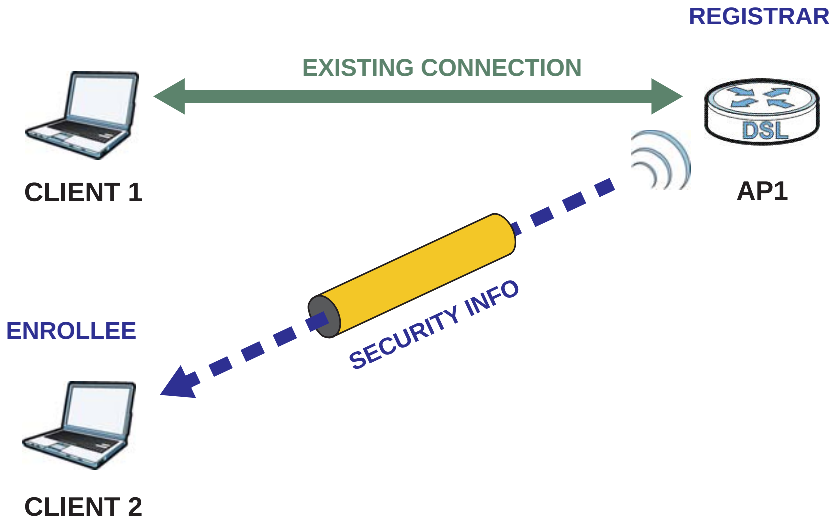
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information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

Figure 41 WPS: Example Network Step 1



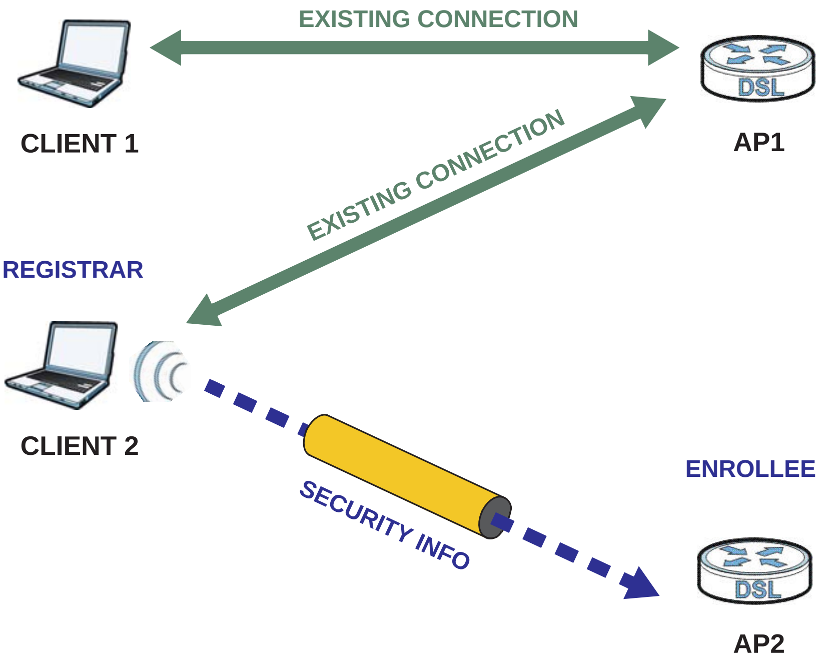
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the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

Figure 42 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 43 WPS: Example Network Step 3



7.8.8.4 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 WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses 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 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.

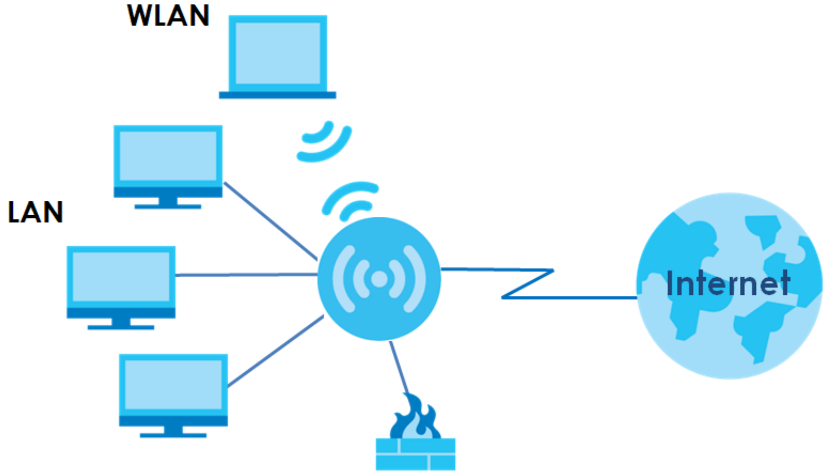
  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of 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 8
Home Networking

8.1 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.



8.1.1 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 8.2 on page 100).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 8.3 on page 104).
- Use the **UPnP** screen to enable UPnP and UPnP NAT traversal on the EMG (Section 8.4 on page 105).
- Use the **Additional Subnet** screen to configure IP alias and public static IP (Section 8.5 on page 108).
- 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 8.6 on page 109).
- Use the **Wake on LAN** screen to remotely turn on a device on the network. (Section 8.7 on page 109).
- Use the **TFTP Server Name** screen to set a TFTP server address which is passed to the clients using DHCP option 66. (Section 8.8 on page 110).

8.1.2 What You Need To Know

8.1.2.1 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.

8.1.2.2 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 11 on page 139 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 8.4.1 on page 106 for examples of installing and using UPnP.

Finding Out More

See Section 8.9 on page 110 for technical background information on LANs.

8.1.3 Before You Begin

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

8.2 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.

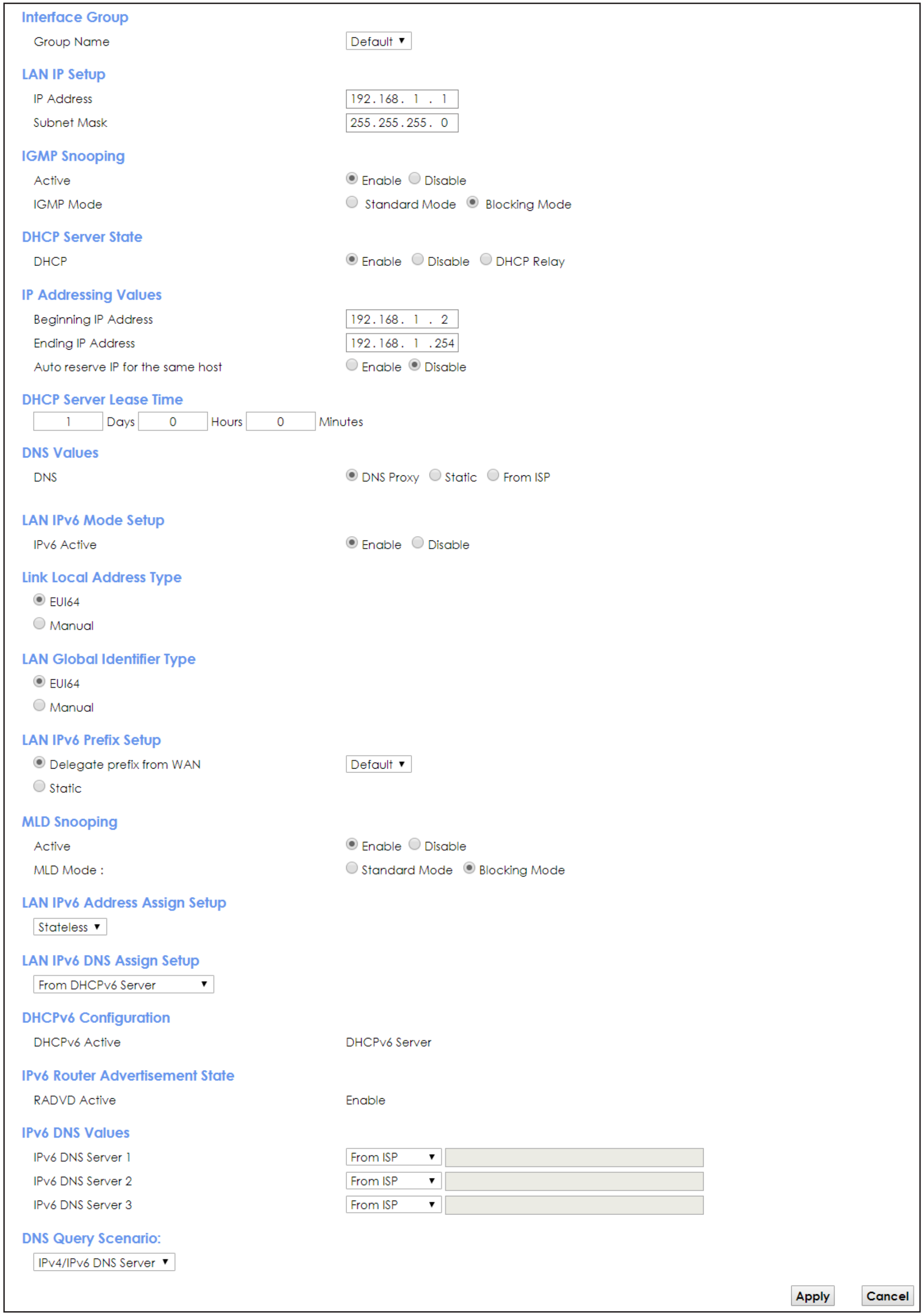
Follow these steps to configure your LAN settings.

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 44 Network Setting > Home Networking > LAN Setup



Interface Group

Group Name: Default ▾

LAN IP Setup

IP Address: 192.168. 1 . 1

Subnet Mask: 255.255.255. 0

IGMP Snooping

Active: ● Enable ○ Disable

IGMP Mode: ○ Standard Mode ● Blocking Mode

DHCP Server State

DHCP: ● Enable ○ Disable ○ DHCP Relay

IP Addressing Values

Beginning IP Address: 192.168. 1 . 2

Ending IP Address: 192.168. 1 .254

Auto reserve IP for the same host: ○ Enable ● Disable

DHCP Server Lease Time

1 Days 0 Hours 0 Minutes

DNS Values

DNS: ● DNS Proxy ○ Static ○ From ISP

LAN IPv6 Mode Setup

IPv6 Active: ● Enable ○ Disable

Link Local Address Type

● EUI64

○ Manual

LAN Global Identifier Type

● EUI64

○ Manual

LAN IPv6 Prefix Setup

● Delegate prefix from WAN: Default ▾

○ Static

MLD Snooping

Active: ● Enable ○ Disable

MLD Mode : ○ Standard Mode ● Blocking Mode

LAN IPv6 Address Assign Setup

Stateless ▾

LAN IPv6 DNS Assign Setup

From DHCPv6 Server ▾

DHCPv6 Configuration

DHCPv6 Active: DHCPv6 Server

IPv6 Router Advertisement State

RADVD Active: Enable

IPv6 DNS Values

IPv6 DNS Server 1: From ISP ▾

IPv6 DNS Server 2: From ISP ▾

IPv6 DNS Server 3: From ISP ▾

DNS Query Scenario:

IPv4/IPv6 DNS Server ▾

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 15 on page 165 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, 192.168.1.1 (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 forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select **Blocking Mode** to block all unknown multicast packets from the WAN.
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	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 forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select **Blocking Mode** to block all unknown multicast packets from the WAN.
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.

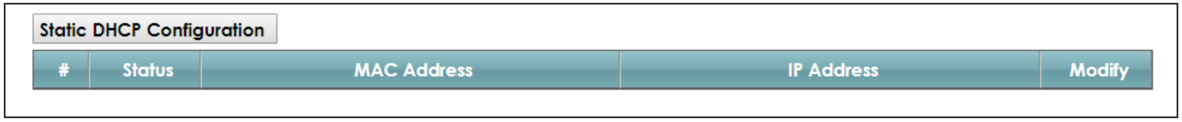
8.3 The Static DHCP Screen

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 45 Network Setting > Home Networking > Static DHCP



#	Status	MAC Address	IP Address	Modify

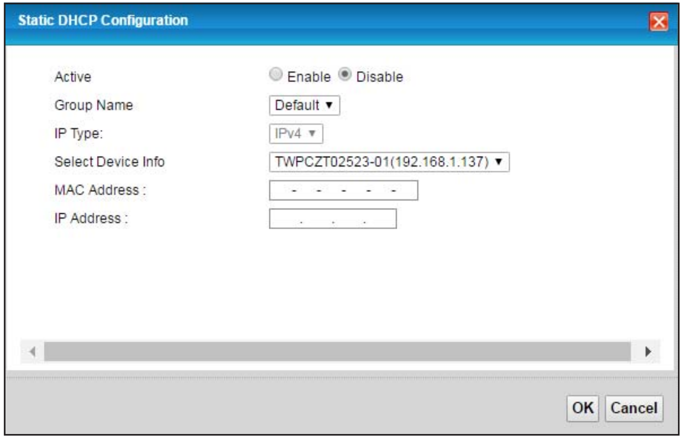
The following table describes the labels in this screen.

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 46 Static DHCP: Static DHCP Configuration/Edit



Static DHCP Configuration

Active ○ Enable ● Disable

Group Name Default ▾

IP Type: IPv4 ▾

Select Device Info TWPCZT02523-01(192.168.1.137) ▾

MAC Address : - - - - -

IP Address : . . .

The following table describes the labels in this screen.

Table 23 Static DHCP: Static DHCP Configuration/Edit

LABEL	DESCRIPTION
Active	Select this 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 15 on page 165 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.

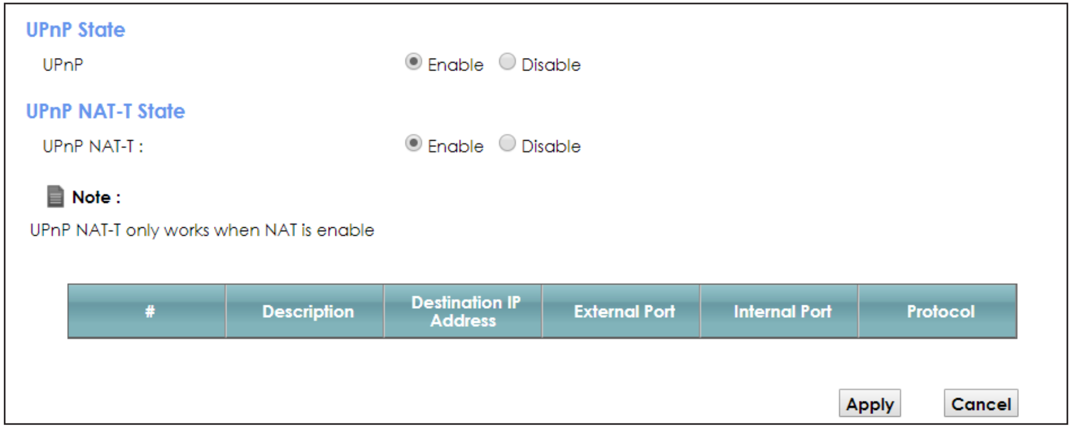
8.4 The UPnP Screen

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 99 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 47 Network Setting > Home Networking > UPnP



UPnP State

UPnP ● Enable ○ Disable

UPnP NAT-T State

UPnP NAT-T : ● Enable ○ Disable

Note :

UPnP NAT-T only works when NAT is enable

#	Description	Destination IP Address	External Port	Internal Port	Protocol

The following table describes the labels in this screen.

Table 24 Network Setting > Home Networking > UPnP

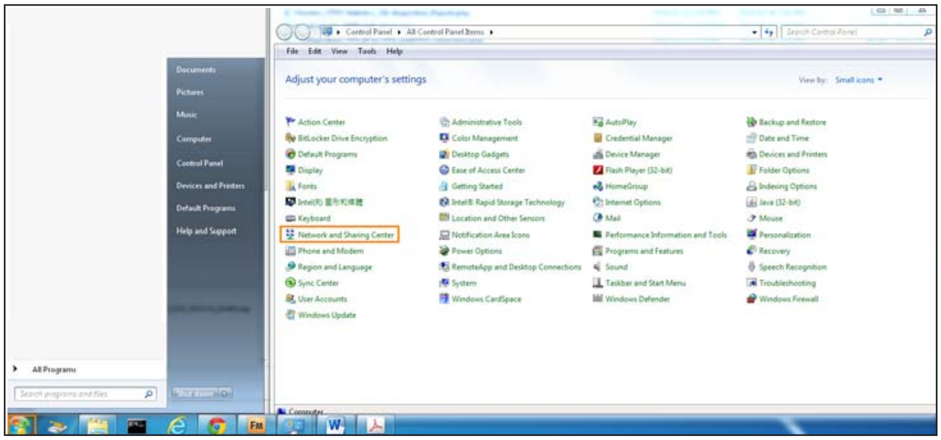
LABEL	DESCRIPTION
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the EMG's IP address (although you must still enter the password to access the web configurator).
UPnP NAT-T	Select **Enable** to allow 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.

8.4.1 Turning On UPnP in Windows 7 Example

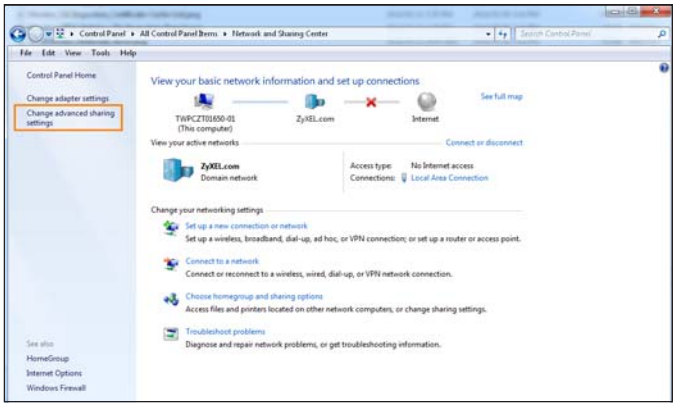
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the EMG.

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**.


Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
File Edit View Tools Help
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
HomeGroup
Internet Options
Windows Firewall
See full map
TWPCZT01650-01 (This computer)
ZyXEL.com
Internet
Connect or disconnect

View your basic network information and set up connections

View your active networks

ZyXEL.com
Domain network

Access type: No Internet access
Connections: Local Area Connection

Change your networking settings

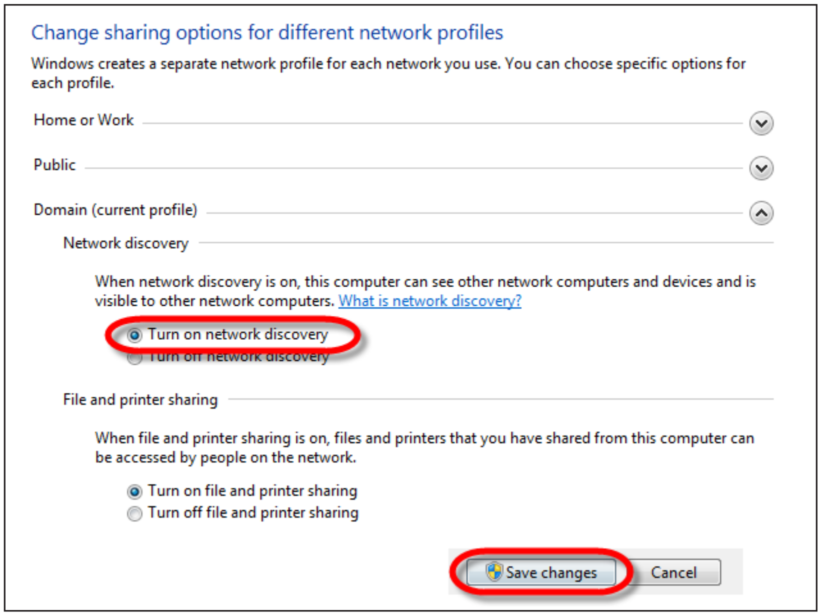
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

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.



Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Home or Work

Public

Domain (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

● Turn on network discovery
○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing
○ Turn off file and printer sharing

8.5 The Additional Subnet Screen

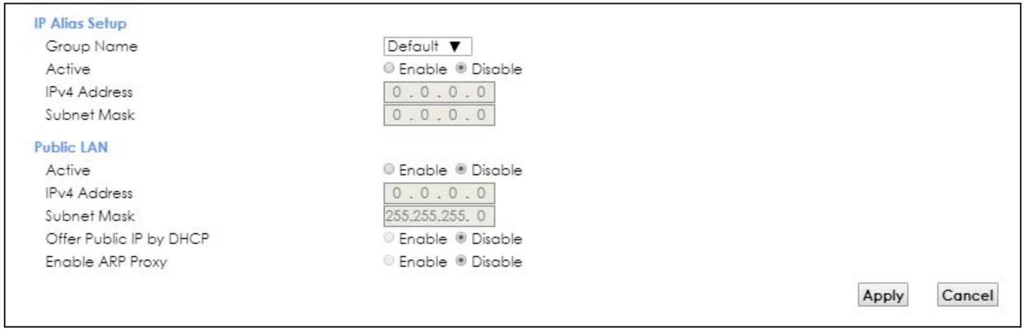
Use the **Additional Subnet** screen to configure IP alias and public static IP.

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 48 Network Setting > Home Networking > Additional Subnet



IP Alias Setup

Group Name: Default ▼

Active: ○ Enable ● Disable

IPv4 Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Public LAN

Active: ○ Enable ● Disable

IPv4 Address: 0 . 0 . 0 . 0

Subnet Mask: 255.255.255. 0

Offer Public IP by DHCP: ○ Enable ● Disable

Enable ARP Proxy: ○ Enable ● Disable

The following table describes the labels in this screen.

Table 25 Network Setting > Home Networking > Additional Subnet

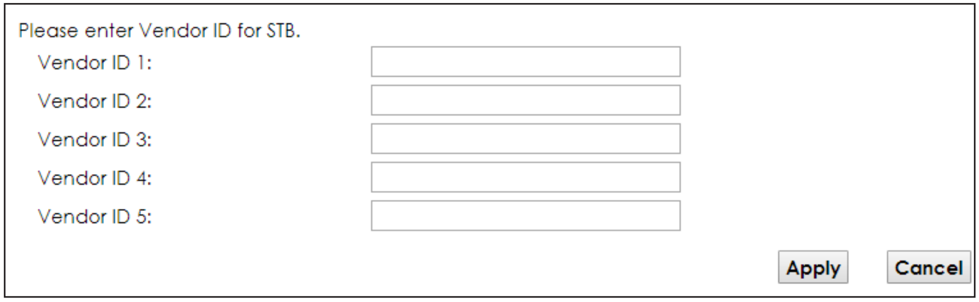
LABEL	DESCRIPTION
IP Alias Setup	
Group Name	Select the interface group name for which you want to configure the IP alias settings. See Chapter 15 on page 165 for how to create a new interface group.
Active	Select **Enable** to configure a LAN network for the EMG.
IPv4 Address	Enter the IP address of 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.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

8.6 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 49 Network Setting > Home Networking > STB Vendor ID



Please enter Vendor ID for STB.

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.

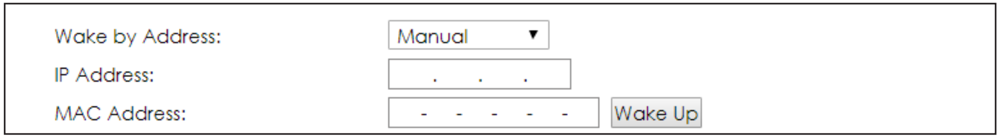
8.7 The Wake on LAN Screen

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 50 Network Setting > Home Networking > Wake on LAN



Wake by Address: Manual

The following table describes the labels in this screen.

Table 27 Network Setting > Home Networking > Wake on LAN

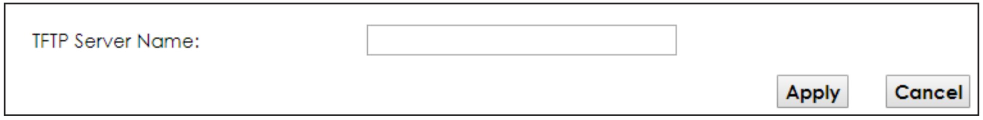
LABEL	DESCRIPTION
Wake by Address	Select **Manual** and enter the IP address or MAC address of the device to turn it on remotely. The drop-down list also lists the IP addresses that can be found in the EMG's ARP table. Select an IP address and it will then automatically update the IP address and MAC 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.

8.8 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 51 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.

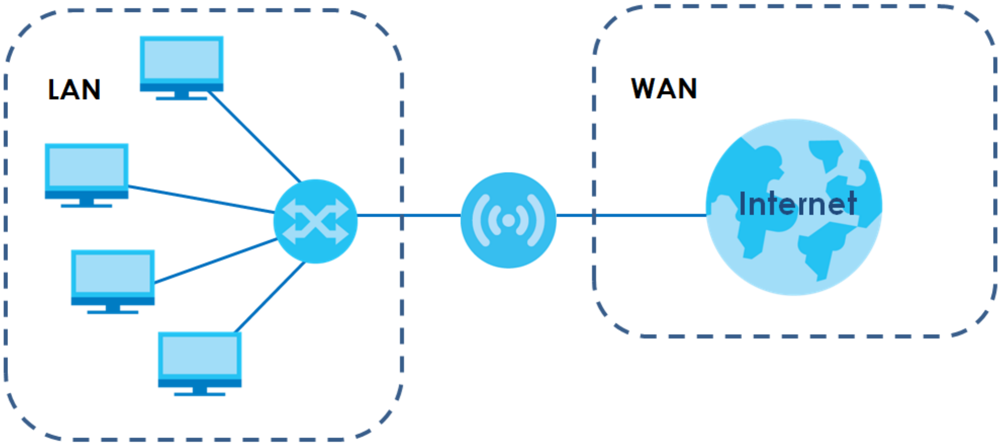
8.9 Technical Reference

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

8.9.1 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 52 LAN and WAN IP Addresses



8.9.2 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.

8.9.3 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.

8.9.4 LAN TCP/IP

The EMG has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the EMG. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your EMG, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your EMG will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the EMG unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, “Address Allocation for Private Internets” and RFC 1466, “Guidelines for Management of IP Address Space”.

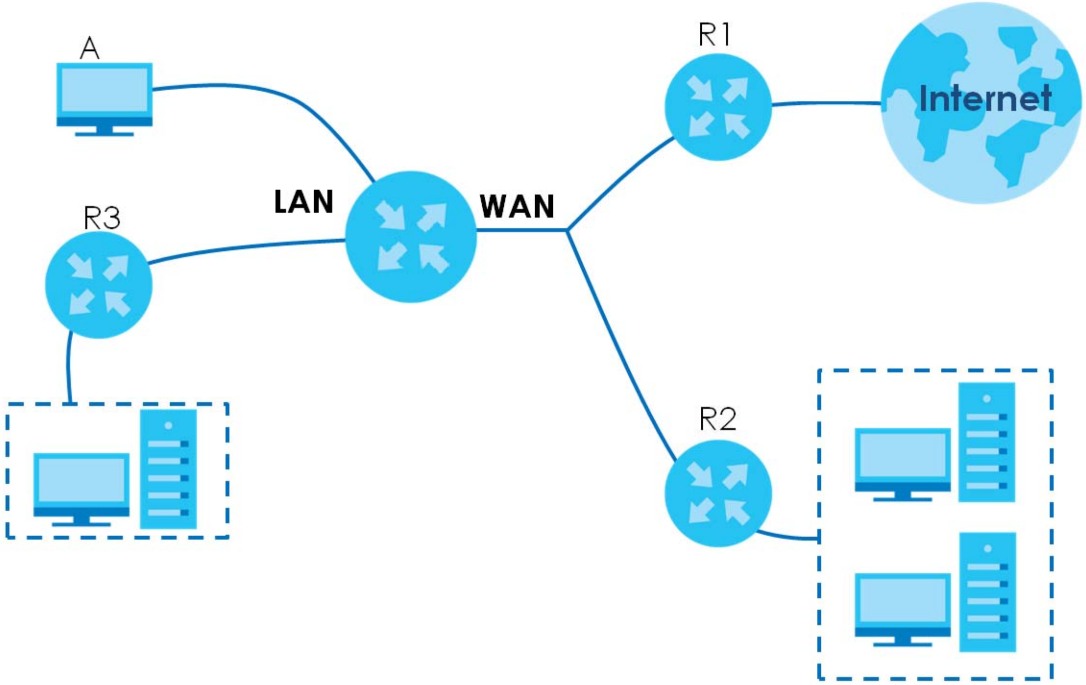
CHAPTER 9 Routing

9.1 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.

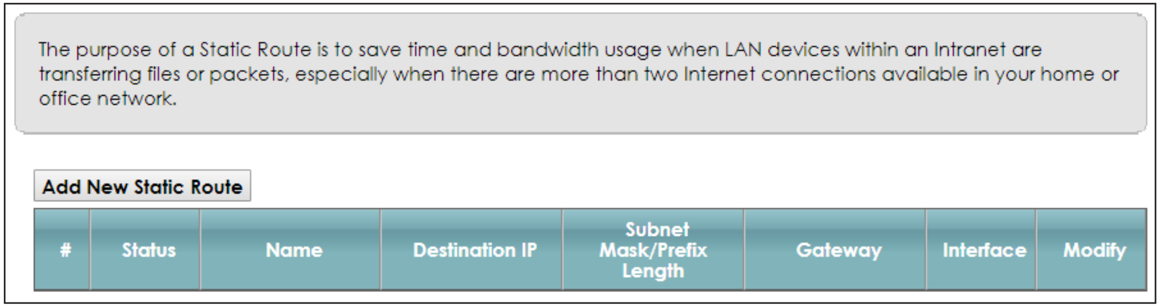
Figure 53 Example of Routing Topology



9.2 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 54 Network Setting > Routing > Static Route



The purpose of a Static Route is to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets, especially when there are more than two Internet connections available in your home or office network.

#	Status	Name	Destination IP	Subnet Mask/Prefix Length	Gateway	Interface	Modify

The following table describes the labels in this screen.

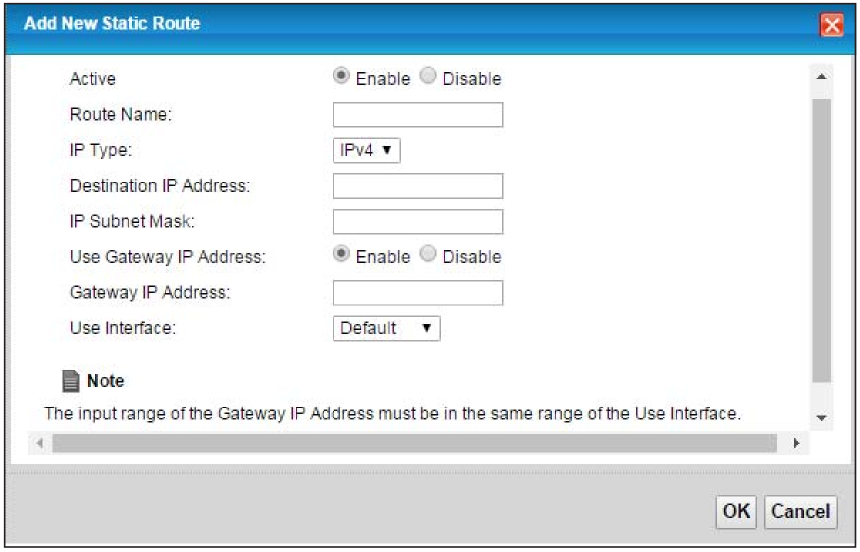
Table 29 Network Setting > Routing > Static Route

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.

9.2.1 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 55 Routing: Add/Edit


Add New Static Route

Active ● Enable ○ Disable

Route Name:

IP Type: IPv4 ▼

Destination IP Address:

IP Subnet Mask:

Use Gateway IP Address: ● Enable ○ Disable

Gateway IP Address:

Use Interface: Default ▼

Note

The input range of the Gateway IP Address must be in the same range of the Use Interface.

