ZYXEL
COMMUNICATIONS

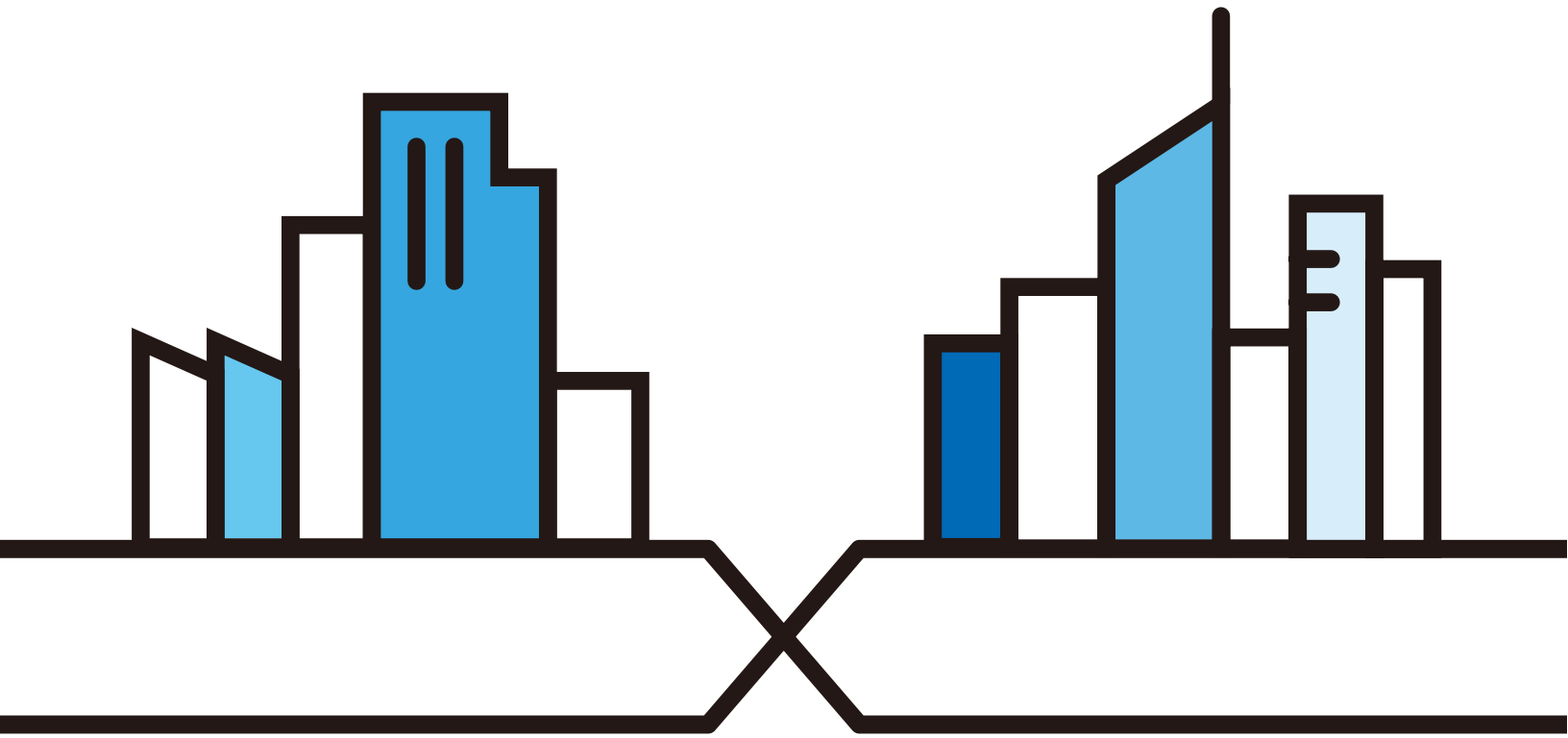
User's Guide

FMG Series

P2P Gigabit Fiber Bridge

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

Version 1.00 Ed 3, 6/2020



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the FMG.

- More Information

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

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

- All models in this series may be referred to as the "FMG" 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, **Advance > QoS Classification** means you first click **Advance** in the navigation panel, and then click the **QoS Classification** tab to get to that screen.

Icons Used in Figures

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

FMG 	Generic Router 	Laptop Computer 
Switch 	Smart TV 	Server 
Desktop 	STB 	Wireless Device 
Firewall 		

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Introducing the FMG

1.1 Overview

The FMG is a Gigabit active fiber bridge.

FMG refers to these models as outlined below:

- FMG3005-R20A
- FMG3010-R20A

The following table describes the feature differences of the FMG by model.

Table 1 FMG Comparison Table

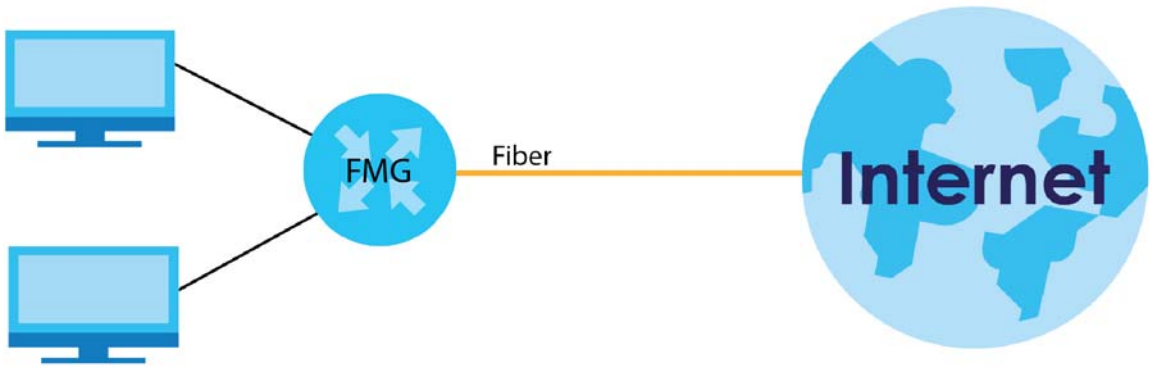
	FMG3005-R20A	FMG3010-R20A
CATV	N	N
Gigabit Ethernet LAN Port	1	4
Fiber Port	Y	Y
Firmware Version	1.00	1.00

1.1.1 Internet Access

Your FMG provides shared Internet access by sliding the FMG down the fiber box gently to fix the FMG into place, so the fiber optic cable connects to the FMG. See the Quick Start Guide for how to do the hardware installation.

In addition, you can connect computers, IPTVs, gaming consoles, and other Ethernet devices to the Ethernet ports for fiber-speed Internet access.

Figure 1 Fiber Connection



1.2 Ways to Manage the FMG

This is recommended for management of the FMG using a (supported) web browser.

1.3 Good Habits for Managing the FMG

Do the following things regularly to make the FMG more secure and to manage the FMG 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 FMG to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the FMG. You could simply restore your last configuration.

1.4 Hardware

This section describes the front, side, and rear panels for each model. Refer to the FMG's Quick Start Guides to see the product drawings and how to make the hardware connections.

1.4.1 Front Panel

The LED indicators are located on the front panel.

Figure 2 FMG3010-R20A Front Panel

Figure 3 FMG3005-R20A Front Panel

1.4.1.1 LEDs (Lights)

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

Table 2 FMG3010-R20A LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The FMG is receiving power and ready for use.
		Blinking	The FMG is self-testing.
	Red	On	The FMG detected an error while self-testing, or there is a device malfunction.
		Blinking	The FMG is upgrading firmware.
		Off	The FMG is not receiving power or LEDs are turned off.
Fiber	Green	On	The FMG has a fiber connection.
		Off	The FMG doesn't have a fiber connection.
ETHERNET1~4	Green	On	The FMG has a successful 10/100/1000 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The FMG is sending or receiving data to/from the LAN at 10/100/1000 Mbps.
		Off	The FMG does not have an Ethernet connection with the LAN.

Table 3 FMG3005-R20A LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
Power	Green	On	The FMG is receiving power and ready for use.
		Blinking	The FMG is self-testing.
	Red	On	The FMG detected an error while self-testing, or there is a device malfunction.
		Blinking	The FMG is upgrading firmware.
		Off	The FMG is not receiving power.
Fiber	Green	On	The FMG has a fiber connection.
		Off	The FMG doesn't have a fiber connection.
Speed	Green	On	The FMG has a successful 1000 Mbps Ethernet connection
		Off	The FMG has a successful 100 Mbps Ethernet connection
LAN	Green	On	The FMG has a successful 10/100/1000 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The FMG is transmitting and receiving data through the LAN.
		Off	The FMG does not have an Ethernet connection with the LAN.

1.4.2 Side Panels

The connection ports and buttons are located on the side panels.

