ZYXEL
Your Networking Ally

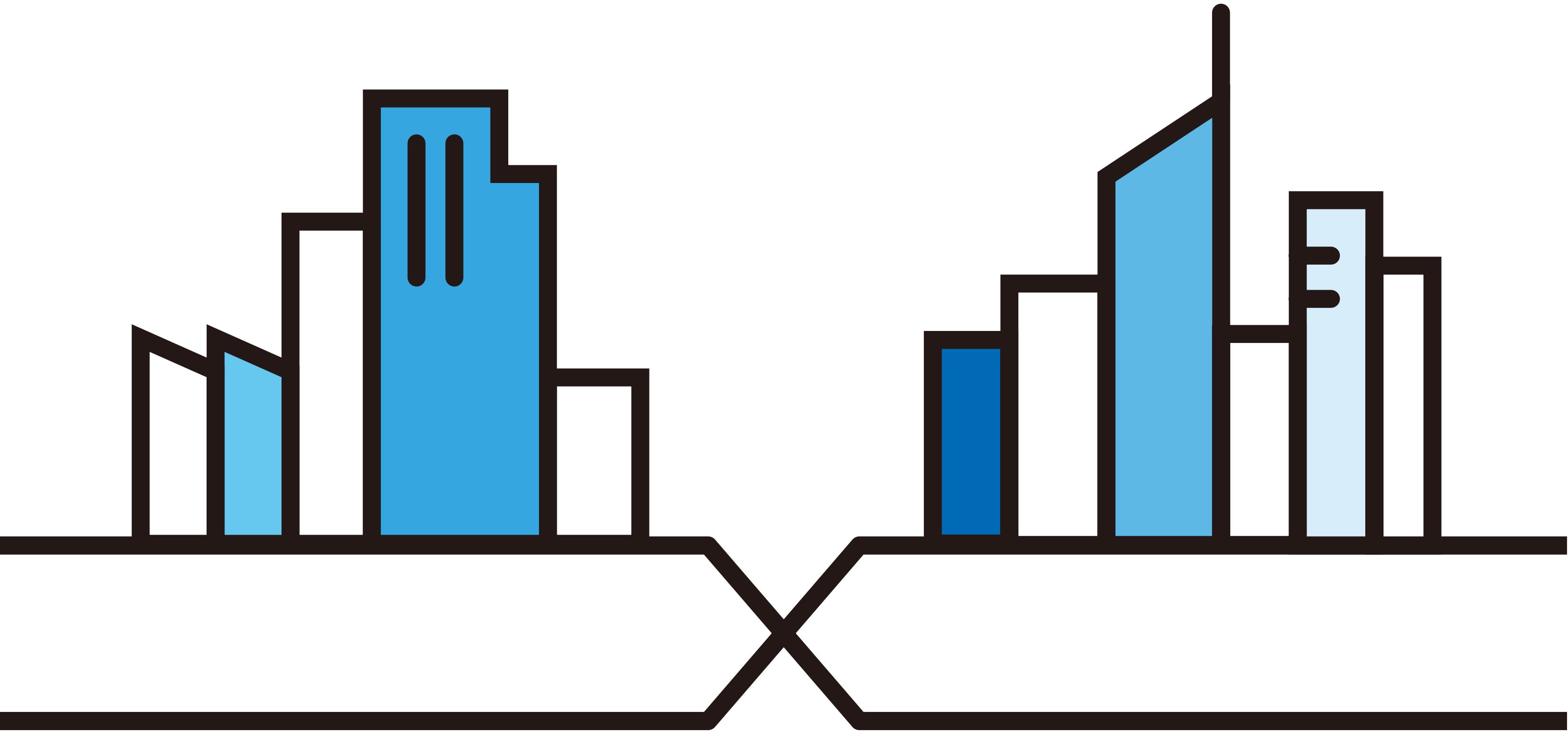
User's Guide

EMG6765-Q10A

AC2200 Gigabit Ethernet MoCA Gateway

Default Login Details	
LAN IP Address	http://192.168.1.1
User Name	admin
Password	(back-label default key)

Version 1.00 Edition 1, 05/2017



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the EMG6765-Q10A and access the Web Configurator wizards. It contains information on setting up your network and configuring for Internet access.

- More Information

  Go to **support.zyxel.com** to find other information on the EMG6765-Q10A.

Contents Overview

Table of Contents

PART I

User's Guide

CHAPTER 1 Introduction

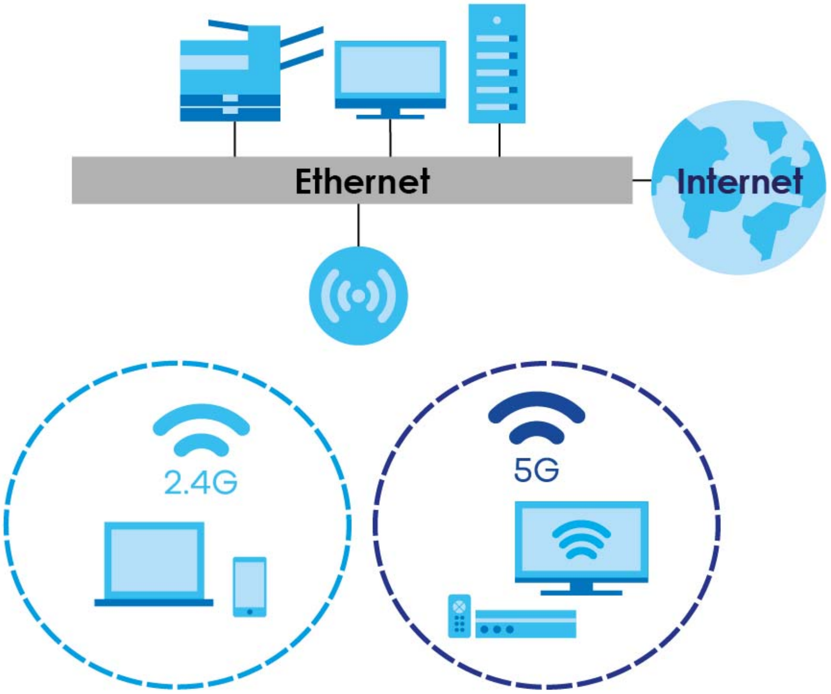
1.1 Overview

This chapter introduces the main features and applications of the EMG6765-Q10A.

The EMG6765-Q10A extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. You can set up a wireless network with other IEEE 802.11a/ac/b/g/n compatible devices.

The EMG6765-Q10A is a dual-band AP and able to function both 2.4G and 5G networks at the same time. You could use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz band for time sensitive traffic like high-definition video, music, and gaming.

Figure 1 Dual-Band Application



A range of services such as a firewall and content filtering are also available for secure Internet computing. There is one USB 2.0 port on the side panel of your EMG6765-Q10A, and the other one is on the rear panel of your EMG6765-Q10A. You can connect USB (version 2.0 or lower) memory sticks, USB hard drives, or USB devices for file sharing. The EMG6765-Q10A automatically detects the USB devices.

Make sure the USB LED is off before removing your USB device. This will remove your USB device safely, preventing file or data loss if it is being transmitted through the USB device.

Note: For the USB function, it is strongly recommended to use version 2.0 or lower USB storage devices (such as memory sticks, USB hard drives) and/or USB devices. Other USB products are not guaranteed to function properly with the EMG6765-Q10A.

The EMG6765-Q10A also comes with one coaxial port that supports MoCA (Multimedia over Coax Alliance) technology. Use MoCA technology to extend your network through a coaxial connection to another MoCA device and/or a device connected to a MoCA adapter.

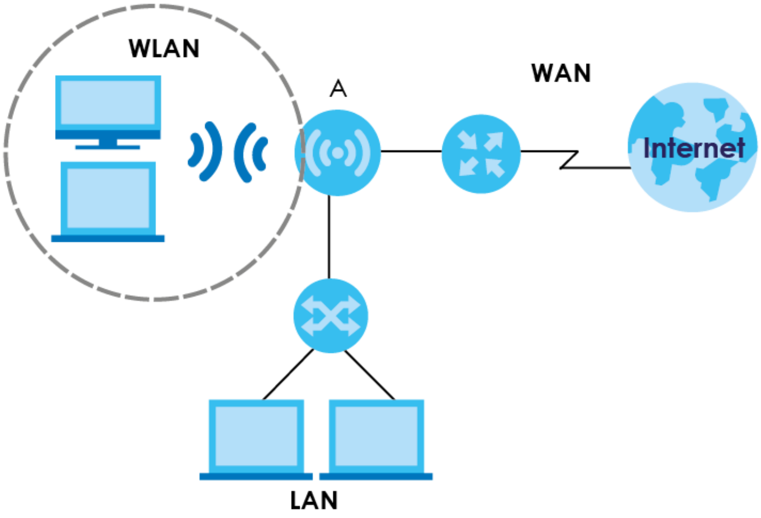
Use a (supported) web browser to manage the EMG6765-Q10A.

1.2 Applications

You can have the following networks with the EMG6765-Q10A:

- **Wired**. You can connect network devices via the Ethernet ports of the EMG6765-Q10A so that they can communicate with each other and access the Internet.
- **Wireless**. Wireless clients can connect to the EMG6765-Q10A to access network resources. You can use WPS (Wi-Fi Protected Setup) to create an instant network connection with another WPS-compatible device.
- **WAN**. Connect to a broadband modem/router for Internet access.

Figure 2 EMG6765-Q10A Networks



1.3 Ways to Manage the EMG6765-Q10A

Use any of the following methods to manage the EMG6765-Q10A.

- WPS (Wi-Fi Protected Setup). You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your EMG6765-Q10A.
- Web Configurator. This is recommended for everyday management of the EMG6765-Q10A using a (supported) web browser.

1.4 Good Habits for Managing the EMG6765-Q10A

Do the following things regularly to make the EMG6765-Q10A more secure and to manage the EMG6765-Q10A 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 EMG6765-Q10A to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the EMG6765-Q10A. You could simply restore your last configuration.

1.5 Resetting the EMG6765-Q10A

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **RESET** button at the back of the EMG6765-Q10A to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the user name will be reset to "admin", the password will be reset to the back-label default key, and the IP address will be reset to "192.168.1.1" (router mode).

1.5.1 RESET Button

1 Make sure the power LED is on.

2 Press and hold the **RESET** button for more than 5 seconds, the power LED begins flashing.

3 Release the **RESET** button. The EMG6765-Q10A reloads factory-default settings and begins to reboot.

1.5.2 The WPS Button

Your EMG6765-Q10A supports Wi-Fi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the Wi-Fi Alliance.

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

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) on 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.

You can use the WPS button ( ) on the side panel of the EMG6765-Q10A to activate WPS in order to quickly set up a wireless network with strong security.

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

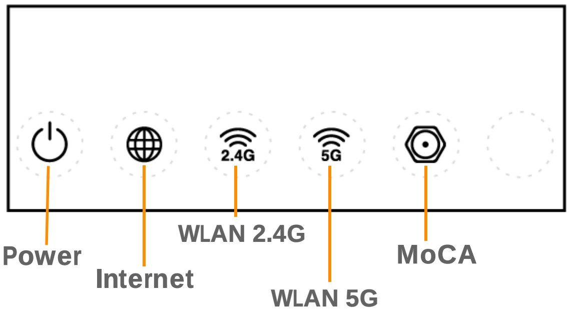
2 Press the WPS button for more than one second and release it. Press the WPS button on another WPS-enabled device within range of the EMG6765-Q10A.

Note: You must activate WPS on the EMG6765-Q10A and on another wireless device within two minutes of each other.

For more information on using WPS, see Section 6.8 on page 48.

1.6 Front Panel

The LED indicators are located on the front panel. Look at the LED lights on the front panel to determine the status of the EMG6765-Q10A. Front Panel



The following table describes the LEDs.

Table 1 Front Panel and Rear panel LEDs

LED	STATUS	DESCRIPTION
Power	On	The EMG6765-Q10A is receiving power and functioning properly.
	Off	The EMG6765-Q10A is not receiving power.
Internet	On	The EMG6765-Q10A has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the connection is up.
	Blinking	The EMG6765-Q10A is sending or receiving IP traffic.
	Off	The EMG6765-Q10A does not have an IP connection.
WLAN 2.4/5G (White)	On	The EMG6765-Q10A is ready, but is not sending/receiving data through the 5G wireless LAN.
	Blinking	The EMG6765-Q10A is sending/receiving data through the 5G wireless LAN. The EMG6765-Q10A is negotiating a WPS connection with a wireless client.
	Off	The wireless LAN is not ready or has failed.
WLAN 2.4/5G (Amber)	On	The EMG6765-Q10A is setting up a WPS connection with a 2.4GHz or 5GHz wireless client.
	Off	The 2.4 GHz or 5GHz WPS process is completed or failed.

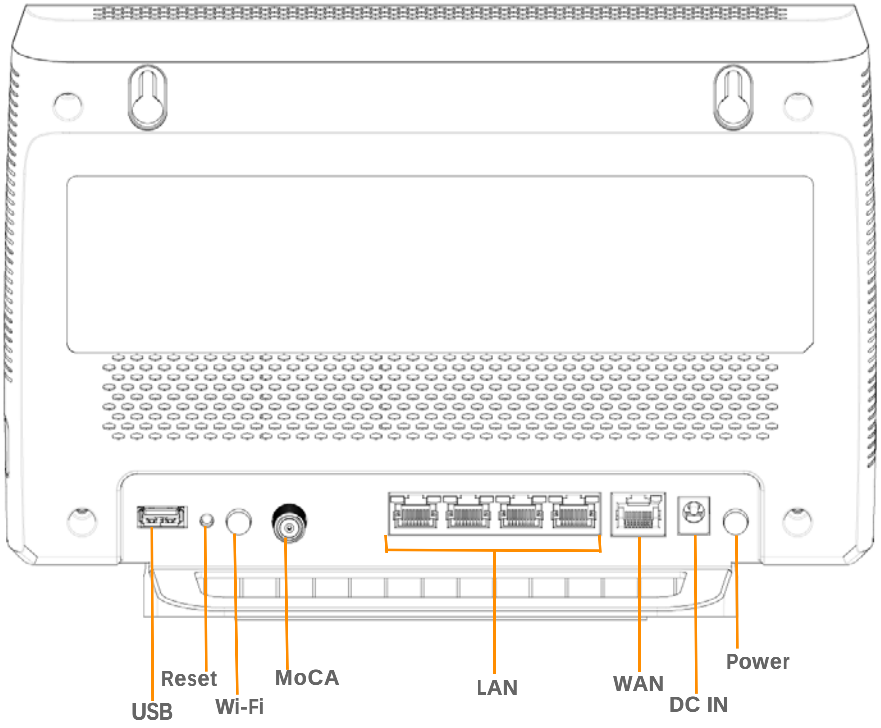
Table 1 Front Panel and Rear panel LEDs (continued)

LED	STATUS	DESCRIPTION
MoCA	On	The MoCA port is connected and the EMG6765-Q10A detects another MoCA device.
	Blinking	The EMG6765-Q10A is communicating with another MoCA device. Data is being transmitted and/or received through the coaxial cables.
	Off	The MoCA port is not connected, or the EMG6765-Q10A does not detect another MoCA device.
LAN 1-4 (Rear Panel)	On	The EMG6765-Q10A's LAN connection is ready.
	Blinking	The EMG6765-Q10A is sending/receiving data through the LAN with a 1000Mbps transmission rate.
	Off	The LAN connection is not ready, or has failed.
WAN (Rear Panel)	On	The EMG6765-Q10A's WAN connection is ready.
	Blinking	The EMG6765-Q10A is sending/receiving data through the WAN.
	Off	The WAN connection is not ready, or has failed.

1.7 Rear Panel

The connection ports are located on the rear panel.

Figure 3 Rear Panel



1.8 Wall Mounting

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

Table 2 Wall Mounting Information

Distance between holes	17.5 cm
M4 Screws	Two
Screw anchors (optional)	Two

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.

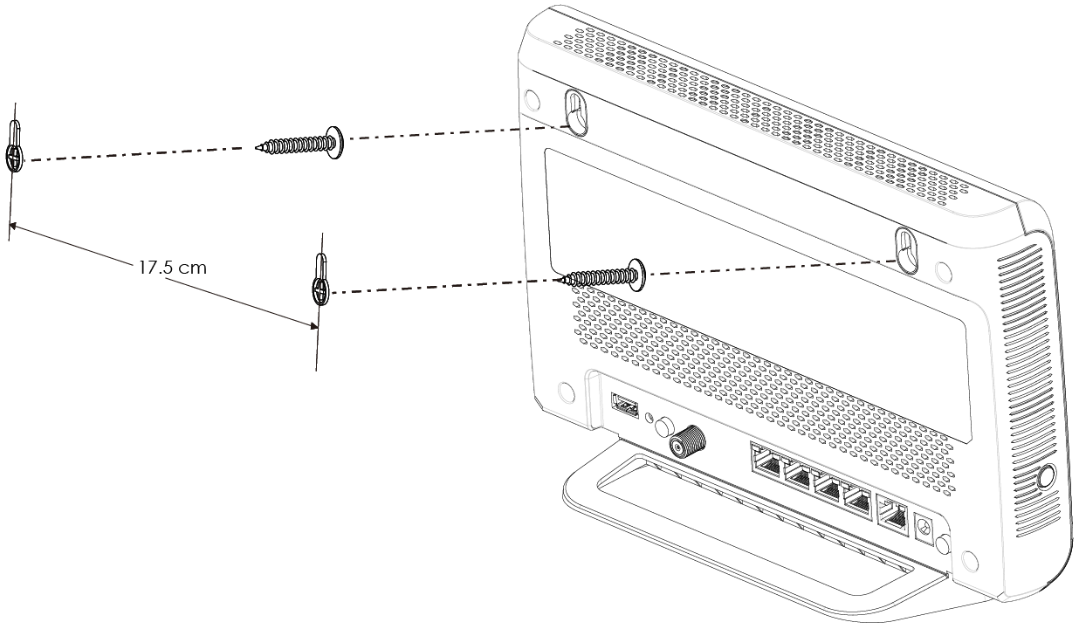
3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

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 EMG6765-Q10A with the connection cables.

5 Align the holes on the back of the EMG6765-Q10A with the screws on the wall. Hang the EMG6765-Q10A on the screws.

Figure 4 Wall Mounting Example



CHAPTER 2
Introducing the Web Configurator

2.1 Overview

This chapter describes how to access the EMG6765-Q10A Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the EMG6765-Q10A via Internet browser. Use Internet Explorer 9.0 and later versions, Mozilla Firefox 21 and later versions, Safari 6.0 and later versions or Google Chrome 26.0 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 device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter (Chapter 26 on page 184) to see how to make sure these functions are allowed in Internet Explorer.

2.2 Login Accounts

With the **admin** account, you cannot access **Remote MGMT** screens and can only view the **Sys OP Mode screen**. The default user name is “admin” and password is the back-label default key.

2.3 Accessing the Web Configurator

1. Make sure your EMG6765-Q10A hardware is properly connected and prepare your computer or computer network to connect to the EMG6765-Q10A (refer to the Quick Start Guide).

2. Launch your web browser.

3. The EMG6765-Q10A is in router mode by default. Type "http://192.168.1.1" as the website address.

   If the EMG6765-Q10A is in access point, the IP address is 192.168.1.2. See Chapter 3 on page 21 for more information about the modes of the EMG6765-Q10A.