The following table describes the labels in this screen.

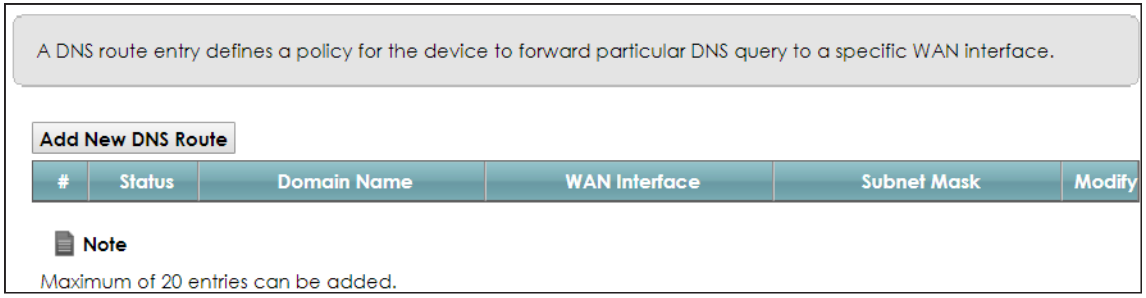
Table 30 Routing: Add/Edit

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.

9.3 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 56   Network Setting > Routing > DNS Route



A DNS route entry defines a policy for the device to forward particular DNS query to a specific WAN interface.

Maximum of 20 entries can be added.

The following table describes the labels in this screen.

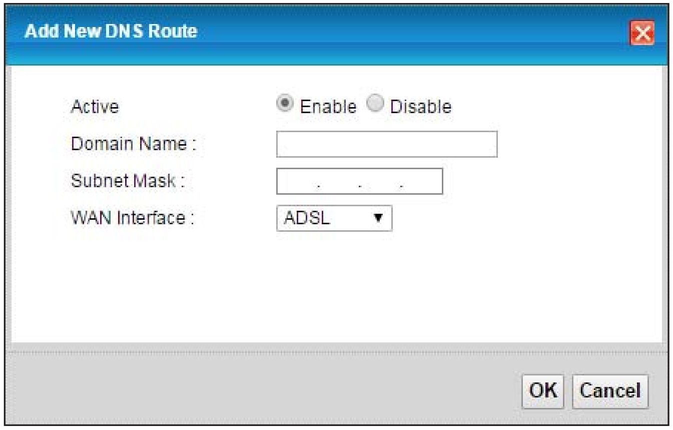
Table 31   Network Setting > Routing > DNS Route

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.
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.

9.3.1 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 57   DNS Route Add



Active ● Enable ○ Disable

Domain Name :

Subnet Mask :

WAN Interface : ADSL

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.

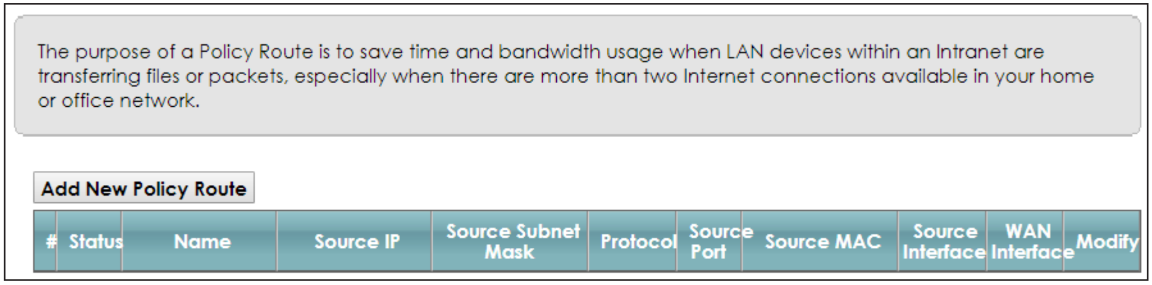
9.4 The Policy Route Screen

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 58 Network Setting > Routing > Policy Route



The purpose of a Policy Route is to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets, especially when there are more than two Internet connections available in your home or office network.

#	Status	Name	Source IP	Source Subnet Mask	Protocol	Source Port	Source MAC	Source Interface	WAN Interface	Modify

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	This is the source subnet mask address.

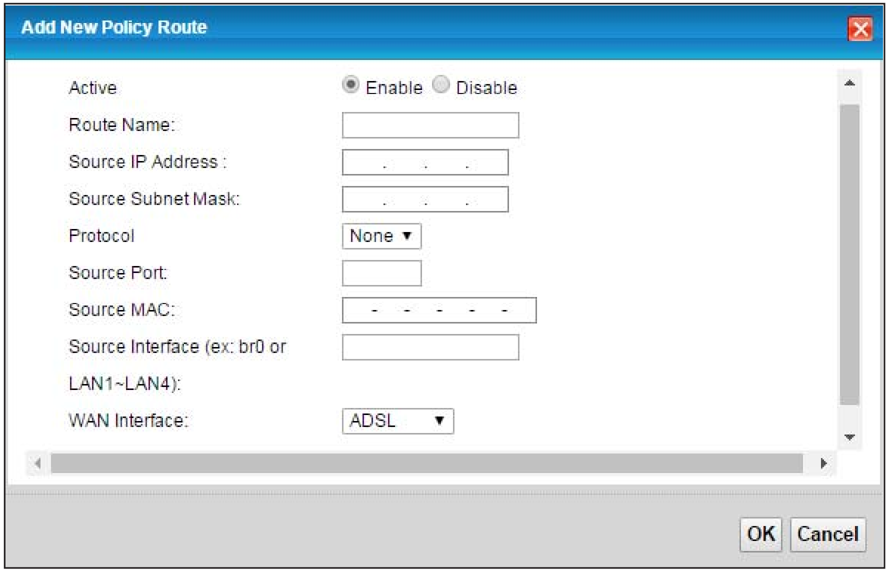
Table 33 Network Setting > Routing >Policy Route (continued)

LABEL	DESCRIPTION
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.

9.4.1 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 59 Policy Route: Add/Edit



Add New Policy Route

Active	● Enable ○ Disable
Route Name:	
Source IP Address :	. . .
Source Subnet Mask:	. . .
Protocol	None
Source Port:	
Source MAC:	- - - - -
Source Interface (ex: br0 or LAN1~LAN4):	
WAN Interface:	ADSL

The following table describes the labels in this screen.

Table 34 Policy Route: Add/Edit (Sheet 1 of 2)

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.

Table 34 Policy Route: Add/Edit (Sheet 2 of 2)

LABEL	DESCRIPTION
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.

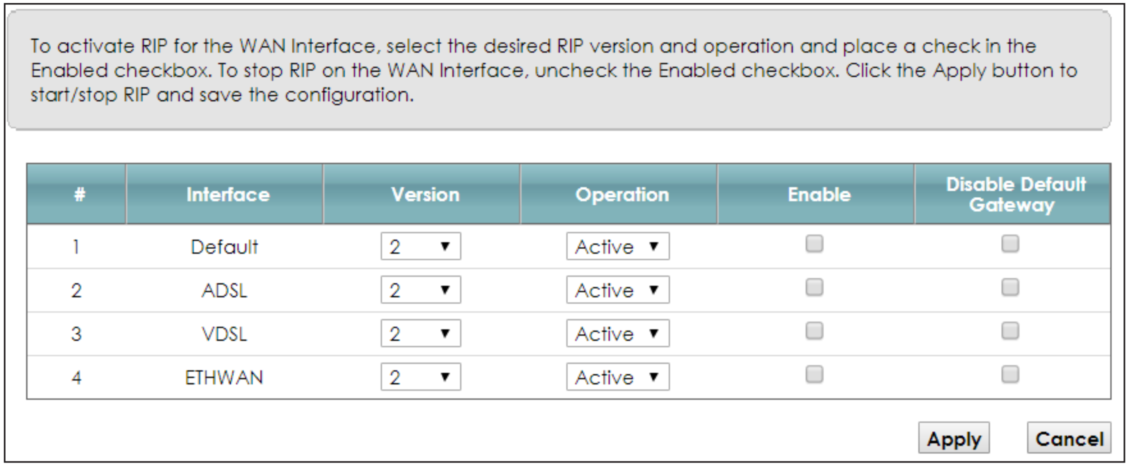
9.5 RIP

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

9.5.1 The RIP Screen

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

Figure 60 RIP



To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the Enabled checkbox. To stop RIP on the WAN Interface, uncheck the Enabled checkbox. Click the Apply button to start/stop RIP and save the configuration.

#	Interface	Version	Operation	Enable	Disable Default Gateway
1	Default	2 ▼	Active ▼	□	□
2	ADSL	2 ▼	Active ▼	□	□
3	VDSL	2 ▼	Active ▼	□	□
4	ETHWAN	2 ▼	Active ▼	□	□

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.

Table 35 RIP

LABEL	DESCRIPTION
Disable Default Gateway	Select the check box to set the EMG 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 10
Quality of Service (QoS)

10.1 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.

10.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable or disable QoS and set the upstream bandwidth (Section 10.3 on page 123).
- Use the **Queue Setup** screen to configure QoS queue assignment (Section 10.4 on page 124).
- Use the **Classification Setup** screen to add, edit or delete QoS classifiers (Section 10.5 on page 127).
- Use the **Shaper Setup** screen to limit outgoing traffic transmission rate on the selected interface (Section 10.6 on page 131).
- Use the **Policer Setup** screen to control incoming traffic transmission rate and bursts (Section 10.7 on page 132).

10.2 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.

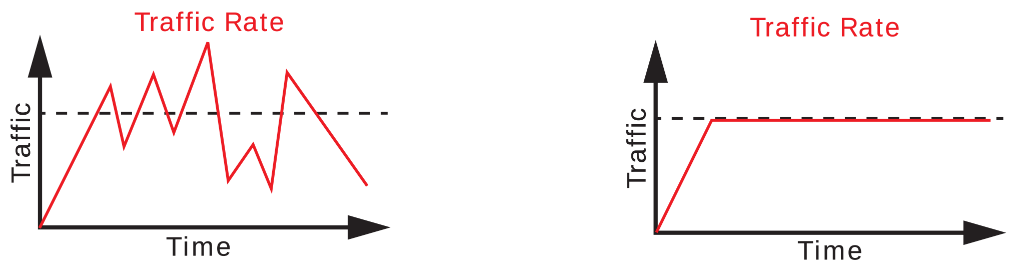
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

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.

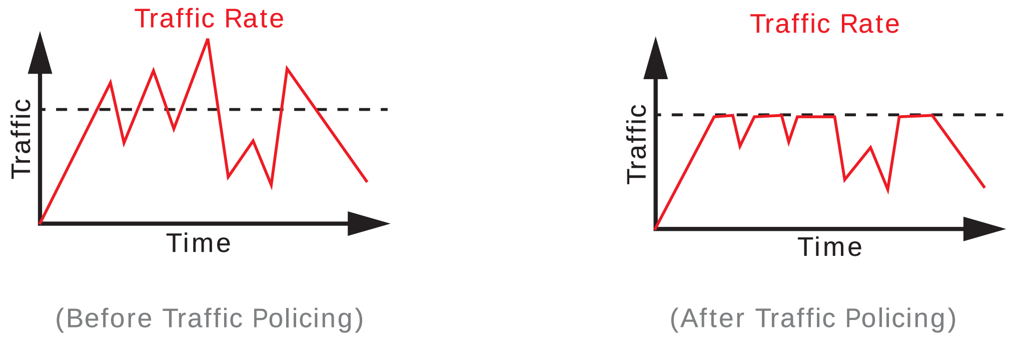


(Before Traffic Shaping)

(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.



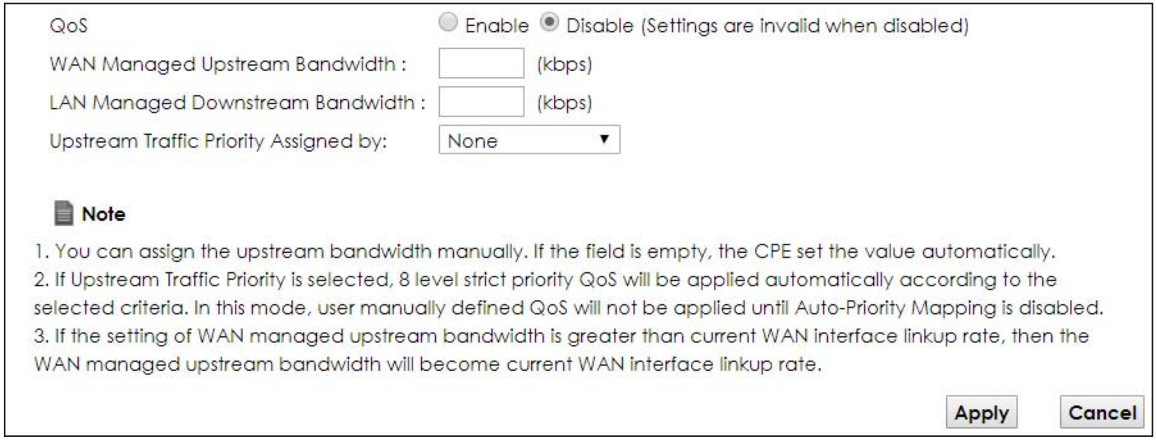
The EMG supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Maker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See Section 10.8 on page 134 for more information on each metering algorithm.

10.3 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 10.1 on page 121 for more information.

Figure 61 Network Settings > QoS > General



QoS	○ Enable ● Disable (Settings are invalid when disabled)
WAN Managed Upstream Bandwidth :	(kbps)
LAN Managed Downstream Bandwidth :	(kbps)
Upstream Traffic Priority Assigned by:	None ▾

Note

1. You can assign the upstream bandwidth manually. If the field is empty, the CPE set the value automatically.
2. If Upstream Traffic Priority is selected, 8 level strict priority QoS will be applied automatically according to the selected criteria. In this mode, user manually defined QoS will not be applied until Auto-Priority Mapping is disabled.
3. If the setting of WAN managed upstream bandwidth is greater than current WAN interface linkup rate, then the WAN managed upstream bandwidth will become current WAN interface linkup rate.

The following table describes the labels in this screen.

Table 36 Network Setting > QoS > General

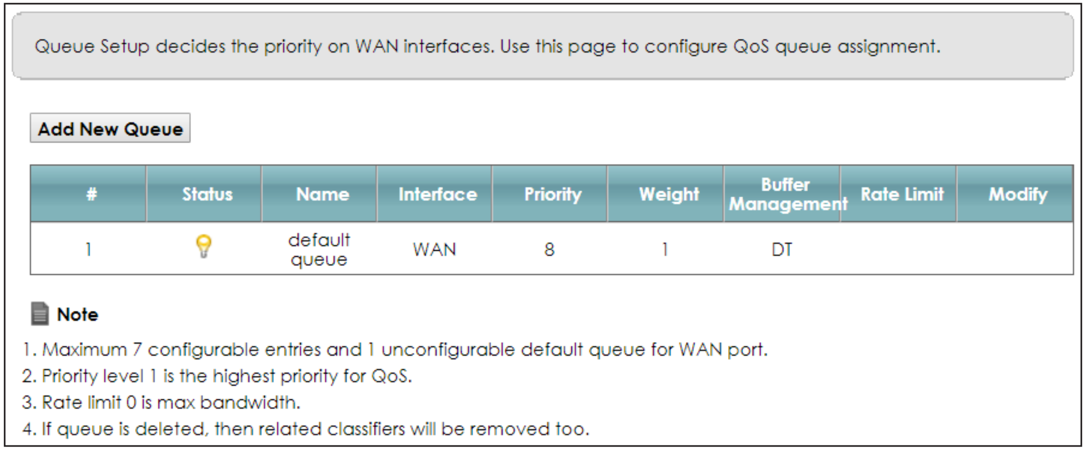
LABEL	DESCRIPTION
QoS	Select the **Enable** check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS. The recommendation is to set this speed to match the interfaces' 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.

10.4 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 62 Network Setting > QoS > Queue Setup



Queue Setup decides the priority on WAN interfaces. Use this page to configure QoS queue assignment.

#	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit	Modify
1	💡	default queue	WAN	8	1	DT		

Note

1. Maximum 7 configurable entries and 1 unconfigurable default queue for WAN port.
2. Priority level 1 is the highest priority for QoS.
3. Rate limit 0 is max bandwidth.
4. If queue is deleted, then related classifiers will be removed too.

The following table describes the labels in this screen.

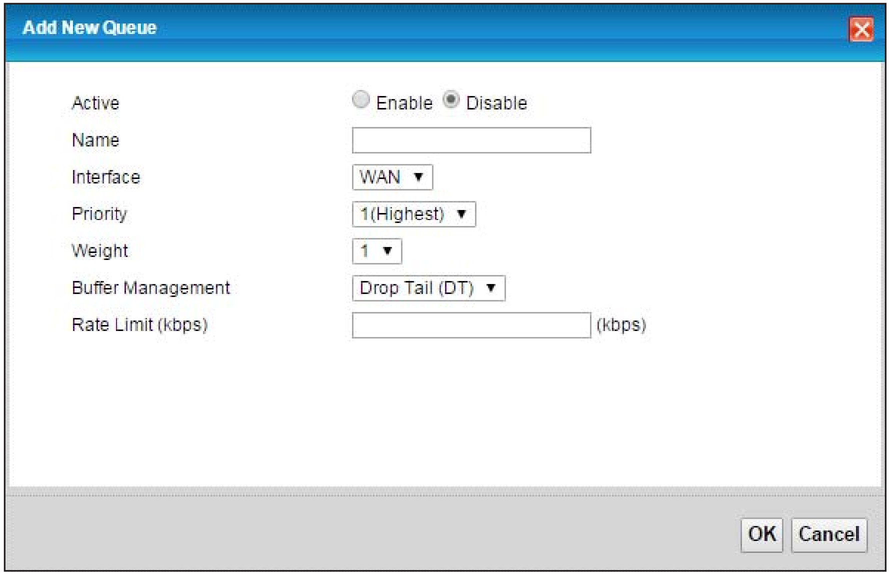
Table 37 Network Setting > QoS > Queue Setup

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.

10.4.1 Adding a QoS Queue

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

Figure 63 Queue Setup: Add



Add New Queue

Active	○ Enable ● Disable
Name	
Interface	WAN ▼
Priority	1(Highest) ▼
Weight	1 ▼
Buffer Management	Drop Tail (DT) ▼
Rate Limit (kbps)	(kbps)

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.

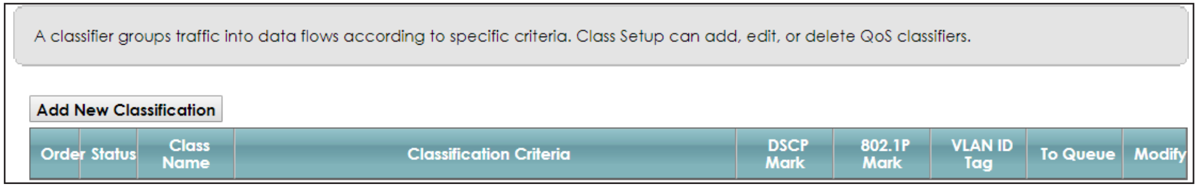
10.5 The Classification Setup Screen

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 64 Network Setting > QoS > Classification Setup



A classifier groups traffic into data flows according to specific criteria. Class Setup can add, edit, or delete QoS classifiers.

Order	Status	Class Name	Classification Criteria	DSCP Mark	802.1P Mark	VLAN ID Tag	To Queue	Modify

The following table describes the labels in this screen.

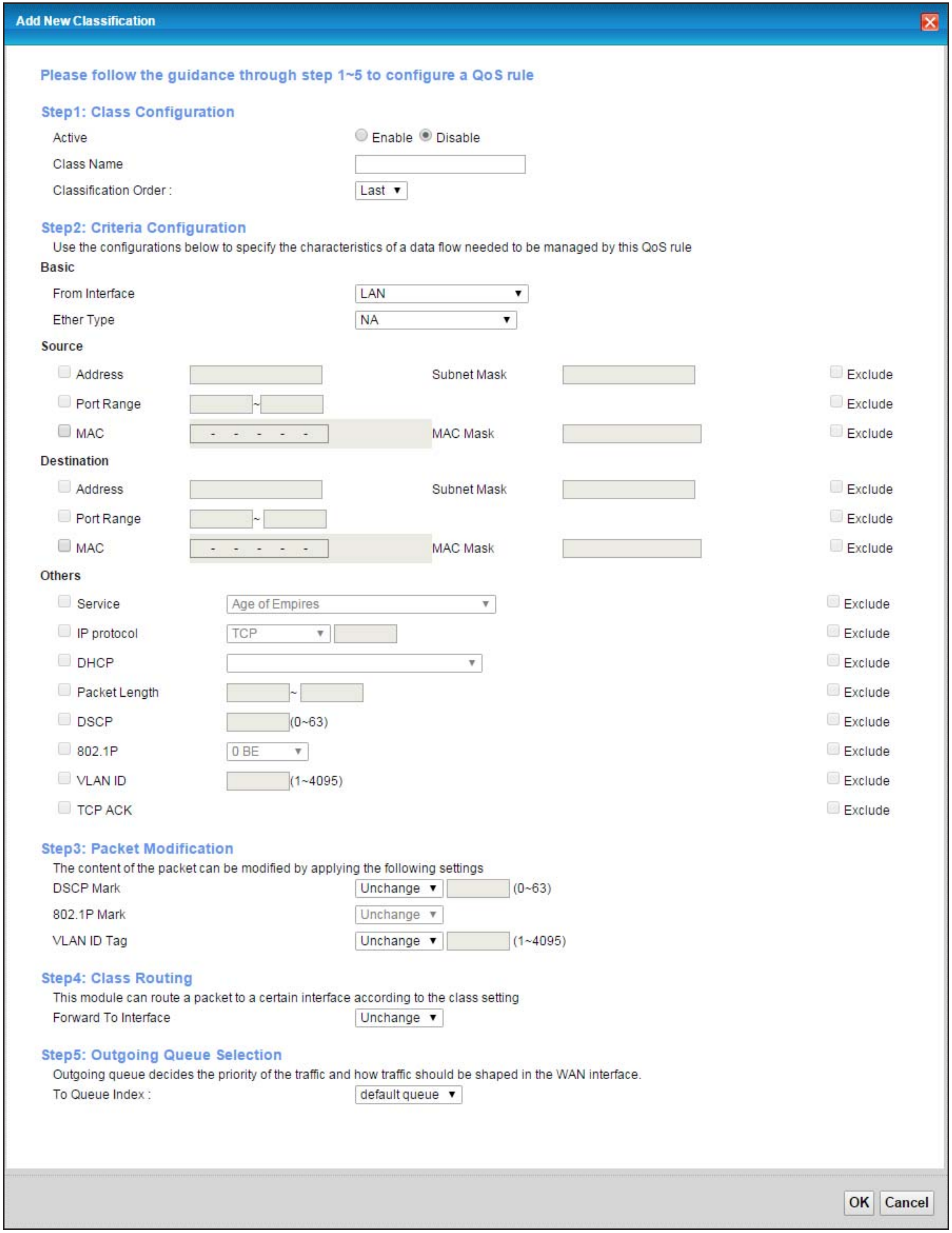
Table 39 Network Setting > QoS > Classification Setup

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.

10.5.1 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 65 Classification Setup: Add/Edit



Add New Classification

Please follow the guidance through step 1~5 to configure a QoS rule

Step1: Class Configuration

Active ○ Enable ● Disable

Class Name

Classification Order : Last

Step2: Criteria Configuration

Use the configurations below to specify the characteristics of a data flow needed to be managed by this QoS rule

Basic

From Interface LAN

Ether Type NA

Source

□ Address — Subnet Mask — □ Exclude

□ Port Range ~ — □ Exclude

□ MAC - - - - - — MAC Mask — □ Exclude

Destination

□ Address — Subnet Mask — □ Exclude

□ Port Range ~ — □ Exclude

□ MAC - - - - - — MAC Mask — □ Exclude

Others

□ Service Age of Empires — □ Exclude

□ IP protocol TCP — □ Exclude

□ DHCP — □ Exclude

□ Packet Length ~ — □ Exclude

□ DSCP (0~63) — □ Exclude

□ 802.1P 0 BE — □ Exclude

□ VLAN ID (1~4095) — □ Exclude

□ TCP ACK — □ Exclude

Step3: Packet Modification

The content of the packet can be modified by applying the following settings

DSCP Mark Unchange (0~63)

802.1P Mark Unchange

VLAN ID Tag Unchange (1~4095)

Step4: Class Routing

This module can route a packet to a certain interface according to the class setting

Forward To Interface Unchange

Step5: Outgoing Queue Selection

Outgoing queue decides the priority of the traffic and how traffic should be shaped in the WAN interface.

To Queue Index : default queue

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.
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	
Basic	
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 can 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. You can also select other options, such as **ARP**, **PPPoE_DISC**, and so on to make configurations according to your needs.
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.

Table 40 Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
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.
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.

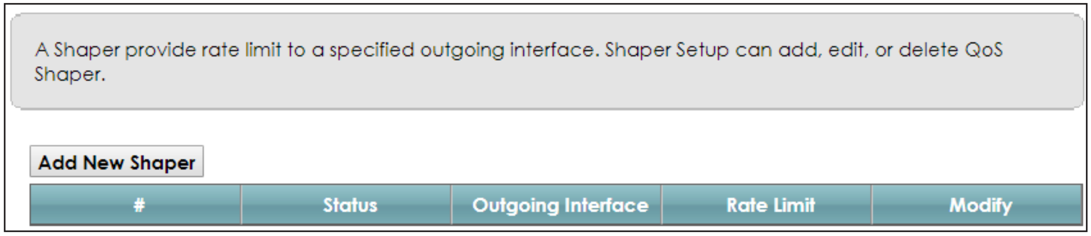
Table 40 Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
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.
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.

10.6 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 66 Network Setting > QoS > Shaper Setup



A Shaper provide rate limit to a specified outgoing interface. Shaper Setup can add, edit, or delete QoS Shaper.

#	Status	Outgoing Interface	Rate Limit	Modify

The following table describes the labels in this screen.

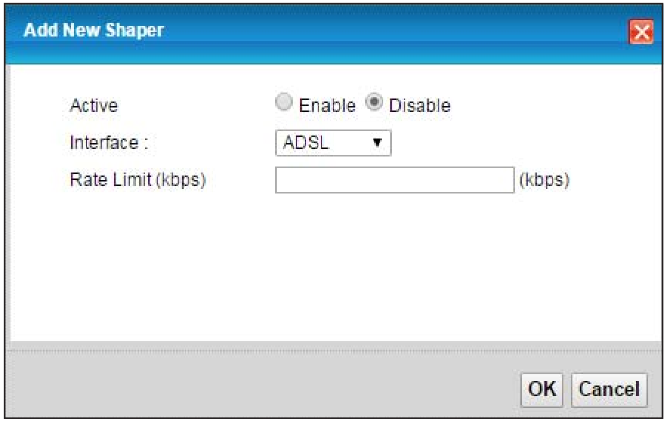
Table 41 Network Setting > QoS > Shaper Setup

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.

10.6.1 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 67 Shaper Setup: Add/Edit



Add New Shaper

Active ○ Enable ● Disable

Interface : ADSL

Rate Limit (kbps) (kbps)

The following table describes the labels in this screen.

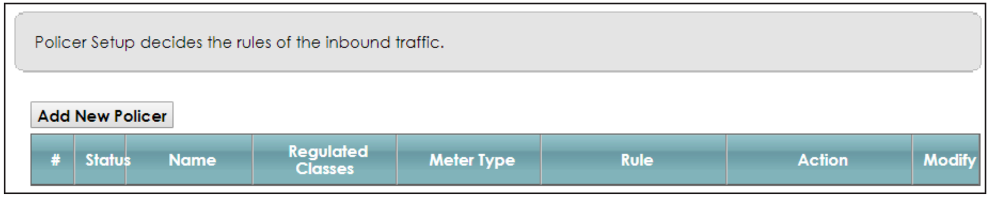
Table 42 Shaper Setup: Add/Edit

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.

10.7 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 68 Network Setting > QoS > Policer Setup



Policer Setup decides the rules of the inbound traffic.

#	Status	Name	Regulated Classes	Meter Type	Rule	Action	Modify

The following table describes the labels in this screen.

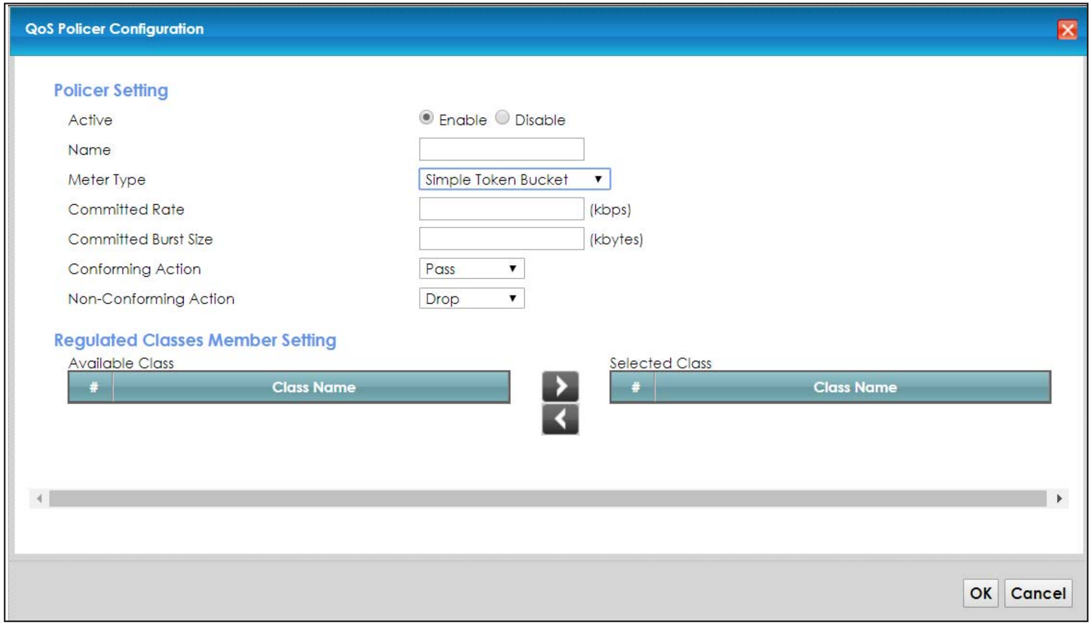
Table 43 Network Setting > QoS > Policer Setup

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

10.7.1 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 69 Policer Setup: Add/Edit



QoS Policer Configuration

Policer Setting

Active ● Enable ○ Disable

Name

Meter Type: Simple Token Bucket

Committed Rate (kbps)

Committed Burst Size (kbytes)

Conforming Action: Pass

Non-Conforming Action: Drop

Regulated Classes Member Setting

Available Class

#	Class Name

Selected Class

#	Class Name

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.
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** (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** (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.

10.8 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 11 Network Address Translation (NAT)

11.1 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.

11.1.1 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 11.2 on page 140).
- Use the **Applications** screen to forward incoming service requests to the server(s) on your local network (Section 11.3 on page 143).
- Use the **Port Triggering** screen to add and configure the EMG's trigger port settings (Section 11.4 on page 145).
- Use the **DMZ** screen to configure a default server (Section 11.5 on page 147).
- Use the **ALG** screen to enable and disable the NAT and SIP (VoIP) ALG in the EMG (Section 11.6 on page 148).
- Use the **Address Mapping** screen to configure the EMG's address mapping settings (Section 11.7 on page 149).
- Use the **Sessions** screen to configure the EMG's maximum number of NAT sessions (Section 11.8 on page 151).