Connection Ports

Figure 4 FMG3010-R20A Side Panel

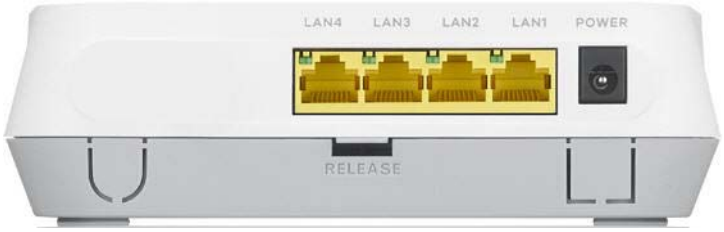


Figure 5 FMG3005-R20A Side Panel

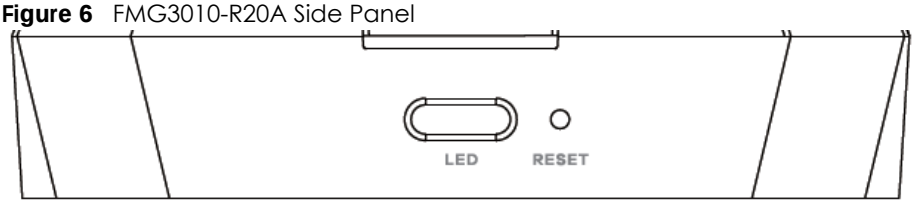
The following table describes the items on the panels.

Table 4 Panel Ports and Buttons

LABEL	DESCRIPTION
FIBER (For FMG3005-R20A)	Connect a fiber cable to the **FIBER** port for fiber-speed Internet access.
LAN	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
Power	Connect the power cable and then press the power button to start the device.
RELEASE	Gently push this in to disconnect the FMG from the fiber box.

Buttons

Figure 6 FMG3010-R20A Side Panel



The following table describes the items on the panels.

Table 5 Panel Ports and Buttons

LABEL	DESCRIPTION
LED	Press the button for more than two seconds to turn on or off the LEDs.
RESET	Press the button for more than five seconds (or until the PWR LED starts to blink), then release it to return the FMG to the factory defaults.

1.4.2.1 The LED Button

Press the **LED** button for more than two seconds to turn on/off the LEDs.

1.4.2.2 The RESET Button

If you forget your password or cannot access the Web Configurator, you will need to use the **RESET** button to reload the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will be reset to the factory default (see the device label), and the LAN IP address will be "192.168.1.1".

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 five seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

1.4.3 Rear Panels

The fiber connector is located on the rear panel. See the Quick Start Guide for how to do the hardware installation.

Figure 7 FMG3010-R20A Rear Panel

1.5 Installation Scenarios

The FMG can be:

- Placed on a desktop.
- Wall-mounted on a wall.

The following table summarizes the installation scenarios of the FMG by model.

Table 6 FMG Series Installation Comparison Table

FMG MODELS	FMG3005-R20A	FMG3010-R20A
Rubber feet for desktop placement	Y	Y
Wall Mounting	Y	Y

Note: Make sure to use the rubber feet when stacking the FMG on a desk.
Make sure there is clearance at the sides and a distance between the screw head and the wall to allow air circulation and the attachment of cables and the power cord.

Note: Make sure the screws are securely fixed to the wall and strong enough to hold the weight of the FMG with the connection cables.

Warning! Do NOT block the ventilation holes on the FMG. Allow clearance for the ventilation holes to prevent your FMG from overheating. Do not store things on the FMG. Do not place a FMG on another high temperature device. Overheating could affect the performance of your FMG, or even damage it.

CHAPTER 2
The Web Configurator

2.1 Overview

The Web Configurator is an HTML-based management interface that allows easy system setup and management via Internet browser. Use a browser that supports HTML5, such Internet Explorer 11, Mozilla Firefox, or Google Chrome. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

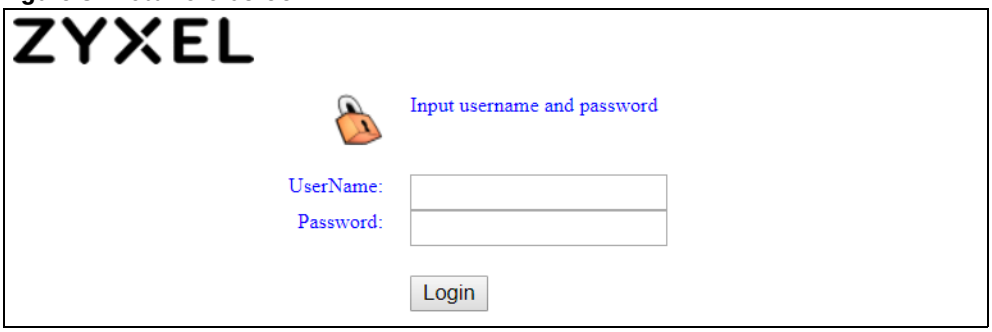
- Web browser pop-up windows from your FMG.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

2.1.1 Accessing the Web Configurator

1. Make sure your FMG hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser. If the FMG does not automatically re-direct you to the login screen, go to http://192.168.1.1.
3. A password screen displays.
4. To access the administrative Web Configurator and manage the FMG, type the default user name **admin** and the randomly assigned default password (see the device label) in the password screen and click **Login**. If you have changed the password, enter your password and click **Login**.

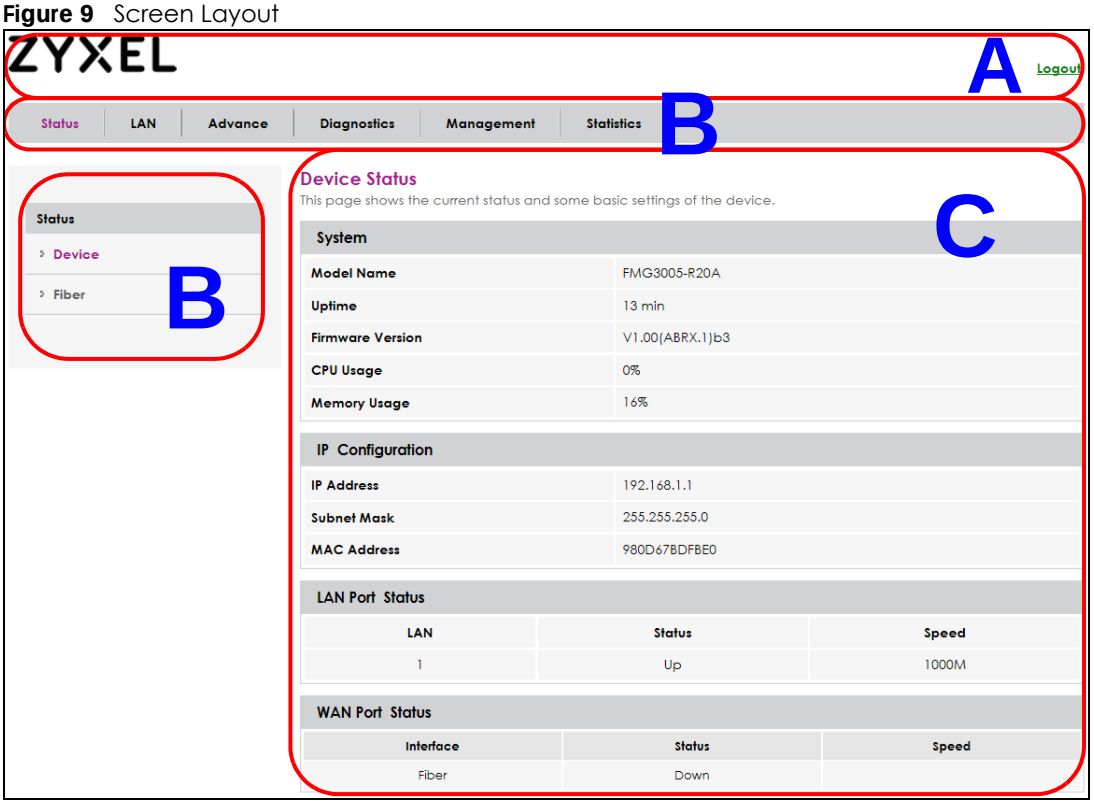
Note: If the management session is left idle for 300 seconds, you have to log in with your password again.