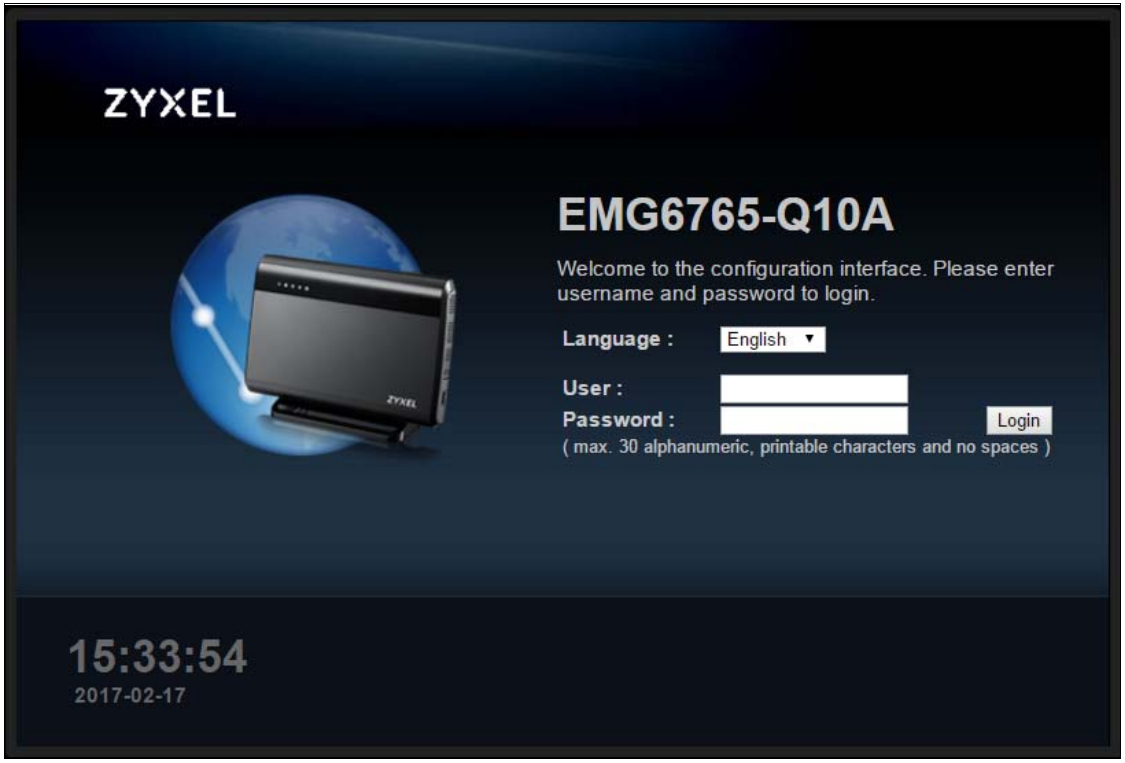
Your computer must be in the same subnet in order to access this website address.

2.3.1 Login Screen

The Web Configurator initially displays the following login screen.

If you are logging in with the "**admin**" account, type the back-label default key as the password. Then click **Login**.

Figure 5 Login screen



EMG6765-Q10A

Welcome to the configuration interface. Please enter username and password to login.

Language : English ▼

User :

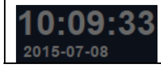
Password :

(max. 30 alphanumeric, printable characters and no spaces)

15:33:54
2017-02-17

The following table describes the labels in this screen.

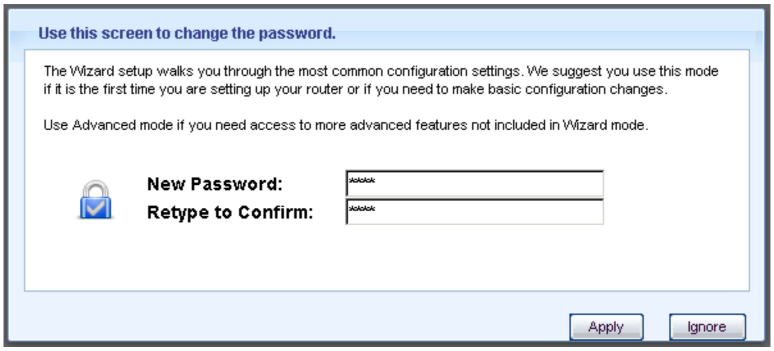
Table 3 Login screen

LABEL	DESCRIPTION
Language	Select the language you want to use to configure the Web Configurator.
User	Type "admin" (default) as the user name.
Password	Type the back-label default key as the password. Click **Login**.
 10:09:33 2015-07-08	This shows the time (hh:mm:ss) and date (yyyy:mm:dd) of the timezone you select in Section 25.5 on page 175. The time is in 24-hour format, for example 15:00 is 3:00 PM.

2.3.2 Password Screen

You should see a screen asking you to change your password (highly recommended) as shown next.

Figure 6 Change Password Screen



Use this screen to change the password.

The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.

Use Advanced mode if you need access to more advanced features not included in Wizard mode.

New Password: ****

Retype to Confirm: ****

The following table describes the labels in this screen.

Table 4 Change Password Screen

LABEL	DESCRIPTION
New Password	Type a new password.
Retype to Confirm	Retype the password for confirmation.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Ignore	Click **Ignore** if you do not want to change the password this time.

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to Chapter 25 on page 173 to change this). Simply log back into the EMG6765-Q10A if this happens.

CHAPTER 3
EMG6765-Q10A Modes

3.1 Overview

This chapter introduces the operating mode of your EMG6765-Q10A, or simply how the EMG6765-Q10A is being used in the network.

3.1.1 Device Modes

This refers to the operating mode of the EMG6765-Q10A, which can act as a:

- **Router**: This is the default device mode of the EMG6765-Q10A. Use this mode to connect the local network to another network, like the Internet. Go to Section 4.2 on page 22 to view the **Status** screen in this mode.
- **Access Point**: Use this mode if you want to extend your network by allowing network devices to connect to the EMG6765-Q10A wirelessly. Go to Section 5.4 on page 31 to view the **Status** screen in this mode.

For more information on these modes and to change the mode of your EMG6765-Q10A, refer to Chapter 25 on page 173.

Note: Choose your device mode carefully to avoid having to change it later.

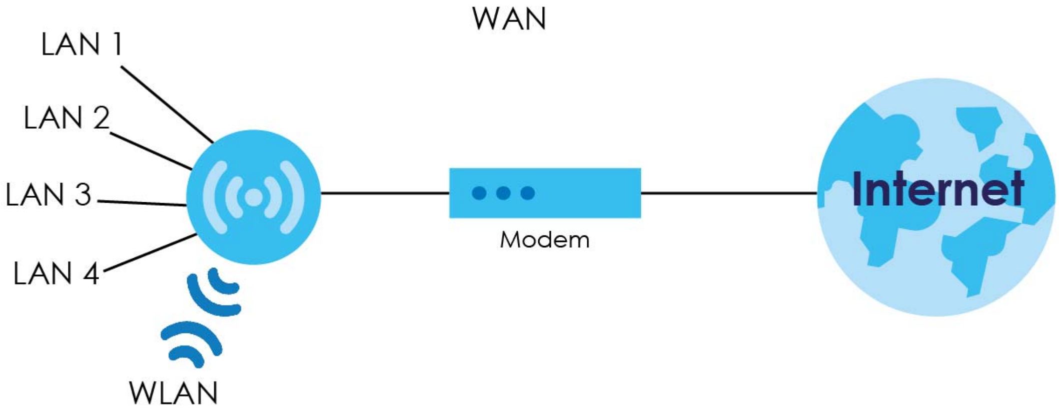
When changing to another mode, the IP address of the EMG6765-Q10A changes. The running applications and services of the network devices connected to the EMG6765-Q10A can be interrupted.

CHAPTER 4 Router Mode

4.1 Overview

The EMG6765-Q10A is set to router mode by default. Routers are used to connect the local network to another network (for example, the Internet). In the figure below, the EMG6765-Q10A connects the local network (**LAN1** ~ **LAN4**) to the Internet.

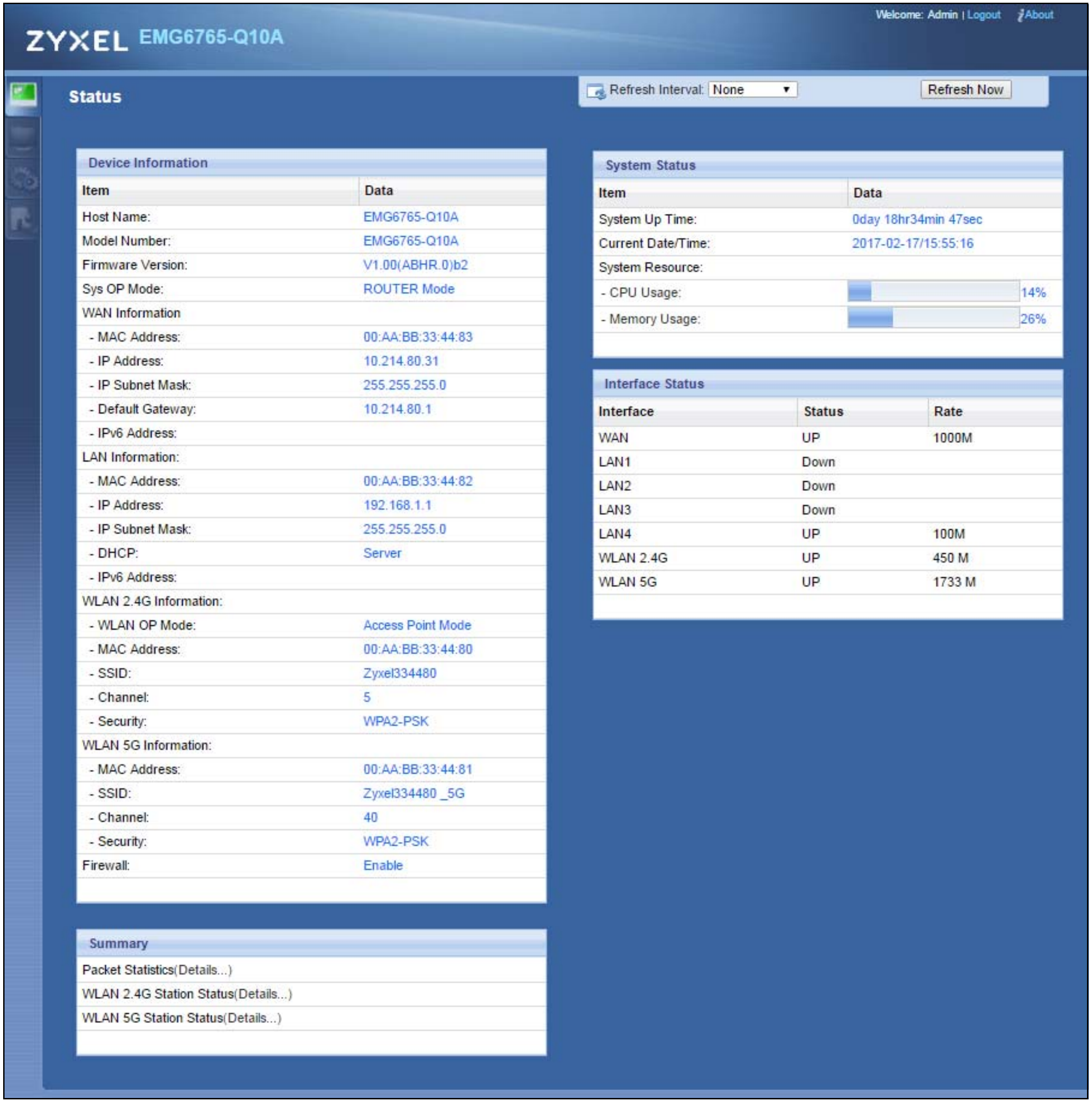
Figure 7 EMG6765-Q10A Network



4.2 Router Mode Status Screen

Click to open the status screen.

Figure 8 Status Screen: Router Mode



Device Information

Item	Data
Host Name:	EMG6765-Q10A
Model Number:	EMG6765-Q10A
Firmware Version:	V1.00(ABHR.0)b2
Sys OP Mode:	ROUTER Mode
WAN Information	
- MAC Address:	00:AA:BB:33:44:83
- IP Address:	10.214.80.31
- IP Subnet Mask:	255.255.255.0
- Default Gateway:	10.214.80.1
- IPv6 Address:	
LAN Information:	
- MAC Address:	00:AA:BB:33:44:82
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
- IPv6 Address:	
WLAN 2.4G Information:	
- WLAN OP Mode:	Access Point Mode
- MAC Address:	00:AA:BB:33:44:80
- SSID:	Zyxel334480
- Channel:	5
- Security:	WPA2-PSK
WLAN 5G Information:	
- MAC Address:	00:AA:BB:33:44:81
- SSID:	Zyxel334480 _5G
- Channel:	40
- Security:	WPA2-PSK
Firewall:	Enable

Summary

Packet Statistics(Details...)
WLAN 2.4G Station Status(Details...)
WLAN 5G Station Status(Details...)

System Status

Item	Data
System Up Time:	0day 18hr34min 47sec
Current Date/Time:	2017-02-17/15:55:16
System Resource:	
- CPU Usage:	14%
- Memory Usage:	26%

Interface Status

Interface	Status	Rate
WAN	UP	1000M
LAN1	Down	
LAN2	Down	
LAN3	Down	
LAN4	UP	100M
WLAN 2.4G	UP	450 M
WLAN 5G	UP	1733 M

The following table describes the icons shown in the **Status** screen.

Table 5 Status Screen Icon Key

ICON	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
About	Click this icon to view copyright and a link for related product information.
Refresh Interval: None	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
Refresh Now	Click this button to refresh the status screen statistics.
🖥	Click this icon to see the **Status** page. The information in this screen depends on the device mode you select.

Table 5 Status Screen Icon Key (continued)

ICON	DESCRIPTION
🖥	Click this icon to see the **Monitor** navigation menu.
⚙	Click this icon to see the **Configuration** navigation menu.
🔧	Click this icon to see the **Maintenance** navigation menu.

The following table describes the labels shown in the **Status** screen.

Table 6 Status Screen: Router Mode

LABEL	DESCRIPTION
Device Information	
Item	This column shows the type of data the EMG6765-Q10A is recording.
Data	This column shows the actual data recorded by the EMG6765-Q10A.
Host Name	This is the **System Name** you enter in the **Maintenance** > **General** screen. It is for identification purposes.
Model Number	This is the model name of your device.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 3.1.1 on page 21) to which the EMG6765-Q10A is set - **Router Mode**.
WAN Information	
MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
IP Address	This shows the WAN port's IP address.
IP Subnet Mask	This shows the WAN port's subnet mask.
Default Gateway	This shows the WAN port's gateway IP address.
IPv6 Address	This shows the IPv6 address of the EMG6765-Q10A on the WAN.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - **Server** or **Disable**.
IPv6 Address	This shows the IPv6 address of the EMG6765-Q10A on the LAN.
WLAN 2.4G Information	
WLAN OP Mode	This is the device mode (Section 3.1.1 on page 21) to which the EMG6765-Q10A's wireless LAN is set - **Access Point Mode**.
MAC Address	This shows the 2.4GHz wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the EMG6765-Q10A in the 2.4GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the EMG6765-Q10A is using.
WLAN 5G Information	
MAC Address	This shows the 5GHz wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the EMG6765-Q10A in the 5GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the EMG6765-Q10A is using.

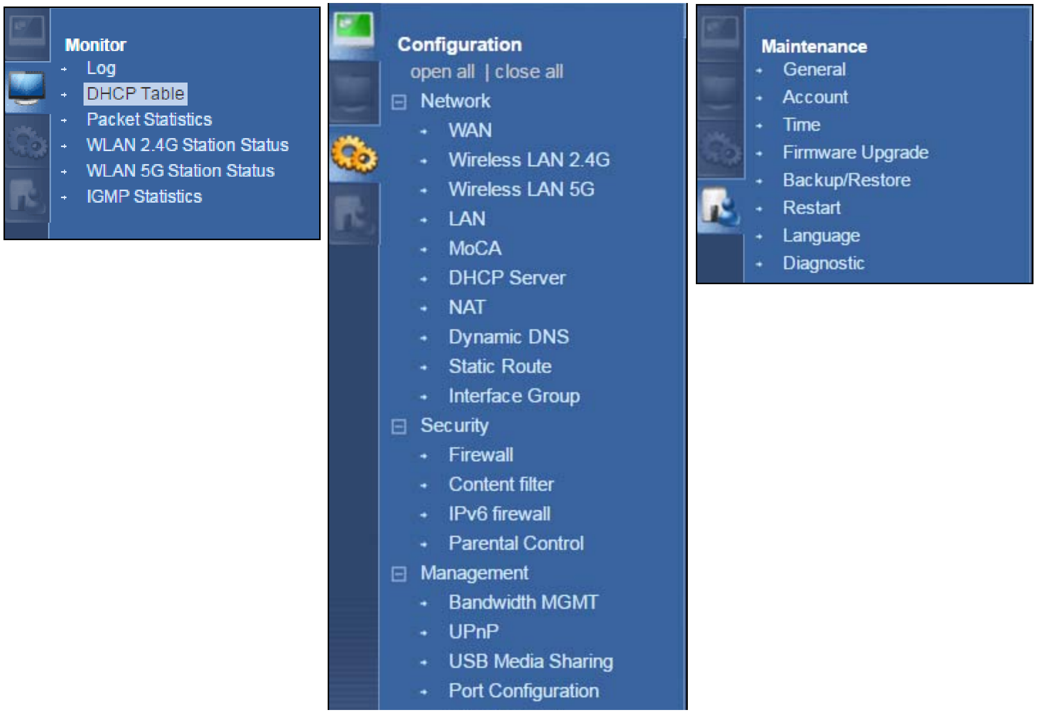
Table 6 Status Screen: Router Mode (continued)

LABEL	DESCRIPTION
Firewall	This shows whether the firewall is enabled or not.
Summary	
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen (Section 7.5 on page 56). Use this screen to view port status and packet specific statistics.
WLAN 2.4G Station Status	Click **Details...** to go to the **Monitor > WLAN 2.4G Station Status** screen (Section 7.6 on page 57). Use this screen to view the wireless stations that are currently associated to the EMG6765-Q10A's 2.4GHz wireless LAN.
WLAN 5G Station Status	Click **Details...** to go to the **Monitor > WLAN 5G Station Status** screen (Section 7.6 on page 57). Use this screen to view the wireless stations that are currently associated to the EMG6765-Q10A's 5GHz wireless LAN.
System Status	
System Up Time	This is the total time the EMG6765-Q10A has been on.
Current Date/Time	This field displays your EMG6765-Q10A's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the EMG6765-Q10A's processing ability is currently used. When this percentage is close to 100%, the EMG6765-Q10A 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 bandwidth management.)
- Memory Usage	This shows what percentage of the heap memory the EMG6765-Q10A is using.
Interface Status	
Interface	This displays the EMG6765-Q10A port types. The port types are: **WAN**, **LAN** and **WLAN**.
Status	For the LAN and WAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the 2.4GHz/5GHz WLAN, it displays **Up** when the 2.4GHz/5GHz WLAN is enabled or **Down** when the 2.4G/5G WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or **N/A** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation. This field displays **N/A** when the line is disconnected. For the 2.4GHz/5GHz WLAN, it displays the maximum transmission rate when the 2.4GHz/5GHz WLAN is enabled and **N/A** when the WLAN is disabled.

4.2.1 Navigation Panel

Use the sub-menus on the navigation panel to configure EMG6765-Q10A features.

Figure 9 Navigation Panel: Router Mode (Admin)



The following table describes the sub-menus.

Table 7 Navigation Panel: Router Mode (Admin)

LINK	TAB	FUNCTION
Status		This screen shows the EMG6765-Q10A's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
MONITOR		
Log	View Log	Use this screen to view the list of activities recorded by your EMG6765-Q10A.
	Log Setting	Use this screen to specify which logs to display in the **View Log** screen.
DHCP Table	DHCP Table	Use this screen to view current DHCP client information.
Packet Statistics	Packet Statistics	Use this screen to view port status and packet specific statistics.
WLAN 2.4G Station Status	Association List	Use this screen to view the wireless stations that are currently associated to the EMG6765-Q10A's 2.4GHz wireless LAN.
WLAN 5G Station Status	Association List	Use this screen to view the wireless stations that are currently associated to the EMG6765-Q10A's 5GHz wireless LAN.
IGMP Statistics	IGMP Statistics	Use this screen to view the EMG6765-Q10A's IGMP multicast group and IGMP traffic statistics.
CONFIGURATION		
Network		
WAN	Management WAN	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers, the WAN MAC address, and VLAN settings.