11.1.2 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 11.9 on page 151 for advanced technical information on NAT.

11.2 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.

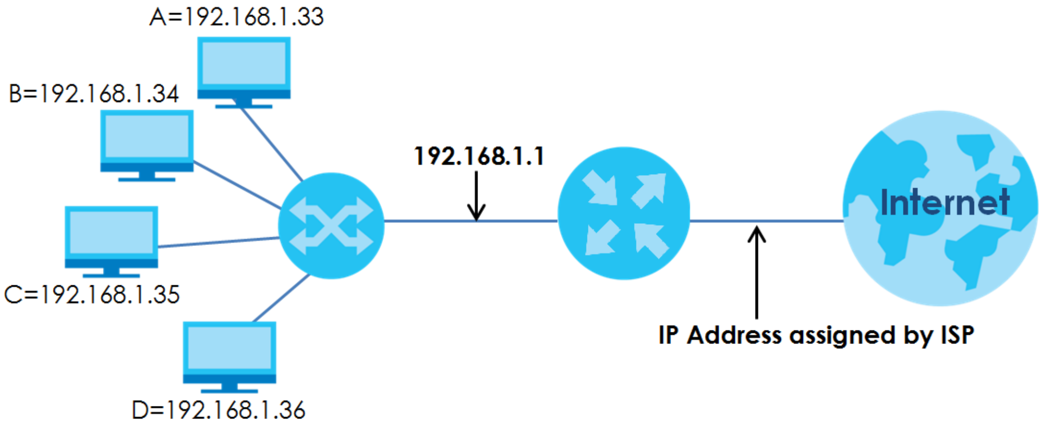
The most often used port numbers and services are shown in Appendix D on page 263. Please refer to RFC 1700 for further information about port numbers.

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.

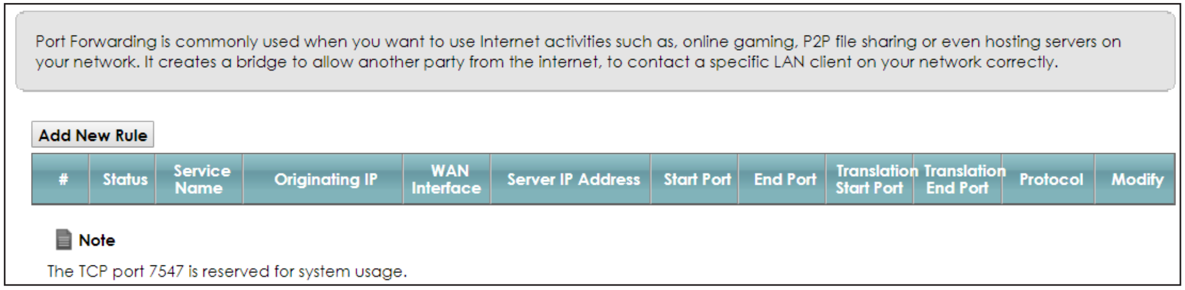
Figure 70 Multiple Servers Behind NAT Example



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

See Appendix D on page 263 for port numbers commonly used for particular services.

Figure 71 Network Setting > NAT > Port Forwarding



Port Forwarding is commonly used when you want to use Internet activities such as, online gaming, P2P file sharing or even hosting servers on your network. It creates a bridge to allow another party from the internet, to contact a specific LAN client on your network correctly.

Add New Rule

#	Status	Service Name	Originating IP	WAN Interface	Server IP Address	Start Port	End Port	Translation Start Port	Translation End Port	Protocol	Modify

Note

The TCP port 7547 is reserved for system usage.

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.
Originating IP	This field displays the source IP address from the WAN interface.
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.

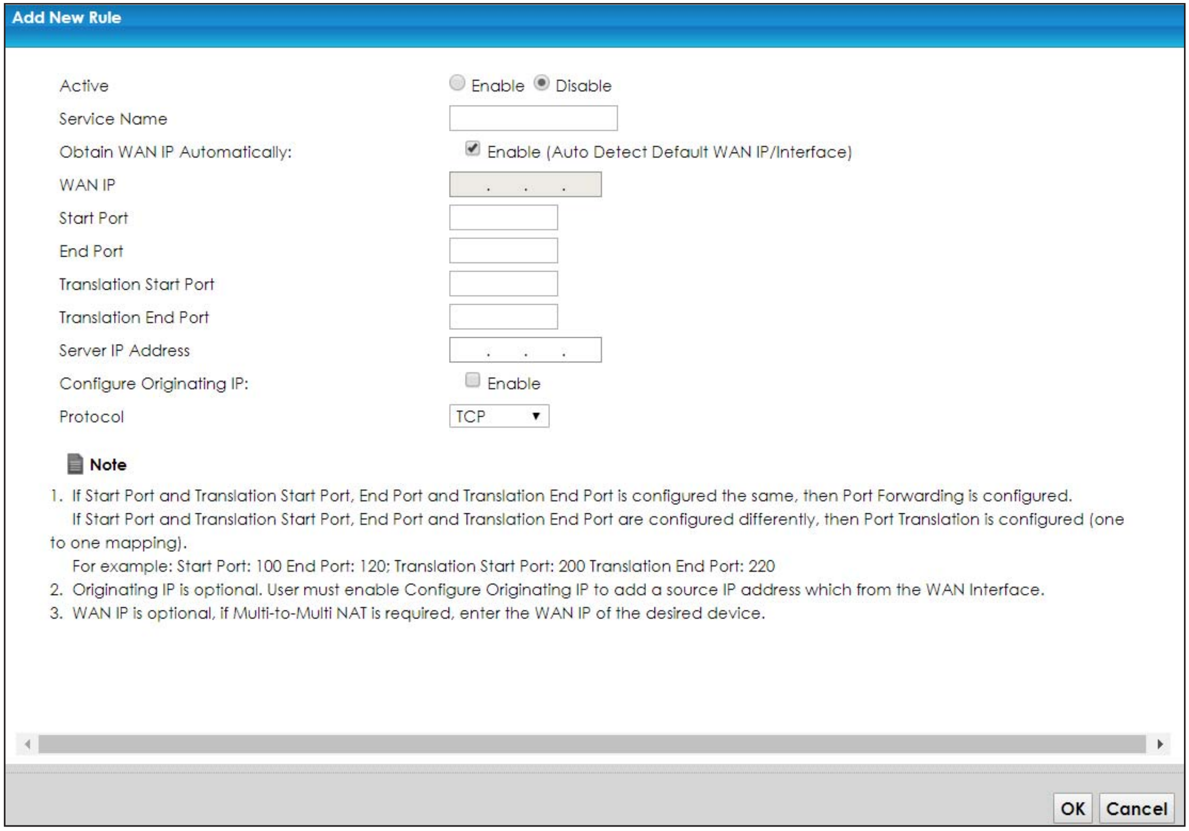
Table 47 Network Setting > NAT > Port Forwarding (continued)

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.

11.2.1 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 72 Port Forwarding: Add/Edit



Add New Rule

Active	○ Enable ● Disable
Service Name	
Obtain WAN IP Automatically:	☑ Enable (Auto Detect Default WAN IP/Interface)
WAN IP	. . .
Start Port	
End Port	
Translation Start Port	
Translation End Port	
Server IP Address	. . .
Configure Originating IP:	□ Enable
Protocol	TCP ▾

Note

1. If Start Port and Translation Start Port, End Port and Translation End Port is configured the same, then Port Forwarding is configured.
   If Start Port and Translation Start Port, End Port and Translation End Port are configured differently, then Port Translation is configured (one to one mapping).
   For example: Start Port: 100 End Port: 120; Translation Start Port: 200 Translation End Port: 220
2. Originating IP is optional. User must enable Configure Originating IP to add a source IP address which from the WAN Interface.
3. WAN IP is optional, if Multi-to-Multi NAT is required, enter the WAN IP of the desired device.

The following table describes the labels in this screen.

Table 48 Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Active	Select **Enable** or **Disable** to activate or deactivate the rule.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
Obtain WAN IP Automatically	Select this option to obtain the WAN IP address of the EMG.
WAN IP	If you're using multi-to-multi NAT, enter a WAN IP address provided by your ISP.

Table 48 Port Forwarding: Add/Edit (continued)

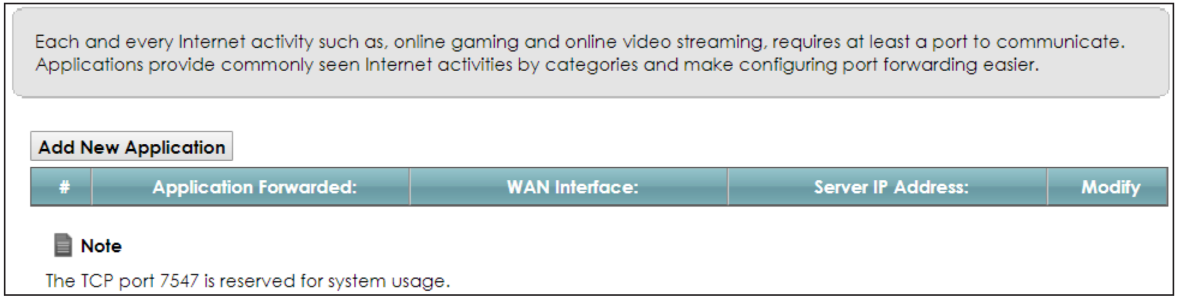
LABEL	DESCRIPTION
Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port** field.
End Port	Enter the last 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.
Configure Originating IP	Select **Enable** to enter the source IP address of WAN interface.
Originating IP	Enter the source IP address of WAN interface.
Protocol	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

11.3 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 73 Network Setting > NAT > Applications



Each and every Internet activity such as, online gaming and online video streaming, requires at least a port to communicate. Applications provide commonly seen Internet activities by categories and make configuring port forwarding easier.

#	Application Forwarded:	WAN Interface:	Server IP Address:	Modify

Note

The TCP port 7547 is reserved for system usage.

The following table describes the labels in this screen.

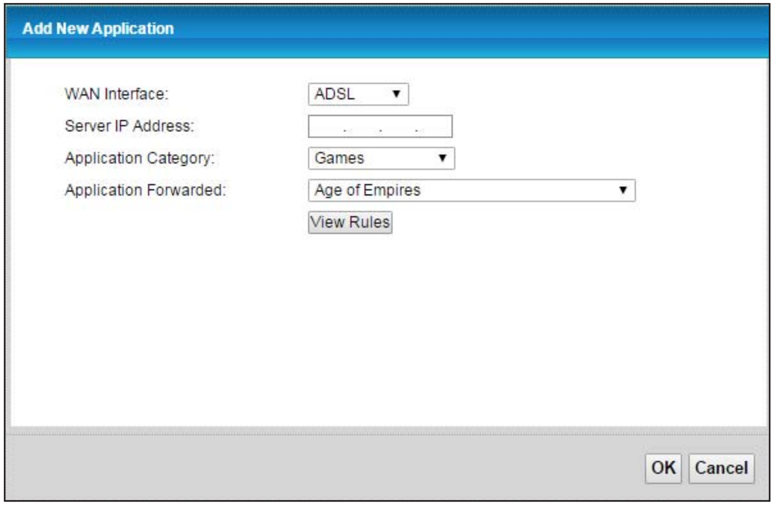
Table 49 Network Setting > NAT > Applications

LABEL	DESCRIPTION
Add New Application	Click this to add a new NAT application rule.
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.

11.3.1 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 74 Network Setting > NAT > Applications: Add



Add New Application

WAN Interface: ADSL

Server IP Address: . . .

Application Category: Games

Application Forwarded: Age of Empires

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.

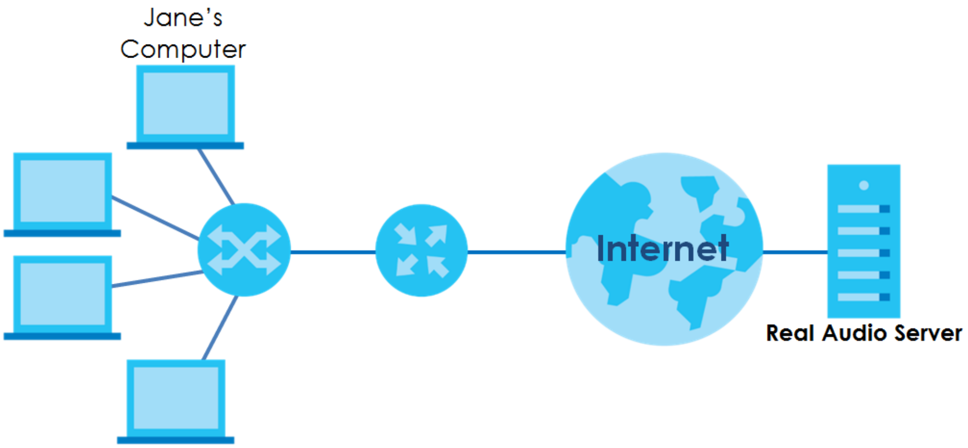
11.4 The Port Triggering Screen

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 75 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.

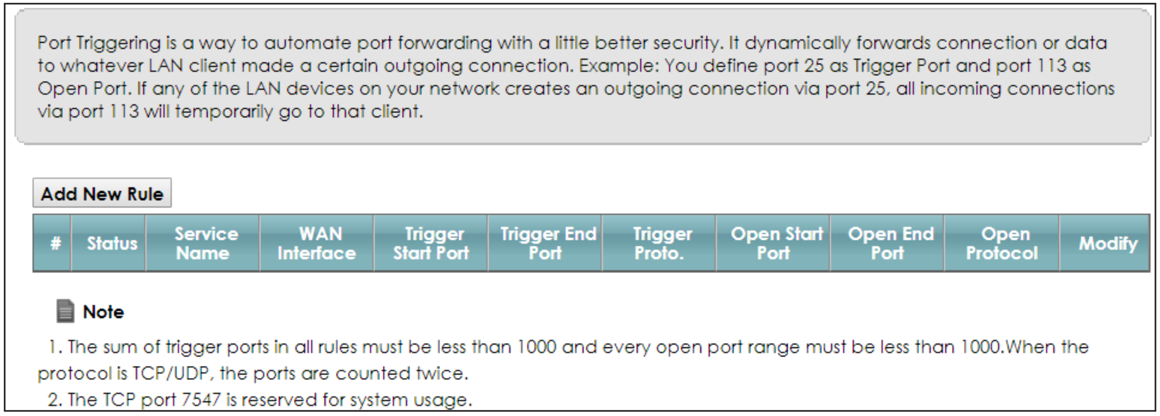
3 The Real Audio server responds using a port number ranging between 6970-7170.

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 76 Network Setting > NAT > Port Triggering



Port Triggering is a way to automate port forwarding with a little better security. It dynamically forwards connection or data to whatever LAN client made a certain outgoing connection. Example: You define port 25 as Trigger Port and port 113 as Open Port. If any of the LAN devices on your network creates an outgoing connection via port 25, all incoming connections via port 113 will temporarily go to that client.

#	Status	Service Name	WAN Interface	Trigger Start Port	Trigger End Port	Trigger Proto.	Open Start Port	Open End Port	Open Protocol	Modify

Note

1. The sum of trigger ports in all rules must be less than 1000 and every open port range must be less than 1000.When the protocol is TCP/UDP, the ports are counted twice.
2. The TCP port 7547 is reserved for system usage.

The following table describes the labels in this screen.

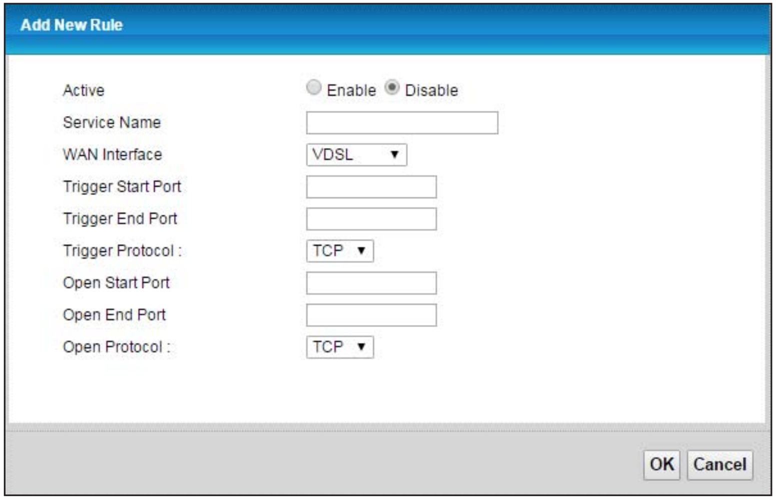
Table 51 Network Setting > NAT > Port Triggering

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 Protocol	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.

11.4.1 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 77 Port Triggering: Add/Edit



Add New Rule

Active	○ Enable ● Disable
Service Name	
WAN Interface	VDSL ▼
Trigger Start Port	
Trigger End Port	
Trigger Protocol :	TCP ▼
Open Start Port	
Open End Port	
Open Protocol :	TCP ▼

The following table describes the labels in this screen.

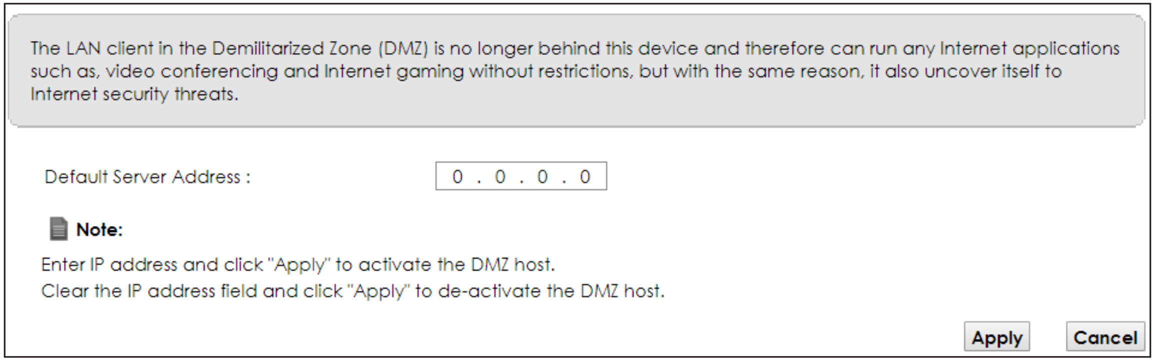
Table 52 Port Triggering: Configuration Add/Edit

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**, or **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**, or **UDP**.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

11.5 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 78 Network Setting > NAT > DMZ



The LAN client in the Demilitarized Zone (DMZ) is no longer behind this device and therefore can run any Internet applications such as, video conferencing and Internet gaming without restrictions, but with the same reason, it also uncover itself to Internet security threats.

Default Server Address : 0 . 0 . 0 . 0

Note:

Enter IP address and click "Apply" to activate the DMZ host.
Clear the IP address field and click "Apply" to de-activate the DMZ host.

The following table describes the fields in this screen.

Table 53 Network Setting > NAT > DMZ

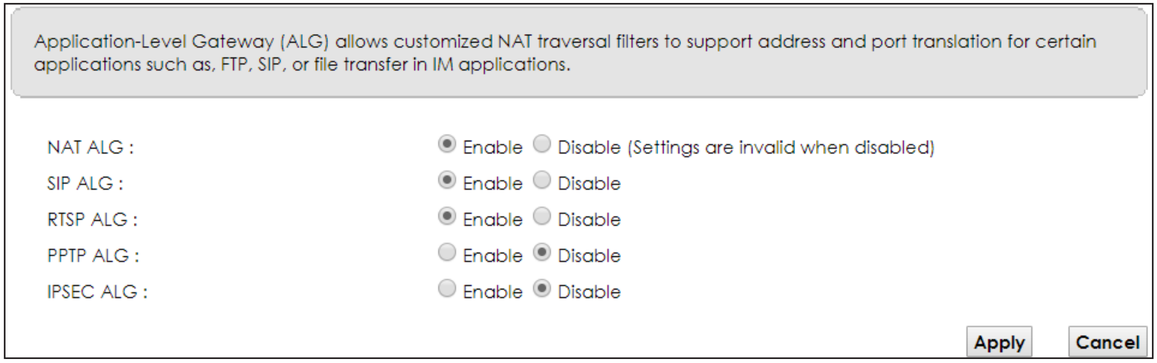
LABEL	DESCRIPTION
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the **NAT Port Forwarding** screen. Note: If you do not assign a **Default Server Address**, the EMG discards all packets received for ports that are not specified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

11.6 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 79 Network Setting > NAT > ALG



Application-Level Gateway (ALG) allows customized NAT traversal filters to support address and port translation for certain applications such as, FTP, SIP, or file transfer in IM applications.

NAT ALG : ● Enable ○ Disable (Settings are invalid when disabled)
SIP ALG : ● Enable ○ Disable
RTSP ALG : ● Enable ○ Disable
PPTP ALG : ○ Enable ● Disable
IPSEC ALG : ○ Enable ● Disable

The following table describes the fields in this screen.

Table 54 Network Setting > NAT > ALG

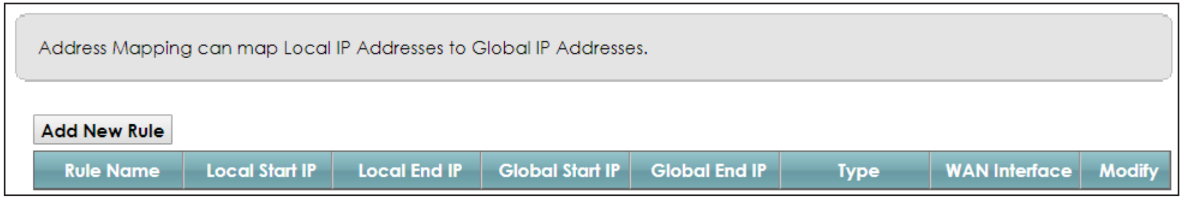
LABEL	DESCRIPTION
NAT ALG	Enable this to make sure applications such as FTP and file transfer in IM applications work correctly with port-forwarding and address-mapping rules.
SIP ALG	Enable this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
RTSP ALG	Enable this 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.
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.

11.7 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 80 Network Setting > NAT > Address Mapping



Address Mapping can map Local IP Addresses to Global IP Addresses.

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.

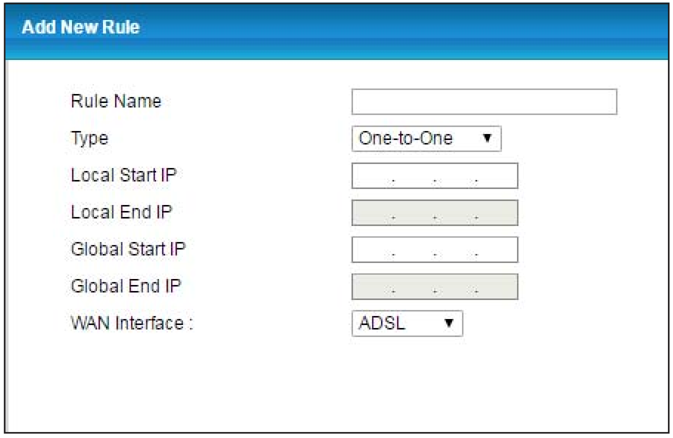
Table 55 Network Setting > NAT > Address Mapping (continued)

LABEL	DESCRIPTION
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	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.

11.7.1 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 81 Address Mapping: Add/Edit



Add New Rule

Rule Name	
Type	One-to-One ▼
Local Start IP	. . .
Local End IP	. . .
Global Start IP	. . .
Global End IP	. . .
WAN Interface :	ADSL ▼

The following table describes the fields in this screen.

Table 56 Address Mapping: Add/Edit

LABEL	DESCRIPTION
Rule Name	This show the name of the rule.
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).

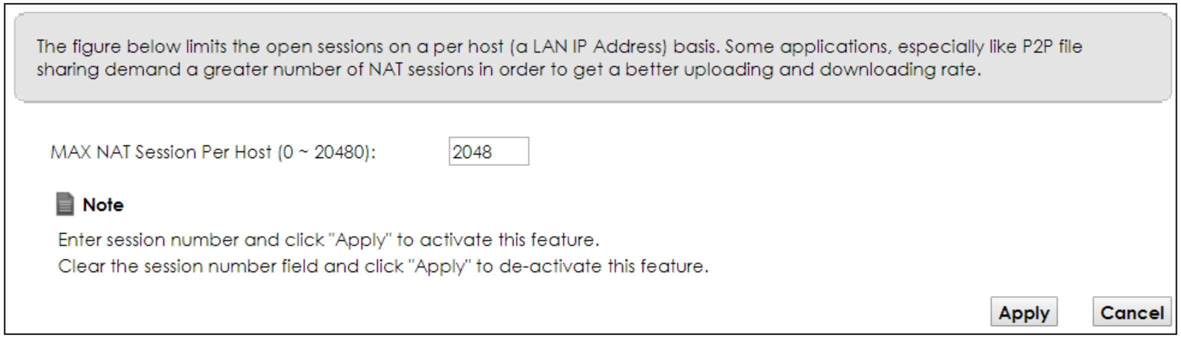
Table 56 Address Mapping: Add/Edit (continued)

LABEL	DESCRIPTION
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.

11.8 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 82 Network Setting > NAT > Sessions



The figure below limits the open sessions on a per host (a LAN IP Address) basis. Some applications, especially like P2P file sharing demand a greater number of NAT sessions in order to get a better uploading and downloading rate.

MAX NAT Session Per Host (0 ~ 20480): 2048

Note

Enter session number and click "Apply" to activate this feature.
Clear the session number field and click "Apply" to de-activate this feature.

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.

11.9 Technical Reference

This part contains more information regarding NAT.

11.9.1 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.

11.9.2 What NAT Does

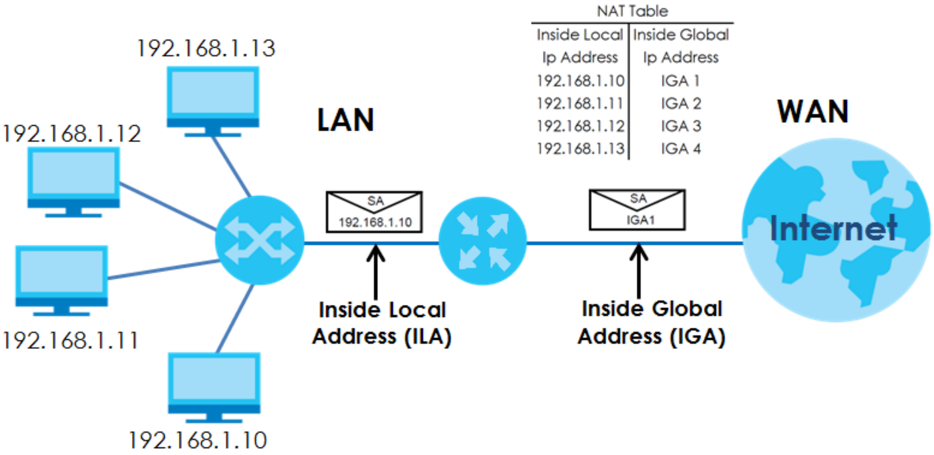
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

11.9.3 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 83 How NAT Works



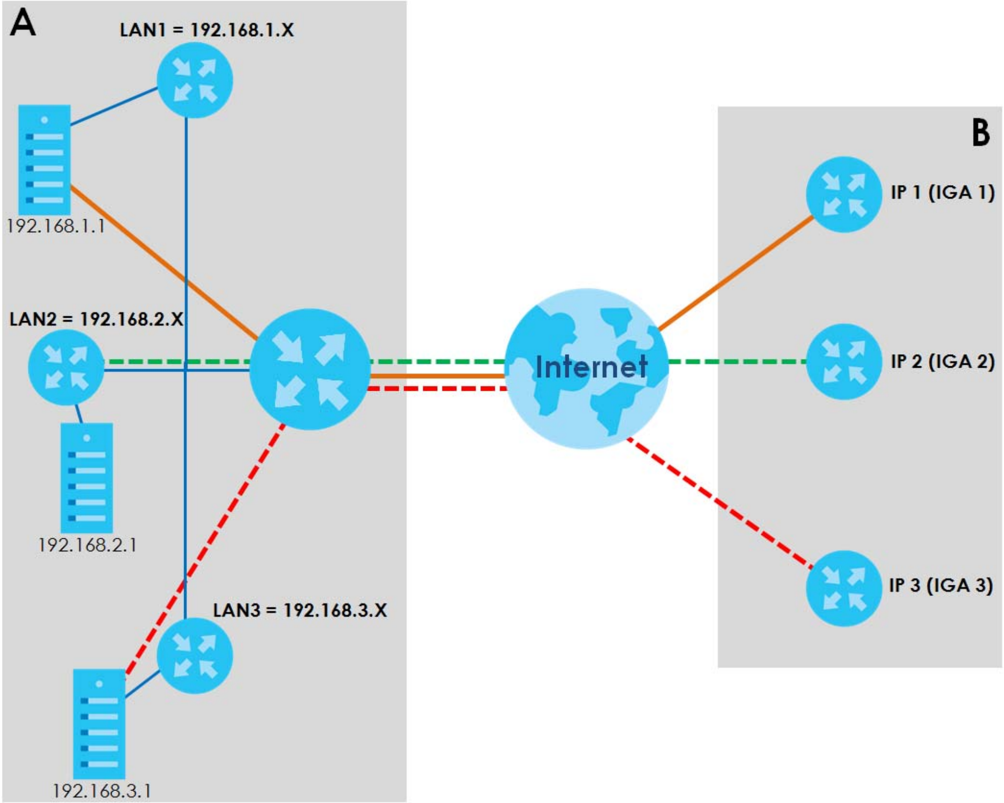
NAT Table

Inside Local Ip Address	Inside Global Ip Address
192.168.1.10	IGA 1
192.168.1.11	IGA 2
192.168.1.12	IGA 3
192.168.1.13	IGA 4

11.9.4 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 84 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.

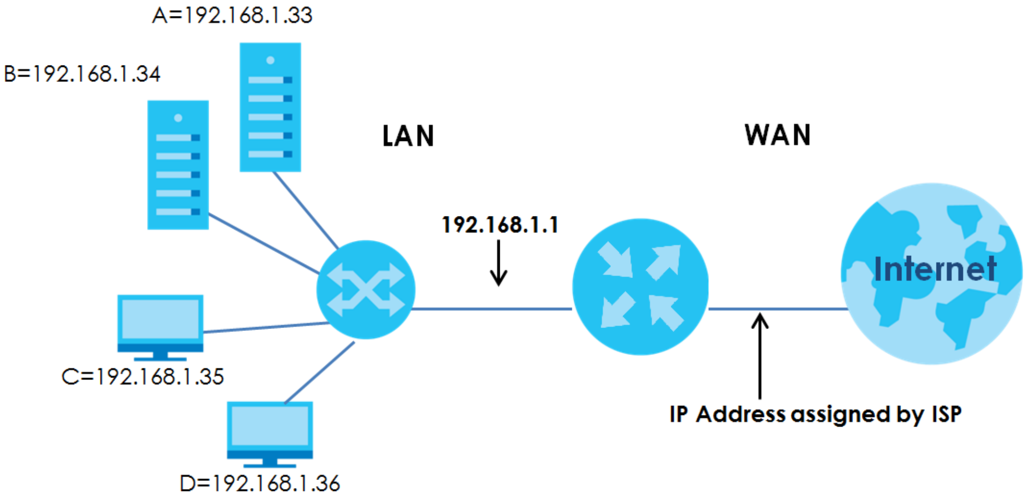
Table 59 Services and Port Numbers

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
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 85 Multiple Servers Behind NAT Example



CHAPTER 12 Dynamic DNS Setup

12.1 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.

12.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes (Section 12.2 on page 157).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the EMG (Section 12.3 on page 158).