Figure 8 Password Screen



2.2 Web Configurator Layout

Figure 9 Screen Layout



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

- **A** - Title Bar
- **B** - Navigation Panel
- **C** - Main Window

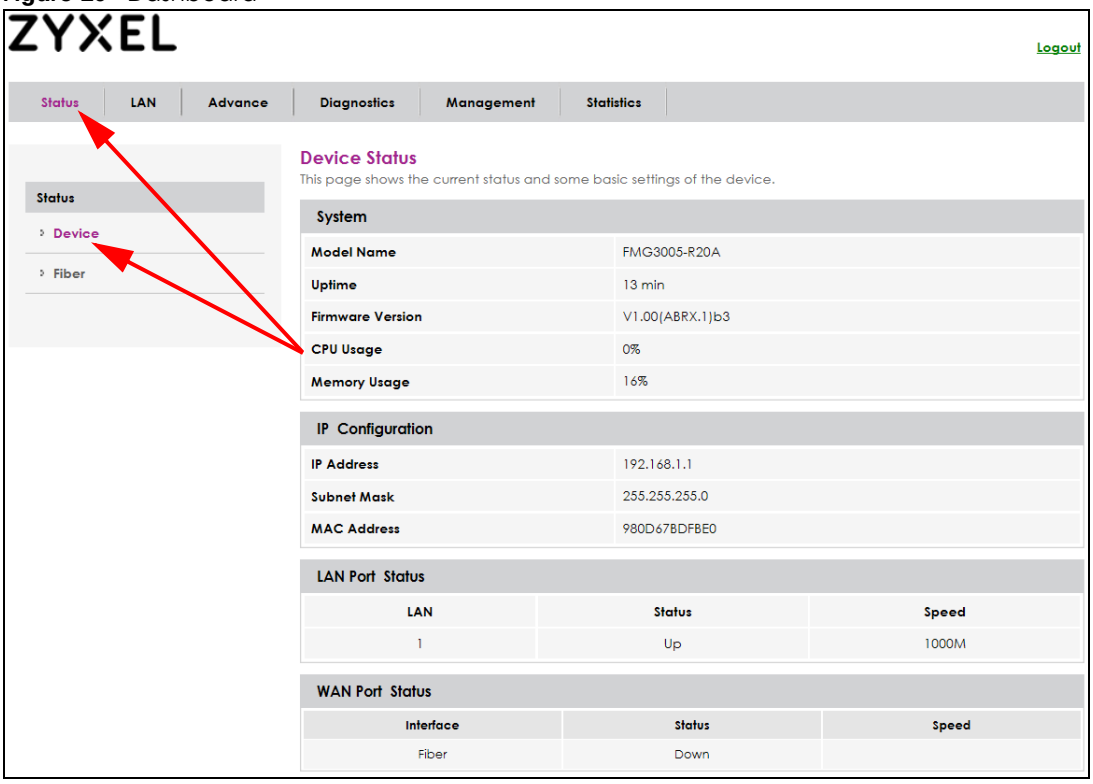
2.2.1 Title Bar

Click **Logout** to log out of the Web Configurator.

2.2.2 Dashboard

Use the menu items in the navigation panel on the right to open screens to configure the FMG's features.

Figure 10 Dashboard



2.2.3 Navigation Panel

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

Note: The menu items on the navigation panel vary among the models. See Section 1.1 on page 9 for more information about the feature differences of the FMG.

Table 7 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		
Device	Device Status	This screen shows the network status of the FMG and computers/devices connected to it.
Fiber	Fiber Status	This screen shows the parameters of temperature, voltage, transmitting power, and receiving power of the fiber connection.
LAN		
Setup LAN Interface	LAN Interface Settings	Use this screen to configure LAN IP address and subnet mask of the FMG.
Advance		
Queue setting	QoS Configuration	Use this screen to configure QoS queues.
QoS classification	QoS Configuration	Use this screen to define a classifier.
Diagnostics		

Table 7 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Ping	Ping Diagnostics	Use this screen to identify problems with the fiber connection. You can ping an IP address to help you identify problems.
Traceroute	Traceroute Diagnostics	Use this screen to identify problems with the fiber connection. You can trace the route that packets take to help you identify problems.
Maintenance		
Reboot	Reboot	Use this screen to reboot the FMG without turning the power off.
Backup/Restore	Backup and Restore Settings	Use this screen to backup and restore your FMG's configuration (settings) or reset the factory default settings.
Password	Password Configuration	Use this screen to change user password on the FMG.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your FMG.
Time Zone	Time Zone Configuration	Use this screen to change your FMG's time and date.
Statistics		
Interface	Interface Statistics	Use this screen to view the status of all network traffic going through the LAN ports of the FMG.
Fiber	Fiber Statistics	Use this screen to view the status of all network traffic going through the fiber connection on the FMG.

PART II
Technical Reference

CHAPTER 3
Status

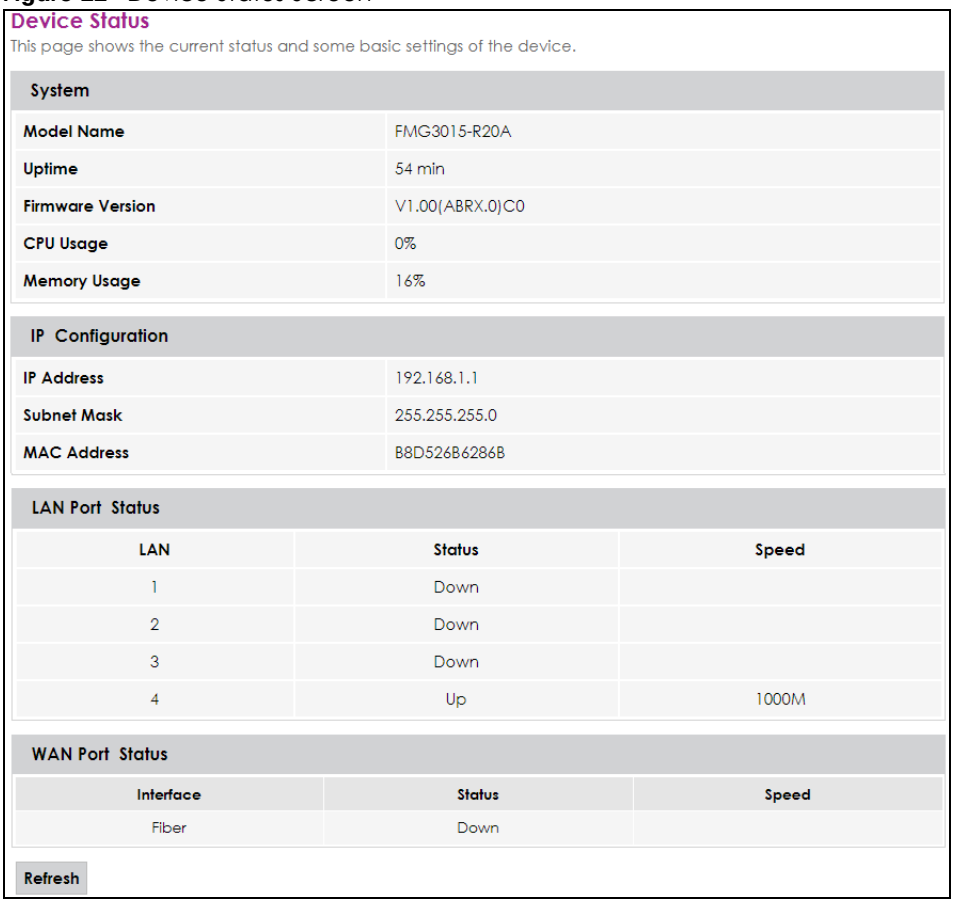
3.1 Overview

You can use the **Status** screens to look at the current status of the FMG and the fiber connection.

3.2 The Device Status Screen

Use this screen to view the status of the FMG. Click **Status > Device** to open this screen.

Figure 11 Device Status Screen



Device Status

This page shows the current status and some basic settings of the device.

System	
Model Name	FMG3015-R20A
Uptime	54 min
Firmware Version	V1.00(ABRX.0)C0
CPU Usage	0%
Memory Usage	16%

IP Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
MAC Address	B8D526B6286B

LAN Port Status

LAN	Status	Speed
1	Down	
2	Down	
3	Down	
4	Up	1000M

WAN Port Status

Interface	Status	Speed
Fiber	Down	

Refresh

Each field is described in the following table.

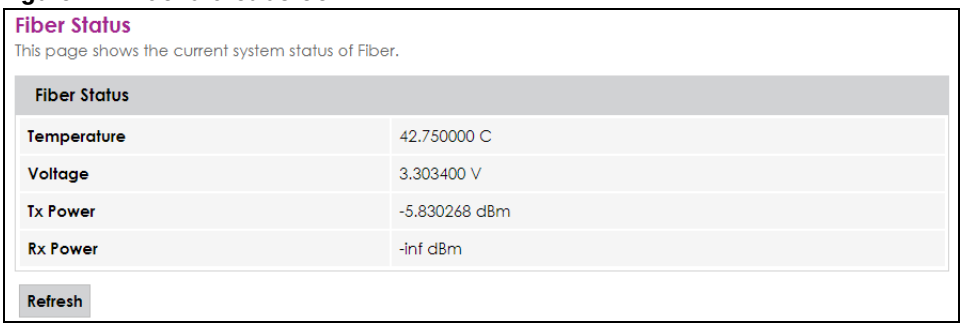
Table 8 Device Status Screen

LABEL	DESCRIPTION
System	
Model Name	This shows the model number of your FMG.
Uptime	This field displays how long the FMG has been running since it last started up. The FMG starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it.
Firmware Version	This is the current version of the firmware inside the FMG.
CPU Usage	This field displays what percentage of the FMG's processing ability is currently used. When this percentage is close to 100%, the FMG 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.
Memory Usage	This field displays what percentage of the FMG's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the FMG is probably becoming unstable, and you should restart the device. See Section 8.2 on page 39, or turn off the device (unplug the power) for a few seconds.
IP Configuration	
IP Address	This is the current IP address of the FMG in the LAN/WAN. If the FMG has a fiber connection, this field will show the WAN IP address.
IP Subnet Mask	This is the current subnet mask in the LAN.
MAC Address	This shows the LAN Ethernet adapter MAC (Media Access Control) Address of your FMG.
LAN/WAN Port Status	
LAN	This column displays each interface the FMG has.
Status	This field indicates the interface's use status. This field displays **Up** when using the interface and **Down** when not using the interface.
Speed	This displays the port speed and duplex setting.
Refresh	Click this to update the information in this screen.