Table 7 Navigation Panel: Router Mode (Admin) (continued)

LINK	TAB	FUNCTION
Wireless LAN 2.4G/5G	General	Use this screen to enable the wireless LAN and configure wireless LAN and wireless security settings.
	More AP	Use this screen to configure multiple BSSs on the EMG6765-Q10A.
	MAC Filter	Use the MAC filter screen to configure the EMG6765-Q10A to block access to devices or block the devices from accessing the EMG6765-Q10A.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
	IP Alias	Use this screen to have the EMG6765-Q10A apply IP alias to create LAN subnets.
	IPv6 LAN	Use this screen to configure the IPv6 address for the EMG6765-Q10A on the LAN.
	IGMP Snooping	Use this screen to activate IGMP snooping and configure IGMP modes.
MoCA	MoCA	Use this screen to set the MoCA Privacy, and enable multimedia and home networking over coaxial cabling.
	Monitor	Use this screen to view the MoCA connection status and information about the connected MoCA device(s).
DHCP Server	General	Use this screen to enable the EMG6765-Q10A's DHCP server.
	Advanced	Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
	Client List	Use this screen to view information related to your DHCP status.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to configure servers behind the EMG6765-Q10A and forward incoming service requests to the server(s) on your local network.
	Port Trigger	Use this screen to change your EMG6765-Q10A's port triggering settings.
Dynamic DNS	Dynamic DNS	Use this screen to set up dynamic DNS.
Static Route	Static Route	Use this screen to configure IP static routes.
Interface Group	Interface Group	Use this screen to add a LAN interface or a VLAN ID to a new group.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
Content Filter	Content Filter	Use this screen to restrict web features and designate a trusted computer.
IPv6 firewall	Services	Use this screen to configure IPv6 firewall rules.
Parental Control	Parental Control	Use this screen to block certain web features and sites containing certain keywords in the URL.
Management		

Table 7 Navigation Panel: Router Mode (Admin) (continued)

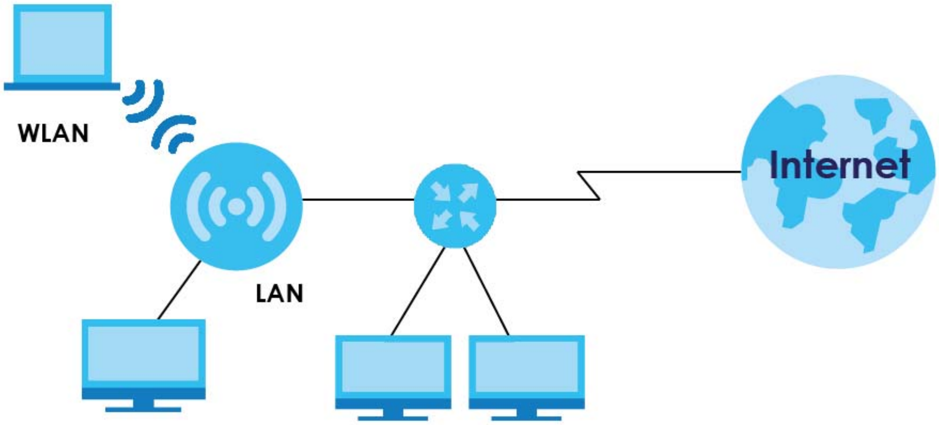
LINK	TAB	FUNCTION
Bandwidth MGMT	General	Use this screen to enable or disable QoS and set the upstream bandwidth.
	Queue Setup	Use this screen to configure QoS queue assignment.
	Class Setup	Use this screen to configure QoS classifiers.
UPnP	UPnP	Use this screen to enable UPnP on the EMG6765-Q10A.
USB Media Sharing	DLNA	Use this screen to have the EMG6765-Q10A function as a DLNA-compliant media server, that lets DLNA-compliant media clients play video, audio, and photo content files stored on the connected USB storage device.
	SAMBA	Use this screen to enable file sharing through the EMG6765-Q10A.
	FTP	Use this screen to have the EMG6765-Q10A act as a FTP server.
Port Configuration	Port Configuration	Use this screen to change the Ethernet port speed and duplex settings.
MAINTENANCE		
General	General	Use this screen to view and change administrative settings such as system and domain names.
Account	User Account	Use this screen to change the password of your EMG6765-Q10A.
Time	Time Setting	Use this screen to change your EMG6765-Q10A's time and date.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your EMG6765-Q10A.
Backup/ Restore	Backup/ Restore	Use this screen to backup and restore the configuration or reset the factory defaults to your EMG6765-Q10A.
Restart	System Restart	This screen allows you to reboot the EMG6765-Q10A without turning the power off.
Language	Language	This screen allows you to select the language you prefer.
Diagnostic	Ping	Use this screen to ping an IP address.
	Trace Route	Use this screen to trace the route packets take to a host.
	Nslookup	Use this screen to perform an nslookup (name server lookup).

CHAPTER 5 Access Point Mode

5.1 Overview

Use your EMG6765-Q10A as an access point (AP) if you already have a router or gateway on your network. In this mode your EMG6765-Q10A bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 10 Wireless Internet Access in Access Point Mode



Many screens that are available in **Router Mode** are not available in **Access Point Mode**, such as bandwidth management and firewall.

5.2 What You Can Do

- Use the **Status** screen to view read-only information about your EMG6765-Q10A (Section 5.4 on page 31).
- Use the **LAN** screen to set the IP address for your EMG6765-Q10A acting as an access point (Section 5.5 on page 33).

5.3 What You Need to Know

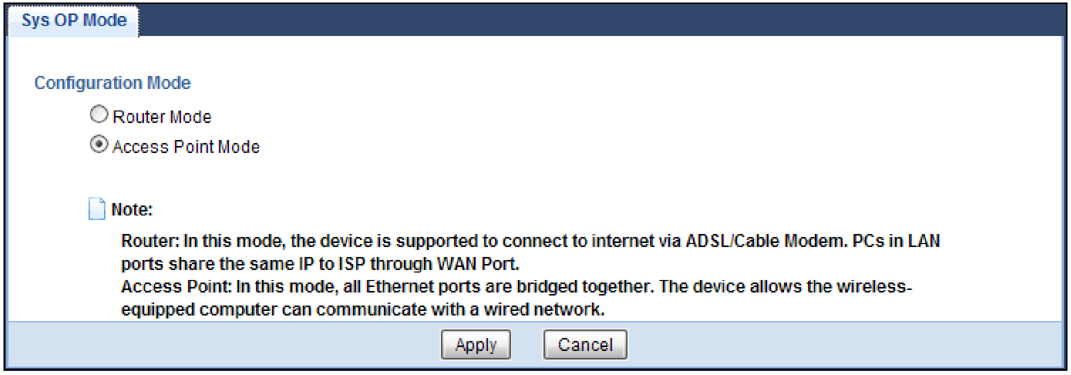
See Chapter 6 on page 36 for a tutorial on setting up a network with the EMG6765-Q10A as an access point.

5.3.1 Setting your EMG6765-Q10A to AP Mode

1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.

2 To use your EMG6765-Q10A as an access point, go to **Maintenance > Sys OP Mode** and select **Access Point Mode**.

Figure 11 Changing to Access Point mode



Sys OP Mode

Configuration Mode

○ Router Mode
● Access Point Mode

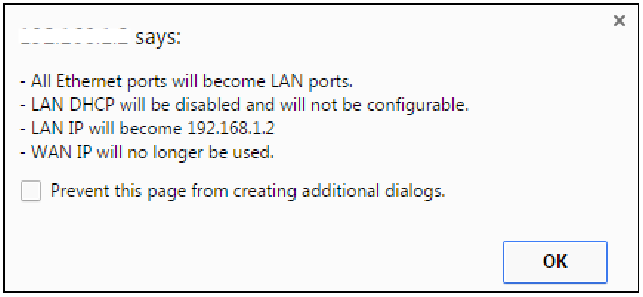
Note:

Router: In this mode, the device is supported to connect to internet via ADSL/Cable Modem. PCs in LAN ports share the same IP to ISP through WAN Port.
Access Point: In this mode, all Ethernet ports are bridged together. The device allows the wireless-equipped computer can communicate with a wired network.

Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your EMG6765-Q10A is already in Access Point mode.

3 When you select **Access Point Mode**, the following pop-up message window appears.

Figure 12 Pop up for Access Point mode



[redacted] says:

- All Ethernet ports will become LAN ports.
- LAN DHCP will be disabled and will not be configurable.
- LAN IP will become 192.168.1.2
- WAN IP will no longer be used.

□ Prevent this page from creating additional dialogs.

Click **OK**. Then click **Apply**. The Web Configurator refreshes once the change to Access Point mode is successful.

5.3.2 Accessing the Web Configurator in Access Point Mode

Log in to the Web Configurator in Access Point mode, do the following:

1 Connect your computer to the LAN port of the EMG6765-Q10A.

2 The default IP address of the EMG6765-Q10A is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix B on page 200 for information on changing your computer's IP address.

4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "192.168.1.2" as the web address in your web browser.

5.3.3 Configuring your WLAN and Maintenance Settings

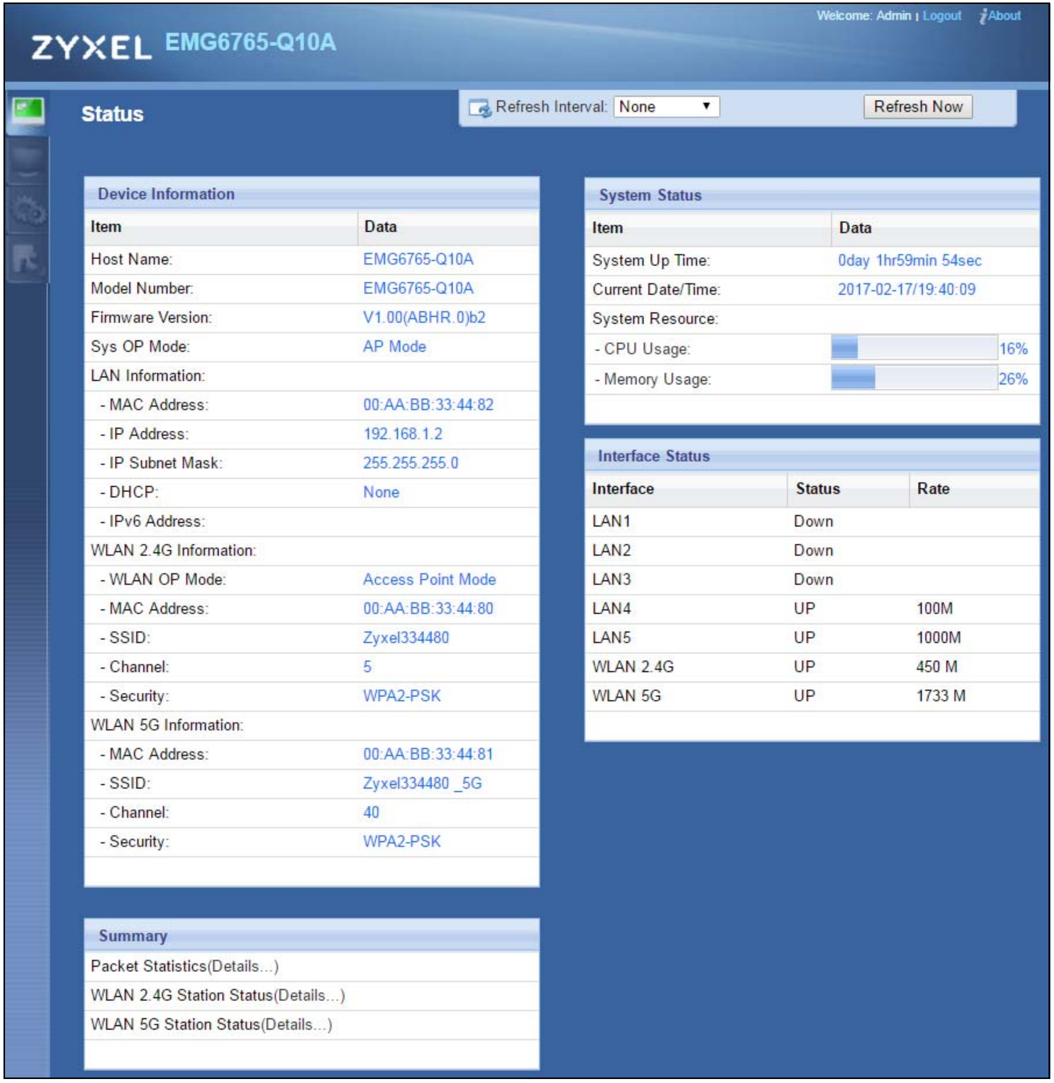
The configuration of wireless and maintenance settings in **Access Point Mode** is the same as for **Router Mode**.

- See Chapter 9 on page 72 for information on the configuring your wireless network.
- See Chapter 25 on page 173 for information on configuring your Maintenance settings.

5.4 AP Mode Status Screen

Click 🖥 to open the **Status** screen.

Figure 13 Status Screen: Access Point Mode



Device Information

Item	Data
Host Name:	EMG6765-Q10A
Model Number:	EMG6765-Q10A
Firmware Version:	V1.00(ABHR.0)b2
Sys OP Mode:	AP Mode
LAN Information:	
- MAC Address:	00:AA:BB:33:44:82
- IP Address:	192.168.1.2
- IP Subnet Mask:	255.255.255.0
- DHCP:	None
- IPv6 Address:	
WLAN 2.4G Information:	
- WLAN OP Mode:	Access Point Mode
- MAC Address:	00:AA:BB:33:44:80
- SSID:	Zyxel334480
- Channel:	5
- Security:	WPA2-PSK
WLAN 5G Information:	
- MAC Address:	00:AA:BB:33:44:81
- SSID:	Zyxel334480 _5G
- Channel:	40
- Security:	WPA2-PSK

System Status

Item	Data
System Up Time:	0day 1hr59min 54sec
Current Date/Time:	2017-02-17/19:40:09
System Resource:	
- CPU Usage:	16%
- Memory Usage:	26%

Interface Status

Interface	Status	Rate
LAN1	Down	
LAN2	Down	
LAN3	Down	
LAN4	UP	100M
LAN5	UP	1000M
WLAN 2.4G	UP	450 M
WLAN 5G	UP	1733 M

Summary

Packet Statistics(Details...)

WLAN 2.4G Station Status(Details...)

WLAN 5G Station Status(Details...)

The following table describes the labels shown in the **Status** screen.

Table 8 Status Screen: Access Point Mode

LABEL	DESCRIPTION
Device Information	
Item	This column shows the type of data the EMG6765-Q10A is recording.
Data	This column shows the actual data recorded by the EMG6765-Q10A.
Host Name	This is the **System Name** you enter in the **Maintenance** > **General** screen. It is for identification purposes.
Model Number	This is the model name of your device.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 3.1.1 on page 21) to which the EMG6765-Q10A is set - **AP Mode**.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - **Client** or **None**.
IPv6 Address	This shows the IPv6 address of the EMG6765-Q10A on the LAN.
WLAN 2.4G Information	
WLAN OP Mode	This is the device mode (Section 3.1.1 on page 21) to which the EMG6765-Q10A's wireless LAN is set - **Access Point Mode**.
MAC Address	This shows the 2.4GHz wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the EMG6765-Q10A in the 2.4GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the EMG6765-Q10A is using.
WLAN 5G Information	
MAC Address	This shows the 5GHz wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the EMG6765-Q10A in the 5GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the EMG6765-Q10A is using.
Summary	
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen (Section 7.5 on page 56). Use this screen to view port status and packet specific statistics.
WLAN 2.4G Station Status	Click **Details...** to go to the **Monitor > WLAN 2.4G Station Status** screen (Section 7.6 on page 57). Use this screen to view the wireless stations that are currently associated to the EMG6765-Q10A's 2.4GHz wireless LAN.
WLAN 5G Station Status	Click **Details...** to go to the **Monitor > WLAN 5G Station Status** screen (Section 7.6 on page 57). Use this screen to view the wireless stations that are currently associated to the EMG6765-Q10A's 5GHz wireless LAN.
System Status	
System Up Time	This is the total time the EMG6765-Q10A has been on.
Current Date/Time	This field displays your EMG6765-Q10A's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the EMG6765-Q10A's processing ability is currently used. When this percentage is close to 100%, the EMG6765-Q10A 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 bandwidth management.)

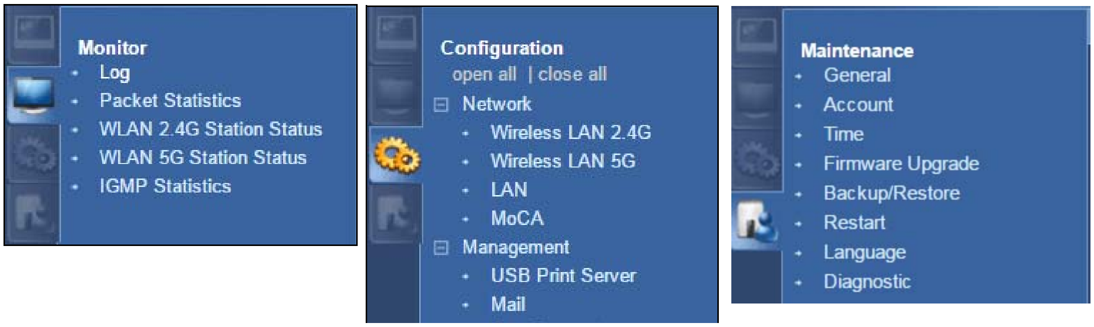
Table 8 Status Screen: Access Point Mode (continued)

LABEL	DESCRIPTION
- Memory Usage	This shows what percentage of the heap memory the EMG6765-Q10A is using.
Interface Status	
Interface	This displays the EMG6765-Q10A port types. The port types are: **LAN** and **WLAN**.
Status	For the LAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the 2.4GHz/5GHz WLAN, it displays **Up** when the 2.4GHz/5GHz WLAN is enabled or **Down** when the 2.4G/5G WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or **N/A** when the line is disconnected. For the 2.4GHz/5GHz WLAN, it displays the maximum transmission rate when the 2.4GHz/5GHz WLAN is enabled and **N/A** when the WLAN is disabled.

5.4.1 Navigation Panel

Use the menu in the navigation panel to configure EMG6765-Q10A features in **Access Point Mode**.

Figure 14 Menu: Access Point Mode (Admin)



Refer to Table 7 on page 26 for descriptions of the labels shown in the navigation panel.

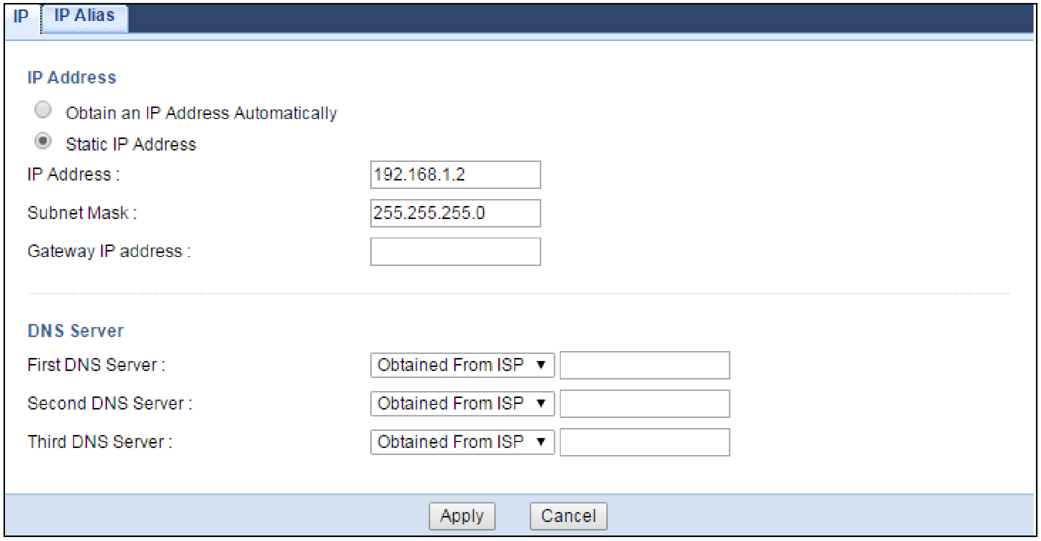
5.5 LAN Screen

Use this section to configure your LAN settings while in **Access Point Mode**.