12.1.2 What You Need To Know

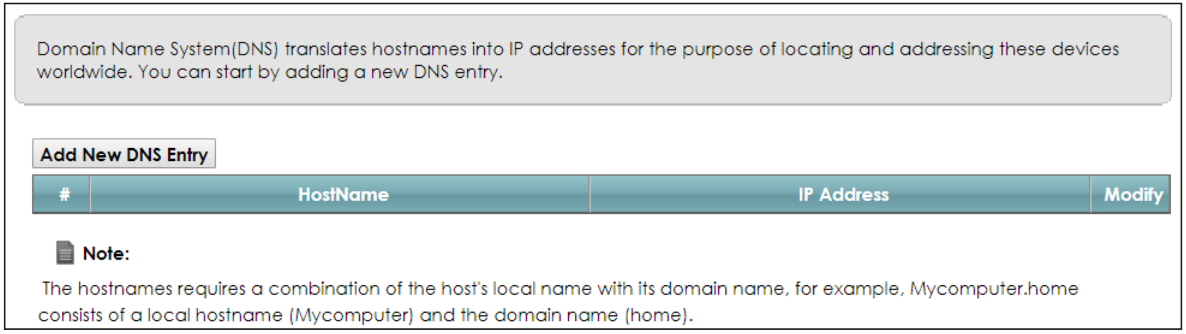
DYNDNS Wildcard

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.

12.2 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.



Domain Name System(DNS) translates hostnames into IP addresses for the purpose of locating and addressing these devices worldwide. You can start by adding a new DNS entry.

Note:

The hostnames requires a combination of the host's local name with its domain name, for example, Mycomputer.home consists of a local hostname (Mycomputer) and the domain name (home).

Figure 86 Network Setting > DNS > DNS Entry

The following table describes the fields in this screen.

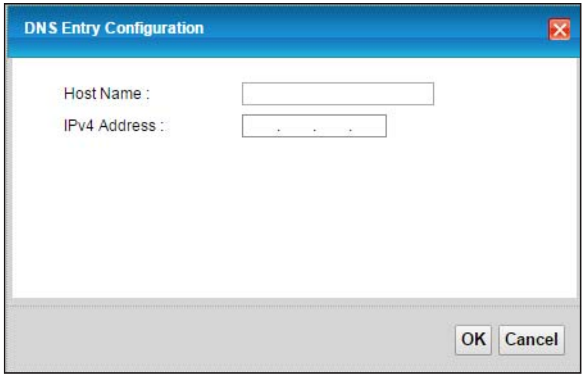
Table 60 Network Setting > DNS > DNS Entry

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.

12.2.1 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 87 DNS Entry: Add/Edit



The following table describes the labels in this screen.

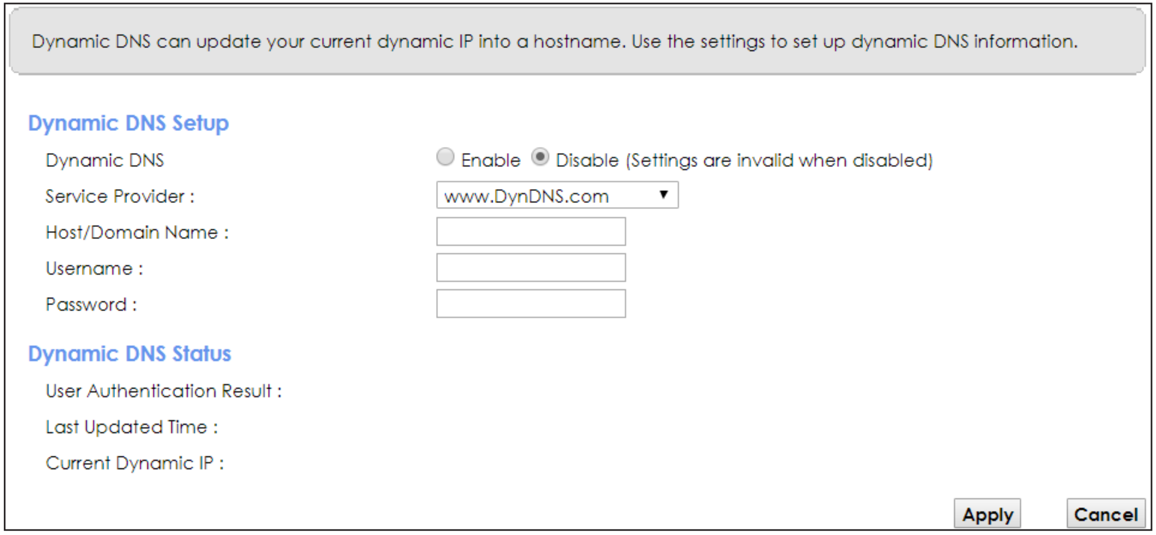
Table 61 DNS Entry: Add/Edit

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.

12.3 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 88 Network Setting > DNS > Dynamic DNS



Dynamic DNS can update your current dynamic IP into a hostname. Use the settings to set up dynamic DNS information.

Dynamic DNS Setup

Dynamic DNS ○ Enable ● Disable (Settings are invalid when disabled)

Service Provider : www.DynDNS.com

Host/Domain Name :

Username :

Password :

Dynamic DNS Status

User Authentication Result :

Last Updated Time :

Current Dynamic IP :

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. If it's not in the drop-down list, please select **DNS user defined**. Fill in the **Connection Type** and **URL Update** fields.
Connection Type	Select a protocol that your Dynamic DNS service server use.
URL Update	Enter an URL of the Dynamic DNS provider.
Host/Domain 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.

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

LABEL	DESCRIPTION
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable Off Line 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	
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 13 IGMP/MLD

13.1 Overview

Use the **IGMP/MLD** screen to configure IGMP/MLD group settings.

13.1.1 What You Need To Know

Multicast and IGMP

See Multicast on page 73 for more information.

Multicast Listener Discovery (MLD)

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

- 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.
- MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.
- MLD filtering controls which multicast groups a port can join.
- An MLD Report message is equivalent to an IGMP Report message, and a MLD Done message is equivalent to an IGMP Leave message.

IGMP Fast Leave

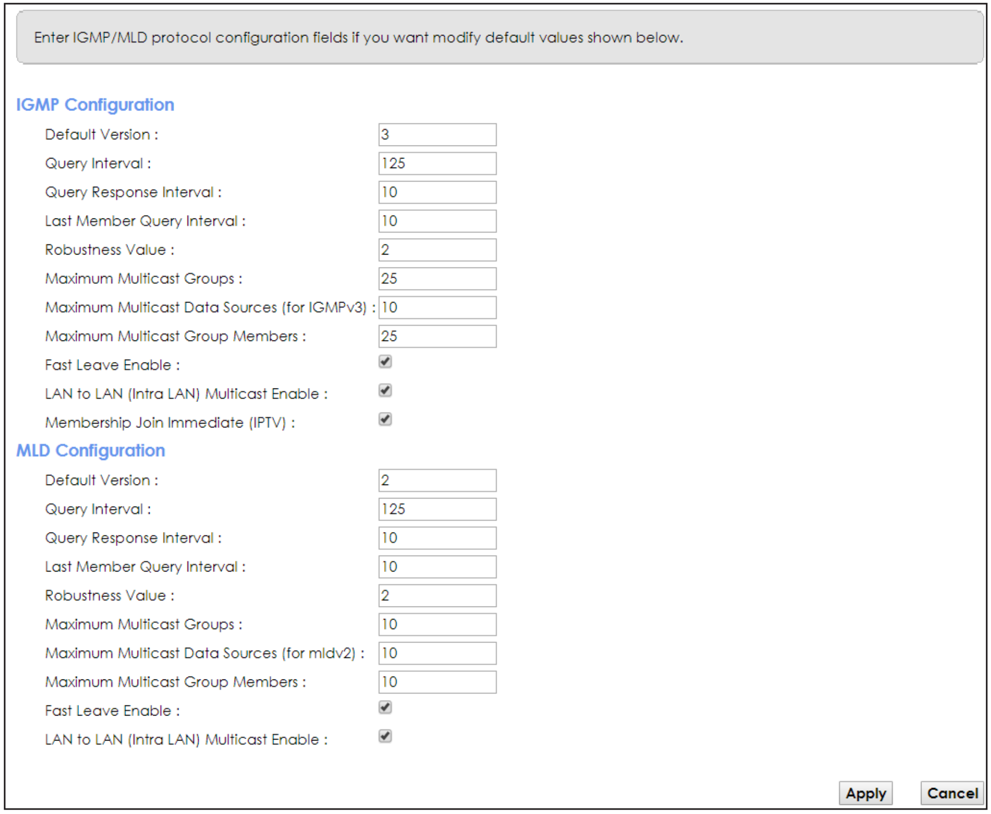
When a host leaves a multicast group (224.1.1.1), it sends an IGMP leave message to inform all routers (224.0.0.2) in the multicast group. When a router receives the leave message, it sends a specific query message to all multicast group (224.1.1.1) members to check if any other hosts are still in the group. Then the router deletes the host’s information.

With the IGMP fast leave feature enabled, the router removes the host’s information from the group member list once it receives a leave message from a host and the fast leave timer expires.

13.2 The IGMP/MLD Screen

Use this screen to configure multicast groups the EMG has joined and which ports have joined it. To open this screen, click **Network Setting > IGMP/MLD**.

Figure 89 Network Setting > IGMP/MLD



Enter IGMP/MLD protocol configuration fields if you want modify default values shown below.

IGMP Configuration

Default Version :	3
Query Interval :	125
Query Response Interval :	10
Last Member Query Interval :	10
Robustness Value :	2
Maximum Multicast Groups :	25
Maximum Multicast Data Sources (for IGMPv3) :	10
Maximum Multicast Group Members :	25
Fast Leave Enable :	☑
LAN to LAN (Intra LAN) Multicast Enable :	☑
Membership Join Immediate (IPTV) :	☑

MLD Configuration

Default Version :	2
Query Interval :	125
Query Response Interval :	10
Last Member Query Interval :	10
Robustness Value :	2
Maximum Multicast Groups :	10
Maximum Multicast Data Sources (for mldv2) :	10
Maximum Multicast Group Members :	10
Fast Leave Enable :	☑
LAN to LAN (Intra LAN) Multicast Enable :	☑

The following table describes the labels in this screen.

Table 63 Network Setting > IGMP/MLD

LABEL	DESCRIPTION
IGMP/MLD Configuration	
Default Version	Enter the version of IGMP (1~3) and MLD (1~2) that you want the EMG to use on the WAN.
Query Interval	Enter the number of seconds the EMG sends a query message to hosts to get the group membership information.
Query Response Interval	Enter the maximum number of seconds the EMG can wait for receiving a General Query message. Multicast routers use general queries to learn which multicast groups have members.
Last Member Query Interval	Enter the maximum number of seconds the EMG can wait for receiving a response to a Group-Specific Query message. Multicast routers use group-specific queries to learn whether any member remains in a specific multicast group.
Robustness Value	Enter the number of times (1~7) the EMG can resend a packet if packet loss occurs due to network congestion.
Maximum Multicast Groups	Enter a number to limit the number of multicast groups an interface on the EMG is allowed to join. Once a multicast member is registered in the specified number of multicast groups, any new IGMP or MLD join report frames are dropped by the interface.
Maximum Multicast Data Sources	Enter a number to limit the number of multicast data sources (1-24) a multicast group is allowed to have. Note: The setting only works for IGMPv3 and MLDv2.
Maximum Multicast Group Members	Enter a number to limit the number of multicast members a multicast group can have.

Table 63 Network Setting > IGMP/MLD (continued)

LABEL	DESCRIPTION
Fast Leave Enable	Select this option to set the EMG to remove a port from the multicast tree immediately (without sending an IGMP or MLD membership query message) once it receives an IGMP or MLD leave message. This is helpful if a user wants to quickly change a TV channel (multicast group change) especially for IPTV applications.
LAN to LAN (Intra LAN) Multicast Enable	Select this to enable LAN to LAN IGMP snooping capability.
Membership Join Immediate (IPTV)	Select this to have the EMG add a host to a multicast group immediately once the EMG receives an IGMP or MLD join message.
Apply	Click **Apply** to save your changes back to the EMG.
Cancel	Click **Cancel** to exit this screen without saving.

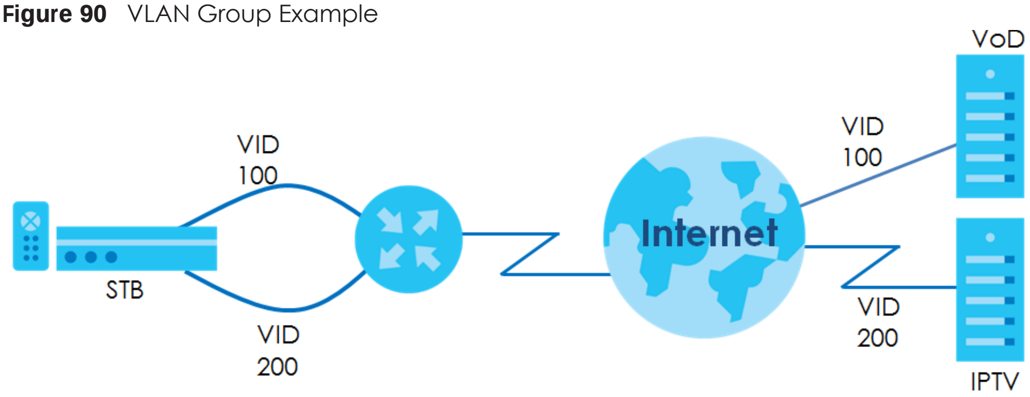
CHAPTER 14 VLAN Group

14.1 Overview

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

In the following example, the EMG 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 can also tag outgoing requests to these servers with these VLAN IDs.

Figure 90 VLAN Group Example



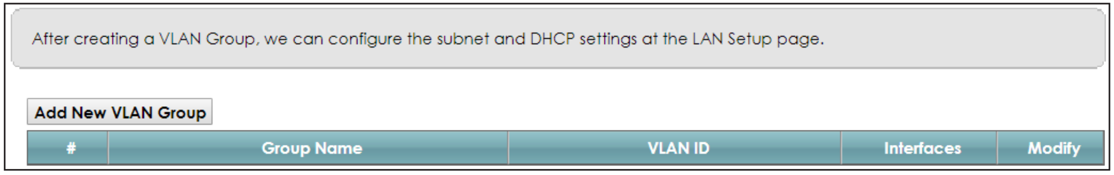
14.1.1 What You Can Do in this Chapter

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

14.2 The VLAN Group Screen

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

Figure 91 Network Setting > Vlan Group



After creating a VLAN Group, we can configure the subnet and DHCP settings at the LAN Setup page.

#	Group Name	VLAN ID	Interfaces	Modify

The following table describes the fields in this screen.

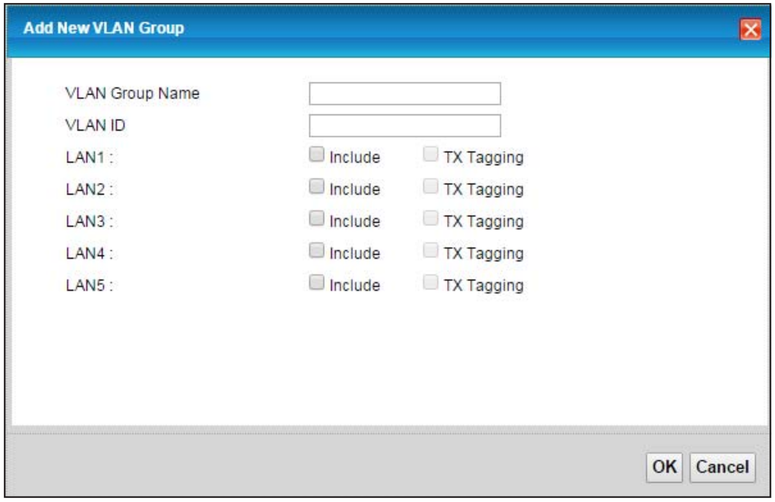
Table 64 Network Setting > Vlan Group

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.

14.2.1 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 92 Add/Edit VLAN Group



Add New VLAN Group

VLAN Group Name

VLAN ID

LAN1 : □ Include □ TX Tagging

LAN2 : □ Include □ TX Tagging

LAN3 : □ Include □ TX Tagging

LAN4 : □ Include □ TX Tagging

LAN5 : □ Include □ TX Tagging

The following table describes the fields in this screen.

Table 65 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 15 Interface Grouping

15.1 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.

15.1.1 What You Can Do in this Chapter

The **Interface Grouping** screens let you create multiple networks on the EMG (Section 15.2 on page 165).

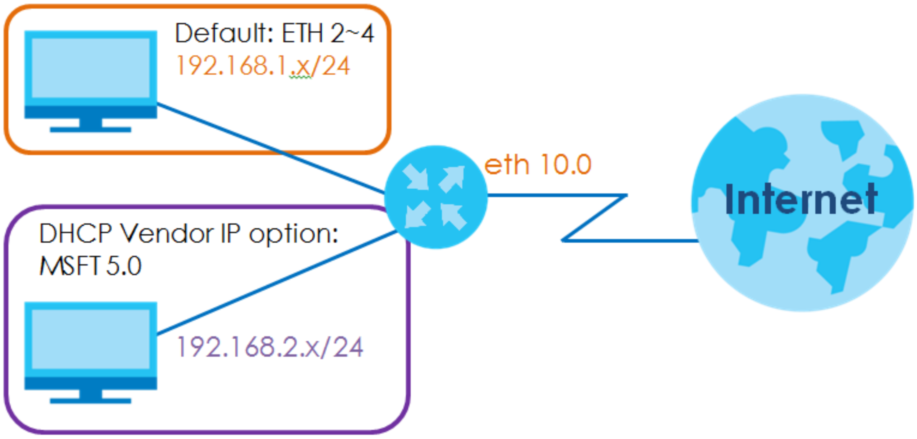
15.2 The Interface Grouping Screen

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 8 on page 98 for more information.

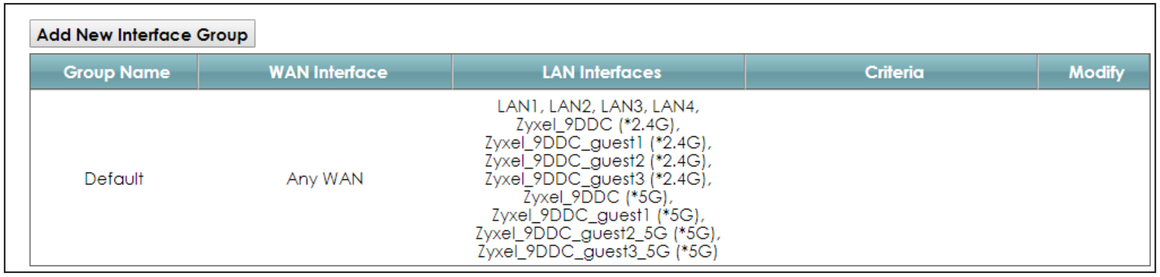
In the following example, the client that sends packets with the DHCP Vendor ID option set to MSFT 5.0 (meaning it is a Windows 2000 DHCP client) is assigned the IP address 192.168.2.2 and uses the WAN eth10.0 interface.

Figure 93 Interface Grouping Application



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

Figure 94 Network Setting > Interface Grouping



Group Name	WAN Interface	LAN Interfaces	Criteria	Modify
Default	Any WAN	LAN1, LAN2, LAN3, LAN4, Zyxel_9DDC (*2.4G), Zyxel_9DDC_guest1 (*2.4G), Zyxel_9DDC_guest2 (*2.4G), Zyxel_9DDC_guest3 (*2.4G), Zyxel_9DDC (*5G), Zyxel_9DDC_guest1 (*5G), Zyxel_9DDC_guest2_5G (*5G), Zyxel_9DDC_guest3_5G (*5G)		

The following table describes the fields in this screen.

Table 66 Network Setting > Interface Grouping

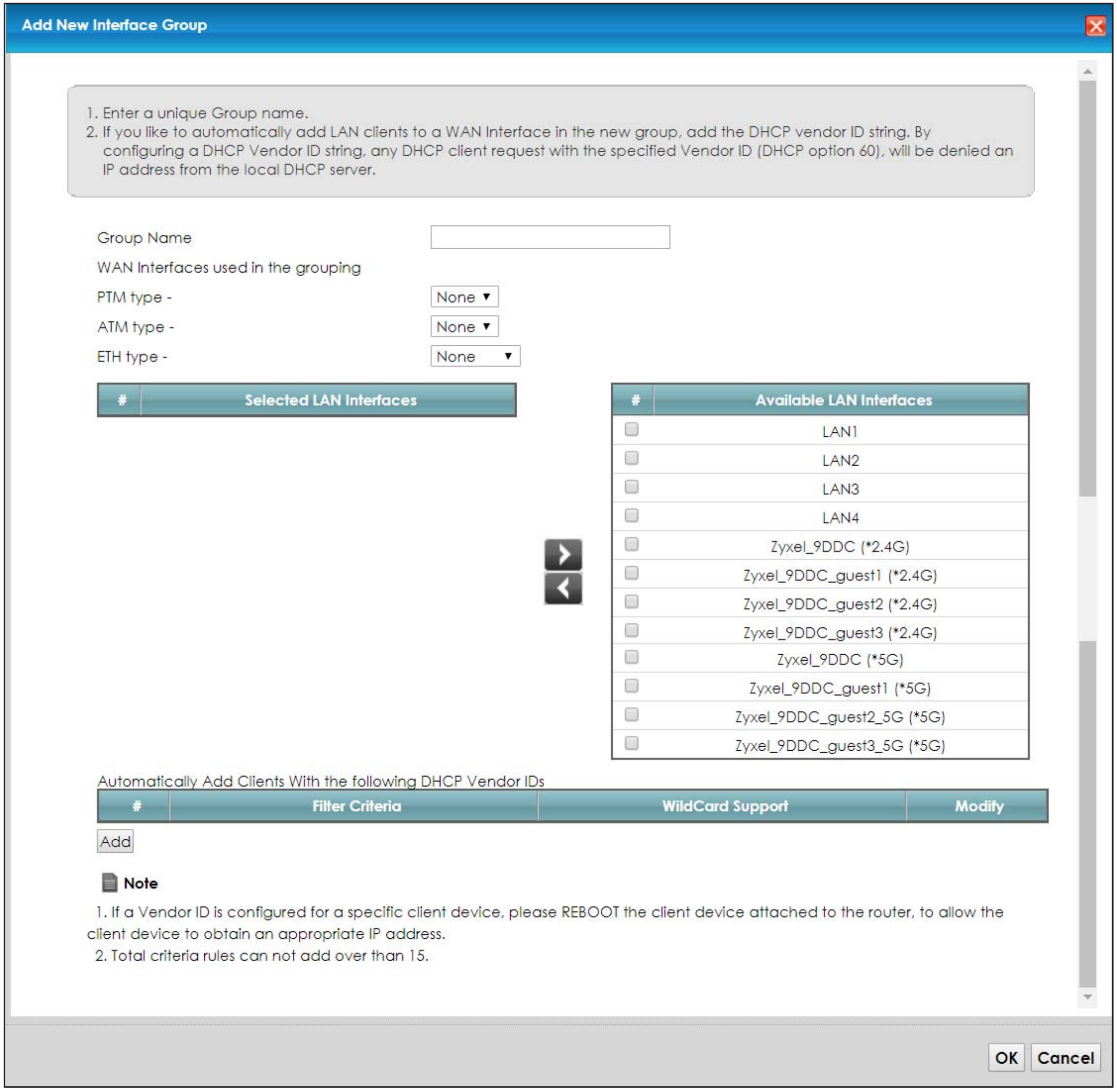
LABEL	DESCRIPTION
Add New Interface Group	Click this button to create a new interface group.
Group Name	This shows the descriptive name of the group.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN interfaces in the group.
Criteria	This shows the filtering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

15.2.1 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 95 Interface Group Configuration



Add New Interface Group

1. Enter a unique Group name.
2. If you like to automatically add LAN clients to a WAN Interface in the new group, add the DHCP vendor ID string. By configuring a DHCP Vendor ID string, any DHCP client request with the specified Vendor ID (DHCP option 60), will be denied an IP address from the local DHCP server.

Group Name

WAN Interfaces used in the grouping

PTM type - None

ATM type - None

ETH type - None

#	Selected LAN Interfaces

#	Available LAN Interfaces
□	LAN1
□	LAN2
□	LAN3
□	LAN4
□	Zyxel_9DDC (*2.4G)
□	Zyxel_9DDC_guest1 (*2.4G)
□	Zyxel_9DDC_guest2 (*2.4G)
□	Zyxel_9DDC_guest3 (*2.4G)
□	Zyxel_9DDC (*5G)
□	Zyxel_9DDC_guest1 (*5G)
□	Zyxel_9DDC_guest2_5G (*5G)
□	Zyxel_9DDC_guest3_5G (*5G)

Automatically Add Clients With the following DHCP Vendor IDs

#	Filter Criteria	WildCard Support	Modify

Note

1. If a Vendor ID is configured for a specific client device, please REBOOT the client device attached to the router, to allow the client device to obtain an appropriate IP address.
2. Total criteria rules can not add over than 15.

The following table describes the fields in this screen.

Table 67 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.
Selected LAN Interfaces Available LAN Interfaces	Select one or more LAN interfaces (Ethernet LAN, HPNA or wireless LAN) in the **Available LAN Interfaces** list and use the left arrow to move them to the **Selected LAN Interfaces** list to add the interfaces to this group. To remove a LAN or wireless LAN interface from the **Selected LAN Interfaces**, use the right-facing arrow.

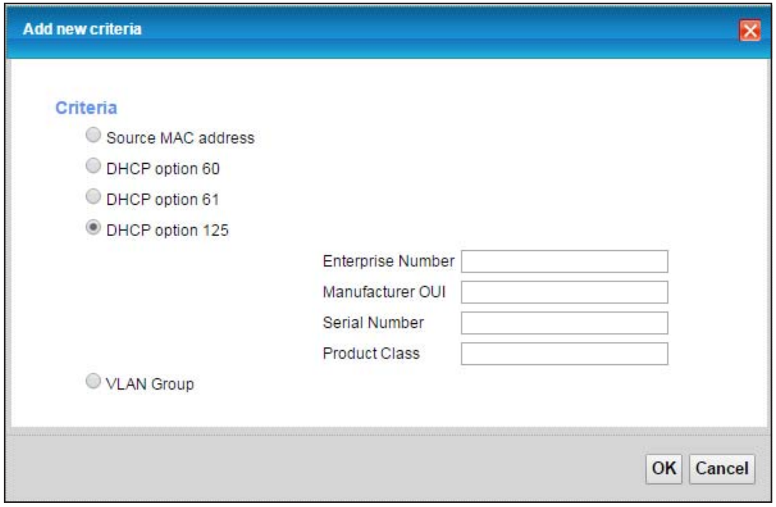
Table 67 Interface Group Configuration (continued)

LABEL	DESCRIPTION
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 15.2.2 on page 168 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.

15.2.2 Interface Grouping Criteria

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

Figure 96 Interface Grouping Criteria



Add new criteria

Criteria

○ Source MAC address

○ DHCP option 60

○ DHCP option 61

● DHCP option 125

Enterprise Number

Manufacturer OUI

Serial Number

Product Class

○ VLAN Group

The following table describes the fields in this screen.

Table 68 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.

Table 68   Interface Grouping Criteria (continued)

LABEL	DESCRIPTION
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 16
Home Connectivity

16.1 Overview

One Connect is a Zyxel-proprietary feature. It complies with the IEEE 1905.1 standard and allows auto-detection and auto-configuration. Auto-configuration enables the Multy-Pro-supported extenders to use the same wireless settings as the controller, the EMG, in a MESH network. See Section 7.7 on page 85 for more information about Zyxel MESH (Multy Pro).

Apart from auto-configuration, you can also check the connection status, do speed test, turn on or turn off the devices in your network, block or allow a device's access and set up a guest Wi-Fi network from the mobile device. You can even use the App to access the EMG's web configurator.

If your wireless router supports Zyxel One Connect, EMG for example, you can download and install the Multy Pro app in your mobile device.

To let the Multy Pro app detect the EMG, the following conditions must be met:

- The mobile device with the App installed must be connected to the EMG wirelessly.
- One Connect is enabled in this screen.

Figure 97 Multy Pro App

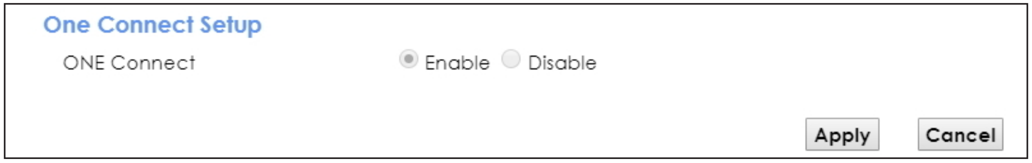
16.2 The Home Connectivity Screen

Use this screen to enable or disable One Connect on the EMG.

Note that when Multy Pro is enabled in the **Network Setting > Wireless > MESH** screen, **One Connect** will be enabled and grayed out automatically. To disable One Connect, please deactivate Multy pro in the **Network Setting > Wireless > MESH** screen.

Click **Network Setting > Home Connectivity** to open the following screen.

Figure 98 Network Setting > Home Connectivity



One Connect Setup

ONE Connect ● Enable ○ Disable

CHAPTER 17
Firewall

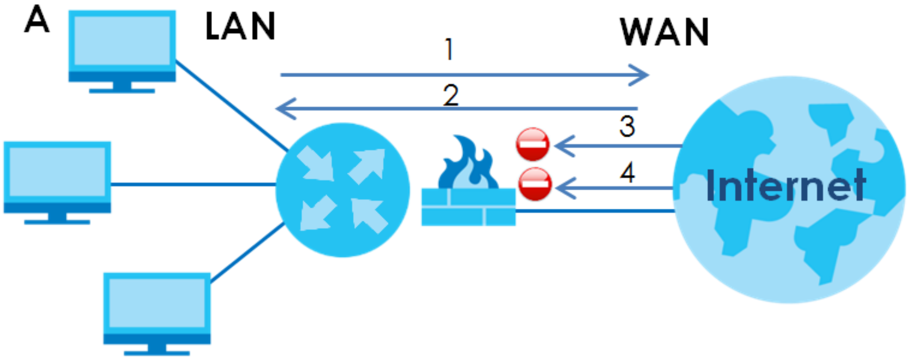
17.1 Overview

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 99 Default Firewall Action



17.1.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the EMG (Section 17.2 on page 172).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 17.3 on page 173).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules (Section 17.4 on page 175).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (.Section 17.5 on page 177).

17.1.2 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

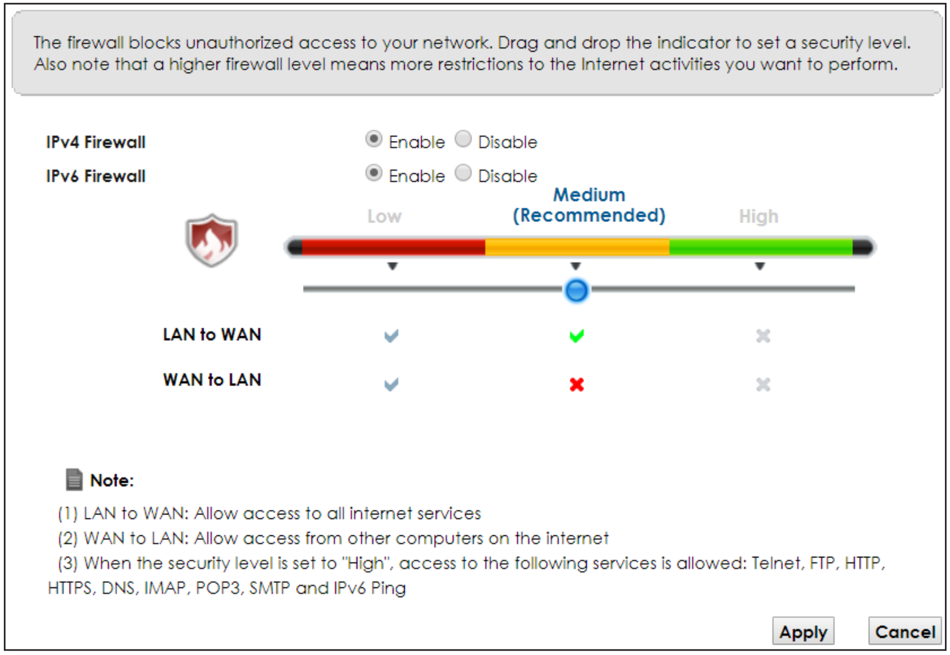
Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

17.2 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 100 Security > Firewall > General



The firewall blocks unauthorized access to your network. Drag and drop the indicator to set a security level. Also note that a higher firewall level means more restrictions to the Internet activities you want to perform.