3.3 Fiber Status

Use this screen to view the status of the FMG. Click **Status > Fiber** to open this screen.

Figure 12 Fiber Status Screen



Each field is described in the following table.

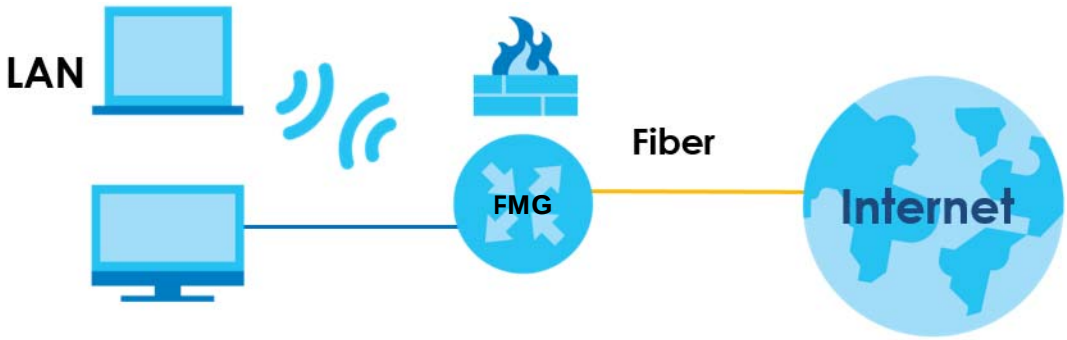
Table 9 Fiber Status Screen

LABEL	DESCRIPTION
Fiber Status	
Temperature	This displays the temperature in Celsius. The normal range is 0-70 degrees.
Voltage	This displays the voltage in Volts. The normal range is 3.13-3.47 Volts.
Tx Power	This displays the optical transmitting power in dBm.
Rx Power	This displays the optical receiving power in dBm. The normal range is -28 to -8 dBm.
Refresh	Click **Refresh** to reload the page.

CHAPTER 4
LAN

4.1 LAN 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.



4.1.1 What You Can Do in this Chapter

- Use the **LAN** screen to set the LAN IP address and subnet mask of your FMG (Section 4.2 on page 24).

4.1.2 What You Need To Know

4.1.2.1 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.

4.2 The Setup LAN Interface Screen

Use this screen to set the Local Area Network IP address and subnet mask of your FMG. Click **LAN > Setup LAN Interface** to open the **Setup LAN Interface** screen.

Follow these steps to configure your LAN settings.

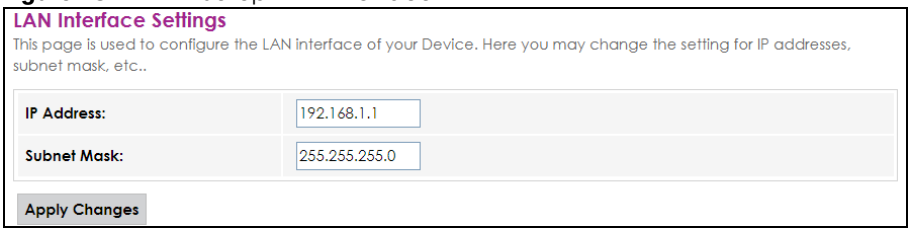
1 Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your FMG.

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 Changes** to save your settings.

If the FMG has a WAN IP address, this screen won't be configurable.

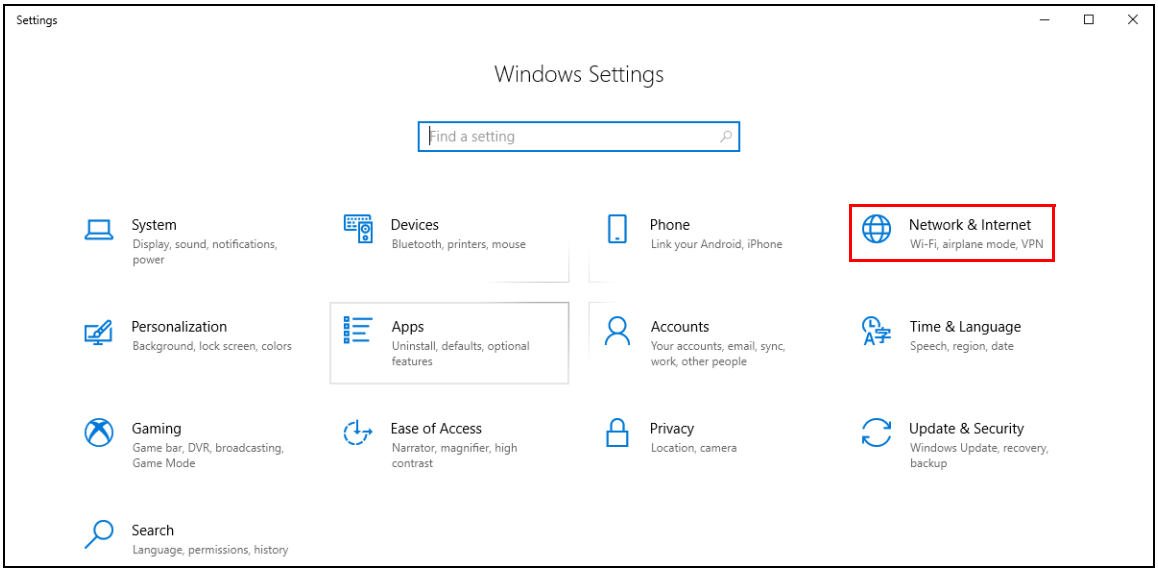
Figure 13 LAN > Setup LAN Interface



The following table describes the fields in this screen.

Table 10 LAN > Setup LAN Interface

LABEL	DESCRIPTION
LAN Interface Settings	
IP Address	Enter the LAN IPv4 IP address you want to assign to your FMG 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 FMG 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.
Apply Changes	Click **Apply Changes** to save your changes.


Settings
Windows Settings
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, other people
Time & Language
Speech, region, date
Gaming
Game bar, DVR, broadcasting, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Privacy
Location, camera
Update & Security
Windows Update, recovery, backup
Search
Language, permissions, history

CHAPTER 5
Advance

5.1 QoS 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 applications such as video-on-demand.

Configure QoS on the FMG 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 FMG 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. There are eight priority levels, with 1 having the highest priority.

This chapter contains information about configuring QoS and editing classifiers.

5.1.1 What You Can Do in this Chapter

- The **Queue setting** screen lets you configure QoS queue assignments (Section 5.3 on page 28).
- The **QoS Classification** screen lets you add, edit or delete QoS classifiers (Section 5.4 on page 29).

5.2 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.

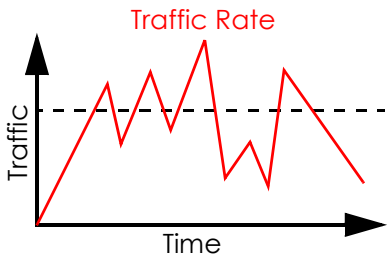
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

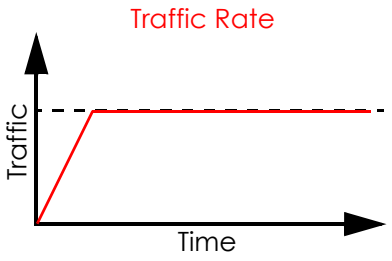
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or 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 FMG uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



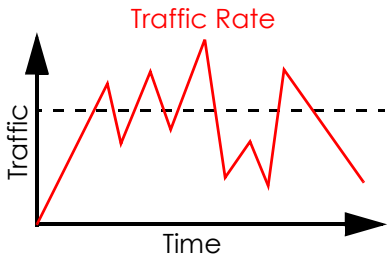
(Before Traffic Shaping)



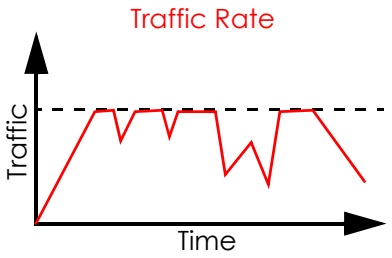
(After Traffic Shaping)

Traffic Policing

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



(Before Traffic Policing)



(After Traffic Policing)

The FMG 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 5.5 on page 31 for more information on each metering algorithm.

5.3 The Queue setting Screen

Click **Advance > Queue setting** to open the screen as shown next.