Click **Network > LAN** to see the screen below.

Note: If you change the IP address of the EMG6765-Q10A in the screen below, you will need to log into the EMG6765-Q10A again using the new IP address.

Figure 15 Network > LAN > IP



IP Address

○ Obtain an IP Address Automatically

● Static IP Address

IP Address :	192.168.1.2
Subnet Mask :	255.255.255.0
Gateway IP address :	

DNS Server

First DNS Server :	Obtained From ISP ▼	
Second DNS Server :	Obtained From ISP ▼	
Third DNS Server :	Obtained From ISP ▼	

The table below describes the labels in the screen.

Table 9 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	
Obtain an IP Address Automatically	When you enable this, the EMG6765-Q10A gets its IP address from the network's DHCP server (for example, your ISP). Users connected to the EMG6765-Q10A can now access the network (i.e., the Internet if the IP address is given by the ISP). The Web Configurator may no longer be accessible unless you know the IP address assigned by the DHCP server to the EMG6765-Q10A. You need to reset the EMG6765-Q10A to be able to access the Web Configurator again (see Section 25.7 on page 178 for details on how to reset the EMG6765-Q10A). Also when you select this, you cannot enter an IP address for your EMG6765-Q10A in the field below.
Static IP Address	Click this if you want to specify the IP address of your EMG6765-Q10A. Or if your ISP or network administrator gave you a static IP address to access the network or the Internet.
IP Address	Type the IP address in dotted decimal notation. The default setting is 192.168.1.2. If you change the IP address you will have to log in again with the new IP address.
Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your EMG6765-Q10A will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the EMG6765-Q10A.
Gateway IP Address	Enter a **Gateway IP Address** (if your ISP or network administrator gave you one) in this field.
DNS Server	

Table 9 Network > LAN > IP (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the EMG6765-Q10A's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

CHAPTER 6 Tutorials

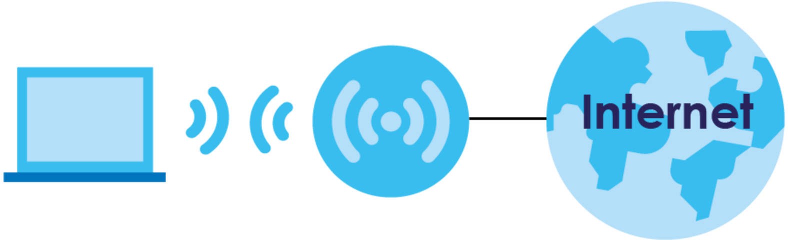
6.1 Overview

This chapter provides tutorials for setting up your EMG6765-Q10A.

- Setting Up a Secure Wireless Network
- Connecting to the EMG6765-Q10A's Wi-Fi Network Using WPS
- Connecting to the EMG6765-Q10A's Wi-Fi Network Without WPS
- Configuring Static Route for Routing to Another Network
- Access the EMG6765-Q10A Using DDNS
- Configuring the MAC Address Filter
- Using Multiple SSIDs on the EMG6765-Q10A

6.2 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 EMG6765-Q10A 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 EMG6765-Q10A.

6.2.1 Configuring the Wireless Network Settings

This example shows how to configure wireless security settings with the following parameters on your EMG6765-Q10A and connect your computer to the EMG6765-Q10A's wireless network.

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

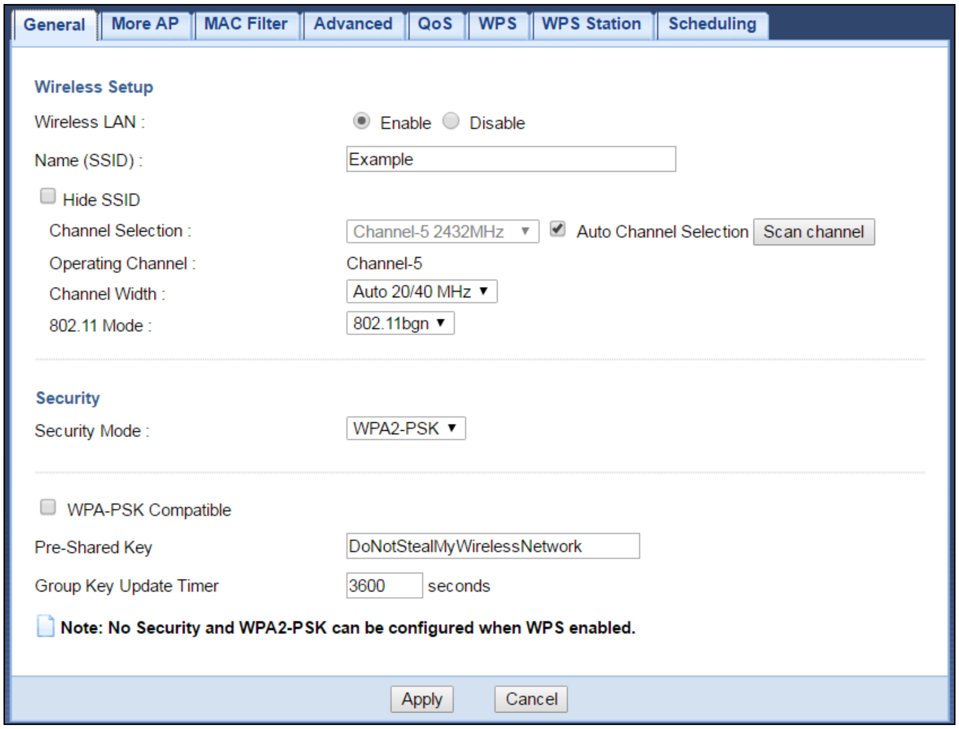
Follow the steps below to configure the wireless settings on your EMG6765-Q10A.

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 2.3 on page 18).

1 Make sure the **Wi-Fi** button (at the back panel of the EMG6765-Q10A) is set **ON**.

2 Click **Configuration > Network > Wireless LAN 2.4G** or **5G** to open the **General** screen.

3 Confirm that the wireless LAN is enabled on the EMG6765-Q10A. Configure the screen using the provided parameters. Click **Apply**.



Wireless Setup

Wireless LAN : ● Enable ○ Disable

Name (SSID) : Example

□ Hide SSID

Channel Selection : Channel-5 2432MHz ☑ Auto Channel Selection Scan channel

Operating Channel : Channel-5

Channel Width : Auto 20/40 MHz

802.11 Mode : 802.11bgn

Security

Security Mode : WPA2-PSK

□ WPA-PSK Compatible

Pre-Shared Key DoNotStealMyWirelessNetwork

Group Key Update Timer 3600 seconds

Note: No Security and WPA2-PSK can be configured when WPS enabled.

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

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the EMG6765-Q10A (see Section 6.3 on page 37). He can also use the notebook's wireless client to search for the EMG6765-Q10A (see Section 6.5 on page 44).

6.3 Connecting to the EMG6765-Q10A's Wi-Fi Network Using WPS

This section gives you an example of how to set up a wireless network using WPS. This example uses the EMG6765-Q10A as the AP and a WPS-enabled Android 4.4.2 smartphone as the wireless client.

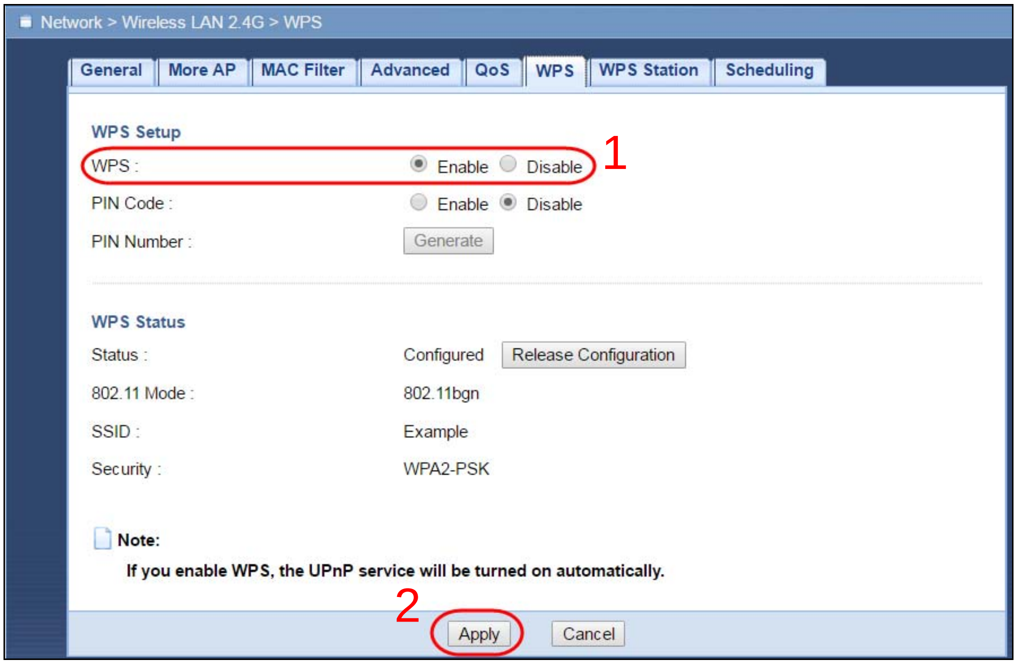
There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 6.3.1 on page 38. This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the EMG6765-Q10A's interface. See Section 6.3.2 on page 39. This is the more secure method, since one device can authenticate the other.

6.3.1 Push Button Configuration (PBC)

1 Make sure that your EMG6765-Q10A is turned on and that it is within range of your computer.

2 Push and hold the WPS button located on the EMG6765-Q10A's side panel for more than 1 second. Alternatively, you may log into EMG6765-Q10A's web configurator and go to the **Configuration > Network > Wireless LAN 2.4G** or **5G > WPS** screen. **Enable** the **WPS** function and click **Apply**. WPS is enabled by default on the EMG6765-Q10A.



WPS Setup

WPS : ● Enable ○ Disable

PIN Code : ○ Enable ● Disable

PIN Number :

WPS Status

Status : Configured

802.11 Mode : 802.11bgn

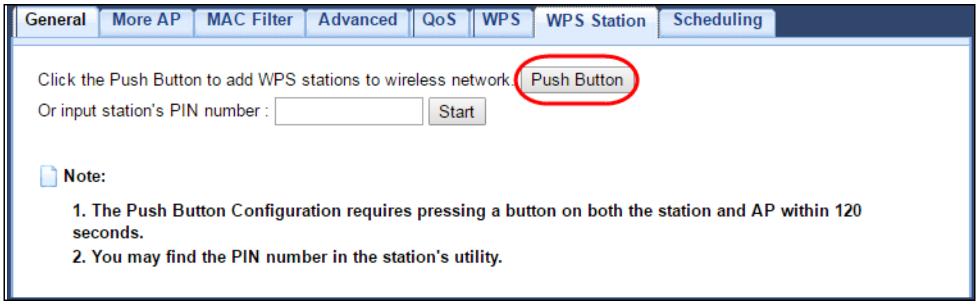
SSID : Example

Security : WPA2-PSK

Note:

If you enable WPS, the UPnP service will be turned on automatically.

3 Then go to the **Configuration > Network > Wireless LAN 2.4G** or **5G > WPS Station** screen and click the **Push button**.



Click the Push Button to add WPS stations to wireless network.

Or input station's PIN number :

Note:

1. The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.

2. You may find the PIN number in the station's utility.

Note: Your EMG6765-Q10A has a WPS button located on the side of the device as well as a WPS button in its web configurator. Both buttons have exactly the same function: you can use one or the other.

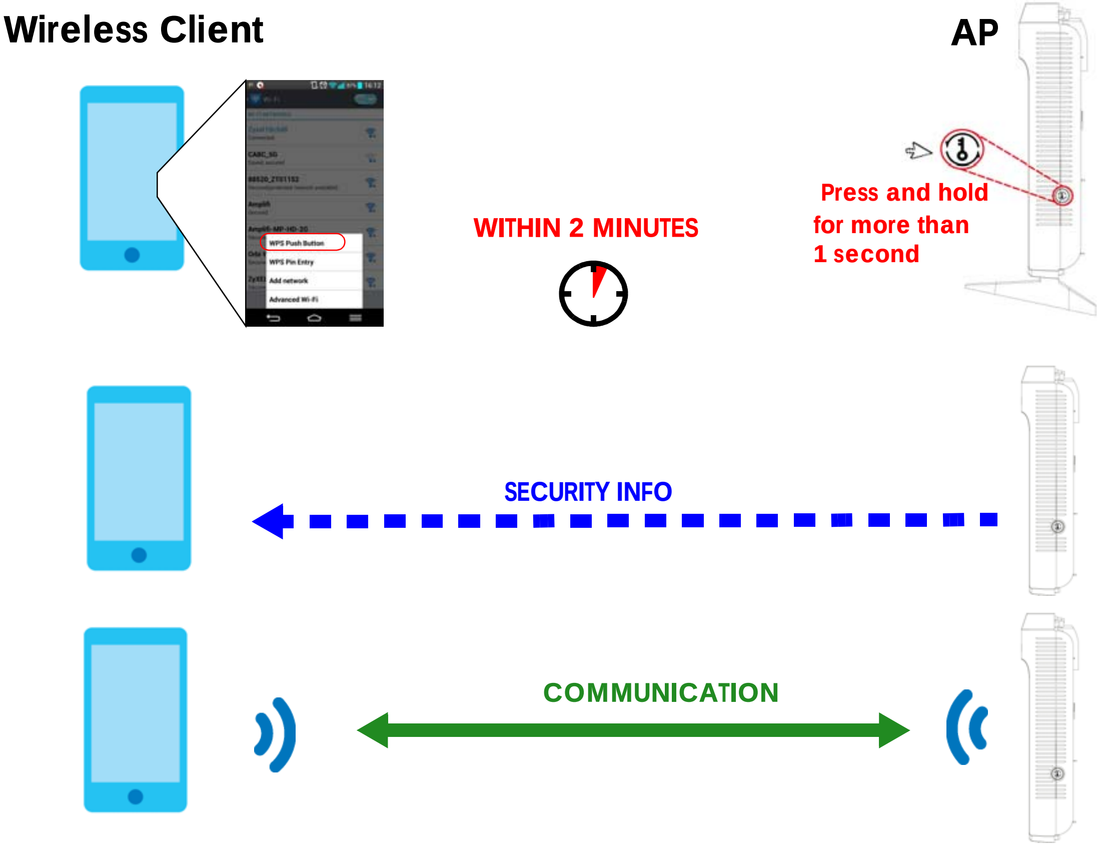
4 Go to your phone settings and turn on Wi-Fi. Open the Wi-Fi networks and tap **WPS Push Button** or the WPS icon (Section 3 on page 14).

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 EMG6765-Q10A 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 EMG6765-Q10A 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 EMG6765-Q10A and wireless client (the Android 4.4.2 phone in this example).

Figure 16 Example WPS Process: PBC Method

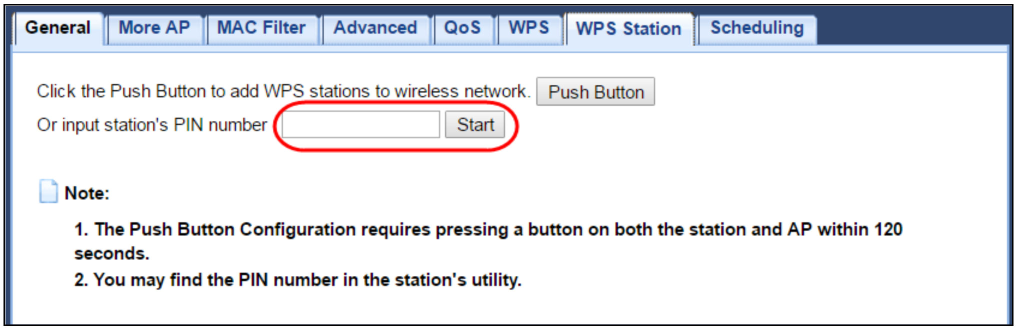


6.3.2 PIN Configuration

When you use the PIN configuration method, you need to check the client's PIN number and use the EMG6765-Q10A's configuration interface.

1 Go to your phone settings and turn on Wi-Fi. Open the Wi-Fi networks list and tap **WPS PIN Entry** to get a PIN number.

2 Then go to **Configuration > Network > Wireless LAN 2.4G** or **5G > WPS Station** screen. Enter the client's PIN number to the **PIN** field. Click the **Start** button (or button next to the PIN field) on the EMG6765-Q10A **WPS Station** screen within two minutes.



Click the Push Button to add WPS stations to wireless network. Push Button

Or input station's PIN number Start

Note:

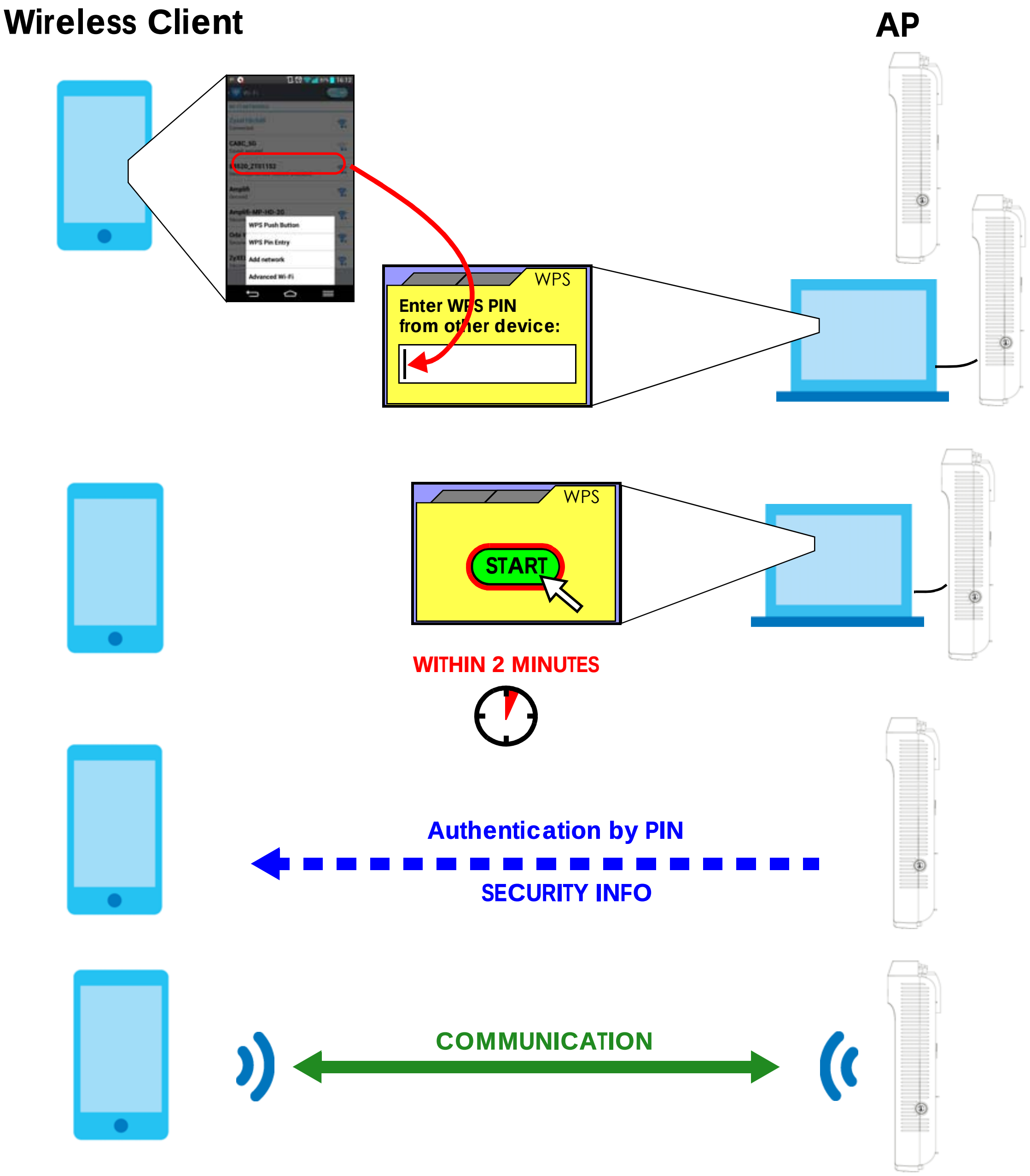
1. The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2. You may find the PIN number in the station's utility.