IPv4 Firewall ● Enable ○ Disable

IPv6 Firewall ● Enable ○ Disable

	Low	Medium (Recommended)	High
LAN to WAN	✓	✓	✗
WAN to LAN	✓	✗	✗

Note:

(1) LAN to WAN: Allow access to all internet services

(2) WAN to LAN: Allow access from other computers on the internet

(3) When the security level is set to "High", access to the following services is allowed: Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP and IPv6 Ping

The following table describes the labels in this screen.

Table 69 Security > Firewall > General

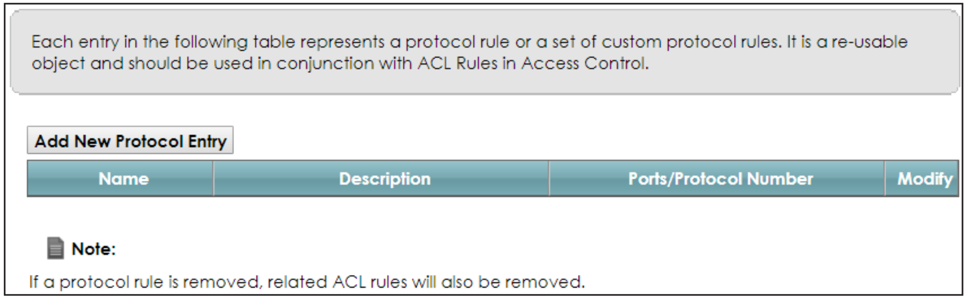
LABEL	DESCRIPTION
Firewall	Select **Enable** to activate the firewall feature on the EMG.
Low	Select **Low** to allow LAN to WAN and WAN to LAN packet directions.
Medium	Select **Medium** to allow LAN to WAN but deny WAN to LAN packet directions.
High	Select **High** to deny LAN to WAN and WAN to LAN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

17.3 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 263 for some examples.

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

Figure 101 Security > Firewall > Protocol



Each entry in the following table represents a protocol rule or a set of custom protocol rules. It is a re-usable object and should be used in conjunction with ACL Rules in Access Control.

Note:

If a protocol rule is removed, related ACL rules will also be removed.

The following table describes the labels in this screen.

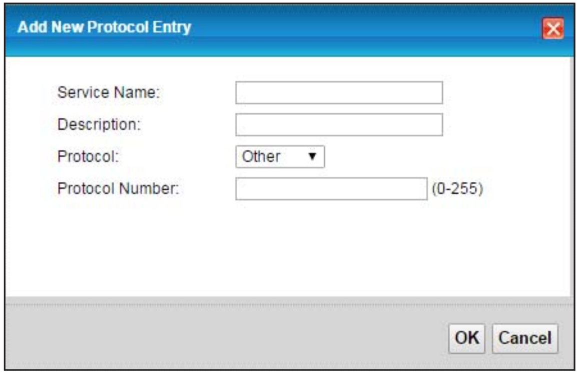
Table 70 Security > Firewall > Protocol

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.

17.3.1 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 102 Security > Firewall > Protocol: Add/Edit



Service Name:	
Description:	
Protocol:	Other ▾
Protocol Number:	(0-255)

The following table describes the labels in this screen.

Table 71 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.

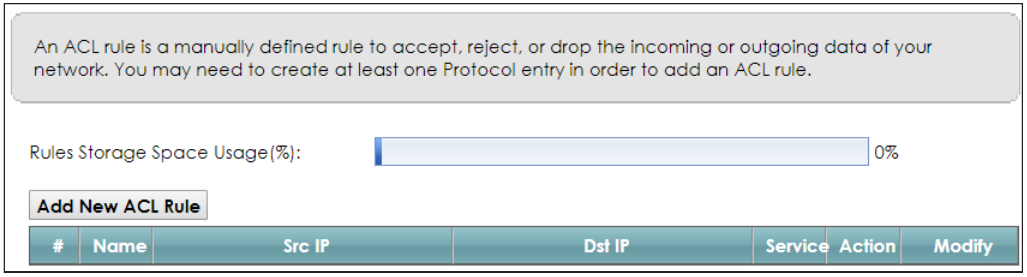
Table 71   Security > Firewall > Protocol: Add/Edit (continued)

LABEL	DESCRIPTION
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.
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.

17.4 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 103   Security > Firewall > Access Control



An ACL rule is a manually defined rule to accept, reject, or drop the incoming or outgoing data of your network. You may need to create at least one Protocol entry in order to add an ACL rule.

Rules Storage Space Usage(%): 0%

The following table describes the labels in this screen.

Table 72   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.

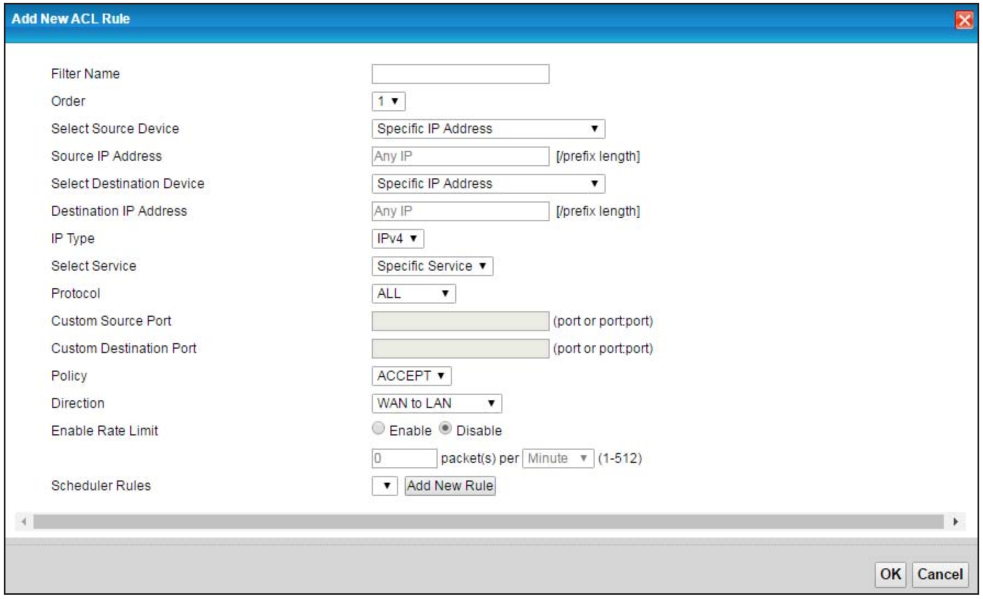
Table 72 Security > Firewall > Access Control (continued)

LABEL	DESCRIPTION
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.

17.4.1 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 104 Access Control: Add/Edit



Add New ACL Rule

Filter Name	
Order	1
Select Source Device	Specific IP Address
Source IP Address	Any IP [/prefix length]
Select Destination Device	Specific IP Address
Destination IP Address	Any IP [/prefix length]
IP Type	IPv4
Select Service	Specific Service
Protocol	ALL
Custom Source Port	(port or port:port)
Custom Destination Port	(port or port:port)
Policy	ACCEPT
Direction	WAN to LAN
Enable Rate Limit	○ Enable ● Disable
	0 packet(s) per Minute (1-512)
Scheduler Rules	Add New Rule

The following table describes the labels in this screen.

Table 73 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.

Table 73 Access Control: Add/Edit (continued)

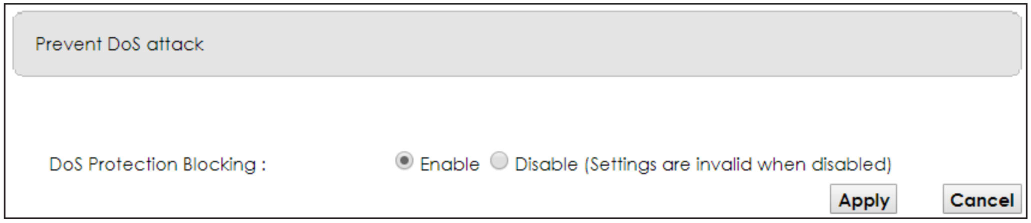
LABEL	DESCRIPTION
Destination IP Address	Enter the destination IP address.
IP Type	Select whether your IP type is **IPv4** or **IPv6**.
Select Service	Select the transport layer protocol that defines your customized port from the drop-down list box. If you want to configure a customized protocol, select **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.
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 this check box 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.

17.5 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 105 Security > Firewall > DoS



Prevent DoS attack

DoS Protection Blocking : ● Enable ○ Disable (Settings are invalid when disabled)

The following table describes the labels in this screen.

Table 74 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 18
MAC Filter

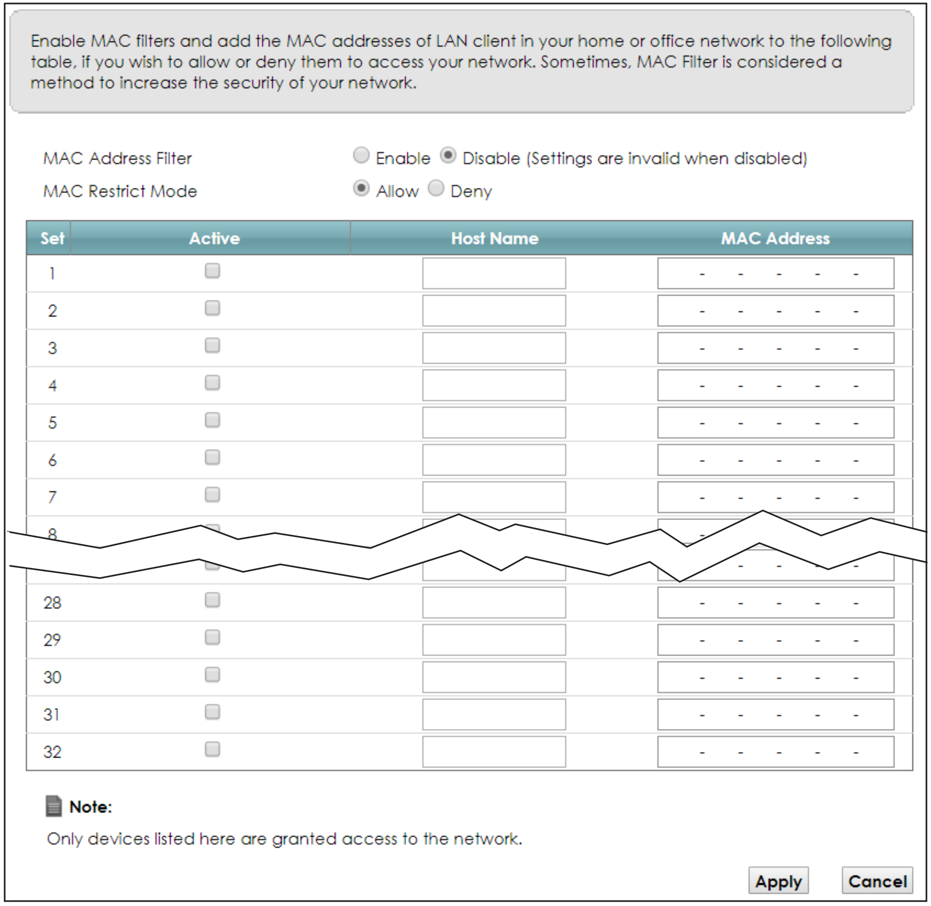
18.1 Overview

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.

18.2 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 106 Security > MAC Filter



Enable MAC filters and add the MAC addresses of LAN client in your home or office network to the following table, if you wish to allow or deny them to access your network. Sometimes, MAC Filter is considered a method to increase the security of your network.

MAC Address Filter ○ Enable ● Disable (Settings are invalid when disabled)

MAC Restrict Mode ● Allow ○ Deny

Set	Active	Host Name	MAC Address
1	□		- - - - -
2	□		- - - - -
3	□		- - - - -
4	□		- - - - -
5	□		- - - - -
6	□		- - - - -
7	□		- - - - -
8	□		- - - - -
28	□		- - - - -
29	□		- - - - -
30	□		- - - - -
31	□		- - - - -
32	□		- - - - -

Note:

Only devices listed here are granted access to the network.

The following table describes the labels in this screen.

Table 75 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 19
Parental Control

19.1 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.

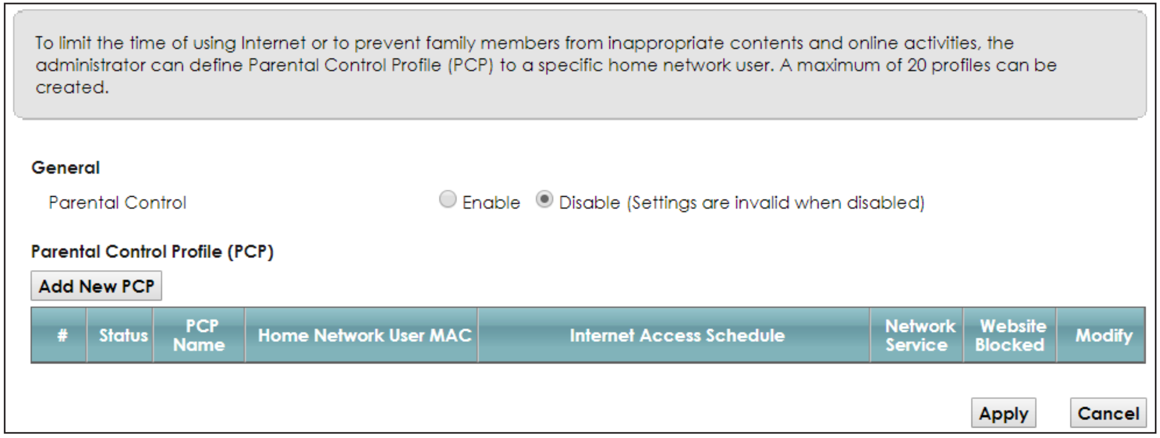
19.2 The Parental Control Screen

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

Note: When One Connect (See Chapter 16 on page 170) and MESH (See Section 7.7 on page 85) are enabled, the EMG automatically turn parental control off and gray it out. You can disable them if you want to use parental control.

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

Figure 107 Security > Parental Control



To limit the time of using Internet or to prevent family members from inappropriate contents and online activities, the administrator can define Parental Control Profile (PCP) to a specific home network user. A maximum of 20 profiles can be created.

General

Parental Control ○ Enable ● Disable (Settings are invalid when disabled)

Parental Control Profile (PCP)

#	Status	PCP Name	Home Network User MAC	Internet Access Schedule	Network Service	Website Blocked	Modify

The following table describes the fields in this screen.

Table 76 Security > Parental Control

LABEL	DESCRIPTION
Parental Control	Select **Enable** to activate parental control.
Add New PCP	Click this if you want to configure a new Parental Control Profile (PCP).
#	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.

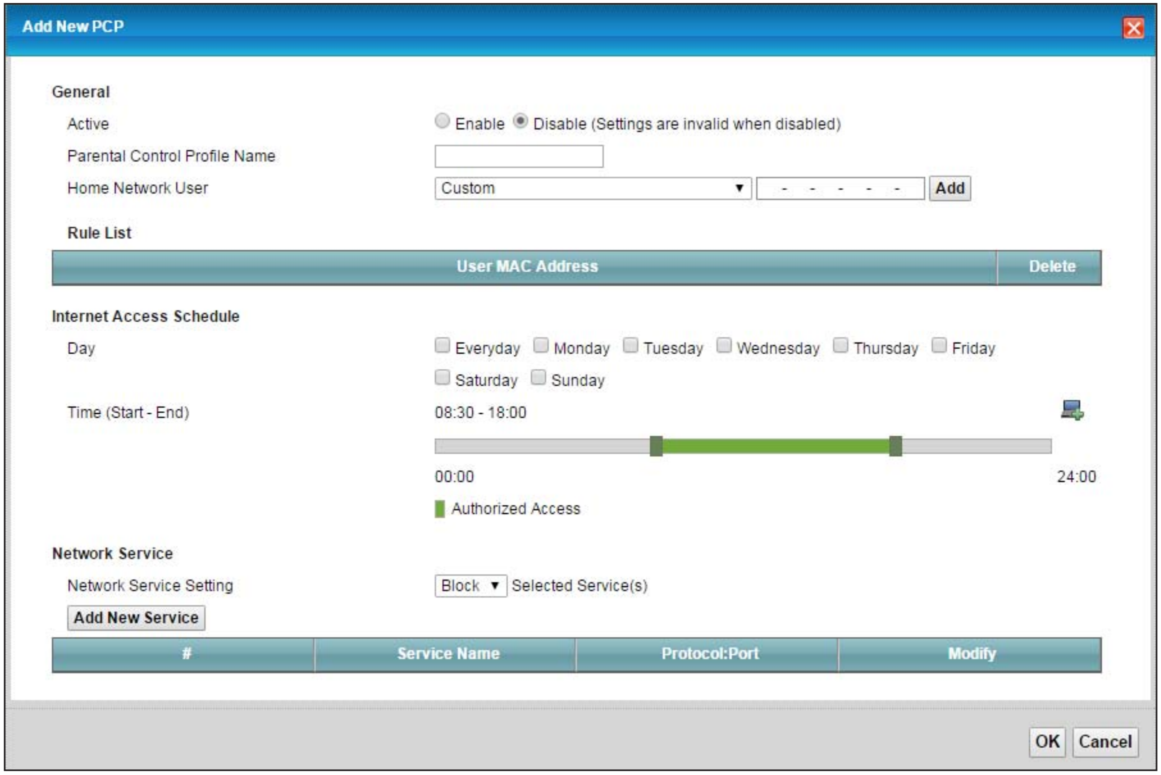
Table 76 Security > Parental Control (continued)

LABEL	DESCRIPTION
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.
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.

19.2.1 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 108 Parental Control Rule: Add/Edit Rule



Add New PCP

General

Active: ○ Enable ● Disable (Settings are invalid when disabled)

Parental Control Profile Name:

Home Network User: Custom ▼ - - - - - Add

Rule List

User MAC Address	Delete

Internet Access Schedule

Day: □ Everyday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

Time (Start - End): 08:30 - 18:00

00:00 24:00

🟩 Authorized Access

Network Service

Network Service Setting: Block ▼ Selected Service(s)

Add New Service

#	Service Name	Protocol:Port	Modify

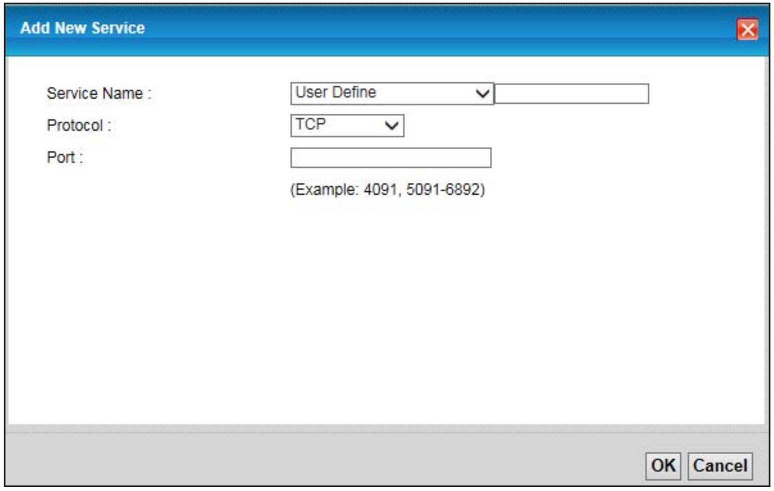
The following table describes the fields in this screen.

Table 77 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 blocks access to all the network services listed below. If you select **Allow**, the EMG blocks access to all the network services 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 **Port** 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.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

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

Figure 109 Parental Control Rule: Add/Edit Rule > Add New Service



Add New Service

Service Name : User Define

Protocol : TCP

Port :

(Example: 4091, 5091-6892)

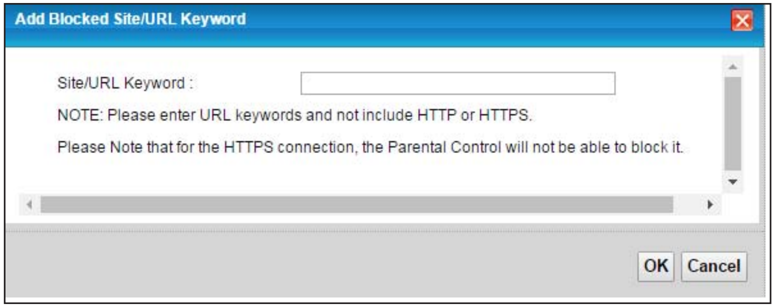
The following table describes the fields in this screen.

Table 78 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 110 Parental Control Rule: Add/Edit Rule > Add Keyword



Add Blocked Site/URL Keyword

Site/URL Keyword :

NOTE: Please enter URL keywords and not include HTTP or HTTPS.

Please Note that for the HTTPS connection, the Parental Control will not be able to block it.

The following table describes the fields in this screen.

Table 79 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 20 Scheduler Rule

20.1 Overview

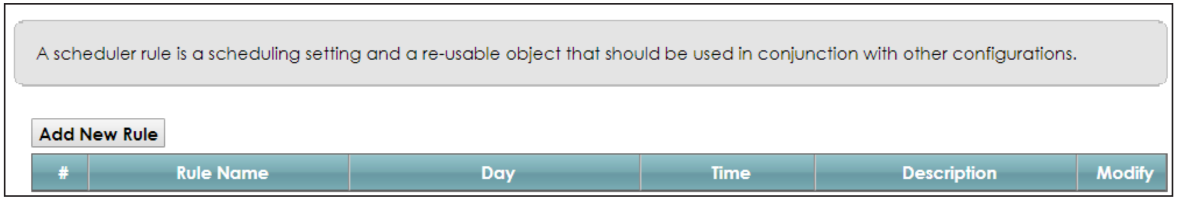
You can define time periods and days during which the EMG performs scheduled rules of certain features (such as Firewall Access Control) in the **Scheduler Rule** screen.

20.2 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 111 Security > Scheduler Rule



A scheduler rule is a scheduling setting and a re-usable object that should be used in conjunction with other configurations.

The following table describes the fields in this screen.

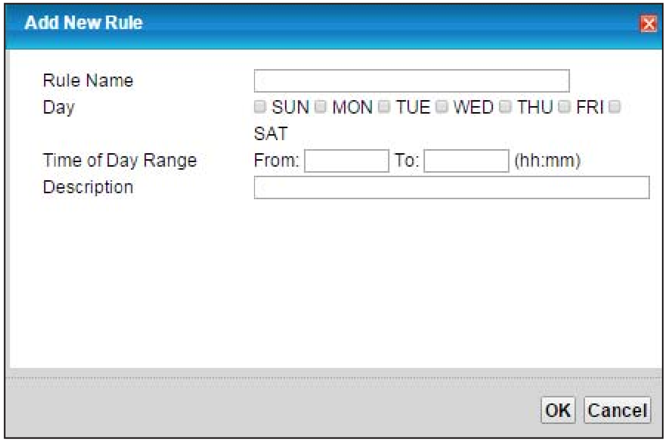
Table 80 Security > Scheduler Rule

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.

20.2.1 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 112 Scheduler Rule: Add/Edit



The following table describes the fields in this screen.

Table 81 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 21 Certificates

21.1 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.

21.1.1 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 21.4 on page 190).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the EMG (Section 21.4 on page 190).

21.2 What You Need to Know

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

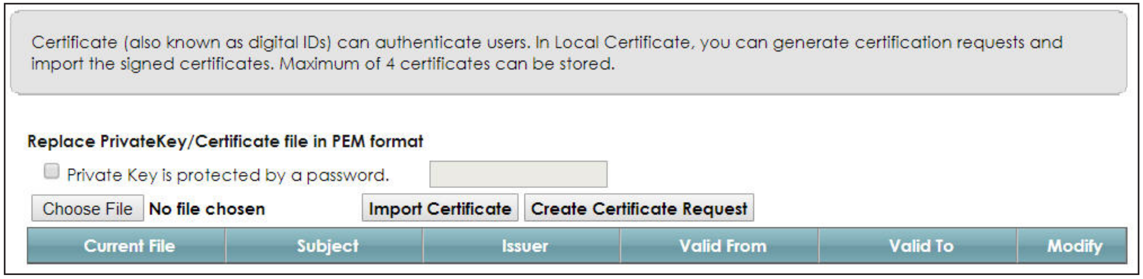
Certification Authority

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.

21.3 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 113 Security > Certificates > Local Certificates



Certificate (also known as digital IDs) can authenticate users. In Local Certificate, you can generate certification requests and import the signed certificates. Maximum of 4 certificates can be stored.

Replace PrivateKey/Certificate file in PEM format

☐ Private Key is protected by a password.

Current File	Subject	Issuer	Valid From	Valid To	Modify

The following table describes the labels in this screen.

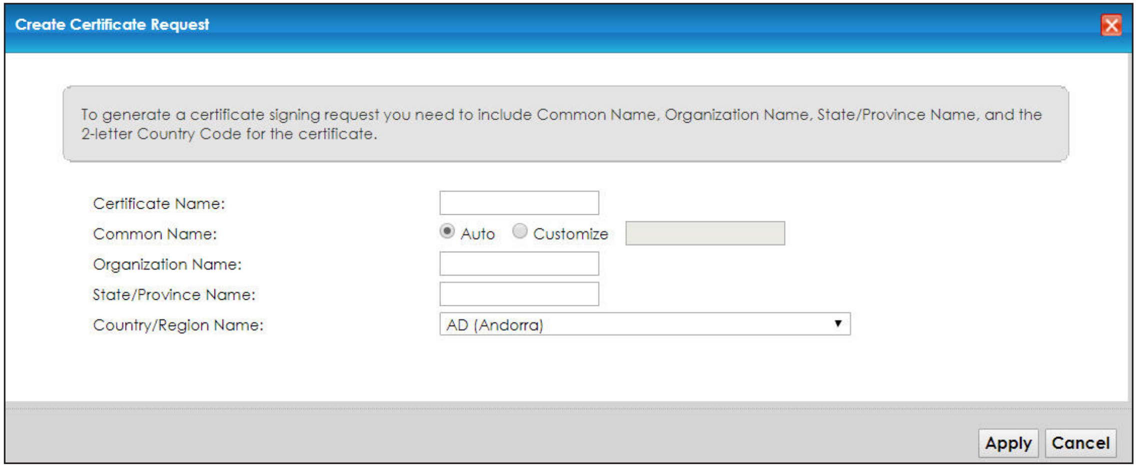
Table 82 Security > Certificates > Local Certificates

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.

21.3.1 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 114 Create Certificate Request



Create Certificate Request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:	
Common Name:	● Auto ○ Customize
Organization Name:	
State/Province Name:	
Country/Region Name:	AD (Andorra)

The following table describes the labels in this screen.

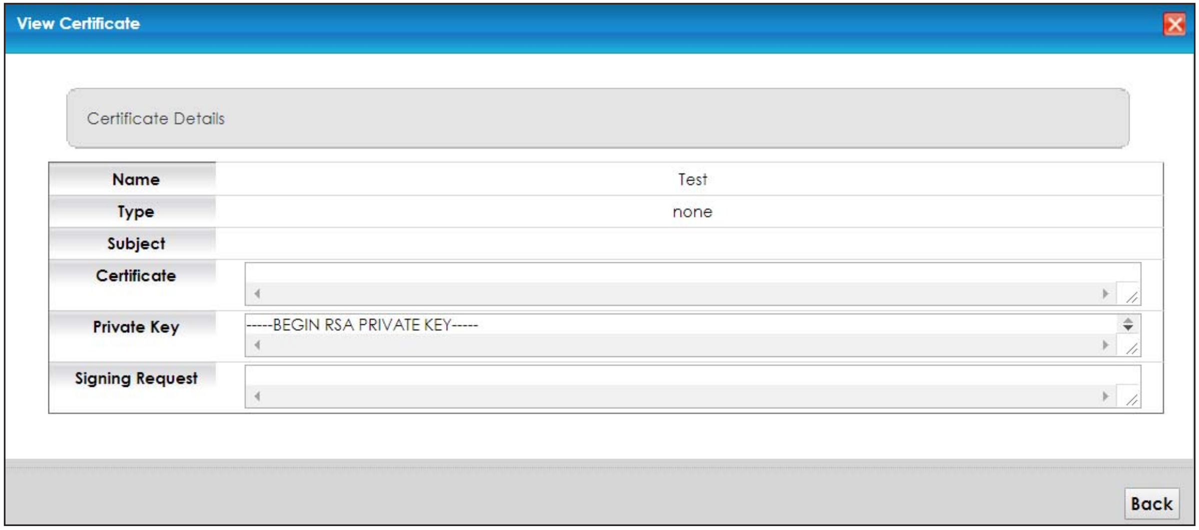
Table 83 Create Certificate Request

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.

21.3.2 View Certificate Request

Click the **View** icon in the **Local Certificates** screen to open the following screen. Use this screen to view in-depth information about the certificate request.

Figure 115 Certificate Request: View



Name	Test
Type	none
Subject	
Certificate	
Private Key	-----BEGIN RSA PRIVATE KEY-----
Signing Request	

The following table describes the fields in this screen.

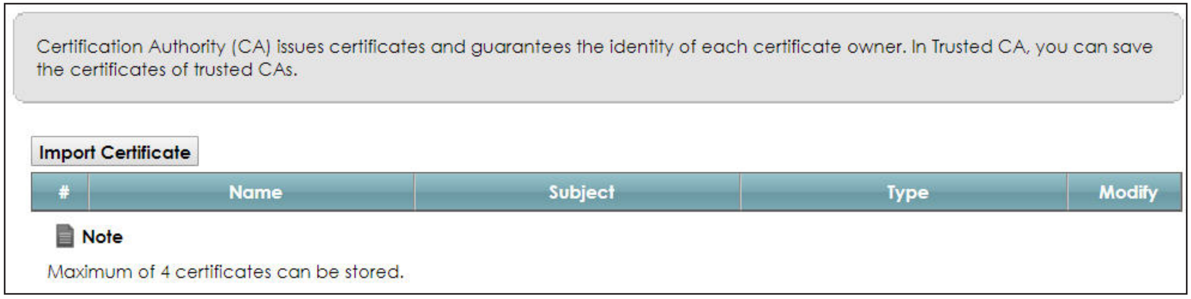
Table 84 Certificate Request: View

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).
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).
Private Key	This field displays the private key of this certificate.
Signing Request	This field displays the CSR (Certificate Signing Request) information of this certificate. The CSR will be provided to a certificate authority, and it includes information about the public key, organization name, domain name, location, and country of this certificate.
Back	Click **Back** to return to the previous screen.

21.4 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 116 Security > Certificates > Trusted CA



Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. In Trusted CA, you can save the certificates of trusted CAs.

Maximum of 4 certificates can be stored.

The following table describes the fields in this screen.