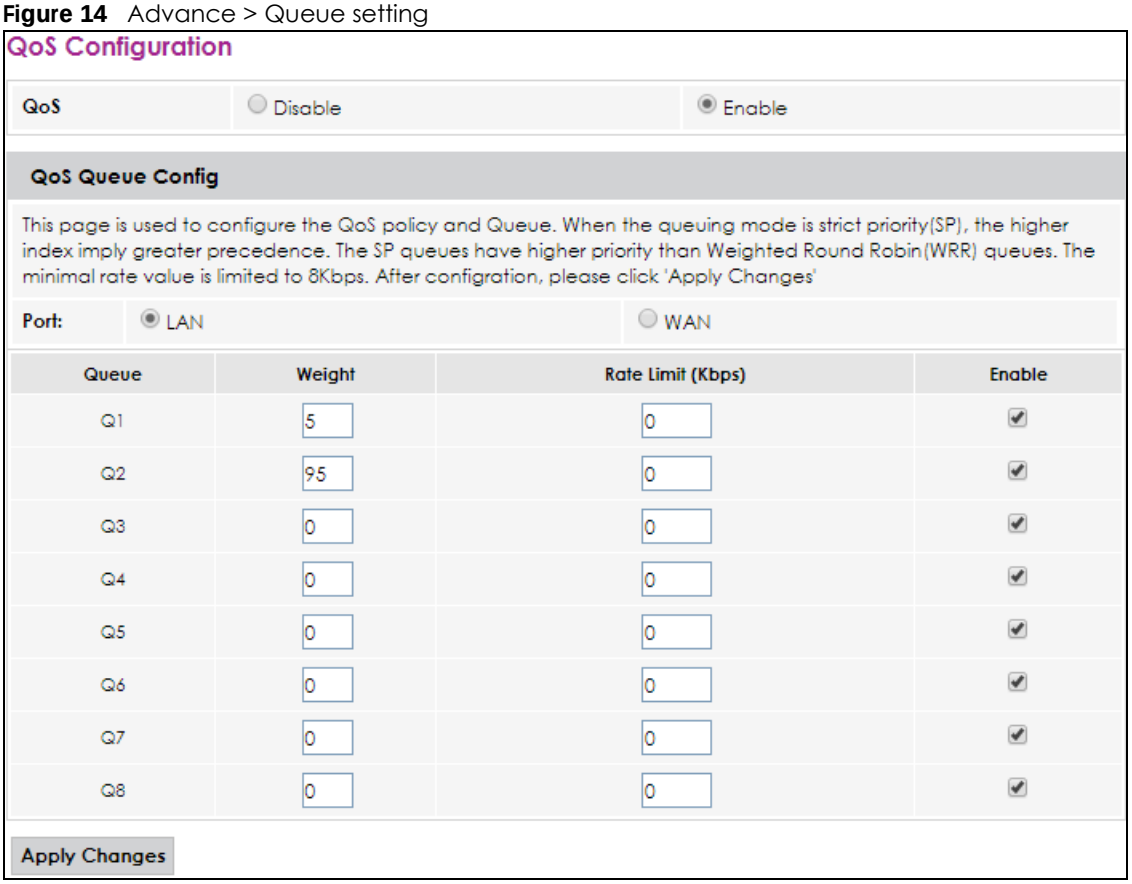
Use this screen to configure QoS queue assignment to decide the priority on WAN/LAN interfaces. Traffic with higher priority gets through faster than those with lower priority. Low-priority traffic is dropped first when the network is congested.

Note: Configure the priority level for a QoS queue from 1 to 8. The smaller the number in the **Priority** column, the higher the priority.

Note: The corresponding classifiers will be removed automatically if a queue is deleted.

Note: Rate limit 0 means there's no rate limit on a queue.

Figure 14 Advance > Queue setting



The following table describes the labels in this screen.

Table 11 Advance > Queue setting

LABEL	DESCRIPTION
QoS	Click this to enable or disable QoS.
Port	Select the interface to which this queue is applied.
Queue	This shows the index number of this queue.
Weight	This shows the weight of this queue.

Table 11 Advance > Queue setting (continued)

LABEL	DESCRIPTION
Rate Limit (Kbps)	This shows the maximum transmission rate allowed for traffic on this queue. Rate limit 0 means there's no rate limit on this queue.
Enable	Select this to enable or disable this queue.
Apply Changes	Click **Apply Changes** to save your changes.

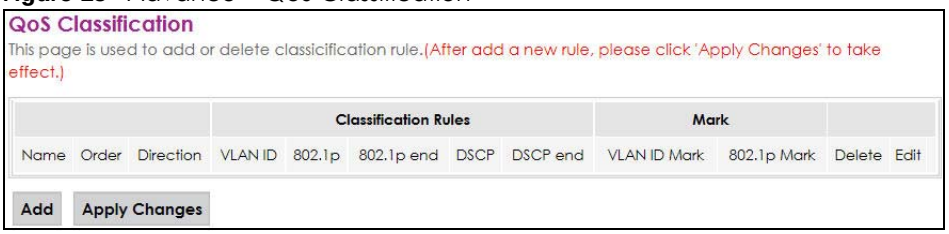
5.4 The QoS Classification Screen

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 FMG forwards 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 **Advance > QoS Classification** to open the following screen.

Figure 15 Advance > QoS Classification



The following table describes the labels in this screen.

Table 12 Advance > QoS Classification

LABEL	DESCRIPTION
Name	Enter a descriptive name of up to 15 printable English keyboard characters, not including spaces.
Order	This is the index number of the entry. The classifiers are applied in order of their numbering.
Direction	Select the direction (**Upstream** or **Downstream**) that you want to allocate using QoS.
Classification Rules	
VLAN ID	This is the VLAN ID number to identify the traffic of this classifier.
802.1p	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.
802.1p end	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.
DSCP	Enter a DSCP (DiffServ Code Point) number between 0 and 63 in this field.
DSCP end	Enter a DSCP (DiffServ Code Point) number between 0 and 63 in this field.
Mark	
VLAN ID Mark	Enter a VLAN ID number with which the FMG replaces the VLAN ID of the frames.

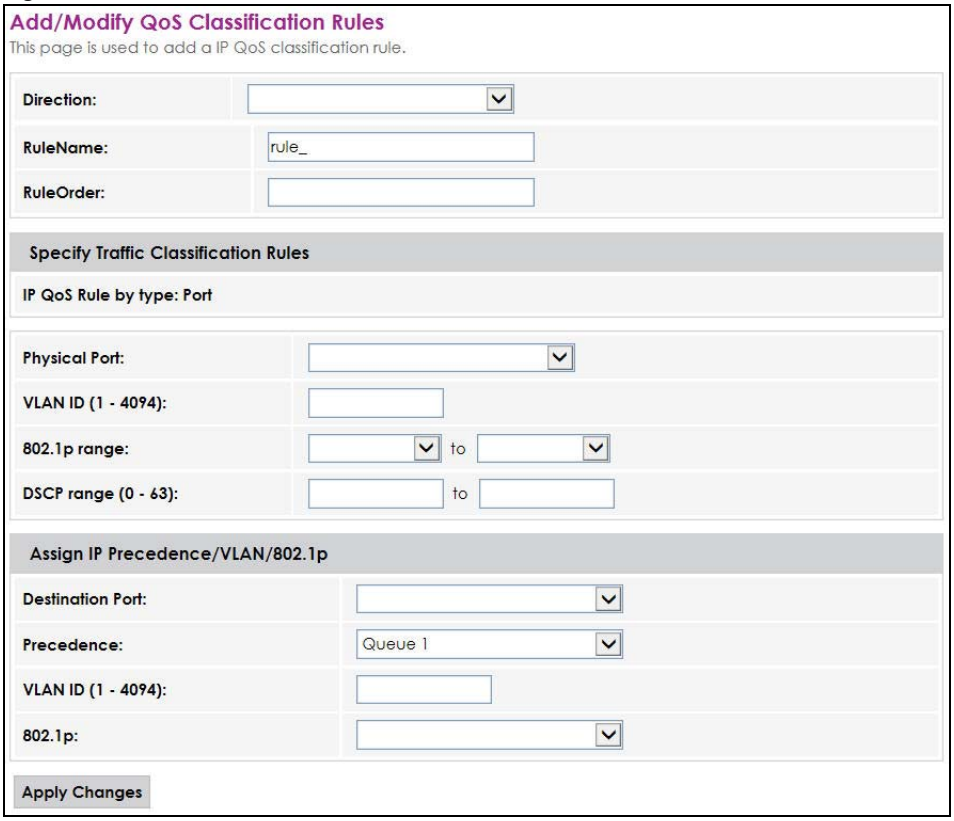
Table 12 Advance > QoS Classification (continued)

LABEL	DESCRIPTION
802.1p Mark	Enter a priority level with which the FMG replaces the IEEE 802.1p priority field in the packets.
Delete	Use this to delete an existing classifier. Note that subsequent rules move up by one when you take this action.
Edit	Use this to edit the classifier.
Add	Click **Add** to create a new classifier.
Apply Changes	Click **Apply Changes** to save your changes.