Note: You can also get a WPS PIN Code in EMG6765-Q10A's **Configuration > Network > Wireless LAN 2.4G** or **5G > WPS** screen. Enable **Pin Code** then click **Generate** and enter this PIN code in the wireless client's configuration utility.

The EMG6765-Q10A authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the EMG6765-Q10A securely.

The following figure shows you how to set up a wireless network and its security on a EMG6765-Q10A and a wireless client (android 4.4.2 smartphone) by using PIN method.

Figure 17 Example WPS Process: PIN Method

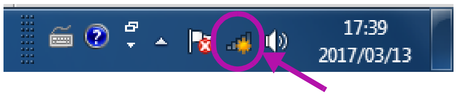


6.4 Connecting to the EMG6765-Q10A's Wi-Fi Network Without WPS

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

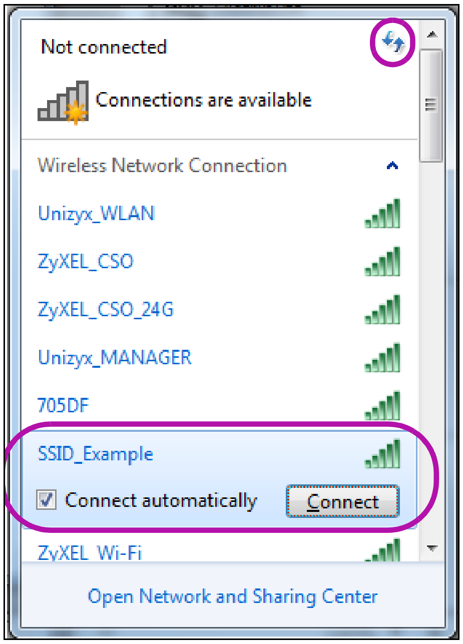
1 The EMG6765-Q10A supports IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, and IEEE 802.11ac wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

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

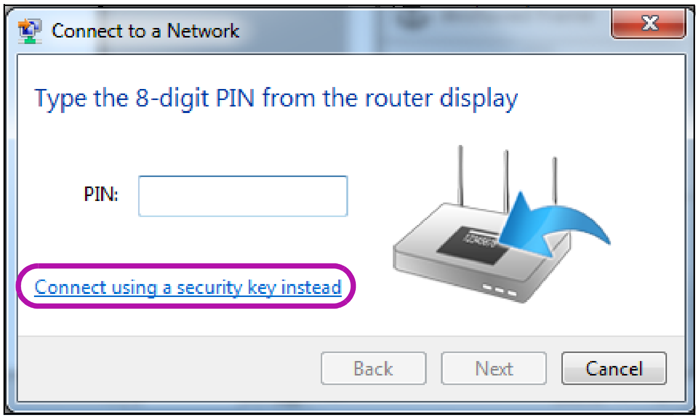


3 The **Wireless Network Connection** screen displays. Click the refresh button to update the list of the available wireless APs within range.

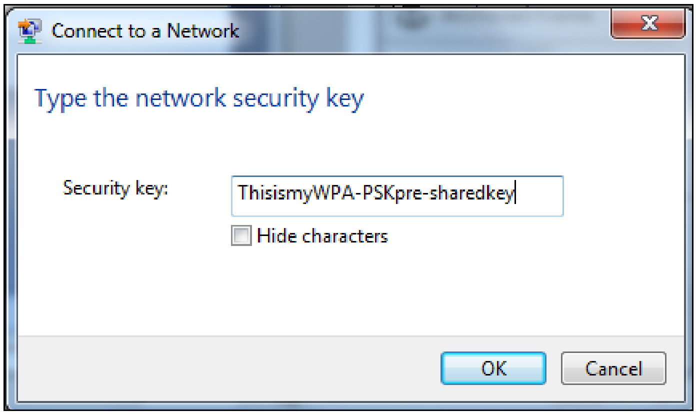
4 Select **SSID_Example** and click **Connect**.



5 The following screen displays if WPS is enabled on the EMG6765-Q10A but you didn't press the WPS button. Click **Connect using as security key instead**.


Connect to a Network
Type the 8-digit PIN from the router display
PIN:
Connect using a security key instead
Back
Next
Cancel

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



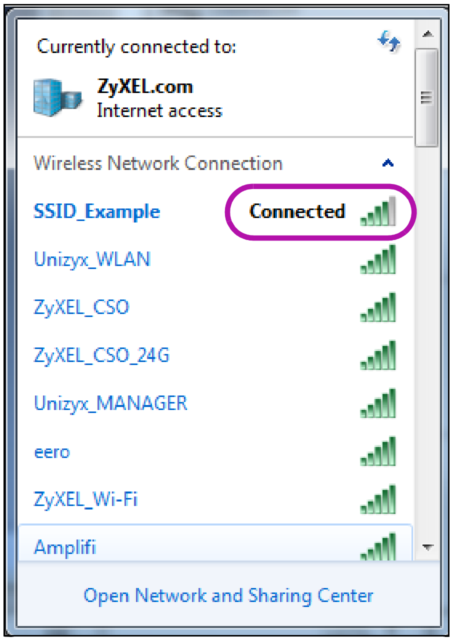
Connect to a Network

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

8 If the wireless client keeps trying to connect to or acquiring an IP address from the EMG6765-Q10A, make sure you entered the correct security key.

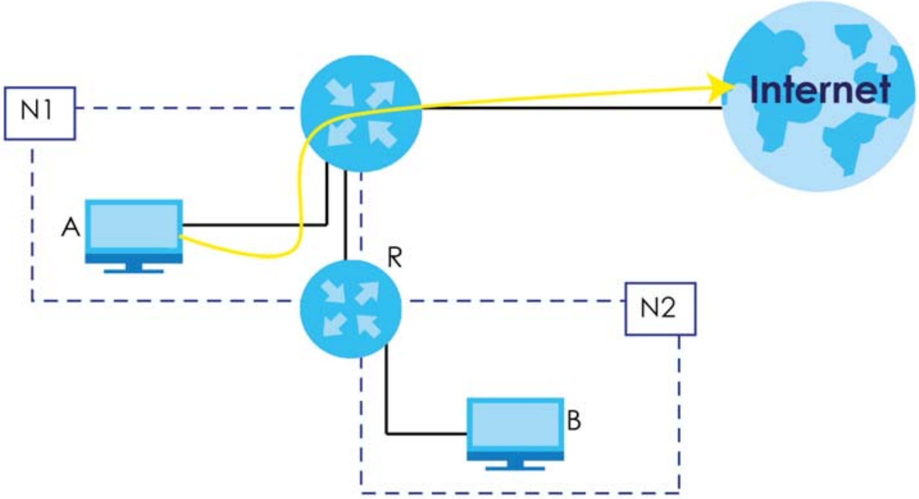
If the connection has limited or no connectivity, make sure the DHCP server is enabled on the EMG6765-Q10A.

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.

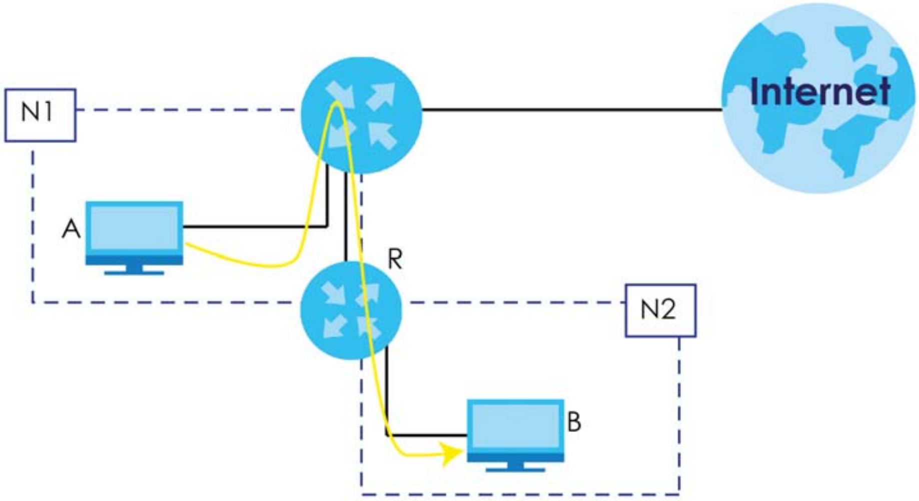
6.5 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the EMG6765-Q10A'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 EMG6765-Q10A'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 EMG6765-Q10A'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 EMG6765-Q10A to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the EMG6765-Q10A routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

Table 10   IP Settings in this Tutorial

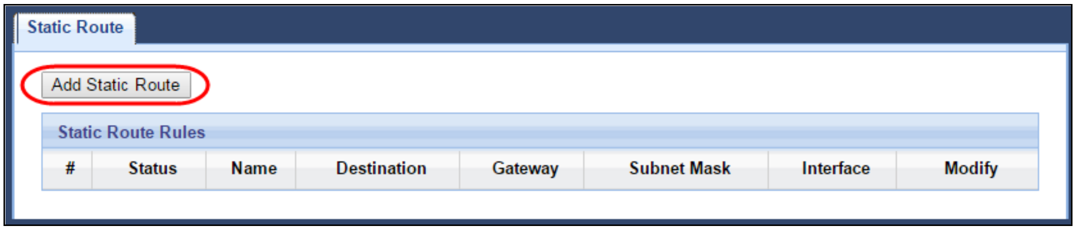
DEVICE / COMPUTER	IP ADDRESS
The EMG6765-Q10A's WAN	172.16.1.1
The EMG6765-Q10A's LAN	192.168.1.1
IP Type	WAN
Use Interface	VDSL
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

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

1 Log into the EMG6765-Q10A's Web Configurator in advanced mode.

2 Click **Configuration > Network > Static Route**.

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



Static Route Rules

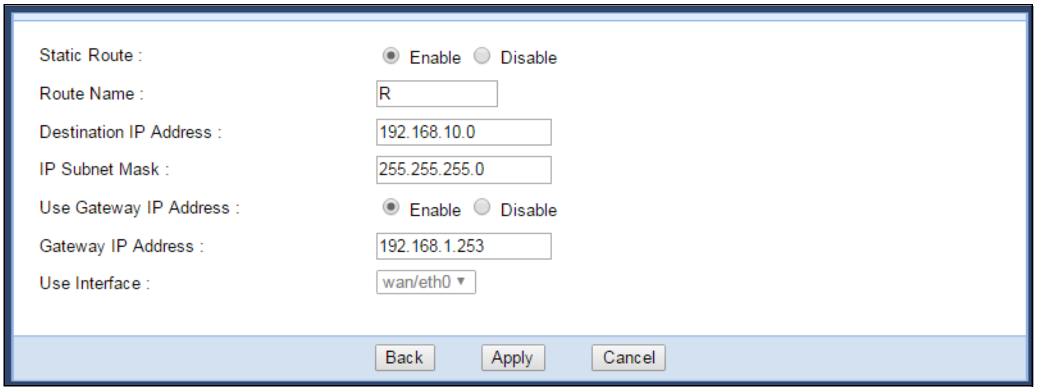
#	Status	Name	Destination	Gateway	Subnet Mask	Interface	Modify

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

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

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

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



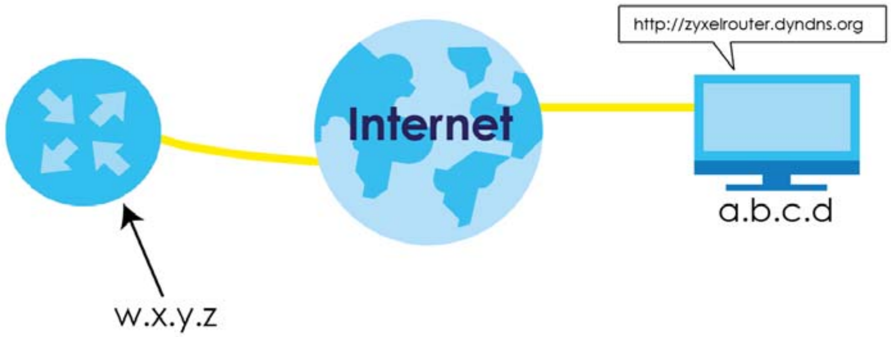
Static Route :	● Enable ○ Disable
Route Name :	R
Destination IP Address :	192.168.10.0
IP Subnet Mask :	255.255.255.0
Use Gateway IP Address :	● Enable ○ Disable
Gateway IP Address :	192.168.1.253
Use Interface :	wan/eth0 ▾

4d Click **Apply**.

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.

6.6 Access the EMG6765-Q10A Using DDNS

If you connect your EMG6765-Q10A to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The EMG6765-Q10A's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the EMG6765-Q10A using a domain name.



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

This tutorial covers:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your EMG6765-Q10A
- Testing the DDNS Setting

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

6.6.1 Registering a DDNS Account on www.dyndns.org

1 Open a browser and type **http://www.dyndns.org**.

2 Apply for a user account. This tutorial uses **UserName1** and **5** 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.

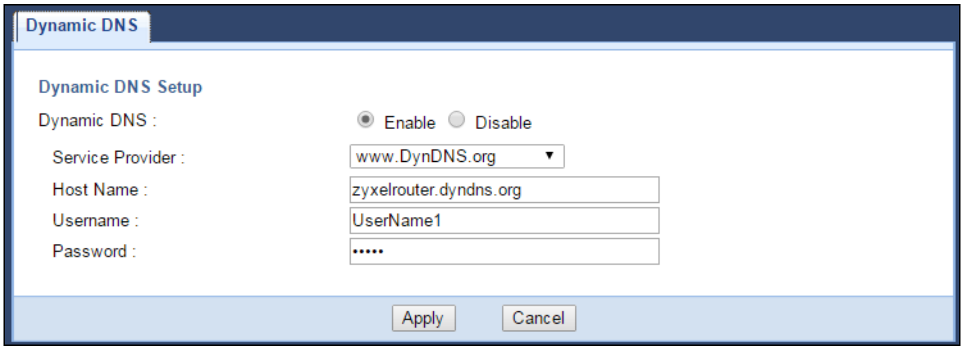
- Hostname: **zyxelrouter.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your EMG6765-Q10A is currently using. You can find the IP address on the EMG6765-Q10A's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the EMG6765-Q10A later.

6.6.2 Configuring DDNS on Your EMG6765-Q10A

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 (**5**).



Dynamic DNS Setup

Dynamic DNS : ● Enable ○ Disable

Service Provider : www.DynDNS.org

Host Name : zyxelrouter.dyndns.org

Username : UserName1

Password : •••••

Click **Apply**.

6.6.3 Testing the DDNS Setting

Now you should be able to access the EMG6765-Q10A 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.

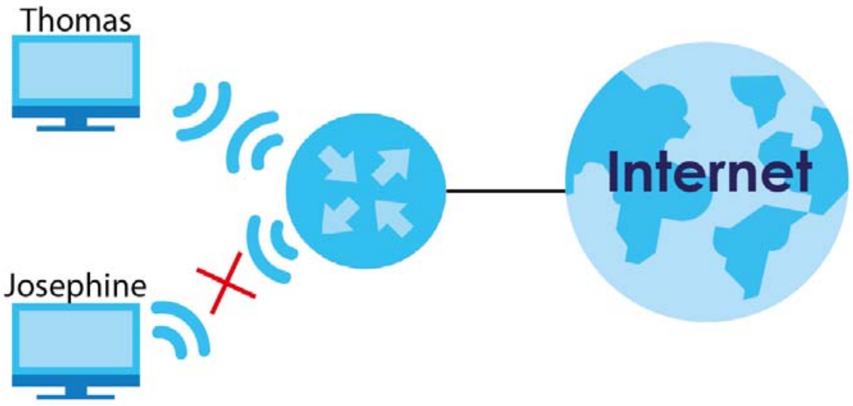
2 Type **http://zyxelrouter.dyndns.org** and press [Enter].

3 The EMG6765-Q10A's login page should appear. You can then log into the EMG6765-Q10A and manage it.

6.7 Configuring the MAC Address Filter

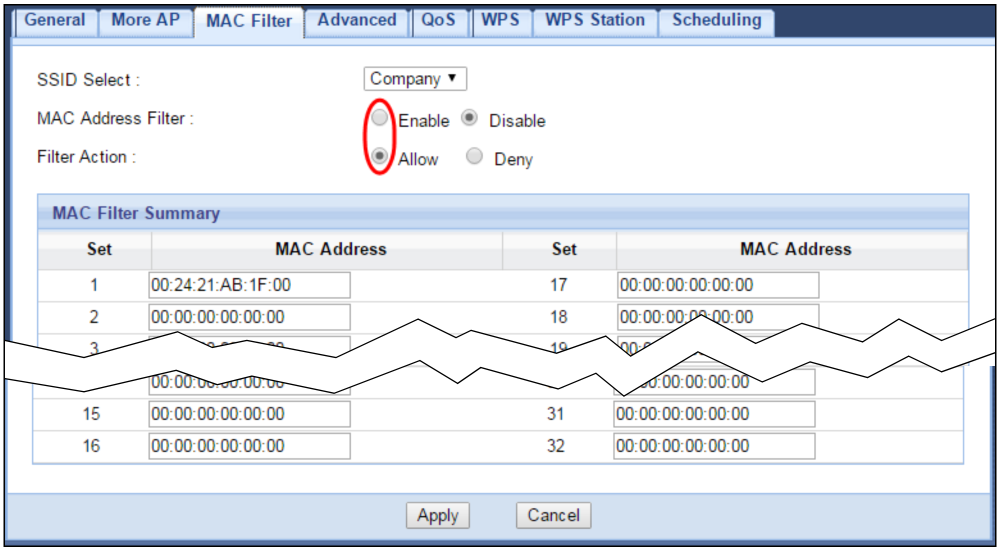
Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

Josephine's computer connects wirelessly to the Internet through the EMG6765-Q10A. Thomas decides to use the **Configuration > Network > Wireless LAN 2.4G** or **5G > MAC Filter** screen to grant wireless network access to his computer but not to Josephine's computer.



1 Click **Configuration > Network > Wireless LAN 2.4G** or **5G** to open the **MAC Filter** screen. Select the **Enable** check box to activate **MAC Address Filter**.

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



SSID Select : Company ▾

MAC Address Filter : ○ Enable ● Disable

Filter Action : ● Allow ○ Deny

MAC Filter Summary

Set	MAC Address	Set	MAC Address
1	00:24:21:AB:1F:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3		19	
	00:00:00:00:00:00		00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

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 EMG6765-Q10A.

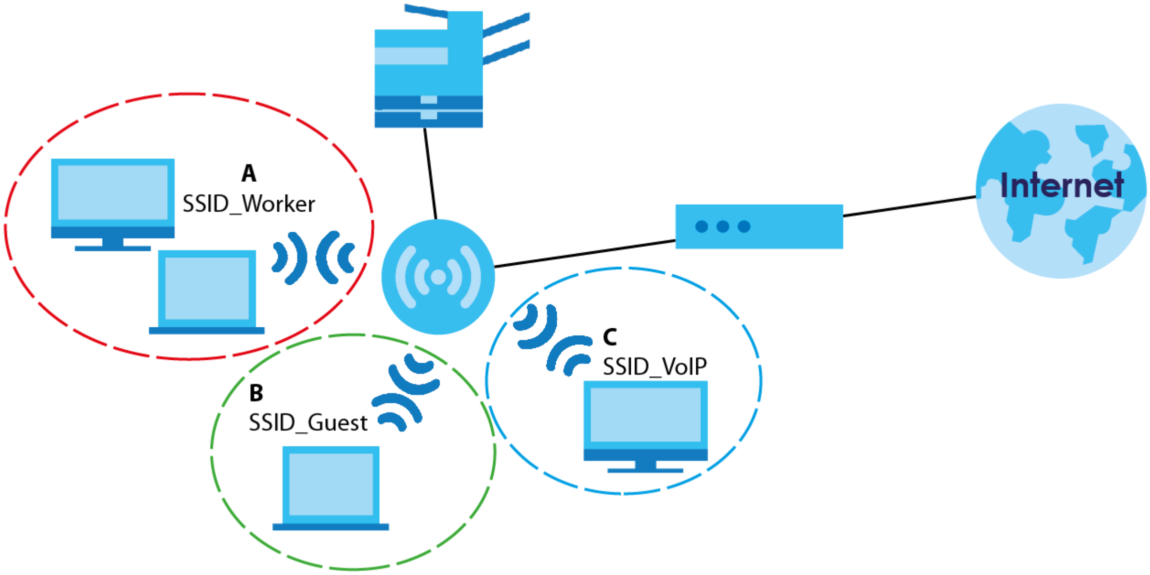
6.8 Using Multiple SSIDs on the EMG6765-Q10A

You can configure more than one SSID on a EMG6765-Q10A. See Section 9.4 on page 81.