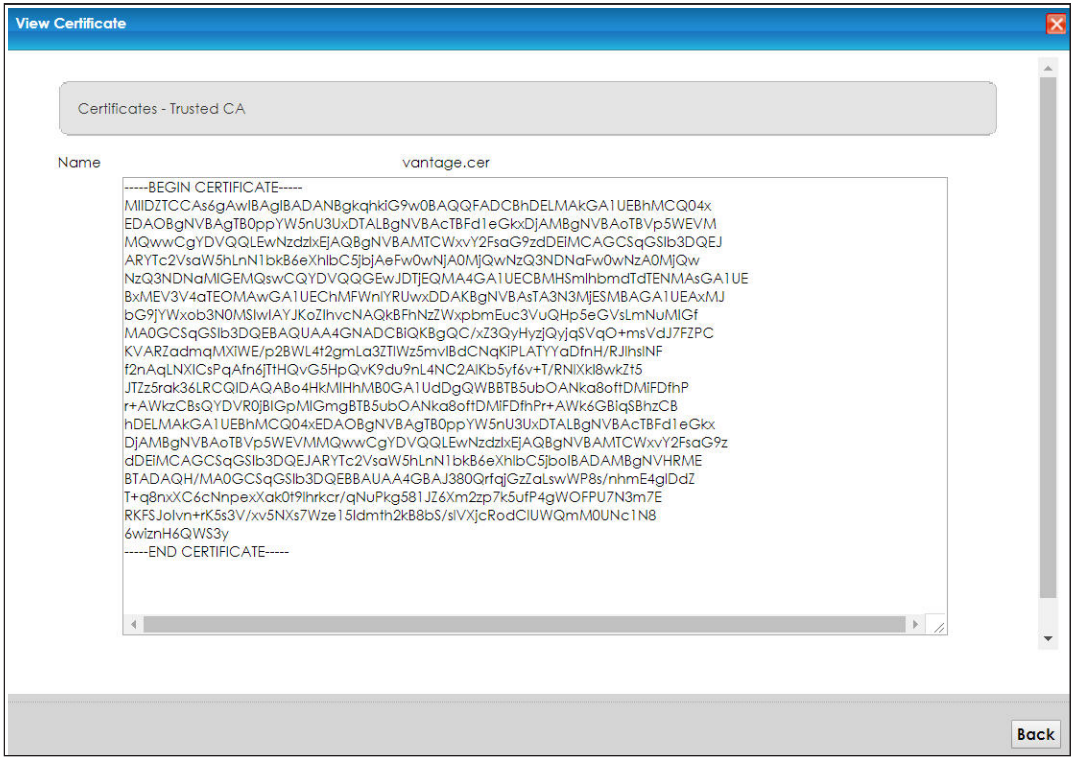
Table 85 Security > Certificates > Trusted CA

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.

21.4.1 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 117 Trusted CA: View



Name vantage.cer

```
-----BEGIN CERTIFICATE-----
MIIDZTCCAs6gAwIBAgIBADANBgkqhkiG9w0BAQQFADCBhDELMAkGA1UEBhMCQ04x
EDAOBgNVBAgTB0ppYW5nU3UxDTALBgNVBAcTBFd1eGkxDjAMBgNVBAoTBVp5WEVM
MQwwCgYDVQQLEwNzdzIxEjAQBgNVBAMTCWxvY2FsaG9zdDEiMCAGCSqGSIb3DQEJ
ARYTc2VsaW5hLnN1bkB6eXhlbC5jbjAeFw0wNjA0MjQwNzQ3NDNaFw0wNzA0MjQw
NzQ3NDNaMIGEMQswCQYDVQQGEwJDTjEQMA4GA1UECBMHSmlhbmdTdTENMAsGA1UE
BxMEV3V4aTEOMAwGA1UEChMFWnlYRUwxDDAKBgNVBAsTA3N3MjESMBAGA1UEAxMJ
bG9jYWxob3N0MSIwIAYJKoZIhvcNAQkBFhNzZWxpbmEuc3VuQHp5eGVsLmNuMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/xZ3QyHyzjQyjqSVqO+msVdJ7FZPC
KVARZadmqMXiWE/p2BWL4t2gmLa3ZTlWz5mvlBdCNqKiPLATYYaDfnH/RJlhsINF
f2nAqLNXICsPqAfn6jTtHQvG5HpQvK9du9nL4NC2AlKb5yf6v+T/RNlXkl8wkZt5
JTZz5rak36LRCQIDAQABo4HkMIHhMB0GA1UdDgQWBBTB5ubOANka8oftDMiFDfhP
r+AWkzCBsQYDVR0jBIGpMIGmgBTB5ubOANka8oftDMiFDfhPr+AWk6GBiqSBhzCB
hDELMAkGA1UEBhMCQ04xEDAOBgNVBAgTB0ppYW5nU3UxDTALBgNVBAcTBFd1eGkx
DjAMBgNVBAoTBVp5WEVMMQwwCgYDVQQLEwNzdzIxEjAQBgNVBAMTCWxvY2FsaG9z
dDEiMCAGCSqGSIb3DQEJARYTc2VsaW5hLnN1bkB6eXhlbC5jboIBADAMBgNVHRME
BTADAQH/MA0GCSqGSIb3DQEBBAUAA4GBAJ380QrfqjGzZaLswWP8s/nhmE4gIDdZ
T+q8nxXC6cNnpexXak0t9Ihrkcr/qNuPkg581JZ6Xm2zp7k5ufP4gWOFPU7N3m7E
RKFSJoIvn+rK5s3V/xv5NXs7Wze15Idmth2kB8bS/sIVXjcRodClUWQmM0UNc1N8
6wiznH6QWS3y
-----END CERTIFICATE-----
```

The following table describes the fields in this screen.

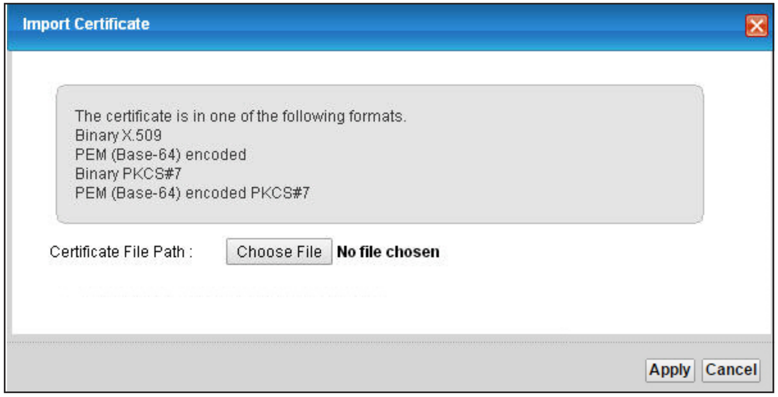
Table 86 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this 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.

21.4.2 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 118 Trusted CA: Import Certificate



The certificate is in one of the following formats.
Binary X.509
PEM (Base-64) encoded
Binary PKCS#7
PEM (Base-64) encoded PKCS#7

Certificate File Path : Choose File No file chosen

The following table describes the fields in this screen.

Table 87 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 22
Log

22.1 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.

22.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs (Section 22.2 on page 195).
- Use the **Security Log** screen to see the security-related logs for the categories that you select (Section 22.3 on page 195).

22.1.2 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 88 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.

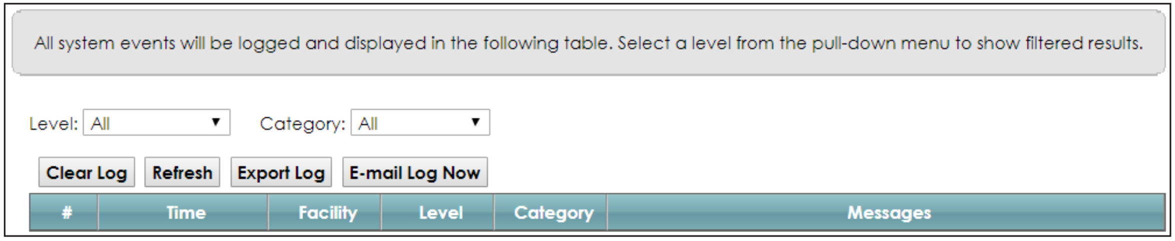
Table 88 Syslog Severity Levels

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.

22.2 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 119 System Monitor > Log > System Log



All system events will be logged and displayed in the following table. Select a level from the pull-down menu to show filtered results.

Level: All ▾ Category: All ▾

The following table describes the fields in this screen.

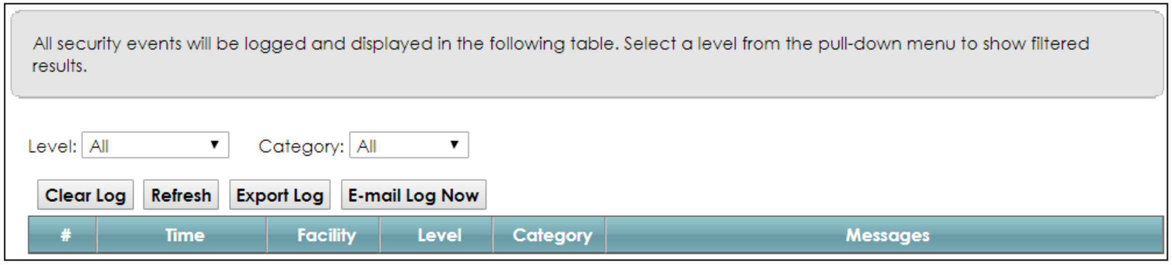
Table 89 System Monitor > Log > System Log

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.

22.3 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 120 System Monitor > Log > Security Log



All security events will be logged and displayed in the following table. Select a level from the pull-down menu to show filtered results.

The following table describes the fields in this screen.

Table 90 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 23 Traffic Status

23.1 Overview

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

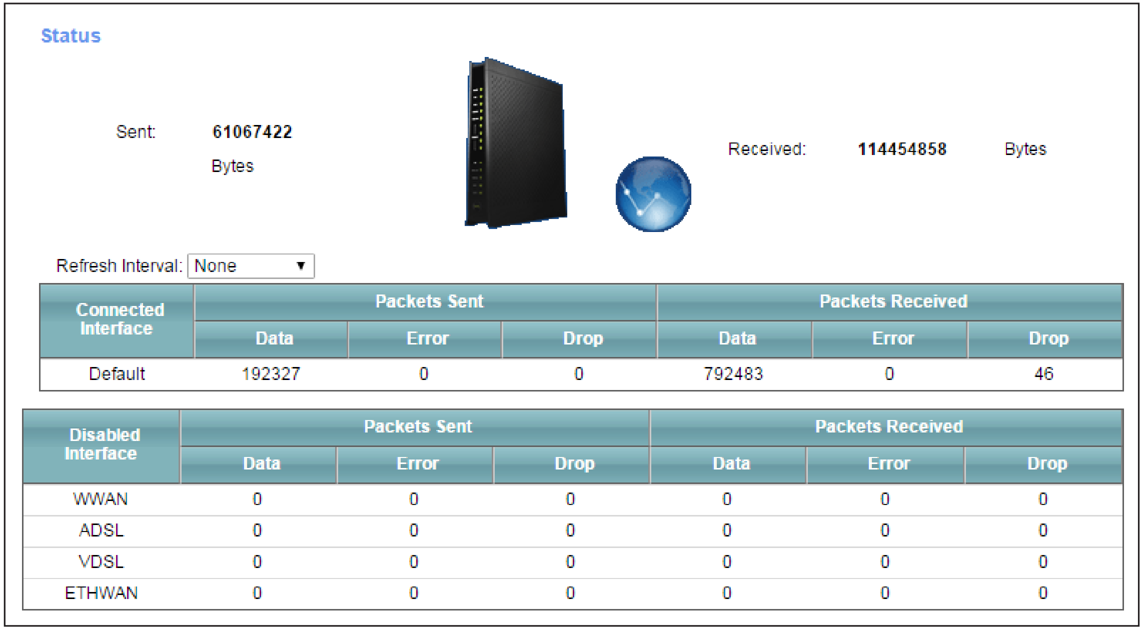
23.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 23.2 on page 197).
- Use the **LAN** screen to view the LAN traffic statistics (Section 23.3 on page 198).
- Use the **NAT** screen to view the NAT status of the EMG's client(s) (Section 23.4 on page 199)

23.2 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 121 System Monitor > Traffic Status > WAN



Status

Sent: **61067422** Bytes

Received: **114454858** Bytes

Refresh Interval: None ▾

Connected Interface	Packets Sent			Packets Received		
	Data	Error	Drop	Data	Error	Drop
Default	192327	0	0	792483	0	46

Disabled Interface	Packets Sent			Packets Received		
	Data	Error	Drop	Data	Error	Drop
WWAN	0	0	0	0	0	0
ADSL	0	0	0	0	0	0
VDSL	0	0	0	0	0	0
ETHWAN	0	0	0	0	0	0

The following table describes the fields in this screen.

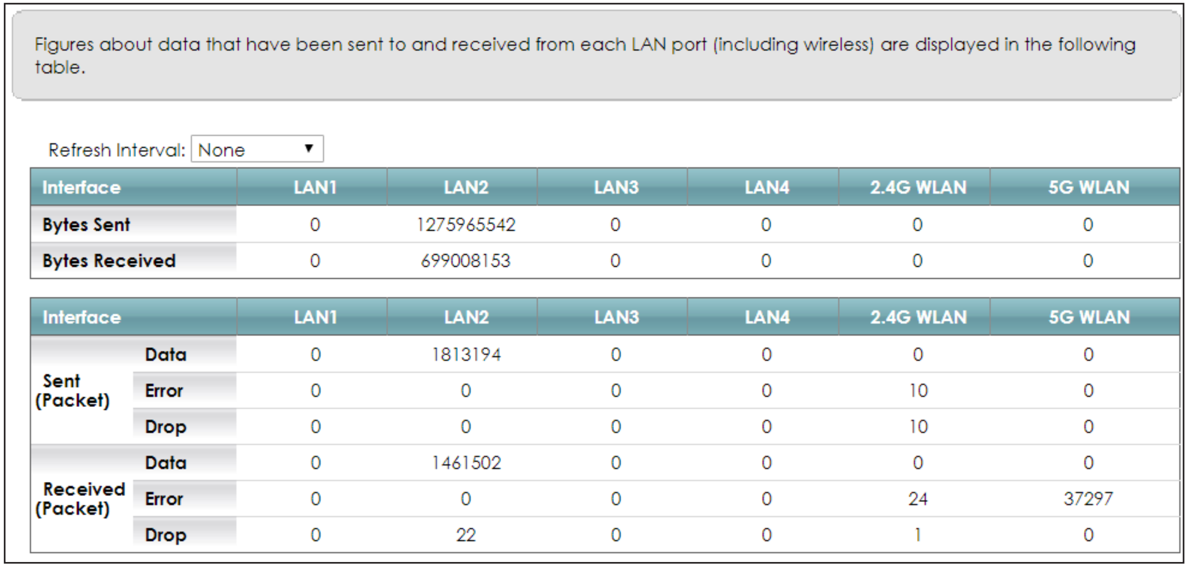
Table 91 System Monitor > Traffic Status > WAN

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	
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.

23.3 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 122 System Monitor > Traffic Status > LAN



Figures about data that have been sent to and received from each LAN port (including wireless) are displayed in the following table.

Refresh Interval: None

Interface	LAN1	LAN2	LAN3	LAN4	2.4G WLAN	5G WLAN
Bytes Sent	0	1275965542	0	0	0	0
Bytes Received	0	699008153	0	0	0	0

Interface		LAN1	LAN2	LAN3	LAN4	2.4G WLAN	5G WLAN
Sent (Packet)	Data	0	1813194	0	0	0	0
	Error	0	0	0	0	10	0
	Drop	0	0	0	0	10	0
Received (Packet)	Data	0	1461502	0	0	0	0
	Error	0	0	0	0	24	37297
	Drop	0	22	0	0	1	0

The following table describes the fields in this screen.

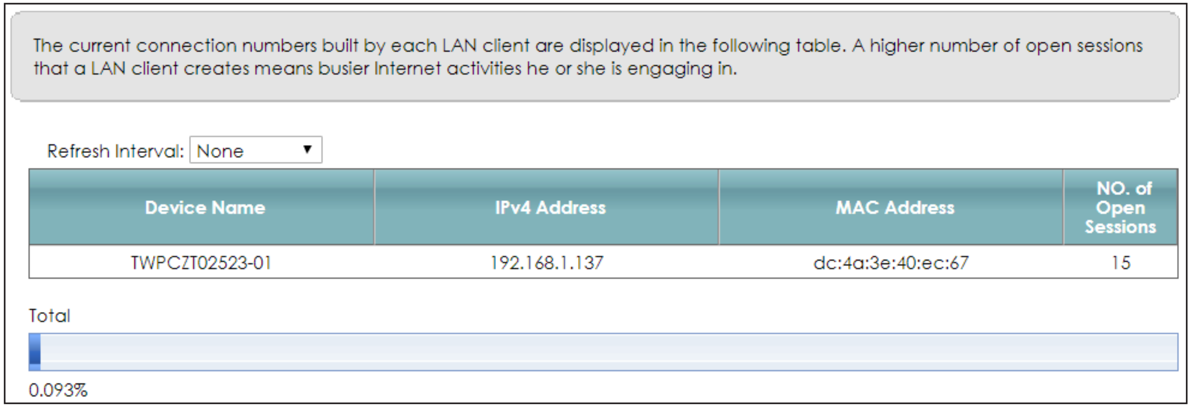
Table 92 System Monitor > Traffic Status > LAN

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.
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.

23.4 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 123 System Monitor > Traffic Status > NAT



The current connection numbers built by each LAN client are displayed in the following table. A higher number of open sessions that a LAN client creates means busier Internet activities he or she is engaging in.

Refresh Interval: None

Device Name	IPv4 Address	MAC Address	NO. of Open Sessions
TWPCZT02523-01	192.168.1.137	dc:4a:3e:40:ec:67	15

Total

0.093%

The following table describes the fields in this screen.

Table 93 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 24
ARP Table

24.1 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.

24.1.1 How ARP Works

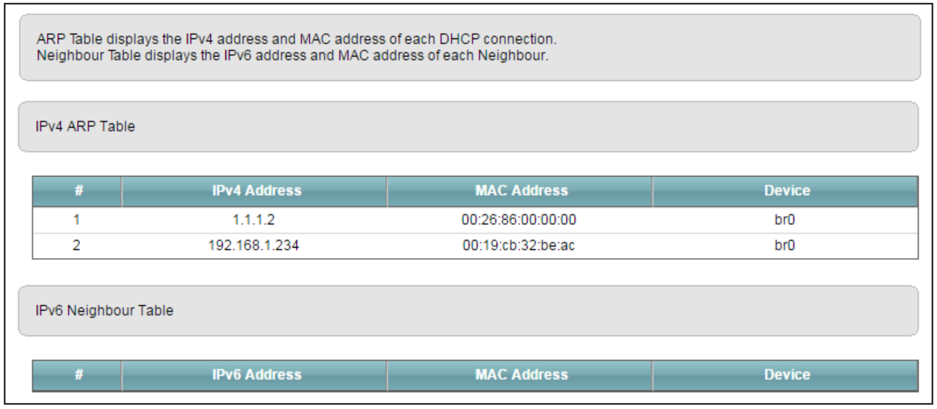
When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

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.

24.2 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 124 System Monitor > ARP Table



ARP Table displays the IPv4 address and MAC address of each DHCP connection.
Neighbour Table displays the IPv6 address and MAC address of each Neighbour.

IPv4 ARP Table

#	IPv4 Address	MAC Address	Device
1	1.1.1.2	00:26:86:00:00:00	br0
2	192.168.1.234	00:19:cb:32:be:ac	br0

IPv6 Neighbour Table

#	IPv6 Address	MAC Address	Device

The following table describes the labels in this screen.

Table 94 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 25
Routing Table

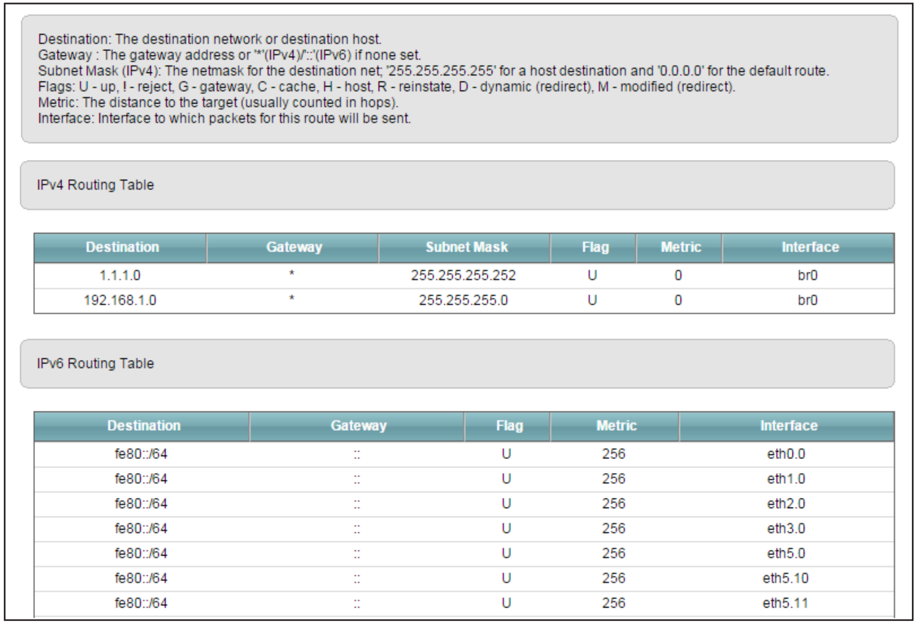
25.1 Overview

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

25.2 The Routing Table Screen

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

Figure 125 System Monitor > Routing Table



Destination: The destination network or destination host.
Gateway : The gateway address or '*'(IPv4)/'::'(IPv6) if none set.
Subnet Mask (IPv4): The netmask for the destination net; '255.255.255.255' for a host destination and '0.0.0.0' for the default route.
Flags: U - up, ! - reject, G - gateway, C - cache, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect).
Metric: The distance to the target (usually counted in hops).
Interface: Interface to which packets for this route will be sent.

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 95 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 95 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. **ethx** indicates an Ethernet WAN interface using IPoE or in bridge mode. **ppp0** indicates a WAN interface using PPPoE or PPPoA.

CHAPTER 26
Multicast Status

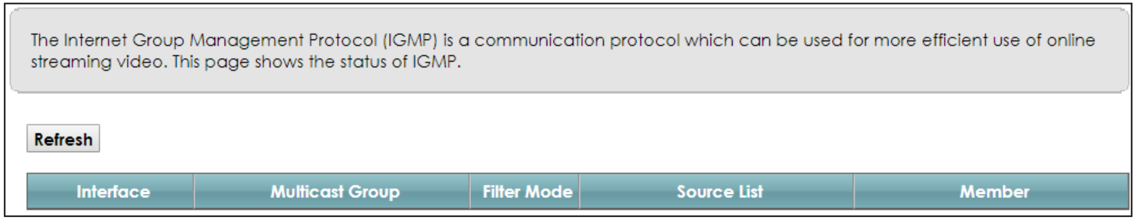
26.1 Overview

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

26.2 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 126 System Monitor > Multicast Status > IGMP Status



The Internet Group Management Protocol (IGMP) is a communication protocol which can be used for more efficient use of online streaming video. This page shows the status of IGMP.

Interface	Multicast Group	Filter Mode	Source List	Member

The following table describes the labels in this screen.

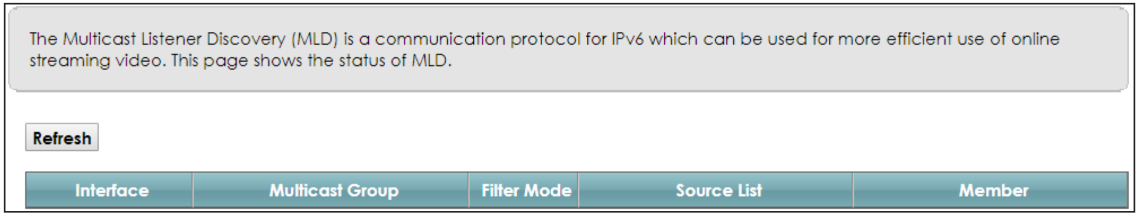
Table 96 System Monitor > Multicast Status > IGMP Status

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.

26.3 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 127 System Monitor > Multicast Status > MLD Status



The Multicast Listener Discovery (MLD) is a communication protocol for IPv6 which can be used for more efficient use of online streaming video. This page shows the status of MLD.

The following table describes the labels in this screen.

Table 97 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 27 System

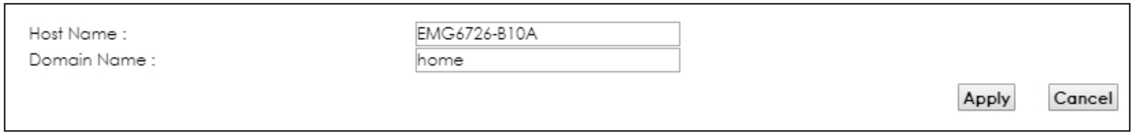
27.1 Overview

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

27.2 The System Screen

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

Figure 128 Maintenance > System



Host Name : EMG6726-B10A

Domain Name : home

The following table describes the labels in this screen.

Table 98 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 28
User Account

28.1 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.

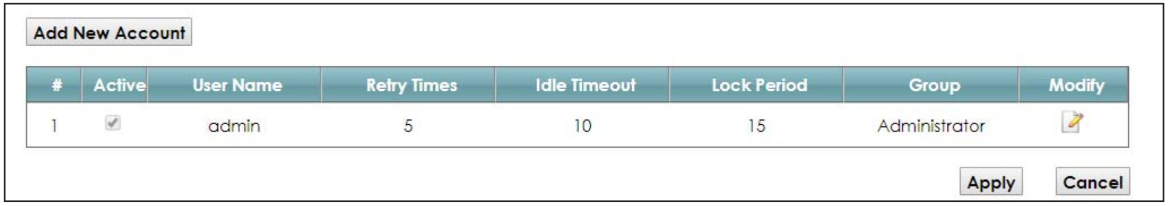
You can create and manage multiple login accounts for your EMG. ‘Admin’ and ‘user’ accounts have different configuration privileges. You can only use an ‘admin’ account to modify or delete a user account. You cannot delete an ‘admin’ account.

For troubleshooting purposes only, there is a support account for qualified technical support engineers. For details about this account, please contact your service provider.

28.2 The User Account Screen

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

Figure 129 Maintenance > User Account



Add New Account

#	Active	User Name	Retry Times	Idle Timeout	Lock Period	Group	Modify
1	☑	admin	5	10	15	Administrator	✎

Apply Cancel

The following table describes the labels in this screen.

Table 99 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account.
#	This is the index number
Active	This field indicates whether the user account is active or not. Clear the check box to disable the user account. Select the check box to enable it.
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.
Idle Timeout	This field displays 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**.

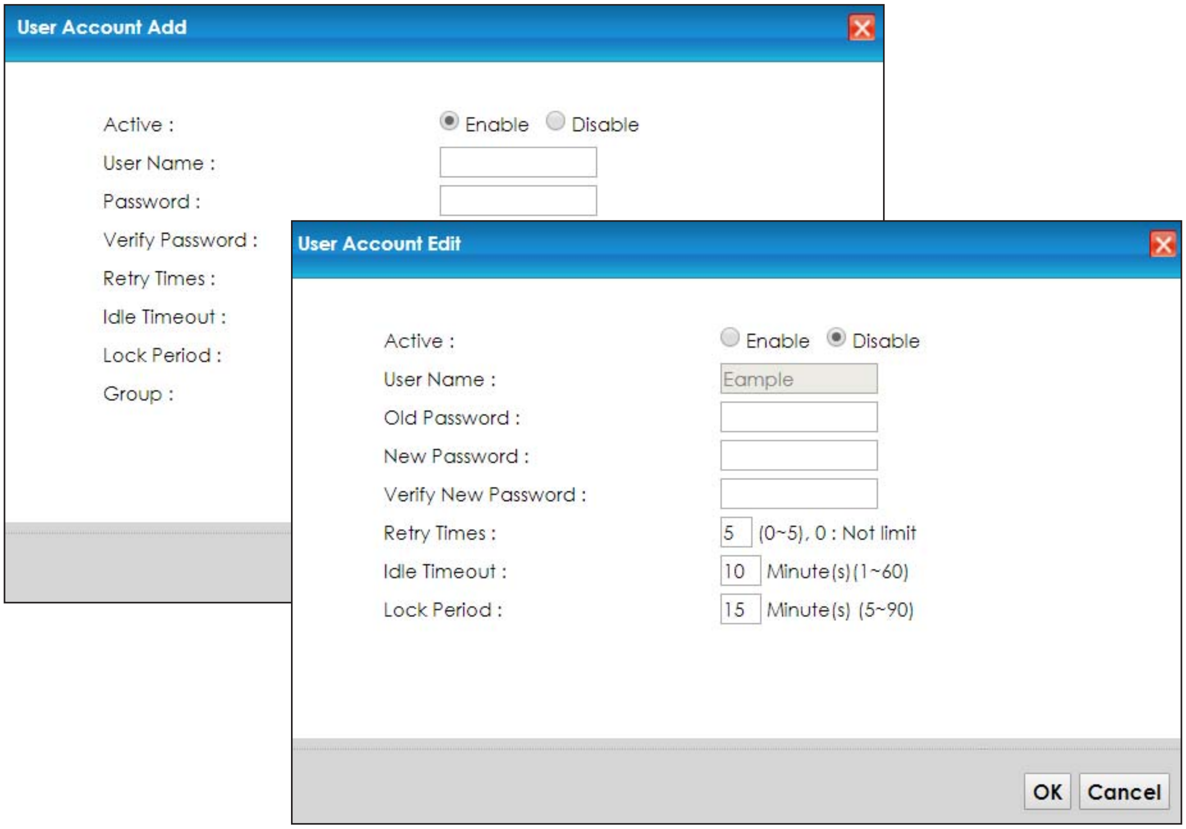
Table 99 Maintenance > User Account (continued) (continued)

LABEL	DESCRIPTION
Group	This field displays whether this user has **Administrator** or **User** privileges.
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 restore your previously saved settings.

28.2.1 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.

Figure 130 Maintenance > User Account > Add/Edit



Active : ● Enable ○ Disable
User Name :
Password :
Verify Password :
Retry Times :
Idle Timeout :
Lock Period :
Group :

Active : ○ Enable ● Disable
User Name : Eample
Old Password :
New Password :
Verify New Password :
Retry Times : 5 (0~5), 0 : Not limit
Idle Timeout : 10 Minute(s)(1~60)
Lock Period : 15 Minute(s) (5~90)

The following table describes the labels in this screen.

Table 100 Maintenance > User Account > Add/Edit

LABEL	DESCRIPTION
Active	Select **Enable** or **Disable** to activate or deactivate the user account.
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 100 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** privileges.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

CHAPTER 29
Remote Management

29.1 Overview

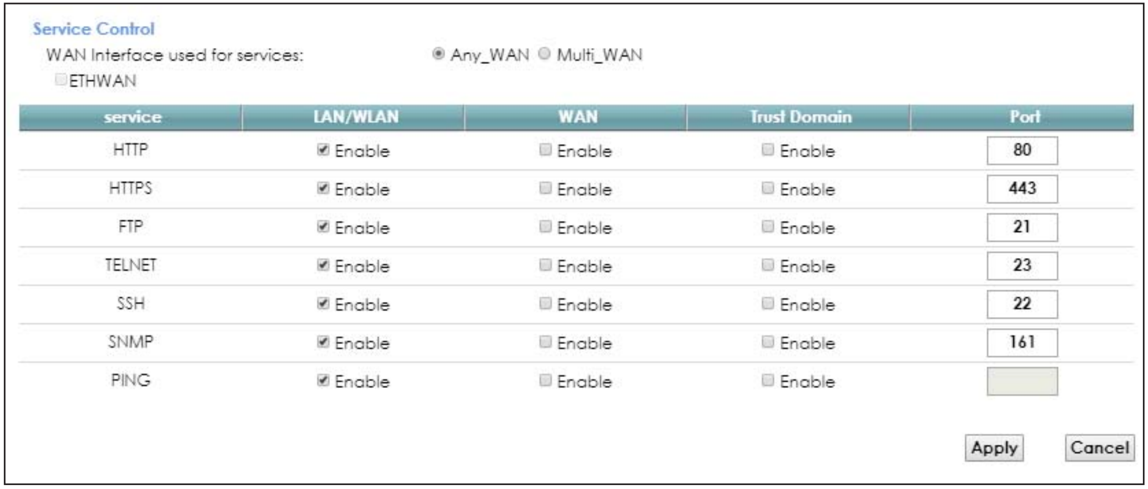
Remote management controls through which interface(s), which services can access the EMG.