5.4.1 Add/Modify QoS Classification Rules

Click **Add** in the **QoS Classification** screen to open the following screen.

Figure 16 QoS Classification



The following table describes the labels in this screen.

Table 13 QoS Classification: Add/Modify

LABEL	DESCRIPTION
Direction	Select the direction (**Upstream** or **Downstream**) that you want to allocate using QoS.
RuleName	Enter a descriptive name of up to 15 printable English keyboard characters, not including spaces.
RuleOrder	Enter a number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply Changes**.
Specify Traffic Classification Rules	

Table 13 QoS Classification: Add/Modify

LABEL	DESCRIPTION
IP QoS Rule by type: Port	
Physical Port	If you want to classify the traffic by an ingress interface, select an interface from the drop-down list box.
VLAN ID (1-4094)	Enter the source VLAN ID in this field.
802.1p range	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.
DSCP range (0 - 63)	Enter a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
Assign IP Precedence/VLAN/802.1p	
Destination Port	If you want to classify the traffic by an engress interface, select an interface from the drop-down list box.
Precedence	Enter a range from Queue1 to 8 to re-assign IP precedence to matched traffic. 1 is the lowest Mark priority and 8 is the highest.
VLAN ID (1-4096)	Enter the target VLAN ID in this field.
802.1p	IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types (between 0 and 7).
Apply Changes	Click **Apply Changes** to save your changes.

5.5 Technical Reference

The following section contains additional technical information about the FMG 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 14 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".

Table 14 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
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

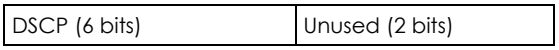
QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

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.



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 FMG, the FMG 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 FMG. On the FMG, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 15 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 FMG stops transmitting until enough tokens are generated.

- If not enough tokens are available, the FMG 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 FMG 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 FMG 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 FMG 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 6
Diagnostic

6.1 Diagnostic Overview

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

The route between a Central Office Very-high-bit-rate Digital Subscriber Line (CO VDSL) switch and one of its Customer-Premises Equipment (CPE) may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

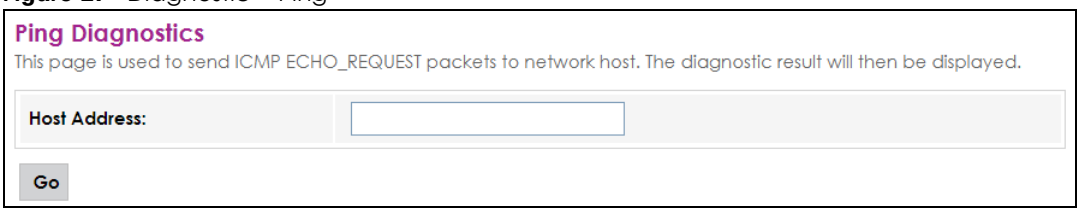
6.1.1 What You Can Do in this Chapter

- The **Ping** screen lets you ping an IP address to a host (Section 6.2 on page 36).
- The **Traceroute** screen lets you trace the route that packets take to a host (Section 6.3 on page 37).

6.2 Ping

Use this screen to ping IP address for troubleshooting. Ping is used to test whether a particular host is reachable. After entering an IP address and clicking **Go** to start a test, the results will show. Click **Diagnostic > Ping** to open the screen shown next.

Figure 17 Diagnostic > Ping



The following table describes the fields in this screen.

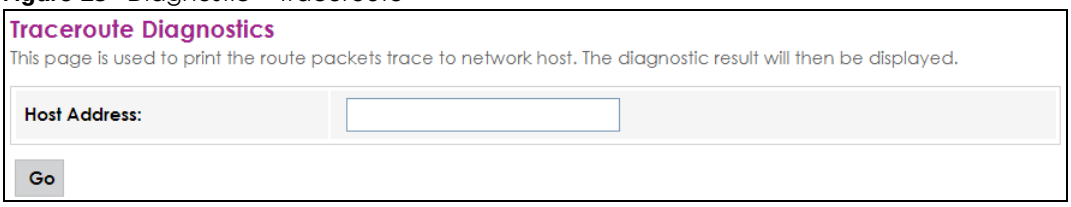
Table 16 Diagnostic > Ping

LABEL	DESCRIPTION
Host Address	Type the IP address of a computer that you want to perform ping in order to test a connection.
Ping	Click this to ping the IPv4 address that you entered.

6.3 Traceroute

Use this screen to trace the route that packets take for troubleshooting. After entering an IP address and clicking **Go** to start a test, the results will show. Click **Diagnostic > Traceroute** to open the screen shown next.

Figure 18 Diagnostic > Traceroute



The following table describes the fields in this screen.

Table 17 Diagnostic > Traceroute

LABEL	DESCRIPTION
Host Address	Type the IP address of a computer that you want to perform traceroute in order to test a connection.
Trace Route	Click this to display the route path and transmission delays between the FMG to the IPv4 address that you entered.

CHAPTER 7
Reboot

7.1 The Reboot Overview

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

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

Figure 19 Maintenance > Reboot

CHAPTER 8
Backup Restore

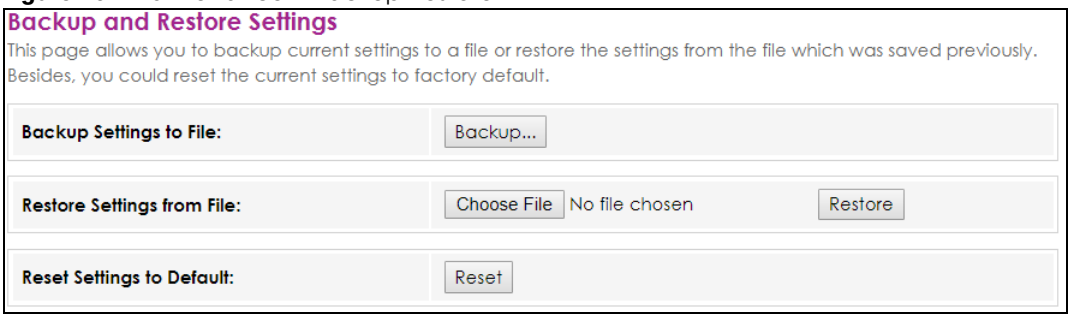
8.1 Backup Restore Overview

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

8.2 The Backup Restore Screen

Click **Maintenance > Backup Restore**. Information related to factory default settings and backup configuration are shown in this screen. You can also use this to restore previous device configurations.

Figure 20 Maintenance > Backup Restore



Backup Configuration

Backup Configuration allows you to back up (save) the FMG's current configuration to a file on your computer. Once your FMG 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 FMG'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 FMG.

Table 18 Restore Configuration

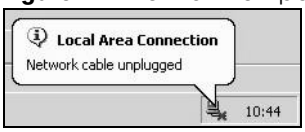
LABEL	DESCRIPTION
Choose File	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Restore	Click this to begin the upload process.

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

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

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

Figure 21 Network Temporarily Disconnected



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).

Reset Configuration

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

Figure 22 Reset Warning Message

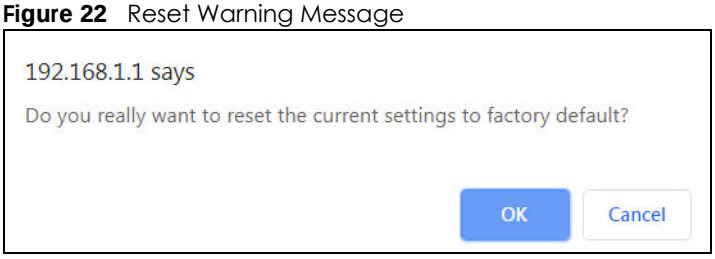
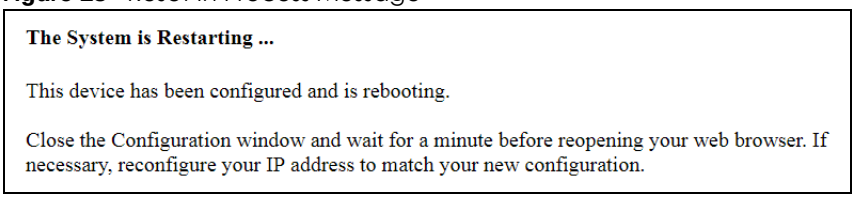


Figure 23 Reset In Process Message



You can also press the **RESET** button on the rear panel to reset your FMG to the factory default mode. Refer to Section 1.4.2.2 on page 13 for more information on the **RESET** button.