This allows you to configure multiple independent wireless networks on the EMG6765-Q10A as if there were multiple APs (virtual APs). Each virtual AP has its own SSID, wireless security type and MAC filtering settings. That is, each SSID on the EMG6765-Q10A represents a different access point/wireless network to wireless clients in the network.

Clients can associate only with the SSIDs for which they have the correct security settings. Clients using different SSIDs can access the Internet and the wired network behind the EMG6765-Q10A (such as a printer).

For example, you may set up three wireless networks (**A**, **B** and **C**) in your office. **A** is for workers, **B** is for guests and **C** is specific to a VoIP device in the meeting room.



6.8.1 Configuring Security Settings of Multiple SSIDs

The EMG6765-Q10A is in router mode by default.

This example shows you how to configure the SSIDs with the following parameters on your EMG6765-Q10A (in router mode).

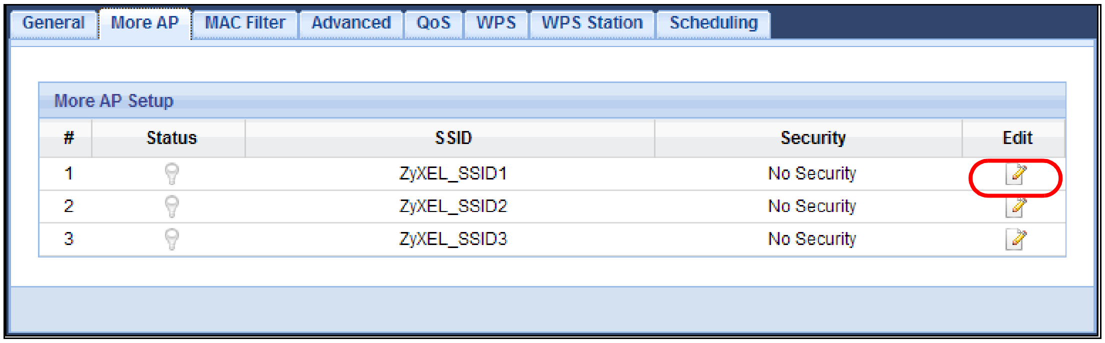
SSID	SECURITY TYPE	KEY	MAC FILTERING
SSID_Worker	WPA2-PSK WPA Compatible	DoNotStealMyWirelessNetwork	Disable
SSID_VoIP	WPA2-PSK	VoIPOnly12345678	Allow 00:A0:C5:01:23:45
SSID_Guest	WPA2-PSK	keyexample123	Disable

1. Connect your computer to the LAN port of the EMG6765-Q10A using an Ethernet cable.
2. The default IP address of the EMG6765-Q10A in router mode is “192.168.1.1”. In this case, your computer must have an IP address in the range between “192.168.1.2” and “192.168.1.254”.
3. Click **Start > Run** on your computer in Windows. Type “cmd” in the dialog box. Enter “ipconfig” to show your computer’s IP address. If your computer’s IP address is not in the correct range then see Appendix B on page 200 for information on changing your computer’s IP address.
4. After you’ve set your computer’s IP address, open a web browser such as Internet Explorer and type “http://192.168.1.1” as the web address in your web browser.

5 Enter the back-label default key as the password and click **Login**.

6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.

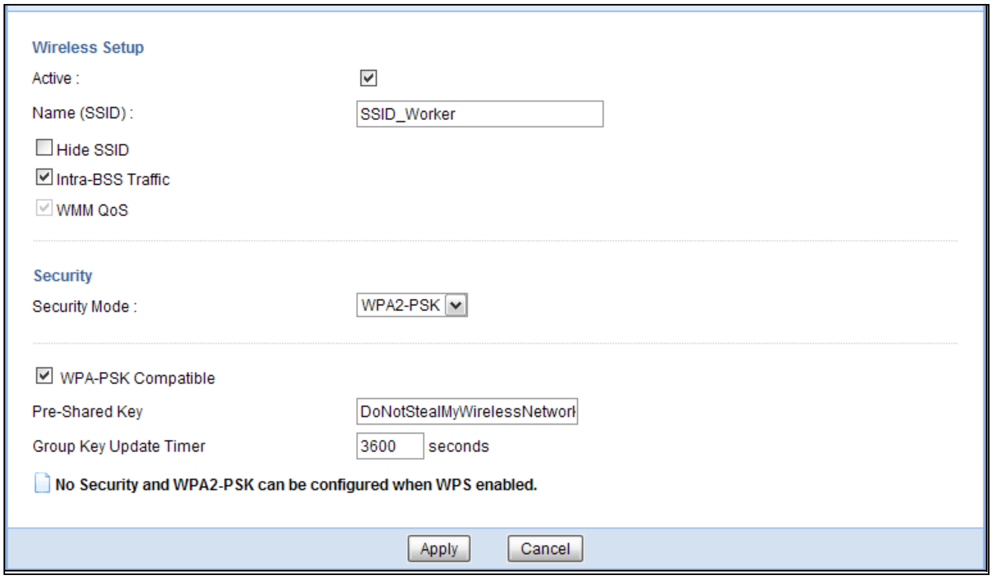
7 Go to **Configuration > Network > Wireless LAN 2.4G > More AP**. Click the **Edit** icon of the first entry to configure wireless and security settings for **SSID_Worker**.



More AP Setup

#	Status	SSID	Security	Edit
1	○	ZyXEL_SSID1	No Security	✎
2	○	ZyXEL_SSID2	No Security	✎
3	○	ZyXEL_SSID3	No Security	✎

8 Configure the screen as follows. In this example, you enable **Intra-BSS Traffic** for **SSID_Worker** to allow wireless clients in the same wireless network to communicate with each other. Click **Apply**.



Wireless Setup

Active : ☑

Name (SSID) : SSID_Worker

☐ Hide SSID

☑ Intra-BSS Traffic

☑ WMM QoS

Security

Security Mode : WPA2-PSK

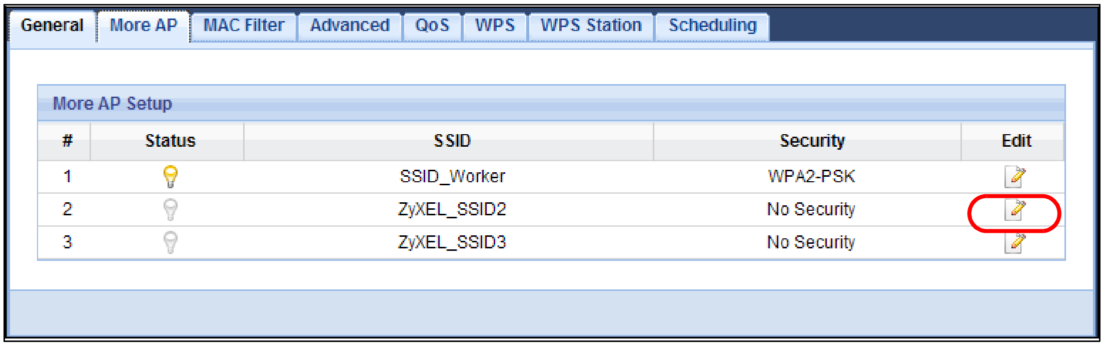
☑ WPA-PSK Compatible

Pre-Shared Key DoNotStealMyWirelessNetworl

Group Key Update Timer 3600 seconds

No Security and WPA2-PSK can be configured when WPS enabled.

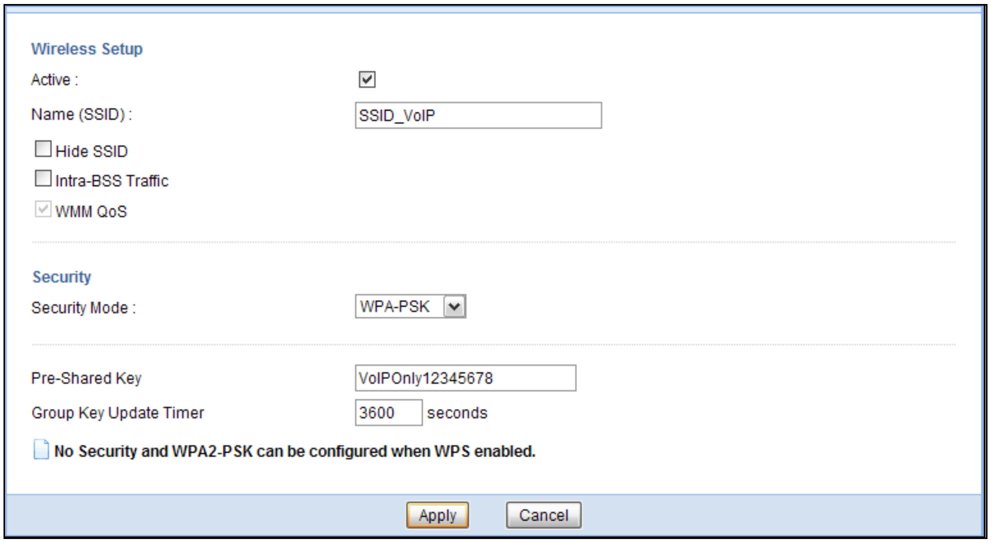
9 Click the **Edit** icon of the second entry to configure wireless and security settings for **SSID_VoIP**.



More AP Setup

#	Status	SSID	Security	Edit
1	●	SSID_Worker	WPA2-PSK	✎
2	○	ZyXEL_SSID2	No Security	✎
3	○	ZyXEL_SSID3	No Security	✎

10 Configure the screen as follows. You do not enable **Intra-BSS Traffic** for **SSID_VoIP**. Click **Apply**.



Wireless Setup

Active : ☑

Name (SSID) : SSID_VoIP

☐ Hide SSID

☐ Intra-BSS Traffic

☑ WMM QoS

Security

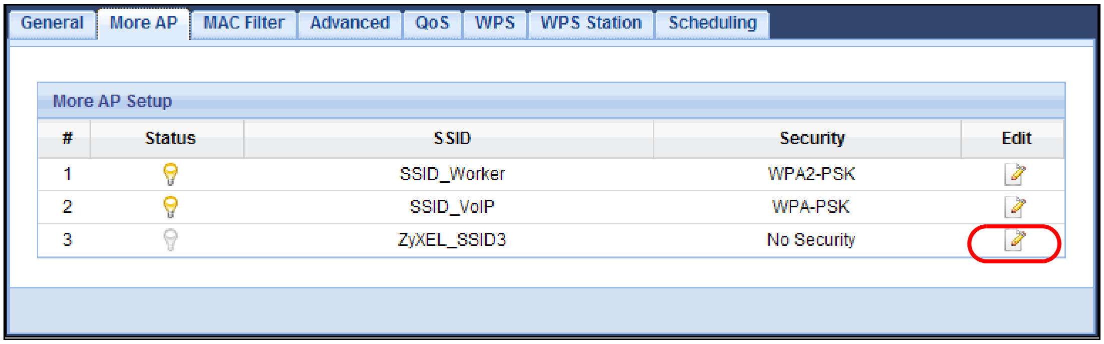
Security Mode : WPA-PSK

Pre-Shared Key VoIPOnly12345678

Group Key Update Timer 3600 seconds

No Security and WPA2-PSK can be configured when WPS enabled.

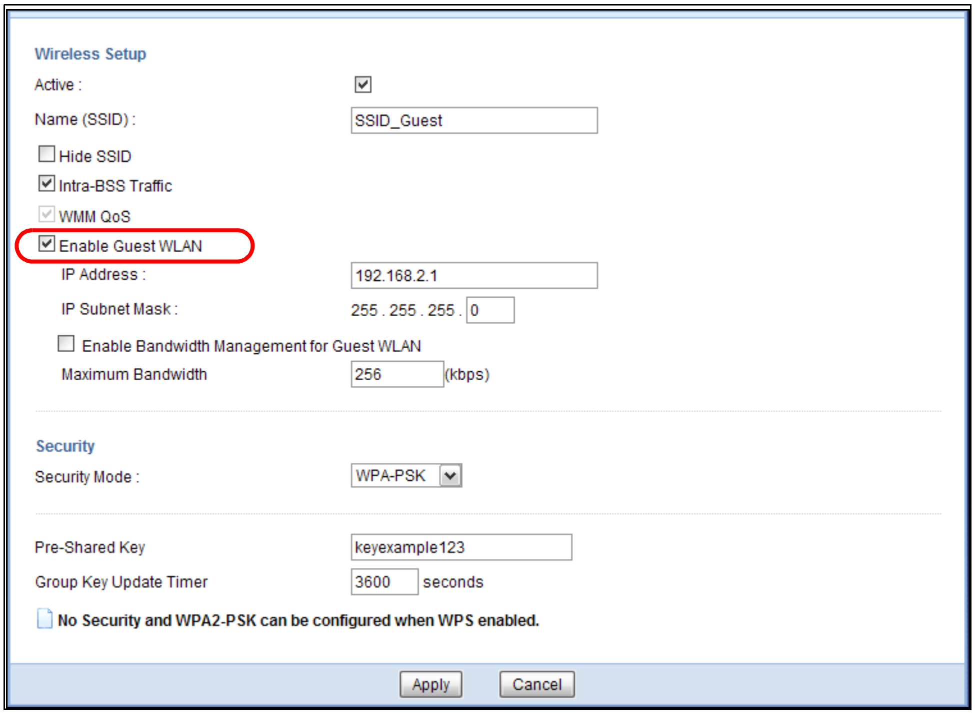
11 Click the **Edit** icon of the third entry to configure wireless and security settings for **SSID_Guest**.



More AP Setup

#	Status	SSID	Security	Edit
1	●	SSID_Worker	WPA2-PSK	✎
2	●	SSID_VoIP	WPA-PSK	✎
3	○	ZyXEL_SSID3	No Security	✎

12 Configure the screen as follows. In this example, you enable **Intra-BSS Traffic** for **SSID_Guest** to allow wireless clients in the same wireless network to communicate with each other. Select **Enable Guest WLAN** to allow clients to access the Internet only. Click **Apply**.



Wireless Setup

Active : ☑

Name (SSID) : SSID_Guest

□ Hide SSID

☑ Intra-BSS Traffic

☑ WMM QoS

☑ Enable Guest WLAN

IP Address : 192.168.2.1

IP Subnet Mask : 255 . 255 . 255 . 0

□ Enable Bandwidth Management for Guest WLAN

Maximum Bandwidth 256 (kbps)

Security

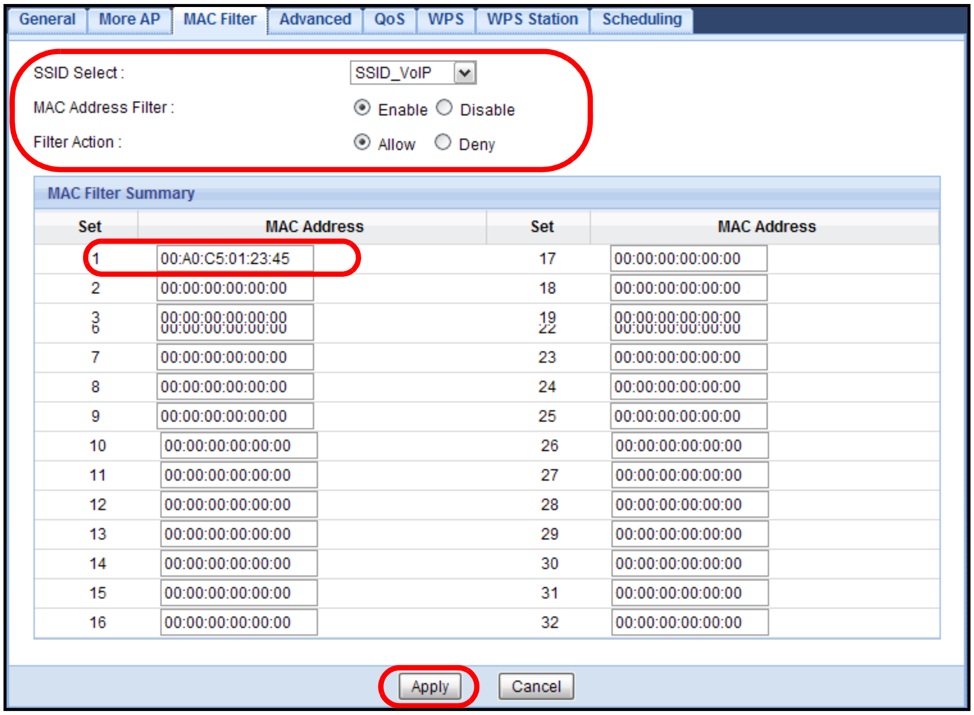
Security Mode : WPA-PSK

Pre-Shared Key keyexample123

Group Key Update Timer 3600 seconds

No Security and WPA2-PSK can be configured when WPS enabled.

13 Click the **MAC Filter** tab to configure MAC filtering for the **SSID_VoIP** wireless network. Select **SSID_VoIP** from the **SSID Select** drop-down list, enable MAC address filtering and set the **Filter Action** to **Allow**. Enter the VoIP device's MAC address in the **Mac Address** field and click **Apply** to allow only the VoIP device to associate with the EMG6765-Q10A using this SSID.



SSID Select : SSID_VoIP

MAC Address Filter : ● Enable ○ Disable

Filter Action : ● Allow ○ Deny

MAC Filter Summary

Set	MAC Address	Set	MAC Address
1	00:A0:C5:01:23:45	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3 6	00:00:00:00:00:00 00:00:00:00:00:00	19 22	00:00:00:00:00:00 00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

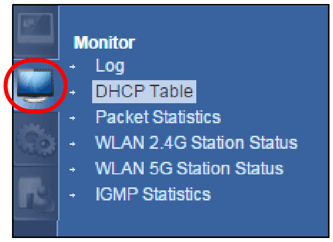
PART II
Technical Reference

CHAPTER 7 Monitor

7.1 Overview

This chapter discusses read-only information related to the device state of the EMG6765-Q10A.

To access the Monitor screens, go to **Expert Mode** after login, then click 🖥.



You can also click the links in the **Summary** table of the **Status** screen to view the packets sent/received as well as the status of clients connected to the EMG6765-Q10A.

7.2 What You Can Do

- Use the **Log** screen to see the logs for the activity on the EMG6765-Q10A (Section 7.3 on page 54).
- Use the **DHCP Table** screen to view information related to your DHCP status (Section 7.4 on page 56).
- use the **Packet Statistics** screen to view port status, packet specific statistics, the "system up time" and so on (Section 7.5 on page 56).
- Use the **WLAN 2.4G/5G Station Status** screen to view the wireless stations that are currently associated to the EMG6765-Q10A (Section 7.6 on page 57).
- Use the **IGMP Statistics** screen (Section 7.7 on page 58) to view multicasting details.