Note: The EMG is managed using the Web Configurator.

29.2 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 131 Maintenance > Remote Management > MGMT Services



Service Control

WAN Interface used for services: ● Any_WAN ○ Multi_WAN

□ ETHWAN

service	LAN/WLAN	WAN	Trust Domain	Port
HTTP	☑ Enable	□ Enable	□ Enable	80
HTTPS	☑ Enable	□ Enable	□ Enable	443
FTP	☑ Enable	□ Enable	□ Enable	21
TELNET	☑ Enable	□ Enable	□ Enable	23
SSH	☑ Enable	□ Enable	□ Enable	22
SNMP	☑ Enable	□ Enable	□ Enable	161
PING	☑ Enable	□ Enable	□ Enable	

The following table describes the fields in this screen.

Table 101 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.
LAN/WLAN	Select the **Enable** check box for the corresponding services that you want to allow access to the EMG from the LAN/WLAN.

Table 101 Maintenance > Remote Management > MGMT Services (continued)

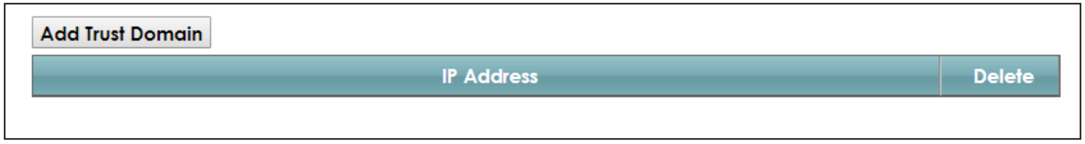
LABEL	DESCRIPTION
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the EMG from all WAN connections.
Trust Domain	Select the **Enable** check box for the corresponding services that you want to allow access to the EMG from the trusted hosts configured 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.
Apply	Click **Apply** to save your changes back to the EMG.
Cancel	Click **Cancel** to restore your previously saved settings.

29.3 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 > Turst 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 132 Maintenance > Remote Management > Trust Domain



The following table describes the fields in this screen.

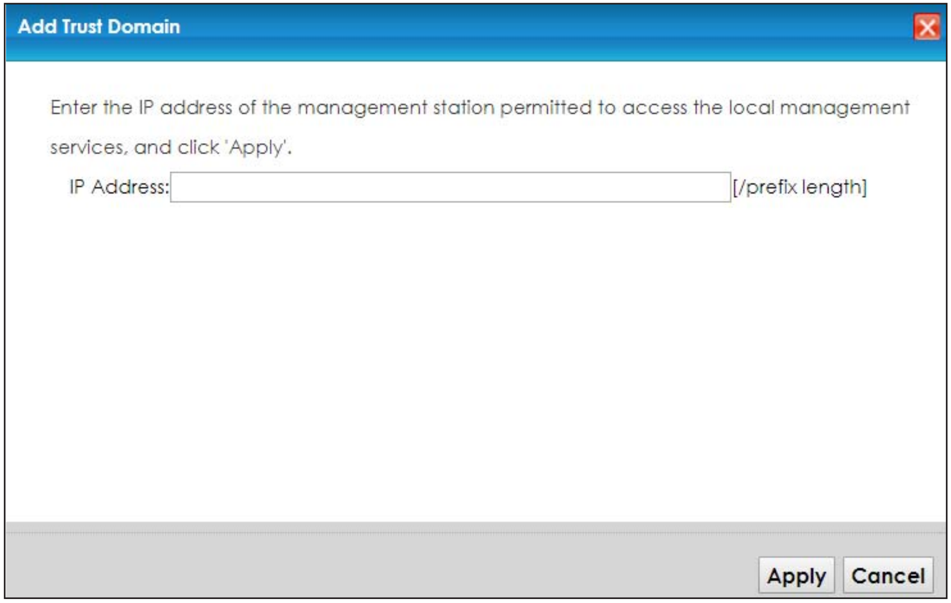
Table 102 Maintenance > Remote Management > Trust Domain

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.

29.3.1 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 133 Maintenance > Remote Management > Trust Domain > Add Trust Domain



Enter the IP address of the management station permitted to access the local management services, and click 'Apply'.

IP Address: [/prefix length]

The following table describes the fields in this screen.

Table 103 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 30
SNMP

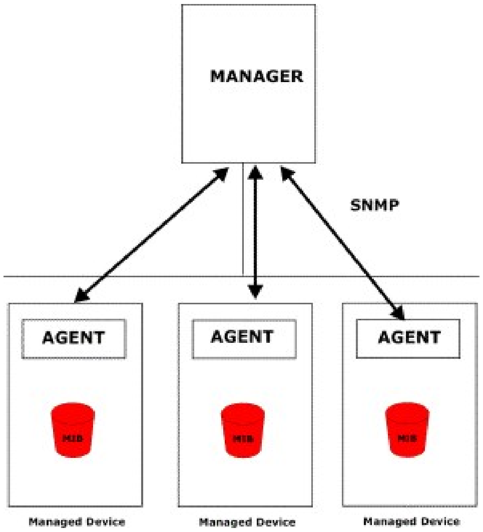
30.1 Overview

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

30.2 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 134 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.

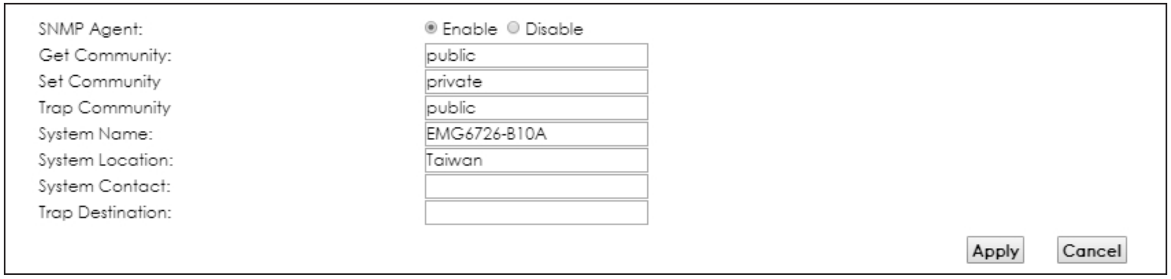
The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows 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 135 Maintenance > SNMP



SNMP Agent:	● Enable ○ Disable
Get Community:	public
Set Community	private
Trap Community	public
System Name:	EMG6726-B10A
System Location:	Taiwan
System Contact:	
Trap Destination:	

The following table describes the fields in this screen.

Table 104 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 31
Time Settings

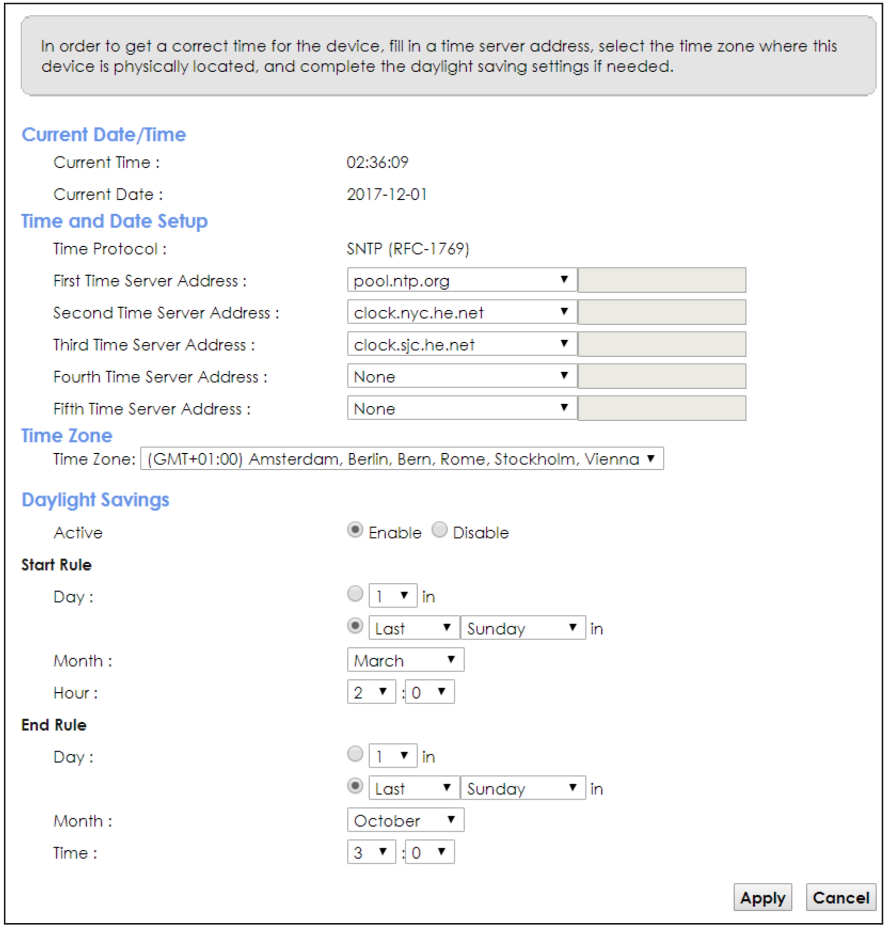
31.1 Overview

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

31.2 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 136 Maintenance > Time



In order to get a correct time for the device, fill in a time server address, select the time zone where this device is physically located, and complete the daylight saving settings if needed.

Current Date/Time

Current Time :	02:36:09
Current Date :	2017-12-01

Time and Date Setup

Time Protocol :	SNTP (RFC-1769)
First Time Server Address :	pool.ntp.org
Second Time Server Address :	clock.nyc.he.net
Third Time Server Address :	clock.sjc.he.net
Fourth Time Server Address :	None
Fifth Time Server Address :	None

Time Zone

Time Zone: (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Daylight Savings

Active	● Enable ○ Disable
Start Rule	
Day :	○ 1 in ● Last Sunday in
Month :	March
Hour :	2 : 0
End Rule	
Day :	○ 1 in ● Last Sunday in
Month :	October
Time :	3 : 0

The following table describes the fields in this screen.

Table 105 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.
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 32
E-mail Notification

32.1 Overview

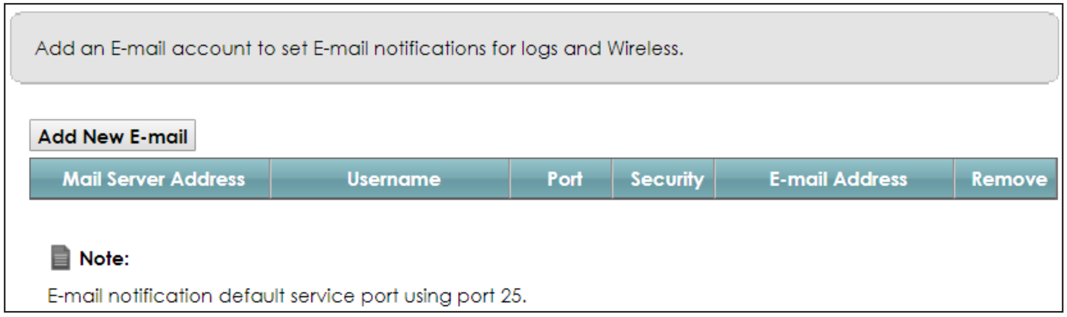
A mail server is an application or a computer that runs such an application to receive, forward and deliver e-mail messages.

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.

32.2 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 137 Maintenance > E-mail Notification



Add an E-mail account to set E-mail notifications for logs and Wireless.

Note:

E-mail notification default service port using port 25.

The following table describes the labels in this screen.

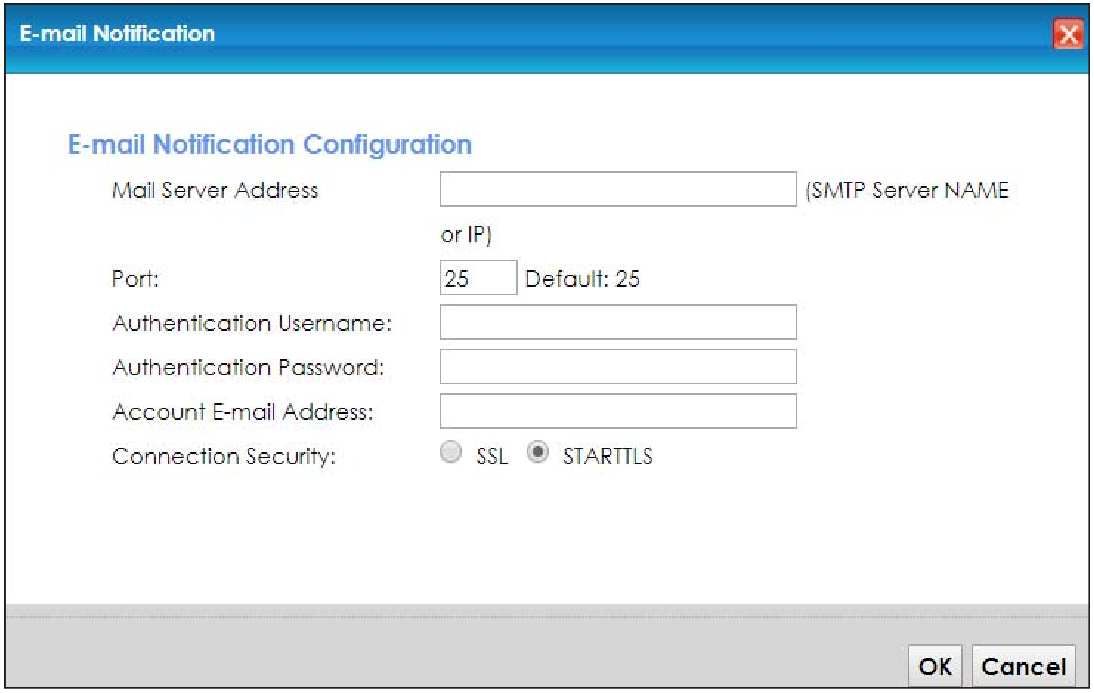
Table 106 Maintenance > E-mail Notification

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).

32.2.1 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 138 Email Notification > Add



The following table describes the labels in this screen.

Table 107 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 EMG. 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 33 Log Setting

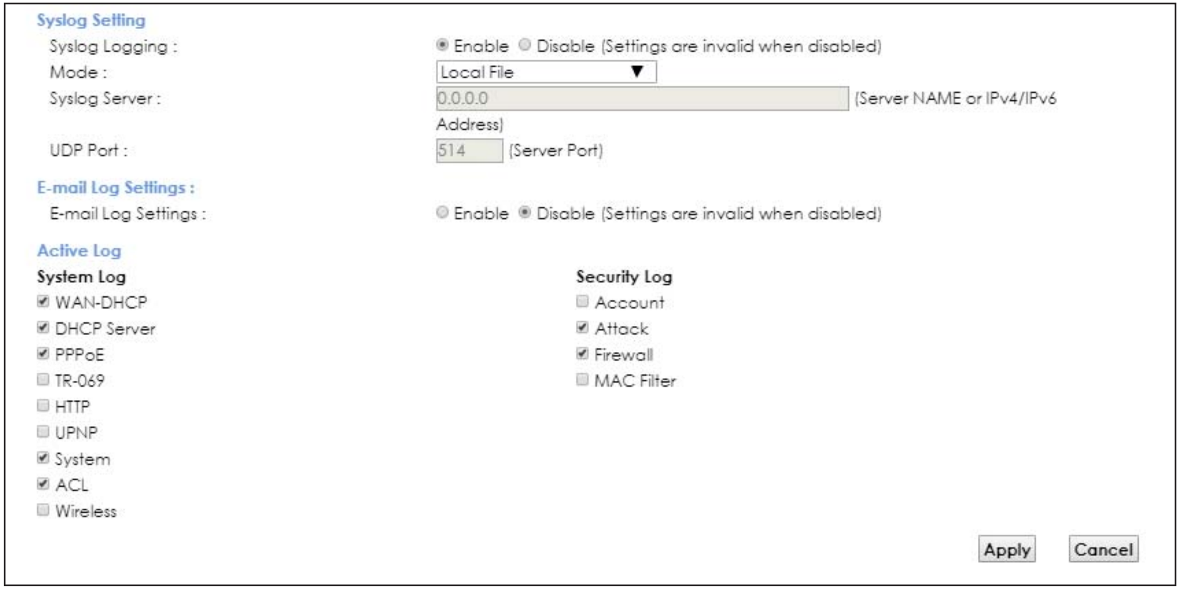
33.1 Overview

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

33.2 The Log Settings Screen

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

Figure 139 Maintenance > Logs Setting



Syslog Setting

Syslog Logging : ● Enable ○ Disable (Settings are invalid when disabled)

Mode : Local File ▼

Syslog Server : 0.0.0.0 (Server NAME or IPv4/IPv6 Address)

UDP Port : 514 (Server Port)

E-mail Log Settings :

E-mail Log Settings : ○ Enable ● Disable (Settings are invalid when disabled)

Active Log

System Log
- ☑ WAN-DHCP
- ☑ DHCP Server
- ☑ PPPoE
- □ TR-069
- □ HTTP
- □ UPNP
- ☑ System
- ☑ ACL
- □ Wireless

Security Log
- □ Account
- ☑ Attack
- ☑ Firewall
- □ MAC Filter

The following table describes the fields in this screen.

Table 108 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.

Table 108 Maintenance > Logs Setting (continued)

LABEL	DESCRIPTION
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 > Email 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.

33.2.1 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 140 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 34 Firmware Upgrade

34.1 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.

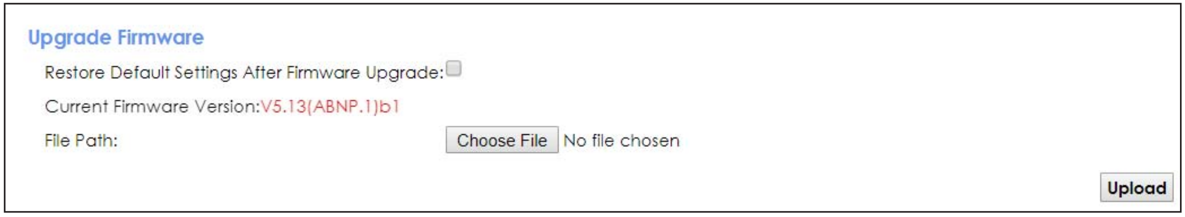
Only use firmware for your device's specific model. Refer to the label on the bottom of your EMG.

34.2 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 141 Maintenance > Firmware Upgrade



Upgrade Firmware

Restore Default Settings After Firmware Upgrade: □

Current Firmware Version: V5.13(ABNP.1)b1

File Path: Choose File No file chosen

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.

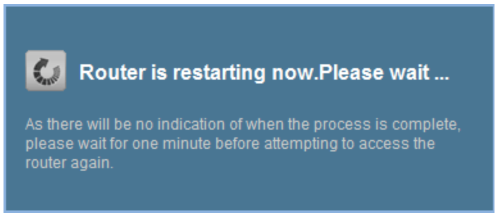
Table 109 Maintenance > Firmware Upgrade

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 109 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 142 Firmware Uploading

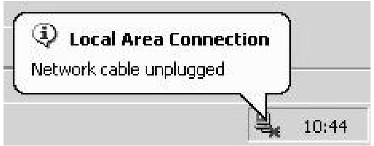


Router is restarting now.Please wait ...

As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

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 143 Network Temporarily Disconnected



Local Area Connection

Network cable unplugged

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

CHAPTER 35
Backup/Restore

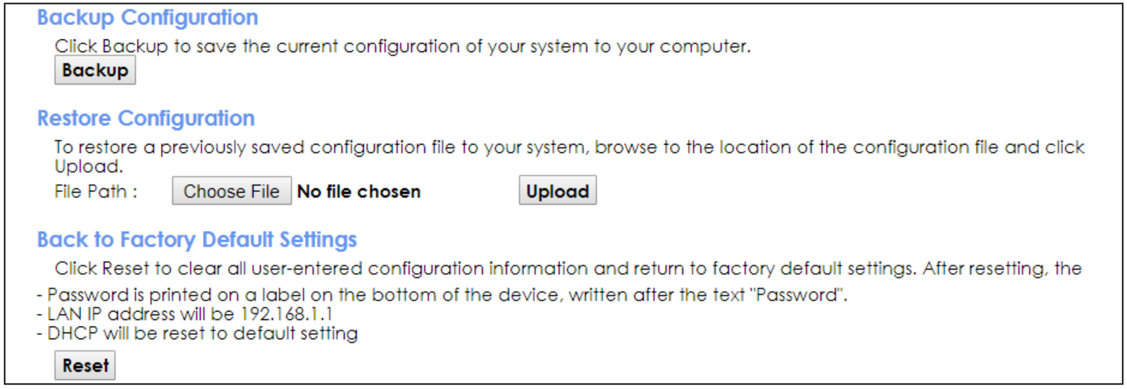
35.1 Overview

The **Backup/Restore** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

35.2 The Backup/Restore Screen

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 144 Maintenance > Backup/Restore



Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path : Choose File No file chosen

Back to Factory Default Settings

Click Reset to clear all user-entered configuration information and return to factory default settings. After resetting, the

- Password is printed on a label on the bottom of the device, written after the text "Password".
- LAN IP address will be 192.168.1.1
- DHCP will be reset to default setting

Backup Configuration

Backup Configuration allows you to back up (save) the EMG's current configuration to a file on your computer. Once your EMG is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the EMG's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your EMG.

Table 110 Restore Configuration

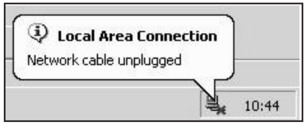
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Choose File** to find it.
Choose File	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.

Do not turn off the EMG while configuration file upload is in progress.

After the EMG configuration has been restored successfully, the login screen appears. Login again to restart the EMG.

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 145 Network Temporarily Disconnected



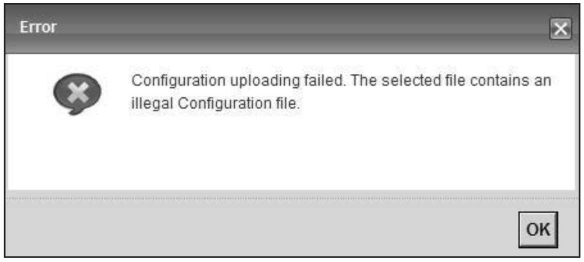
Local Area Connection

Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Configuration** screen.

Figure 146 Configuration Upload Error



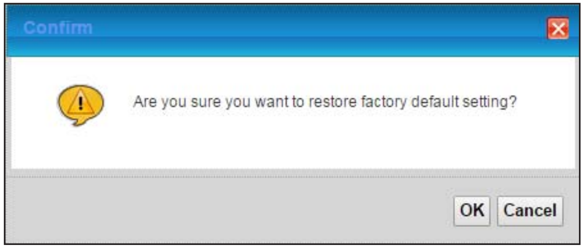
Error

Configuration uploading failed. The selected file contains an illegal Configuration file.

Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the EMG to its factory defaults. The following warning screen appears.

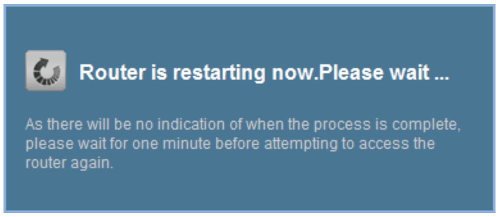
Figure 147 Reset Warning Message



Confirm

Are you sure you want to restore factory default setting?

Figure 148 Reset In Process Message



Router is restarting now.Please wait ...

As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

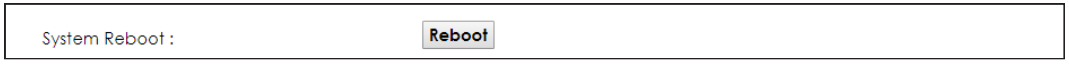
You can also press the **RESET** button on the rear panel to reset the factory defaults of your EMG. Refer to Section 1.4.5 on page 22 for more information on the **RESET** button.

35.3 The Reboot Screen

System restart allows you to reboot the EMG remotely without turning the power off. You may need to do this if the EMG hangs, for example.

Click **Maintenance > Reboot**. Click **Reboot** to have the EMG reboot. This does not affect the EMG's configuration.

Figure 149 Maintenance > Reboot



System Reboot :

CHAPTER 36 Diagnostic

36.1 Overview

The **Diagnostic** screens display information to help you identify problems with the EMG.

The route between a CO switch and one of its CPE may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

36.1.1 What You Can Do in this Chapter

- The **Ping & TraceRoute & NsLookup** screen lets you ping an IP address or trace the route packets take to a host (Section 36.3 on page 229).
- The **802.1ag** screen lets you perform CFM actions (Section 36.4 on page 229).
- The **802.3ah** screen lets you configure link OAM port parameters(Section 36.5 on page 231).

36.2 What You Need to Know

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

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

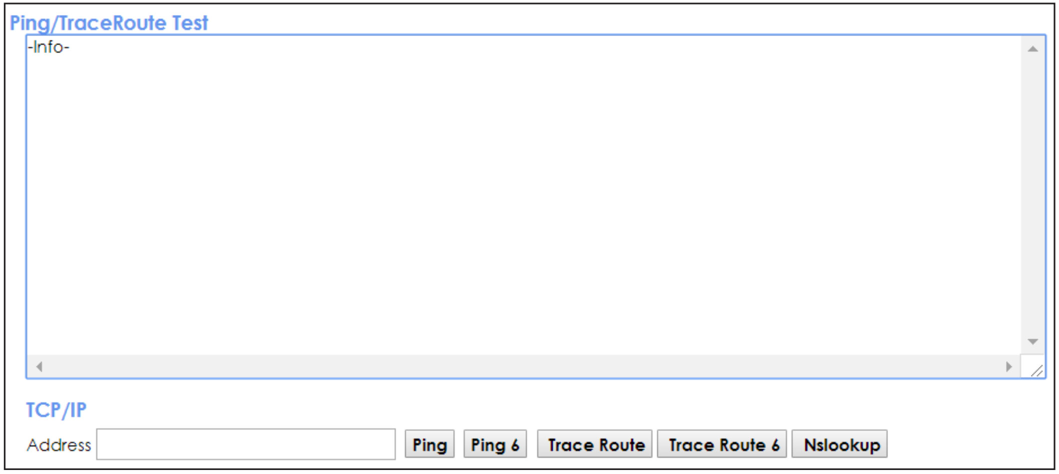
CFM provides two tests to discover connectivity faults.

- Loopback test - checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test - provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

36.3 Ping & TraceRoute & NsLookup

Use this screen to ping, traceroute, or nslookup an IP address. Click **Maintenance > Diagnostic > Ping&TraceRoute&NsLookup** to open the screen shown next.

Figure 150 Maintenance > Diagnostic > Ping &TraceRoute&NsLookup



The following table describes the fields in this screen.

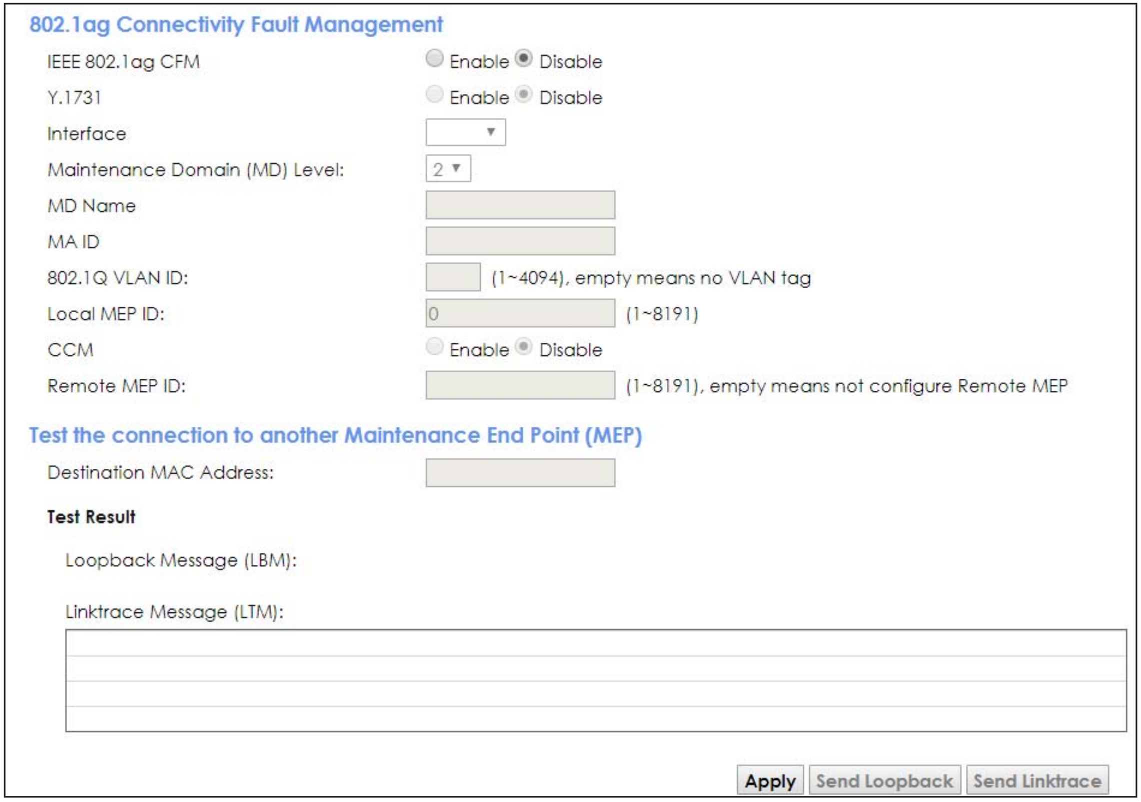
Table 111 Maintenance > Diagnostic > Ping & TraceRoute & NsLookup

LABEL	DESCRIPTION
URL or IP Address	Type the IP address of a computer that you want to perform ping, traceroute, or nslookup in order to test a connection.
Ping	Click this to ping the IPv4 address that you entered.
Ping 6	Click this to ping the IPv6 address that you entered.
Trace Route	Click this to display the route path and transmission delays between the EMG to the IPv4 address that you entered.
Trace Route 6	Click this to display the route path and transmission delays between the EMG to the IPv6 address that you entered.
Nslookup	Click this button to perform a DNS lookup on the IP address of a computer you enter.

36.4 802.1ag

Click **Maintenance > Diagnostic** > **802.1ag** to open the following screen. Use this screen to perform CFM actions.

Figure 151 Maintenance > Diagnostic > 802.1ag



802.1ag Connectivity Fault Management

IEEE 802.1ag CFM ○ Enable ● Disable

Y.1731 ○ Enable ● Disable

Interface

Maintenance Domain (MD) Level: 2

MD Name

MA ID

802.1Q VLAN ID: (1~4094), empty means no VLAN tag

Local MEP ID: 0 (1~8191)

CCM ○ Enable ● Disable

Remote MEP ID: (1~8191), empty means not configure Remote MEP

Test the connection to another Maintenance End Point (MEP)

Destination MAC Address:

Test Result

Loopback Message (LBM):

Linktrace Message (LTM):

The following table describes the fields in this screen.