CHAPTER 9
Password

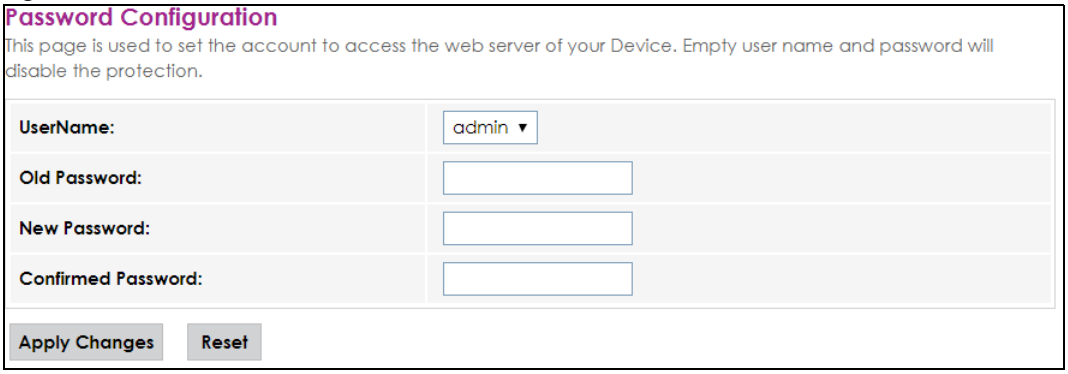
9.1 Password Overview

In the **Password** screen, you can change the login password for the "admin" account.

9.2 The Password Screen

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

Figure 24 Maintenance > Password



The following table describes the labels in this screen.

Table 19 Maintenance > Password

LABEL	DESCRIPTION
User Name	This field displays **admin** used to log into the FMG web configurator.
Old Password	Type the existing system password (see the device label for the default password).
New Password	Type your new system password (up to 30 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 FMG.
Confirmed Password	Type the new password again for confirmation.
Apply Changes	Click **Apply Changes** to save your changes.
Reset	Click **Reset** to return to clear the fields in this screen.

CHAPTER 10
Firmware Upgrade

10.1 Firmware Upgrade Overview

This screen lets you upload new firmware to your FMG. You can download new firmware releases from your nearest Zyxel FTP site (or www.zyxel.com) to upgrade your device's performance.

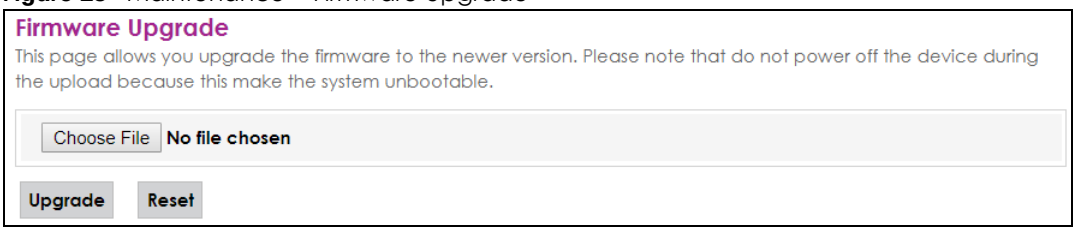
Only use firmware for your device's specific model. Refer to the device label of your FMG.

10.2 The Firmware Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. Download the latest firmware file from the Zyxel website and upload it to your FMG using this screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the FMG will reboot.

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

Figure 25 Maintenance > Firmware Upgrade

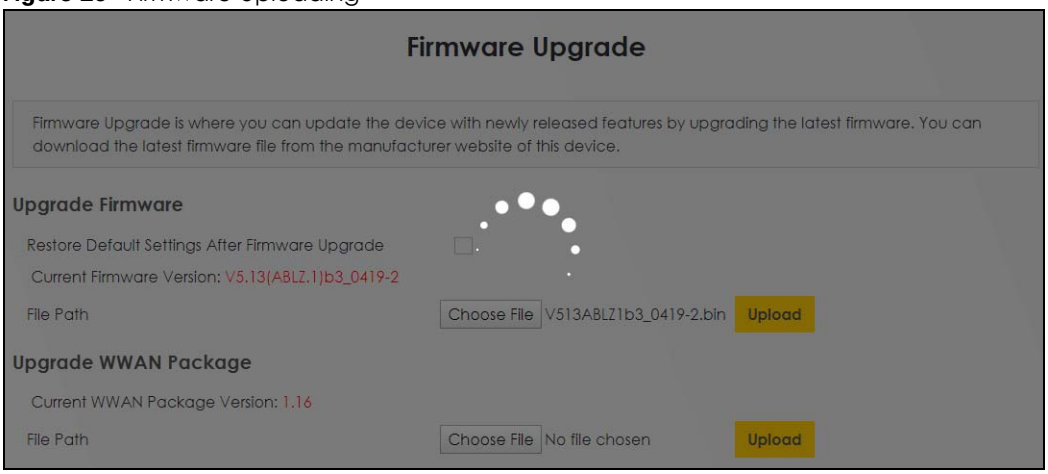


The following table describes the labels in this screen. After you see the firmware updating screen, wait two minutes before logging into the FMG again.

Table 20 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.
Upgrade	Click this to begin the upload process. This process may take up to two minutes.
Reset	Click this to clear the selected file.

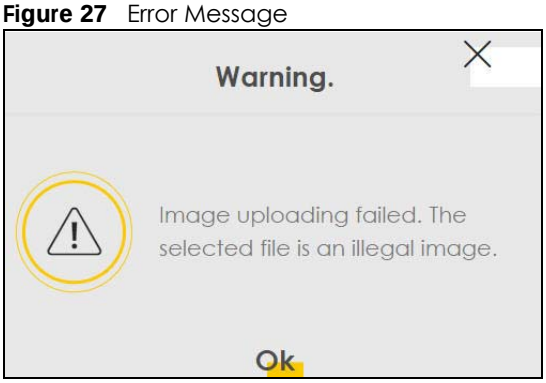
Figure 26 Firmware Uploading



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

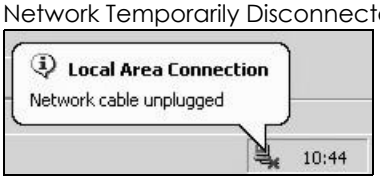
If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 27 Error Message



Note that the FMG automatically restarts during the upload, causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Network Temporarily Disconnected



CHAPTER 11
Time Zone

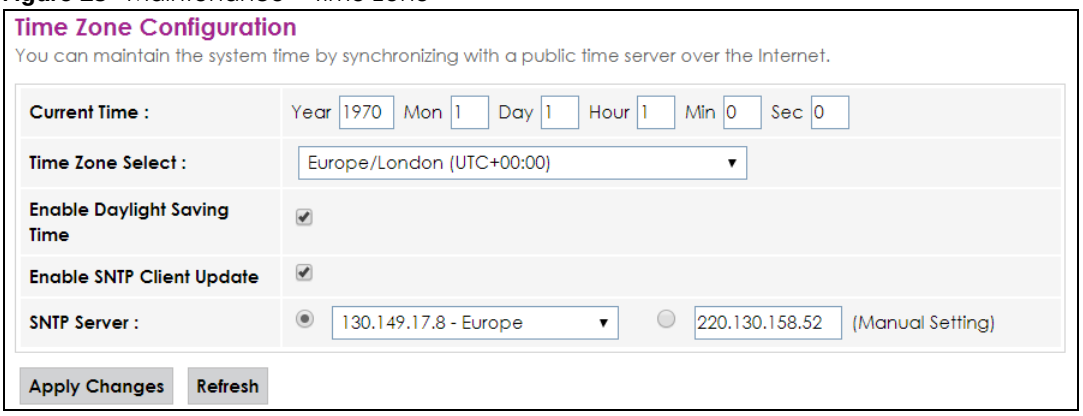
11.1 Time Zone Overview

Use the **Time Zone** screen to setup the system time and SNTP (Simple Network Time Protocol) server settings.

11.2 The Time Zone Screen

In the navigation panel, click **Maintenance** > **Time Zone** to display the screen as shown.

Figure 28 Maintenance > Time Zone



The following table describes the labels in this screen.

Table 21 Maintenance > Time Zone

LABEL	DESCRIPTION
Current Time	This field displays the time of your FMG. Each time you reload this page, the FMG synchronizes the time with the time server.
Time Zone Select	Select the time zone from the dropdown list.
Enable Daylight Saving Time	Select the check box to use Daylight Saving Time to offset the system time or clear the check box to not adjust system time.
Enable SNTP Client Update	Select the check box to enable using a simple network time protocol (SNTP) server to manage the system time or clear the check box to manually manage system time.
SNTP Server	Enter the address of the simple network time protocol (SNTP) server as an IP address (192.168.0.1) or as a URL (www.zyxel.com). Enter the port number of the SNTP server. The numeric value can be between 1 and 65535.
Apply	Click **Apply** to save the changes.
Refresh	Click **Refresh** to reload the page.

CHAPTER 12
Statistics

12.1 Overview

Use the **Statistics** screens to look at the network traffic status and statistics of the LAN interfaces and fiber connection.