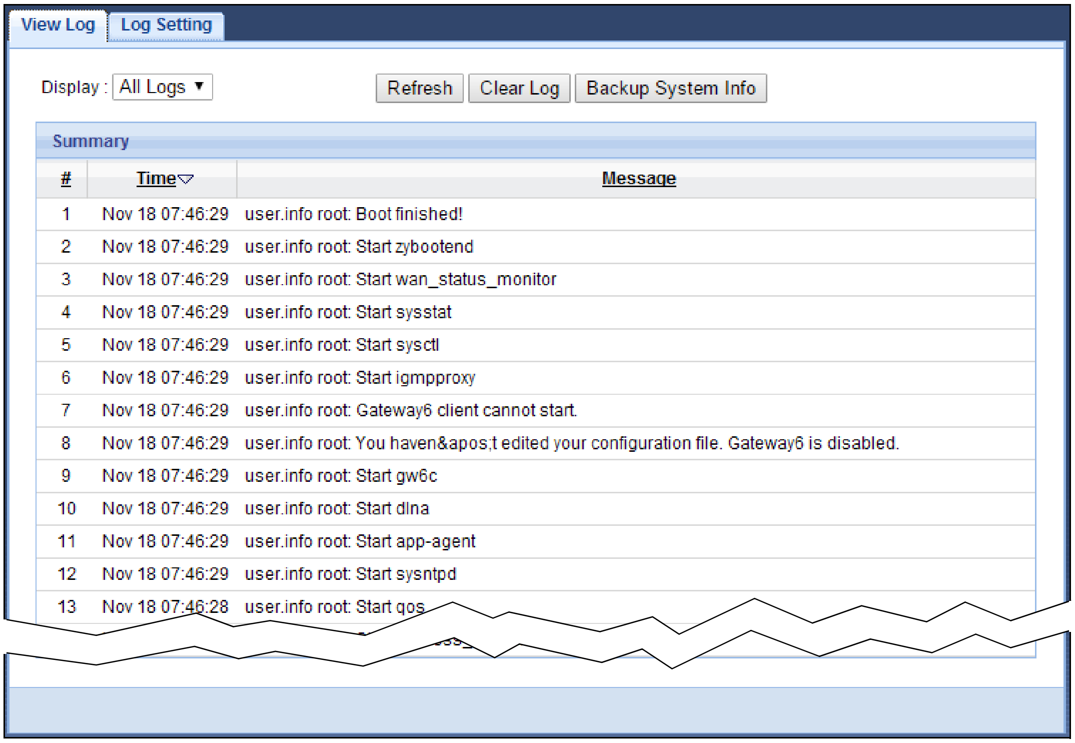
7.3 The Log Screen

The Web Configurator allows you to look at all of the EMG6765-Q10A's logs in one location.

7.3.1 View Log

Use the **View Log** screen to see the logged messages for the EMG6765-Q10A. The log wraps around and deletes the old entries after it fills. Select what logs you want to see from the **Display** drop list. The log choices depend on your settings in the **Log Setting** screen. Click **Refresh** to renew the log screen. Click **Clear Log** to delete all the logs Click **Backup System Info** to download a folder containing EMG6765-Q10A current backup information.

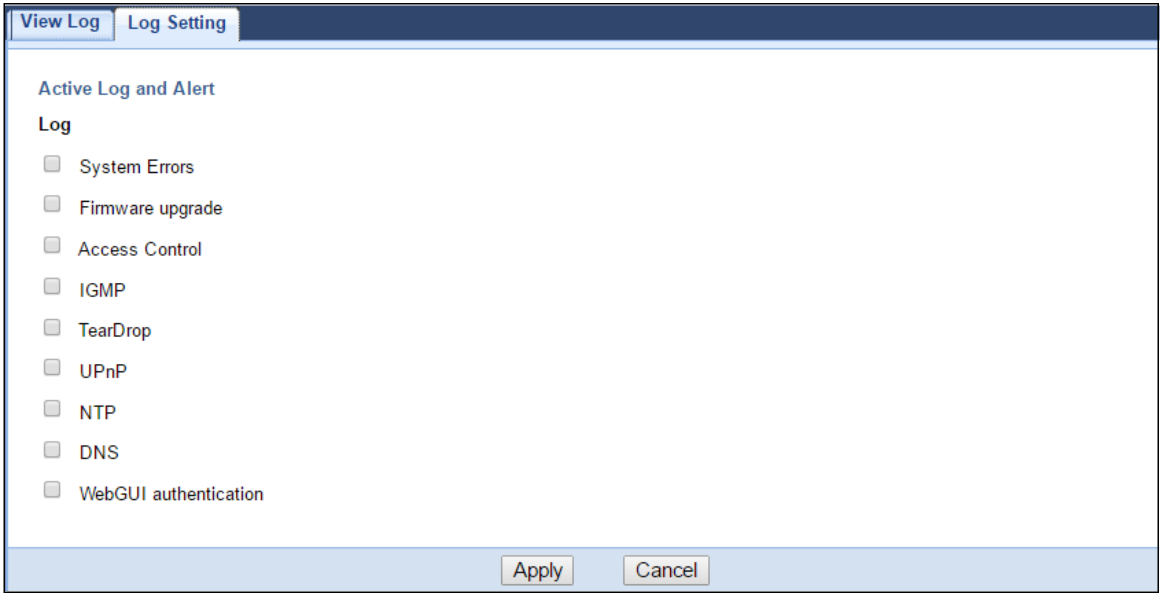
Figure 18 View Log



#	Time▽	Message
1	Nov 18 07:46:29	user.info root: Boot finished!
2	Nov 18 07:46:29	user.info root: Start zybootend
3	Nov 18 07:46:29	user.info root: Start wan_status_monitor
4	Nov 18 07:46:29	user.info root: Start sysstat
5	Nov 18 07:46:29	user.info root: Start sysctl
6	Nov 18 07:46:29	user.info root: Start igmpproxy
7	Nov 18 07:46:29	user.info root: Gateway6 client cannot start.
8	Nov 18 07:46:29	user.info root: You haven&apos;t edited your configuration file. Gateway6 is disabled.
9	Nov 18 07:46:29	user.info root: Start gw6c
10	Nov 18 07:46:29	user.info root: Start dlna
11	Nov 18 07:46:29	user.info root: Start app-agent
12	Nov 18 07:46:29	user.info root: Start sysntpd
13	Nov 18 07:46:28	user.info root: Start qos

You can configure which logs to display in the **View Log** screen. Go to the **Log Setting** screen and select the logs you wish to display. Click **Apply** to save your settings. Click **Cancel** to start the screen afresh.

Figure 19 Log Settings



Active Log and Alert

Log

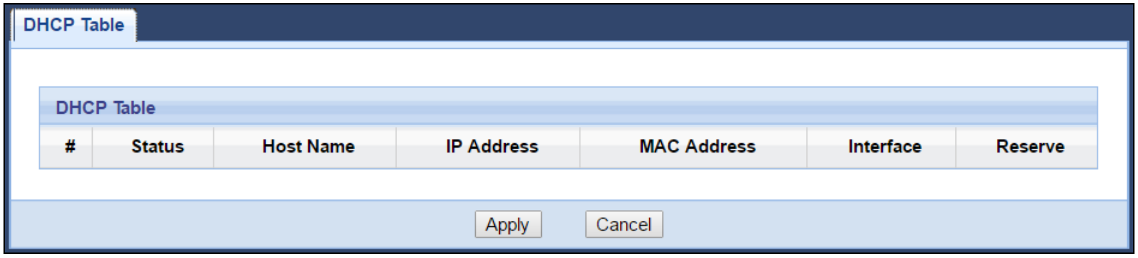
□ System Errors
□ Firmware upgrade
□ Access Control
□ IGMP
□ TearDrop
□ UPnP
□ NTP
□ DNS
□ WebGUI authentication

7.4 DHCP Table

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 EMG6765-Q10A's LAN as a DHCP server or disable it. When configured as a server, the EMG6765-Q10A provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on that network, or else the computer must be manually configured.

Click **Monitor > DHCP Table** or **Configuration > Network > DHCP Server > Client List**. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **MAC Address**, and **IP Address**) of all network clients using the EMG6765-Q10A's DHCP server.

Figure 20 Monitor > DHCP Table



DHCP Table

DHCP Table

#	Status	Host Name	IP Address	MAC Address	Interface	Reserve

The following table describes the labels in this screen.

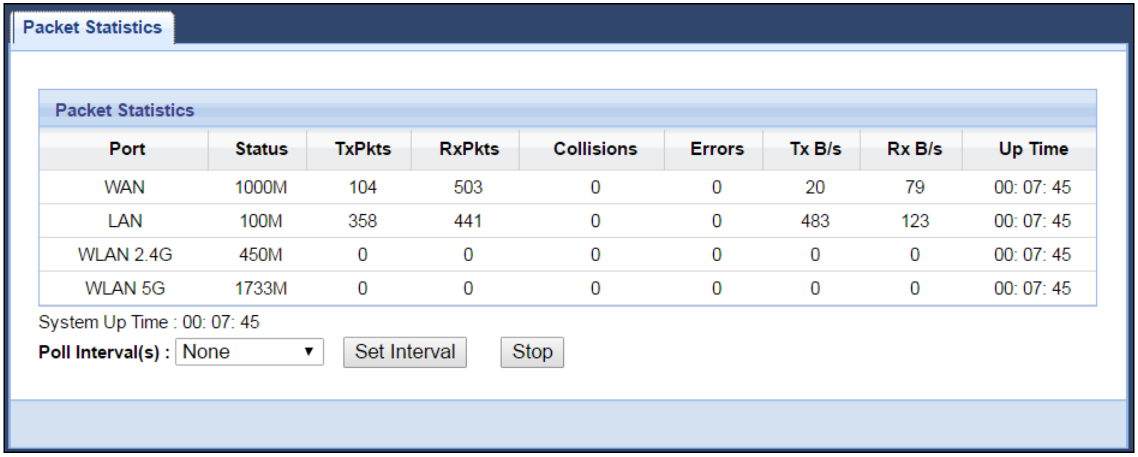
Table 11 Monitor > DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
Status	This field displays whether the connection to the host computer is up (a yellow bulb) or down (a gray bulb).
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Interface	This field identifies the interface that assigned an IP address to a DHCP client.
Reserve	Select this if you want to reserve the IP address for this specific MAC address.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

7.5 Packet Statistics

Click **Monitor > Packet Statistics** or the **Packet Statistics (Details...)** hyperlink in the **Status** screen. Read-only information here includes port status, packet specific statistics and the "system up time". The **Poll Interval(s)** field is configurable and is used for refreshing the screen.

Figure 21 Monitor > Packet Statistics



Packet Statistics

Port	Status	TxPkts	RxPkts	Collisions	Errors	Tx B/s	Rx B/s	Up Time
WAN	1000M	104	503	0	0	20	79	00: 07: 45
LAN	100M	358	441	0	0	483	123	00: 07: 45
WLAN 2.4G	450M	0	0	0	0	0	0	00: 07: 45
WLAN 5G	1733M	0	0	0	0	0	0	00: 07: 45

System Up Time : 00: 07: 45

Poll Interval(s) : None

The following table describes the labels in this screen.

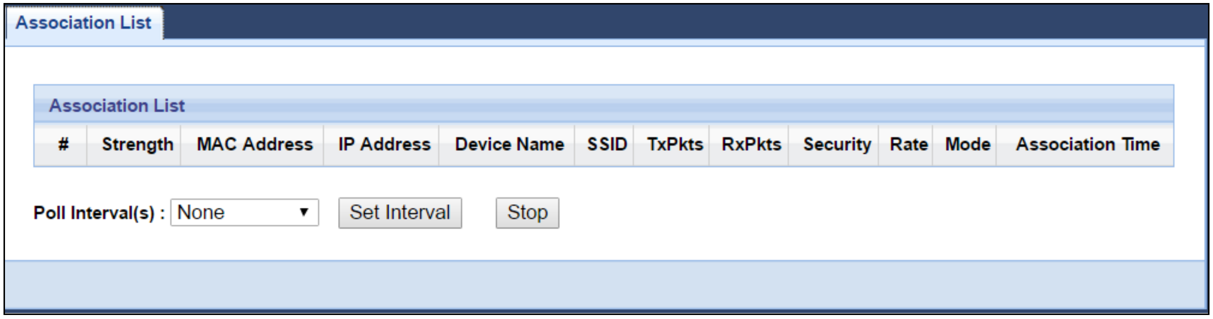
Table 12 Monitor > Packet Statistics

LABEL	DESCRIPTION
Port	This is the EMG6765-Q10A's interface type.
Status	For the LAN ports, this displays the port speed and duplex setting or **Down** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation. This field displays **Down** when the line is disconnected. For the 2.4GHz or 5GHz WLAN, it displays the maximum transmission rate when the WLAN is enabled and **Down** when the WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Errors	This is the number of received errors on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total time the EMG6765-Q10A has been for each session.
System Up Time	This is the total time the EMG6765-Q10A has been on.
Poll Interval(s)	Enter the time interval in seconds for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

7.6 WLAN Station Status

Click **Monitor > WLAN 2.4G/5G Station Status** or the **WLAN 2.4G/5G Station Status (Details...)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the EMG6765-Q10A's 2.4GHz or 5GHz wireless network in the **Association List**. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Figure 22 Monitor > WLAN Station Status



The following table describes the labels in this screen.

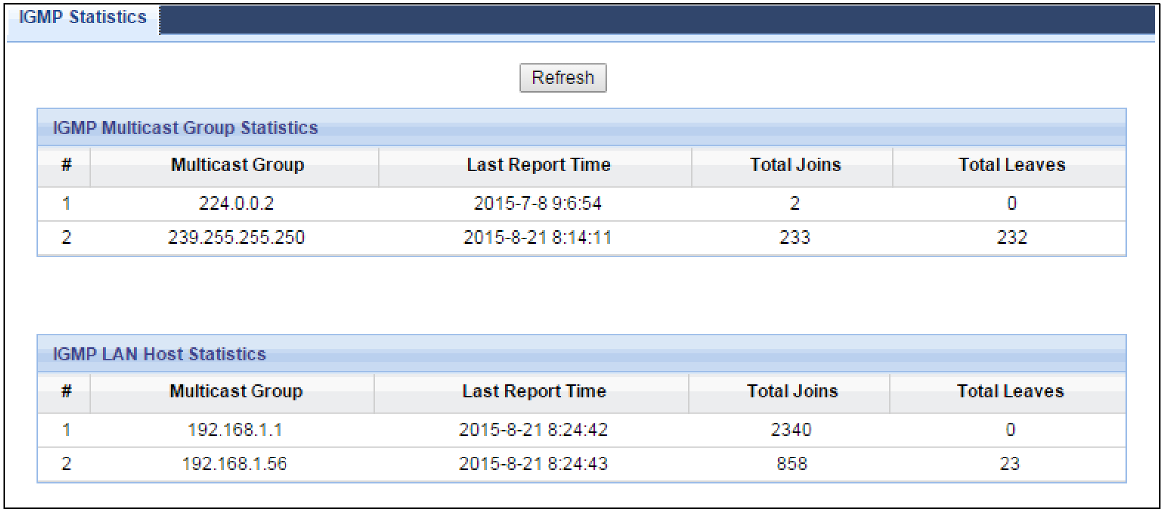
Table 13 Monitor > WLAN Station Status

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
Strength	This field displays the station's wireless connection signal strength.
MAC Address	This field displays the MAC address of an associated wireless station.
IP Address	This field displays the IP address of an associated wireless station.
Device Name	This field displays the name of an associated wireless station.
SSID	This field displays the name of the EMG6765-Q10A's wireless network to which the station is connected.
TxPkts	This field displays the number of packets transmitted by the station through the wireless connection.
RxPkts	This field displays the number of packets received by the station through the wireless connection.
Security	This field displays which secure encryption method is being used by the station to connect to the network.
Rate	This field displays the wireless station's transmission rate.
Mode	This field displays the wireless standard supported by the wireless station.
Association Time	This field displays the time a wireless station first associated with the EMG6765-Q10A's WLAN.
Poll Interval(s)	Enter the time interval in seconds for refreshing this screen in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing the screen.

7.7 IGMP Statistics

Use this screen to look at the current number of IGMP-related packets received for each IGMP multicast group and from each LAN host. Click **Monitor > IGMP Statistics** to open the following screen.

Figure 23 Monitor > IGMP Statistics



IGMP Multicast Group Statistics

#	Multicast Group	Last Report Time	Total Joins	Total Leaves
1	224.0.0.2	2015-7-8 9:6:54	2	0
2	239.255.255.250	2015-8-21 8:14:11	233	232

IGMP LAN Host Statistics

#	Multicast Group	Last Report Time	Total Joins	Total Leaves
1	192.168.1.1	2015-8-21 8:24:42	2340	0
2	192.168.1.56	2015-8-21 8:24:43	858	23

The following table describes the labels in this screen.

Table 14 Monitor > IGMP Statistics

LABEL	DESCRIPTION
Refresh	Click this button to update the information in the screen.
IGMP Multicast Group Statistics	This section shows statistics about the number of IGMP-related packets received for each IGMP multicast group.
#	This field is a sequential value, and it is not associated with a specific IGMP Statistics.
Multicast Group	This field displays the IP address of the IGMP multicast group for which the EMG6765-Q10A received IGMP-related packets.
Last Report Time	This field displays when the EMG6765-Q10A received the latest packet for this IGMP multicast group.
Total Joins	This field displays the total number of Join packets the EMG6765-Q10A has received for this IGMP multicast group.
Total Leaves	This field displays the total number of Leave packets the EMG6765-Q10A has received for this IGMP multicast group.
IGMP LAN Host Statistics	This section shows statistics about the number of IGMP-related packets received from each LAN host.
#	This field is a sequential value, and it is not associated with a specific IGMP Statistics.
Multicast Group	This field displays the IP address of a LAN computer that has sent the EMG6765-Q10A IGMP-related packets.
Last Report Time	This field displays when the EMG6765-Q10A received the latest packet from this LAN IP address for this IGMP multicast group.
Total Joins	This field displays the total number of Join packets the EMG6765-Q10A has received from this LAN IP address.
Total Leaves	This field displays the total number of Leave packets the EMG6765-Q10A has received from this LAN IP address.

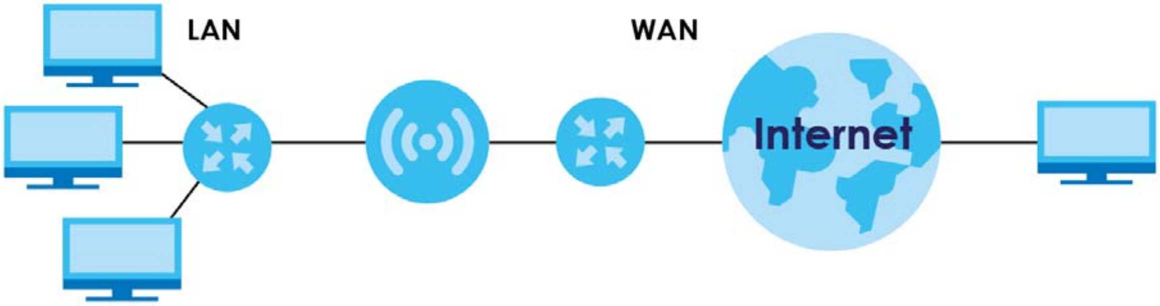
CHAPTER 8
WAN

8.1 Overview

This chapter discusses the EMG6765-Q10A's **WAN** screens. Use these screens to configure your EMG6765-Q10A 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 24 LAN and WAN



8.2 What You Can Do

- Use the **Internet Connection** screen to enter your ISP information and set how the computer acquires its IP, DNS and WAN MAC addresses (Section 8.4 on page 62).

8.3 What You Need To Know

The information in this section can help you configure the screens for your WAN connection, as well as enable/disable some advanced features of your EMG6765-Q10A.

8.3.1 Configuring Your Internet Connection

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over

Ethernet) or PPTP (Point-to-Point Tunneling Protocol), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the EMG6765-Q10A, which makes it accessible from an outside network. It is used by the EMG6765-Q10A to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the EMG6765-Q10A 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) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

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 EMG6765-Q10A 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 EMG6765-Q10A's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

WAN MAC Address

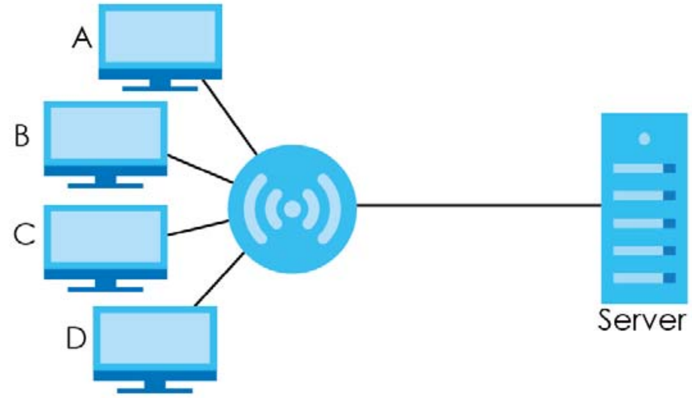
The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to configuration file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

Multicast

Traditionally, IP packets are transmitted in one of either 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.