Table 112 Maintenance > Diagnostic > 802.1ag

LABEL	DESCRIPTION
802.1ag Connectivity Fault Management	
IEEE 802.1ag CFM	Select **Enable** or **Disable** to activate or deactivate the IEEE802.1ag CFM (Connectivity Fault Management) specification, which allows network administrators to identify manage connection faults.
Y.1731	Select **Enable** or **Disable** to activate or deactivate Y.1731, which monitors Ethernet performance.
Interface	Select the interface on which you want to enable the IEE 802.1ag CFM.
Maintenance Domain (MD) Level	Select a level (0-7) under which you want to create an MA.
MEG ID	Enter the Maintenance Entity Group Identifier. This identifies the MEG that the MEP belongs to.
MD Name	Enter a descriptive name for the MD (Maintenance Domain).
MA ID	Enter a descriptive name to identify the Maintenance Association.
802.1Q VLAN ID	Type a VLAN ID (1-4094) for this MA.
Local MEP ID	Enter the local Maintenance Endpoint Identifier (1~8191).
CCM	Select **Enable** to continue sending MEP information by CCM (Connectivity Check Messages). When CCMs are received the EMG will always process it, no matter if **CCM** is enabled or not.
Remote MEP ID	Enter the remote Maintenance Endpoint Identifier (1~8191).
Test the connection to another Maintenance End Point (MEP)	

Table 112 Maintenance > Diagnostic > 802.1ag (continued)

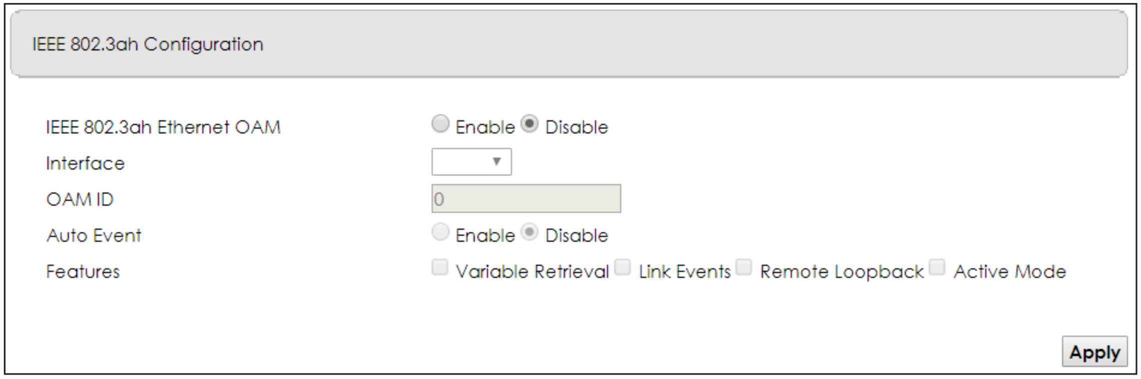
LABEL	DESCRIPTION
Destination MAC Address	Enter the target device's MAC address to which the EMG performs a CFM loopback and linktrace test.
Test Result	
Loopback Message (LBM)	This shows **Pass** if a Loop Back Messages (LBMs) responses are received. If LBMs do not get a response it shows **Fail**.
Linktrace Message (LTM)	This shows the MAC address of MEPs that respond to the LTMs.
Apply	Click this button to save your changes.
Send Loopback	Click this button to have the selected MEP send the LBM (Loop Back Message) to a specified remote end point.
Send Linktrace	Click this button to have the selected MEP send the LTMs (Link Trace Messages) to a specified remote end point.

36.5 802.3ah

Click **Maintenance > Diagnostic** > **803.ah** to open the following screen. Use this screen to the link monitoring protocol IEEE 802.3ah Link Layer Ethernet OAM (Operations, Administration and Maintenance.

Link layer Ethernet OAM (Operations, Administration and Maintenance) as described in IEEE 802.3ah is a link monitoring protocol. It utilizes OAM Protocol Data Units or OAM PDU's to transmit link status information between directly connected Ethernet devices. Both devices must support IEEE 802.3ah. Because link layer Ethernet OAM operates at layer two of the OSI (Open Systems Interconnection Basic Reference) model, neither IP or SNMP are necessary to monitor or troubleshoot network connection problems.

Figure 152 Maintenance > Diagnostic > 802.3ah



IEEE 802.3ah Configuration

IEEE 802.3ah Ethernet OAM ○ Enable ● Disable

Interface

OAM ID 0

Auto Event ○ Enable ● Disable

Features □ Variable Retrieval □ Link Events □ Remote Loopback □ Active Mode

Apply

The following table describes the labels in this screen.

Table 113 Maintenance > Diagnostics > 802.3ah

LABEL	DESCRIPTION
IEEE 802.3ah Ethernet OAM	Select **Enable** or **Disable** to activate or deactivate the Ethernet OAM on the specified interface.
Interface	Select the interface on which you want to enable the IEEE802.3ah.
OAM ID	Enter a positive integer to identify this node.

Table 113 Maintenance > Diagnostics > 802.3ah

LABEL	DESCRIPTION
Auto Event	Select **Enable** for the EMG to detect link status and send a notification when an error (such as errors in symbol, frames, or seconds) is detected. Otherwise, click **Disable** and you will not be notified.
Features	Select **Variable Retrieval** so the EMG can respond to requests for information, such as requests for Ethernet counters and statistics, about link events. Select **Link Events** so the EMG can interpret link events, such as link fault and dying asp.Link events are set in event notification PDUs (Protocol Data Units), and indicate when the number of errors in a certain given interval (time, number of frames, number of symbols, or number of errored frame seconds) exceeds a specified threshold. Organizations may create organization-specific link event TLVs as well. Select **Remote Loopback** so the EMG can accept loopback control PDUs to convert EMG into loopback mode. Select **Active Mode** so the EMG initiates OAM discovery, send information PDUs; and may send event notification PDUs, variable request/response PDUs, or loopback control PDUs.
Apply	Click this button to save your changes.

CHAPTER 37 Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- EMG Access and Login
- Internet Access
- Wireless Internet Access
- UPnP

37.1 Power, Hardware Connections, and LEDs

The EMG does not turn on. None of the LEDs turn on.

1. Make sure the EMG is turned on.
2. Make sure you are using the power adaptor or cord included with the EMG.
3. Make sure the power adaptor or cord is connected to the EMG and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the EMG off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.4.2 on page 20.
2. Check the hardware connections.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the EMG off and on.
5. If the problem continues, contact the vendor.

37.2 EMG Access and Login

I forgot the IP address for the EMG.

1 The default LAN IP address is 192.168.1.1.

2 If you changed the IP address and have forgotten it, you might get the IP address of the EMG by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the EMG (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.4.5 on page 22.

I forgot the password.

1 See the cover page for the default login names and associated passwords.

2 If those do not work, you have to reset the device to its factory defaults. See Section 1.4.5 on page 22.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address (Section 8.2 on page 100), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the EMG.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.4.2 on page 20.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.

4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance > Remote MGMT**).

5 Reset the device to its factory defaults, and try to access the EMG with the default IP address. See Section 1.4.5 on page 22.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the EMG using another service, such as Telnet. If you can access the EMG, check the remote management settings and firewall rules to find out why the EMG does not respond to HTTP.

I can see the **Login** screen, but I cannot log in to the EMG.

1. Make sure you have entered the password correctly. See the cover page for the default login names and associated passwords. The field is case-sensitive, so make sure [Caps Lock] is not on.
2. You cannot log in to the web configurator while someone is using Telnet to access the EMG. Log out of the EMG in the other session, or ask the person who is logged in to log out.
3. Turn the EMG off and on.
4. If this does not work, you have to reset the device to its factory defaults. See Section 37.1 on page 233.

I cannot Telnet to the EMG.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

37.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and Section 1.4.2 on page 20.
2. Make sure you entered your ISP account information correctly in the **Network Setting > Broadband** screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 If you are trying to access the Internet wirelessly, make sure that you enabled the wireless LAN in the EMG and your wireless client and that the wireless settings in the wireless client are the same as the settings in the EMG.

4 Disconnect all the cables from your device and reconnect them.

5 If the problem continues, contact your ISP.

I cannot connect to the Internet using an Ethernet connection.

1 Make sure you have the Ethernet WAN port connected to a modem or router.

2 Make sure you converted LAN port number five as WAN. Click **Enable** in **Network Setting** > **Broadband** > **Ethernet WAN** screen.

3 Make sure you configured a proper Ethernet WAN interface (**Network Setting > Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.

4 Check that the LAN interface you are connected to is in the same interface group as the Ethernet WAN connection (**Network Setting > Interface Grouping**).

5 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot access the EMG anymore. I had access to the EMG, but my connection is not available anymore.

1 Your session with the EMG may have expired. Try logging into the EMG again.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and Section 1.4.2 on page 20.

3 Turn the EMG off and on.

4 If the problem continues, contact your vendor.

37.4 Wireless Internet Access

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

What is a Server Set ID (SSID)?

An SSID is a name that uniquely identifies a wireless network. The AP and all the clients within a wireless network must use the same SSID.

37.5 UPnP

When using UPnP and the EMG reboots, my computer cannot detect UPnP.

1. Disconnect the Ethernet cable from the EMG's LAN port or from your computer.
2. Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

PART III
Appendices

Appendices contain general information. Some information may not apply to your device.

APPENDIX A
Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See *https://www.zyxel.com/homepage.shtml* and also *https://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml* for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- http://www.zyxel.com

Asia

China

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- https://www.zyxel.com/cn/zh/

India

- Zyxel Technology India Pvt Ltd
- https://www.zyxel.com/in/en/

Kazakhstan

- Zyxel Kazakhstan
- https://www.zyxel.kz

Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- Zyxel Communications Corporation
- https://www.zyxel.com/tw/zh/

Thailand

- Zyxel Thailand Co., Ltd
- https://www.zyxel.com/th/th/

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- https://www.zyxel.com/vn/vi

Europe

Belarus

- Zyxel BY
- https://www.zyxel.by

Belgium

- Zyxel Communications B.V.
- https://www.zyxel.com/be/nl/

- https://www.zyxel.com/be/fr/

Bulgaria

- Zyxel България
- https://www.zyxel.com/bg/bg/

Czech Republic

- Zyxel Communications Czech s.r.o
- https://www.zyxel.com/cz/cs/

Denmark

- Zyxel Communications A/S
- https://www.zyxel.com/dk/da/

Estonia

- Zyxel Estonia
- https://www.zyxel.com/ee/et/

Finland

- Zyxel Communications
- https://www.zyxel.com/fi/fi/

France

- Zyxel France
- https://www.zyxel.fr

Germany

- Zyxel Deutschland GmbH
- https://www.zyxel.com/de/de/

Hungary

- Zyxel Hungary & SEE
- https://www.zyxel.com/hu/hu/

Italy

- Zyxel Communications Italy
- https://www.zyxel.com/it/it/

Latvia

- Zyxel Latvia
- https://www.zyxel.com/lv/lv/

Lithuania

- Zyxel Lithuania
- https://www.zyxel.com/lt/lt/

Netherlands

- Zyxel Benelux
- https://www.zyxel.com/nl/nl/

Norway

- Zyxel Communications
- https://www.zyxel.com/no/no/

Poland

- Zyxel Communications Poland
- https://www.zyxel.com/pl/pl/

Romania

- Zyxel Romania
- https://www.zyxel.com/ro/ro

Russia

- Zyxel Russia
- https://www.zyxel.com/ru/ru/

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- https://www.zyxel.com/sk/sk/

Spain

- Zyxel Communications ES Ltd
- https://www.zyxel.com/es/es/

Sweden

- Zyxel Communications
- https://www.zyxel.com/se/sv/

Switzerland

- Studerus AG
- https://www.zyxel.ch/de
- https://www.zyxel.ch/fr

Turkey

- Zyxel Turkey A.S.
- https://www.zyxel.com/tr/tr/

UK

- Zyxel Communications UK Ltd.
- https://www.zyxel.com/uk/en/

Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

South America

Argentina

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Colombia

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Ecuador

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

South America

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Middle East

Israel

- Zyxel Communications Corporation
- http://il.zyxel.com/

Middle East

- Zyxel Communications Corporation
- https://www.zyxel.com/me/en/

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- https://www.zyxel.com/us/en/

Oceania

Australia

- Zyxel Communications Corporation
- https://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- https://www.zyxel.com/za/en/

APPENDIX B Wireless LANs

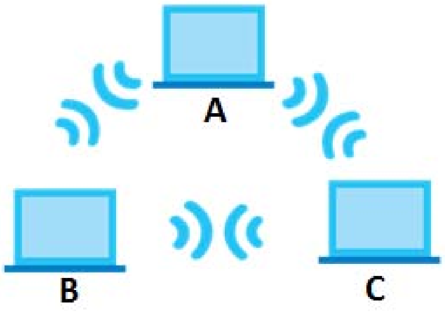
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 153 Peer-to-Peer Communication in an Ad-hoc Network

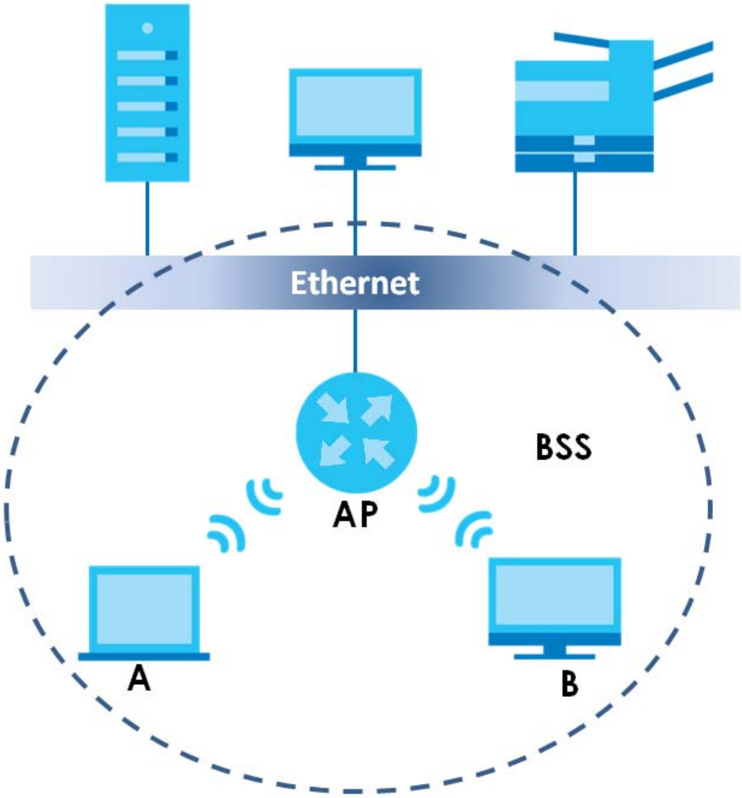


BSS

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

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

Figure 154 Basic Service Set



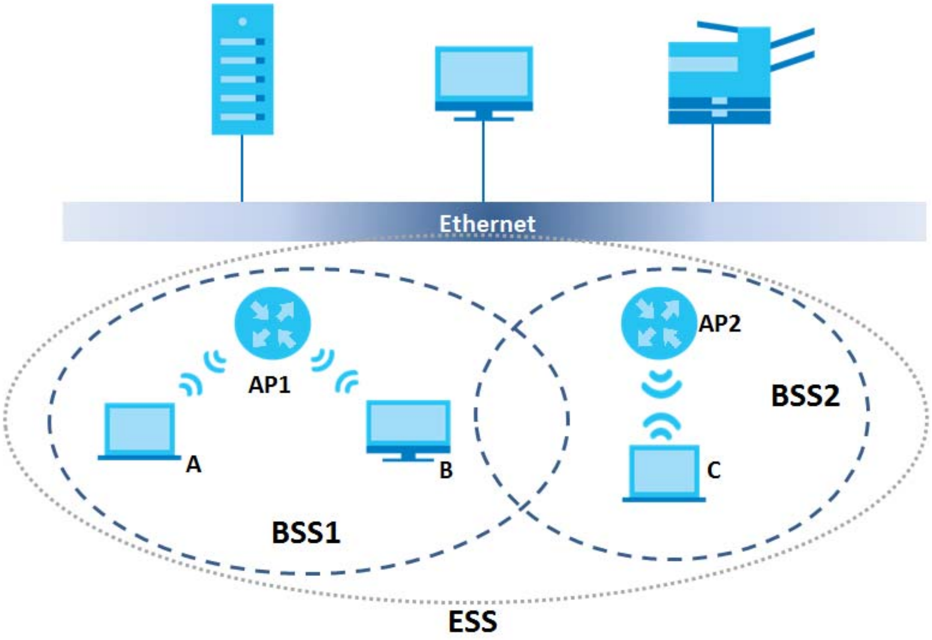
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 155 Infrastructure WLAN



Channel

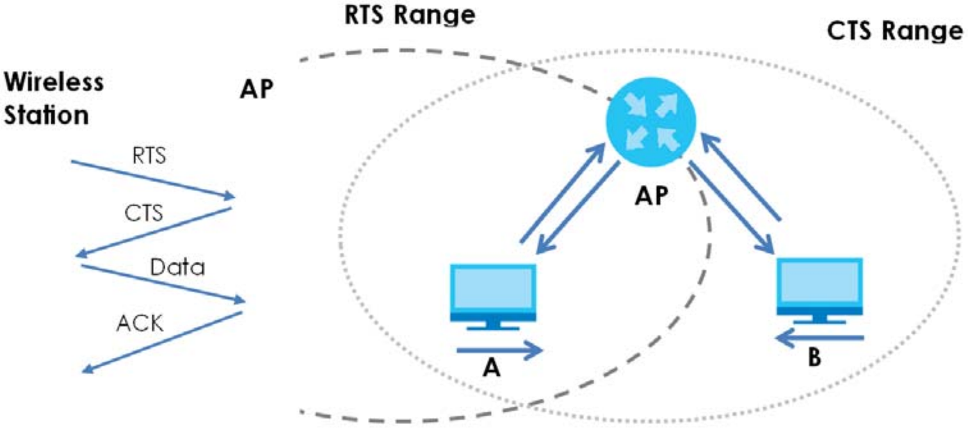
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 156 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 114 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the EMG are data encryption, wireless client authentication, restricting access by device MAC address and hiding the EMG identity.

The following figure shows the relative effectiveness of these wireless security methods available on your EMG.

Table 115 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
Most Secure	MAC Address Filtering

Note: You must enable the same wireless security settings on the EMG and on all wireless clients that you want to associate with it.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.

- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client’s network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

Encryption

AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. AES includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

WPA2-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA2-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys.

User Authentication

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA2-PSK Application Example

A WPA2-PSK application looks as follows.

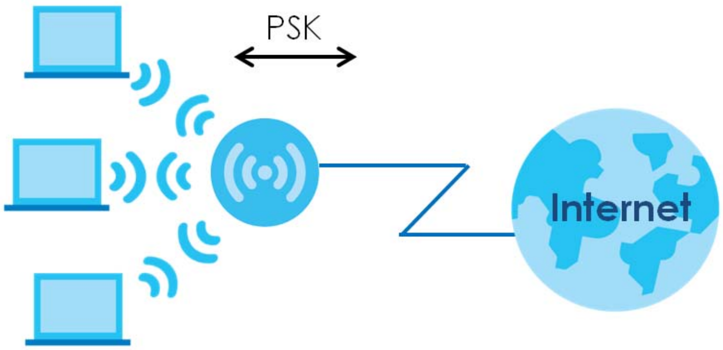
1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2. The AP checks each wireless client's password and allows it to join the network only if the password matches.

3. The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4. The AP and wireless clients use the AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 157 WPA2-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 116 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY
Open	None	No
WPA2-PSK	AES	Yes

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna’s coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

APPENDIX C
IPv6

Overview

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.

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`.

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.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a “private IP address” in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 117 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a “public IP address” in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to "0.0.0.0" in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to "127.0.0.1" in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 118 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 119 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0

Table 119 Reserved Multicast Address (continued)

MULTICAST ADDRESS
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

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.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

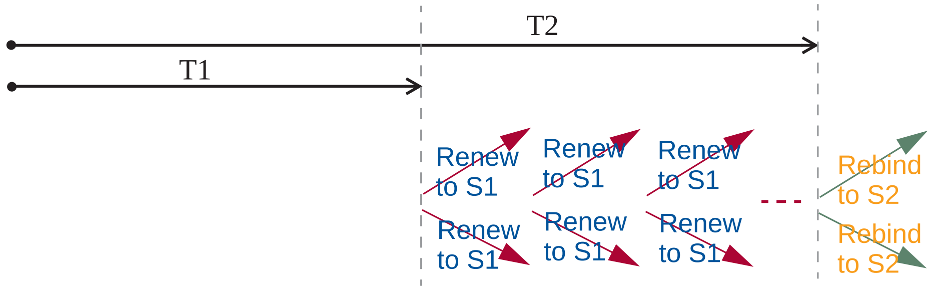
The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

MAC	00 : 13 : 49 : 12 : 34 : 56
EUI-64	02 : 13 : 49 : FF : FE : 12 : 34 : 56

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.

The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The EMG uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the EMG passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor’s reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor’s link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being “reachable” means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.

- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The EMG maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the EMG configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the EMG also sends out a neighbor solicitation message. When the EMG receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the EMG uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The EMG creates an entry in the default router list cache if the router can be used as a default router.

When the EMG needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the EMG uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is unlink, the address is considered as the next hop. Otherwise, the EMG determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the EMG looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the EMG cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

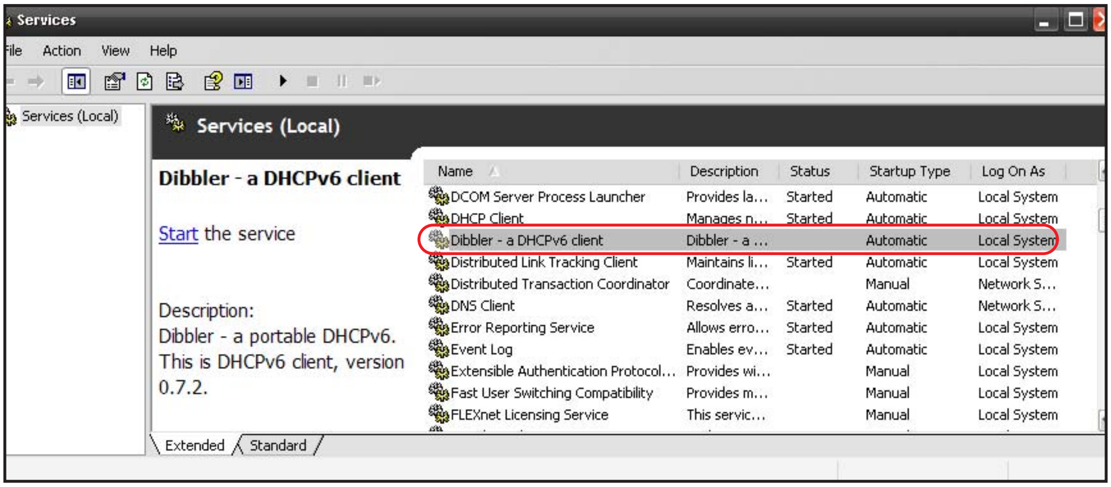
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1 Install Dibbler and select the DHCPv6 client option on your computer.

2 After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.

3 Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.

4 Double click **Dibbler - a DHCPv6 client**.



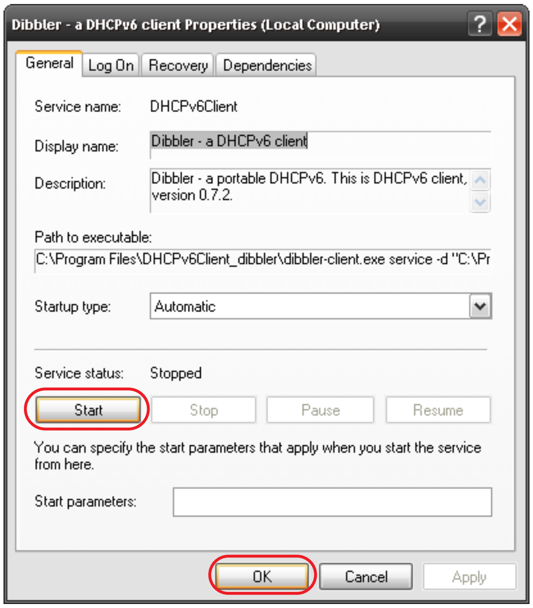
Dibbler - a DHCPv6 client

Start the service

Description:
Dibbler - a portable DHCPv6. This is DHCPv6 client, version 0.7.2.

Name	Description	Status	Startup Type	Log On As
DCOM Server Process Launcher	Provides la...	Started	Automatic	Local System
DHCP Client	Manages n...	Started	Automatic	Local System
Dibbler - a DHCPv6 client	Dibbler - a ...		Automatic	Local System
Distributed Link Tracking Client	Maintains li...	Started	Automatic	Local System
Distributed Transaction Coordinator	Coordinate...		Manual	Network S...
DNS Client	Resolves a...	Started	Automatic	Network S...
Error Reporting Service	Allows erro...	Started	Automatic	Local System
Event Log	Enables ev...	Started	Automatic	Local System
Extensible Authentication Protocol...	Provides wi...		Manual	Local System
Fast User Switching Compatibility	Provides m...		Manual	Local System
FLEXnet Licensing Service	This servic...		Manual	Local System

5 Click **Start** and then **OK**.



Service name: DHCPv6Client

Display name: Dibbler - a DHCPv6 client

Description: Dibbler - a portable DHCPv6. This is DHCPv6 client, version 0.7.2.

Path to executable:
C:\Program Files\DHCPv6Client_dibbler\dibbler-client.exe service -d "C:\Pr

Startup type: Automatic

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

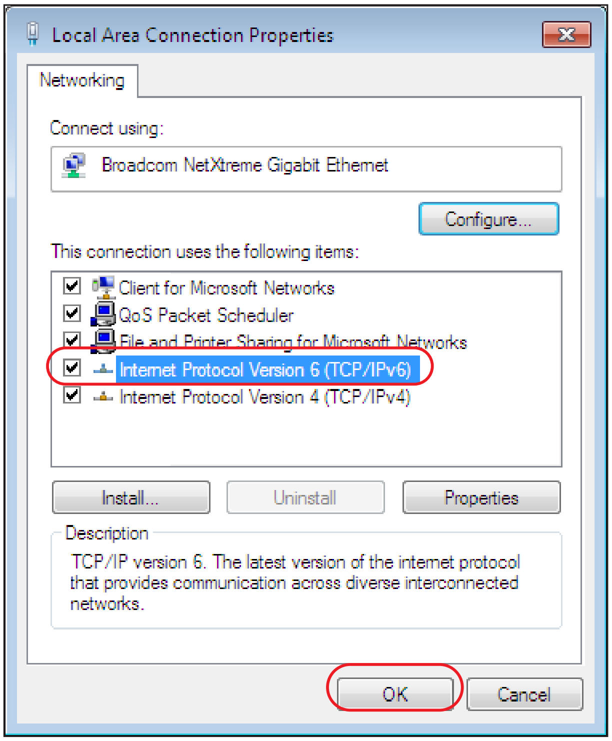
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.



Connect using:

Broadcom NetXtreme Gigabit Ethernet

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

APPENDIX D
Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s**) is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 120 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.

Table 120   Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.

Table 120 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

APPENDIX E
Legal Information

Copyright

Copyright © 2019 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

UNITED STATES of AMERICA

The following information applies if you use the product within USA area.

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

  (1) This device may not cause harmful interference, and

  (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 40 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment.

CANADA

The following information applies if you use the product within Canada area.

Industry Canada ICES Statement

CAN ICES-3 (B)/NMB-3(B)

Industry Canada RSS-GEN & RSS-247 statement

- This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
- This radio transmitter (2468C-VMG4927B50A) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Antenna Information

NO.	MODEL NAME	TYPE	MANUFACTURER	GAIN	CONNECTOR
1	65-031-049008B	Dipole	Airgain	4.5	N/A
2	65-031-049007B	Dipole	Airgain	4.1	N/A
3	65-031-049009B	Dipole	Airgain	3.1	N/A
4	65-031-049003B	Dipole	Airgain	0.36	i-pex(MHF)
5	65-031-049004B	Dipole	Airgain	0.36	i-pex(MHF)
6	65-031-049005B	Dipole	Airgain	0.36	i-pex(MHF)
7	65-031-049006B	Dipole	Airgain	0.36	i-pex(MHF)

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- The worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz , the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
- Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio (2468C-VMG4927B50A) de modèle s'il fait partie du matériel de catégoriel) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Informations Antenne

NUMÉRO	NOM DU MODÈLE	TYPE	FABRICANT	GAIN	CONNECTEUR
1	65-031-049008B	Dipole	Airgain	4.5	N/A
2	65-031-049007B	Dipole	Airgain	4.1	N/A
3	65-031-049009B	Dipole	Airgain	3.1	N/A
4	65-031-049003B	Dipole	Airgain	0.36	i-pex(MHF)
5	65-031-049004B	Dipole	Airgain	0.36	i-pex(MHF)
6	65-031-049005B	Dipole	Airgain	0.36	i-pex(MHF)
7	65-031-049006B	Dipole	Airgain	0.36	i-pex(MHF)

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3) du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes.

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

Industry Canada radiation exposure statement

This device complies with IC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 39 cm between the radiator and your body.

Déclaration d’exposition aux radiations:

Cet équipement est conforme aux limites d’exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 39 cm de distance entre la source de rayonnement et votre corps.

EUROPEAN UNION

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20cm between the radio equipment and your body.

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕC. **National Restrictions** • The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details. • Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens. • Les liaisons sans fil pour une utilisation en extérieur d’une distance supérieure à 300 mètres doivent être notifiées à l’Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE..
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. **National Restrictions** • In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. • I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.

Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. **National Restrictions** • This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a “general authorization.” Please check http://www.sviluppoeconomico.gov.it/ for more details. • Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una “Autorizzazione Generale”. Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. **National Restrictions** • The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details. • 2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale şi alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.

Notes:

- Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
- The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Important Safety Instructions

- Caution! The RJ-45 jacks are not used for telephone line connection.
- Caution! Do not use this product near water, for example a wet basement or near a swimming pool.
- Caution! Avoid using this product (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Caution! Always disconnect all telephone lines from the wall outlet before servicing or disassembling this product.
- Attention: Les prises RJ-45 ne sont pas utilisés pour la connexion de la ligne téléphonique.
- Attention: Ne pas utiliser ce produit près de l'eau, par exemple un sous-sol humide ou près d'une piscine.
- Attention: Évitez d'utiliser ce produit (autre qu'un type sans fil) pendant un orage. Il peut y avoir un risque de choc électrique de la foudre.
- Attention: Toujours débrancher toutes les lignes téléphoniques de la prise murale avant de réparer ou de démonter ce produit.

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive

(Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless setting, please refer to "Wireless" chapter for more detail.)

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

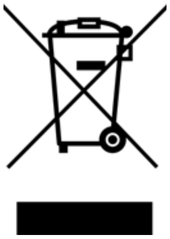
Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 第十二條 經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。 低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用， 俟無干擾之虞，始得繼續使用。
- 無線資訊傳設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作， 發射的信號應維持於操作頻帶中
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 若使用高增益指向性天線，該產品僅應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。

- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 (如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備， 在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備， 插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
∿	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
⎓	Direct current (DC): DC if the unidirectional flow or movement of electric charge carriers.
⏚	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
⧈	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Index