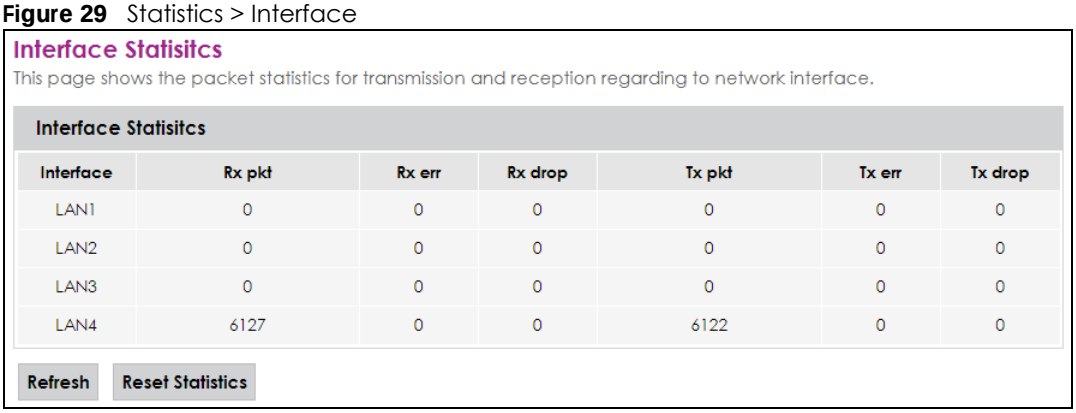
12.1.1 What You Can Do in this Chapter

- Use the **Interface** screen to view the LAN traffic statistics (Section 12.2 on page 45).
- Use the **Fiber** screen to view the traffic statistics of the fiber connection (Section 12.3 on page 46).

12.2 Interface

Click **Statistics > Interface** to open the following screen. Figures about data that have been sent to and received from each LAN port (including wireless) are displayed in the following table.

Figure 29 Statistics > Interface



The following table describes the fields in this screen.

Table 22 Statistics > Interface

LABEL	DESCRIPTION
Interface	This shows the LAN or WLAN interface.
Rx pkt	This indicates the number of received packets on this interface.
Rx err	This indicates the number of frames with errors received on this interface.
Rx drop	This indicates the number of received packets dropped on this interface.
Tx pkt	This indicates the number of transmitted packets on this interface.
Tx err	This indicates the number of frames with errors transmitted on this interface.
Tx drop	This indicates the number of outgoing packets dropped on this interface.

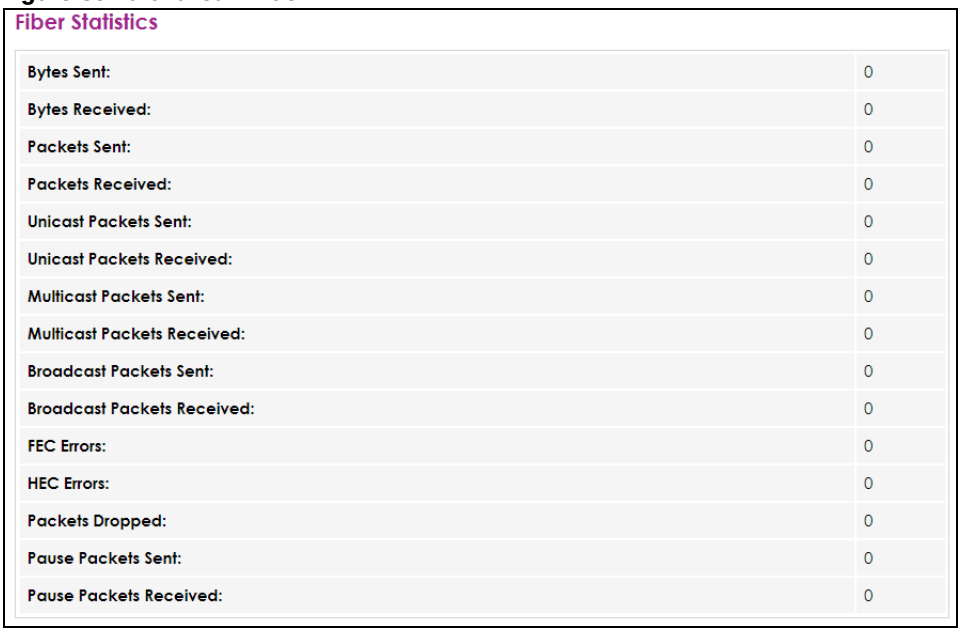
Table 22 Statistics > Interface (continued)

LABEL	DESCRIPTION
Refresh	Click **Refresh** to reload the page.
Reset Statistics	Click **Reset Statistics** to clear the statistics.

12.3 Fiber

Click **Statistics > Fiber** to open the following screen. Figures about data that have been sent out to and received on the fiber connection are displayed in the following table.

Figure 30 Statistics > Fiber



The following table describes the fields in this screen.

Table 23 Statistics > Fiber

LABEL	DESCRIPTION
Bytes Sent	This indicates the number of bytes transmitted on the fiber connection.
Bytes Received	This indicates the number of bytes received on this interface.
Packets Sent	This indicates the number of transmitted packets on the fiber connection.
Packets Received	This indicates the number of received packets on the fiber connection.
Unicast Packets Sent	This indicates the number of unicast packets transmitted.
Unicast Packets Received	This indicates the number of unicast packets received.
Multicast Packets Sent	This indicates the number of multicast packets transmitted.
Multicast Packets Received	This indicates the number of multicast packets received.

Table 23 Statistics > Fiber (continued)

LABEL	DESCRIPTION
Broadcast Packets Sent	This indicates the number of broadcast packets transmitted.
Broadcast Packets Received	This indicates the number of broadcast packets received.
FEC Errors	This indicates the number of FEC (Forward Error Correction) errors on the fiber connection. FEC is a technique to control errors in packets and correct errors without transmitting the packets again. FEC adds redundant information in the packets, so the receivers can identify and correct the errors in the packets.
HEC Errors	This indicates the number of HEC (Header Error Control) errors on the fiber connection. HEC is a technique to detect and correct errors in the headers of a cell. If there's a single-bit error, HEC will detect and correct it. If there's a two-bit error, HEC can only detect the error, and the cell containing a two-bit error will be dropped. If errors occur in more than two bits, HEC neither detect nor correct the errors.
Packets Dropped	This indicates the number of packets dropped.
Pause Packets Sent	This field shows the number of 802.3x pause packets transmitted. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.
Pause Packets Received	This field shows the number of 802.3x pause packets received. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.

CHAPTER 13
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
- FMG Access and Login
- Internet Access

13.1 Power, Hardware Connections, and LEDs

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

1. Make sure the FMG is turned on.
2. Make sure you are using the power adapter included with the FMG.
3. Make sure the power adapter is connected to the FMG and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Press the **LED** button for more than two seconds to turn on the LEDs.
5. Turn the FMG off and on.
6. 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 1.4.1.1 on page 11.
2. Check the hardware connections.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the FMG off and on.
5. If the problem continues, contact the vendor.

13.2 FMG Access and Login

I forgot the IP address for the FMG.

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 FMG 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 FMG (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 1.4.2.2 on page 13.

I forgot the login password.

1. See the device label for the default login name and associated password.
2. If those do not work, you have to reset the device to its factory defaults. See Section 1.4.2.2 on page 13.

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 4.2 on page 24), 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 FMG.
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.4.1.1 on page 11.
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
4. Reset the device to its factory defaults, and try to access the FMG with the default IP address. See Section 1.4.2.2 on page 13.
5. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

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

1. Make sure you have entered the password correctly. See the cover page for the default login user name and associated password. The field is case-sensitive, so make sure [Caps Lock] is not on.
2. Turn the FMG off and on.
3. If this does not work, you have to reset the device to its factory defaults. See Section 13.1 on page 48.

13.3 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 1.4.1.1 on page 11.
2. Disconnect all the cables from your device and reconnect them.
3. Make sure the dust cap is removed from the FMG and fiber box.
4. If the problem continues, contact your ISP.

13.4 Cable Television Service

My cable television service doesn't work.

1. Disconnect the coaxial cable from the FMG, and connect it again.
2. Contact your service provider.

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
Legal Information

Copyright

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

CANADA

The following information applies if you use the product within Canada area

Innovation, Science and Economic Development Canada ICES statement

CAN ICES-3 (B)/NMB-3(B)

EUROPEAN UNION

The following information applies if you use the product within the European Union.

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.
- This reminder is provided to call the CATV systems installer's attention to Section 820-93 of the National Electric Code which provide grounding and, in particular, specify that the Coaxial cable shield shall be connected to the grounding system of the building, so close to the point of cable entry as practical.
- This product complies with 21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007.
- CLASS 1 LASER PRODUCT
- APPAREIL À LASER DE CLASS 1
- PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.
- PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

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.

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

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 at www.zyxel.com to receive e-mail notices of firmware upgrades and related information.

Trademarks

ZyNOS (Zyxel Network Operating System) and ZON (Zyxel One Network) are registered trademarks of Zyxel Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Open Source Licenses

This product may contain 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 . If you cannot find it there, contact your vendor or Zyxel Technical Support at support@zyxel.com.tw

To obtain the source code covered under those Licenses, please contact your vendor or Zyxel Technical Support at support@zyxel.com.

Index

Q

R

S

T

U

W