Figure 25 Multicast Example



In the multicast example above, systems A and D comprise one multicast group. In multicasting, the server only needs to send one data stream and this is delivered to systems A and D.

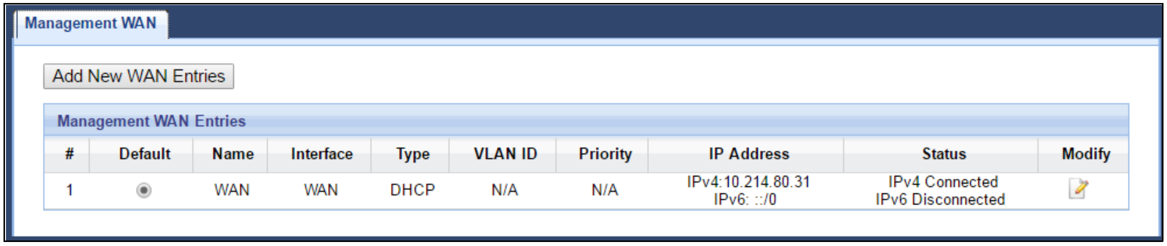
IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. The EMG6765-Q10A supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**).

At start up, the EMG6765-Q10A queries all directly connected networks to gather group membership. After that, the EMG6765-Q10A periodically updates this information. IP multicasting can be enabled/ disabled on the EMG6765-Q10A WAN interface in the Web Configurator (**WAN**). Select **None** to disable IP multicasting on these interfaces.

8.4 Management WAN

Use this screen to view, change, or add your EMG6765-Q10A's Internet access settings. Click **Configuration** > **Network** > **WAN**. The following screen opens.

Figure 26 Network > WAN > Management WAN



Management WAN Entries

#	Default	Name	Interface	Type	VLAN ID	Priority	IP Address	Status	Modify
1	●	WAN	WAN	DHCP	N/A	N/A	IPv4:10.214.80.31 IPv6: ::/0	IPv4 Connected IPv6 Disconnected	✎

The following table describes the labels in this screen.

Table 15 Network > WAN > Management WAN

LABEL	DESCRIPTION
Add New WAN Entries	Click this to create a new WAN interface entry.
Management WAN Entries	
#	This is the index number of the connection.
Default	Select the WAN interface that you want to configure as default.
Name	This is the service name of the connection.
Interface	This is the interface of the connection.
Type	This shows the type of interface used by this connection.
VLAN ID	This indicates the VLAN ID number assigned to traffic sent through this connection.
Priority	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.
IP Address	This is the WAN IP address used by this connection.
Status	This shows the status of the connection.
Modify	Click the **Edit** icon to configure the connection. Click the **Delete** icon to delete this connection from the EMG6765-Q10A. A window displays asking you to confirm that you want to delete the connection.

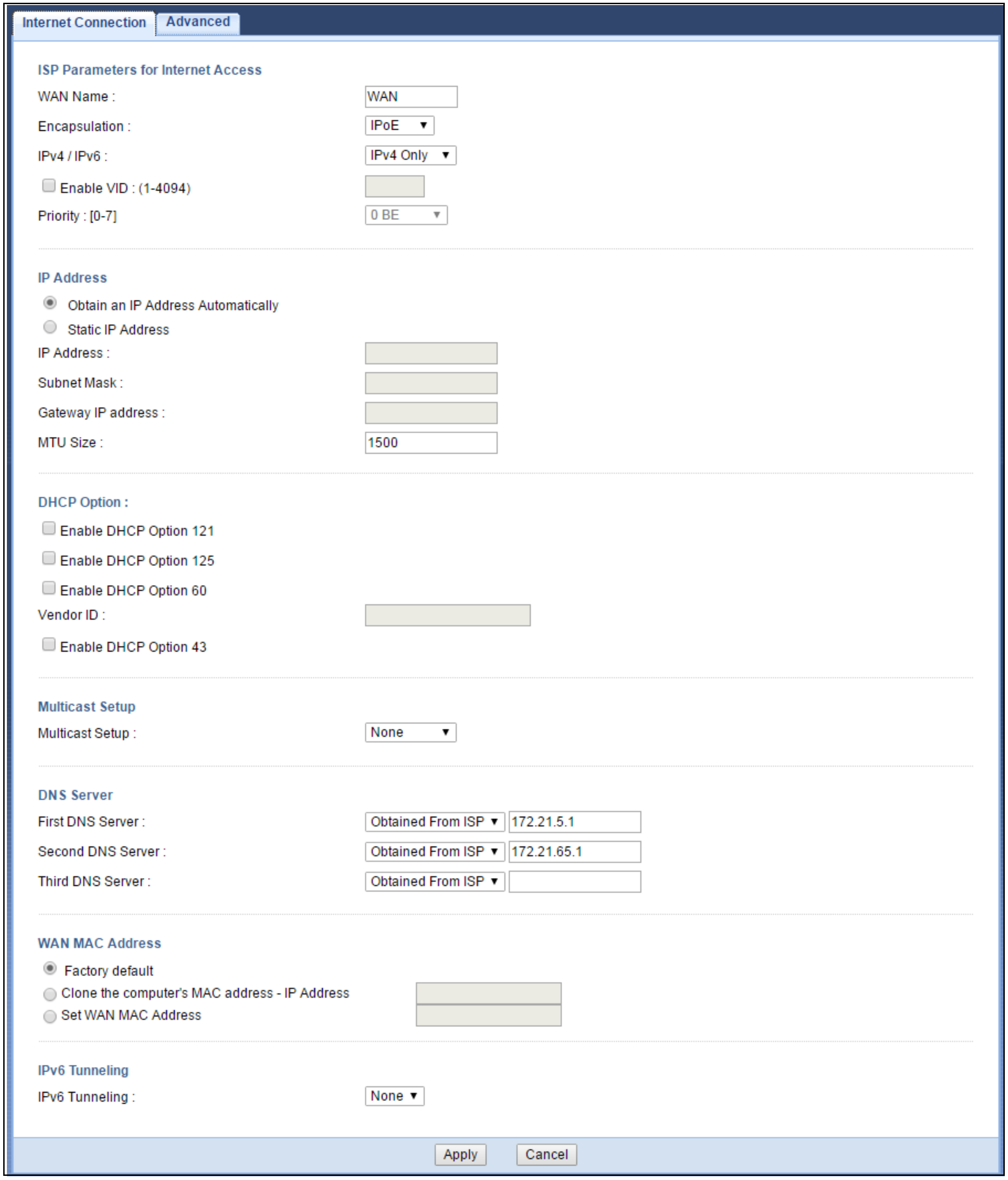
8.4.1 Add/Edit WAN Connection

Click the **Add New WAN Entries** in the **Configuration** > **WAN** screen or the **Edit** icon next to the connection you want to configure. Use this screen to configure a WAN connection. The screen varies depending on the encapsulation you select.

8.4.1.1 IPoE Encapsulation

This screen displays when you select **IPoE** encapsulation.

Figure 27 Network > WAN > Internet Connection: IPoE Encapsulation (IPv4 Only)



ISP Parameters for Internet Access

WAN Name : WAN

Encapsulation : IPoE

IPv4 / IPv6 : IPv4 Only

□ Enable VID : (1-4094)

Priority : [0-7] 0 BE

IP Address

● Obtain an IP Address Automatically

○ Static IP Address

IP Address :

Subnet Mask :

Gateway IP address :

MTU Size : 1500

DHCP Option :

□ Enable DHCP Option 121

□ Enable DHCP Option 125

□ Enable DHCP Option 60

Vendor ID :

□ Enable DHCP Option 43

Multicast Setup

Multicast Setup : None

DNS Server

First DNS Server : Obtained From ISP 172.21.5.1

Second DNS Server : Obtained From ISP 172.21.65.1

Third DNS Server : Obtained From ISP

WAN MAC Address

● Factory default

○ Clone the computer's MAC address - IP Address

○ Set WAN MAC Address

IPv6 Tunneling

IPv6 Tunneling : None

The following table describes the labels in this screen.

Table 16 Network > WAN > Internet Connection: IPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
WAN Name	Enter the name to use for this connection definition.
Encapsulation	You must choose the **IPoE** option when the WAN port is used as a regular Ethernet.
IPv4 / IPv6	Select **IPv4 Only** if you want the EMG6765-Q10A to run IPv4 only. Select **Dual Stack** to allow the EMG6765-Q10A to run IPv4 and IPv6 at the same time. Select **IPv6 Only** if you want the EMG6765-Q10A to run IPv6 only.

Table 16 Network > WAN > Internet Connection: IPoE Encapsulation (continued)

LABEL	DESCRIPTION
Enable VID	Enter a VLAN identifier between 11 to 4094 (the 802.1Q tag specifies only a priority and is referred to as a priority tag). VID 1 (the default VLAN ID) is reserved for a management VLAN. Note: This field is not available when you are configuring the default WAN entry.
Priority	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.
IP Address This is not available when you select **IPv6 Only** in the **IPv6/IPv4** field.	
Obtain an IP Address Automatically	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Static IP Address**.
Subnet Mask	Enter the **Subnet Mask** in this field.
Gateway IP Address	Enter a **Gateway IP Address** (if your ISP gave you one) in this field.
MTU Size	Enter the MTU (Maximum Transmission Unit) size for each packet. If a larger packet arrives, the EMG6765-Q10A divides it into smaller fragments.
DHCP Option This is not available when you select **IPv6 Only** in the **IPv6/IPv4** field.	
Enable DHCP Option 121	Select this to enable the classless route option 121.
Enable DHCP Option 125	Select this to add vendor specific information to DHCP requests that the EMG6765-Q10A sends to a DHCP server when getting a WAN IP address.
Enable DHCP Option 60	Select this to identify the vendor and functionality of the EMG6765-Q10A in DHCP requests that the EMG6765-Q10A sends to a DHCP server when getting a WAN IP address.
Vendor ID	Enter the Vendor Class Identifier (Option 60), such as the type of hardware or firmware.
Enable DHCP Option 43	Select this for clients and servers to exchange vendor specific information.
Multicast Setup	Select **IGMPv1/v2** to turn on IGMP (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.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the EMG6765-Q10A's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the EMG6765-Q10A's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.

Table 16 Network > WAN > Internet Connection: IPoE Encapsulation (continued)

LABEL	DESCRIPTION
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
IPv6 Tunneling The EMG6765-Q10A uses tunnel interfaces in Generic Routing Encapsulation (GRE), IPv6 in IPv4, and 6to4 tunnels. GRE tunnels encapsulate a wide variety of network layer protocol packet types inside IP tunnels. A GRE tunnel serves as a virtual point-to-point link between the EMG6765-Q10A and another router over an IPv4 network.	
IPv6 Tunneling	Enable **IPv6 Rapid Deployment** (**6rd**) to tunnel IPv6 traffic from the local network through the ISP's IPv4 network. The EMG6765-Q10A generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router to connect to the native IPv6 Internet. The local network can also use IPv4 services. The EMG6765-Q10A uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet. Enable **6to4** to enable IPv6 packets to cross IPv4 networks. the EMG6765-Q10A should get a public IPv4 address for the WAN. The EMG6765-Q10A adds an IPv4 IP header to an IPv6 packet when transmitting the packet to the Internet. In reverse, the EMG6765-Q10A removes the IPv4 header from an IPv6 packet when receiving it from the Internet. Enable **6in4** if the EMG6765-Q10A has a public IPv4 IP address given from your ISP and you want to transmit your Ipv6 packets to one and only one remote site whose LAN network is also an IPv6 network. This is available only when you select **IPv4 Only** in the **IPv6/IPv4** field.
Automatically configured by DHCPC	Select this to have the EMG6765-Q10A detect the relay server's IP address automatically through DHCP.
Manually Configured	Select this if you have the IPv4 address of the relay server.
Border Relay IPv4 Address	Specify the relay server's IPv4 address.
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.
Service Provider IPv6 Prefix length	Enter the IPv6 prefix length. An IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address.
IPv4 mask length	Enter the subnet mask number (1~32) for the IPv4 network.
IPv6 Address	This is not available when you select **IPv4 Only** in the **IPv6/IPv4** field.
Obtain an IP Address Automatically	Select this if you want to obtain an IPv6 address from a DHCPv6 server.
Static IP Address	Select this if you have a fixed IPv6 address assigned by your ISP.
IPv6 Address	Enter the IPv6 address assigned by your ISP.
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 EMG6765-Q10A's interface(s). The gateway helps forward packets to their destinations.
Link Local Only	Select this if you want the IPv6 address to be generated automatically by EMG6765-Q10A.

Table 16 Network > WAN > Internet Connection: IPoE Encapsulation (continued)

LABEL	DESCRIPTION
IPv6 DNS server This is not available when you select **IPv4 Only** in the **IPv6/IPv4** field.	
Obtain IPv6 DNS info Automatically	Select this to have the EMG6765-Q10A get the IPv6 DNS server addresses from the ISP automatically.
Use the following Static DNS IPv6 Address	Select this to have the EMG6765-Q10A use the IPv6 DNS server addresses you configure manually.
IPv6 DNS Server	Enter the IPv6 DNS server address assigned by the ISP.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.4.1.2 PPPoE Encapsulation

The EMG6765-Q10A supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

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

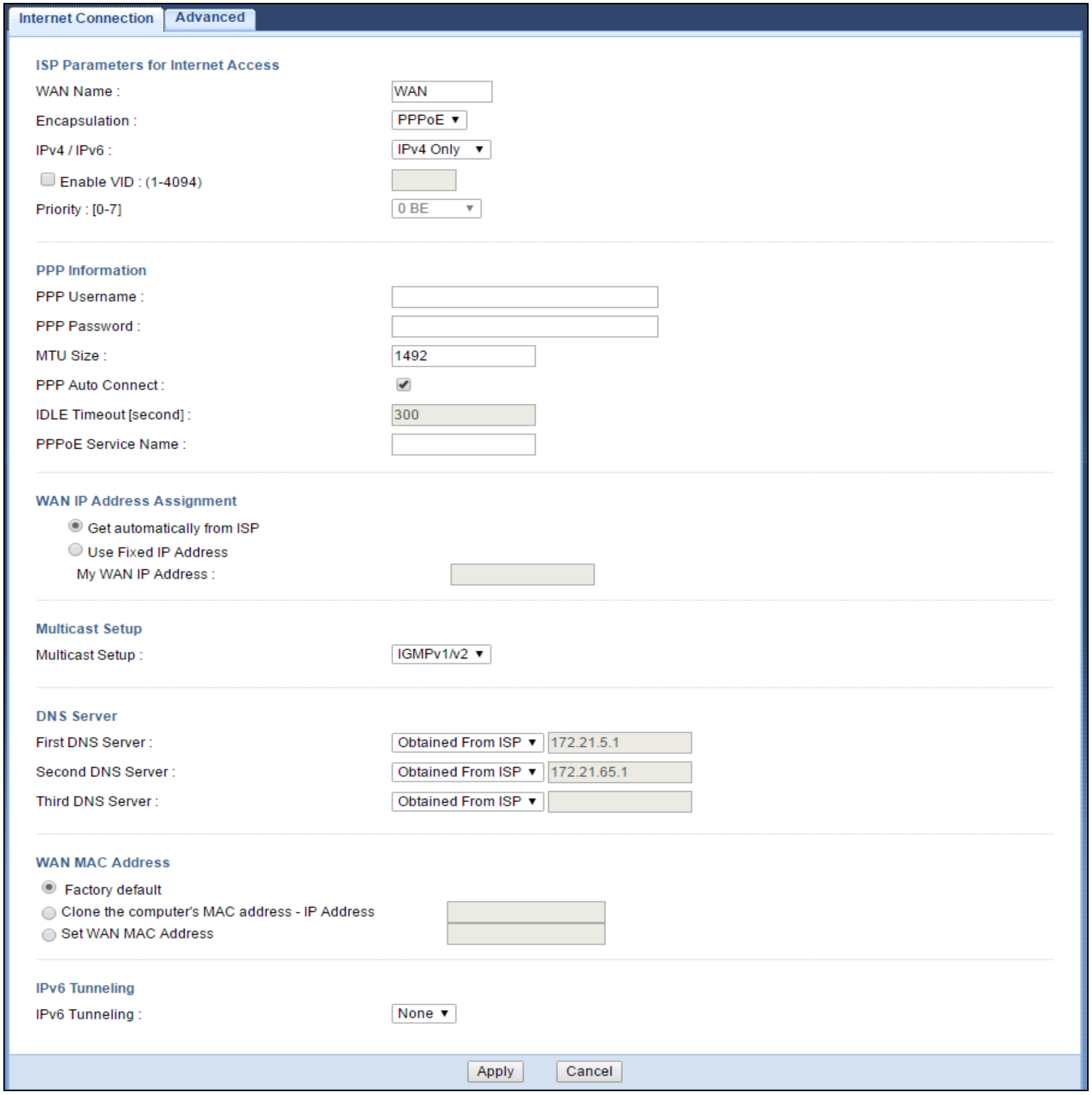
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

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 EMG6765-Q10A (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the EEMG6765-Q10A does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

This screen displays when you select **PPPoE** encapsulation.

Figure 28 Network > WAN > Internet Connection: PPPoE Encapsulation (IPv4 Only)



ISP Parameters for Internet Access

WAN Name : WAN

Encapsulation : PPPoE

IPv4 / IPv6 : IPv4 Only

□ Enable VID : (1-4094)

Priority : [0-7] 0 BE

PPP Information

PPP Username :

PPP Password :

MTU Size : 1492

PPP Auto Connect : ☑

IDLE Timeout [second] : 300

PPPoE Service Name :

WAN IP Address Assignment

● Get automatically from ISP

○ Use Fixed IP Address

My WAN IP Address :

Multicast Setup

Multicast Setup : IGMPv1/v2

DNS Server

First DNS Server : Obtained From ISP 172.21.5.1

Second DNS Server : Obtained From ISP 172.21.65.1

Third DNS Server : Obtained From ISP

WAN MAC Address

● Factory default

○ Clone the computer's MAC address - IP Address

○ Set WAN MAC Address

IPv6 Tunneling

IPv6 Tunneling : None

The following table describes the labels in this screen.

Table 17 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
WAN Name	Enter the name to use for this connection definition.
Encapsulation	You must choose the **PPPoE** option when the WAN port is used as a regular Ethernet.
IPv4 / IPv6	Select **IPv4 Only** if you want the EMG6765-Q10A to run IPv4 only. Select **Dual Stack** to allow the EMG6765-Q10A to run IPv4 and IPv6 at the same time. Select **IPv6 Only** if you want the EMG6765-Q10A to run IPv6 only.

Table 17 Network > WAN > Internet Connection: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
Enable VID	Enter a VLAN identifier between 11 to 4094 (the 802.1Q tag specifies only a priority and is referred to as a priority tag). VID 1 (the default VLAN ID) is reserved for a management VLAN. Note: This field is not available when you are configuring the default WAN entry.
Priority	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.
PPP Information	
PPP Username	Type the user name given to you by your ISP.
PPP Password	Type the password associated with the user name above.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your EMG6765-Q10A can receive and process.
PPP Auto Connect	Select this option if you do not want the connection to time out.
Idle Timeout (second)	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.
PPPoE Service Name	Enter the PPPoE service name specified in the ISP account.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
Multicast Setup	Select **IGMPv1/v2** to turn on IGMP (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.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the EMG6765-Q10A's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the EMG6765-Q10A's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
IPv6 Tunneling The EMG6765-Q10A uses tunnel interfaces in Generic Routing Encapsulation (GRE), IPv6 in IPv4, and 6to4 tunnels. GRE tunnels encapsulate a wide variety of network layer protocol packet types inside IP tunnels. A GRE tunnel serves as a virtual point-to-point link between the EMG6765-Q10A and another router over an IPv4 network.	

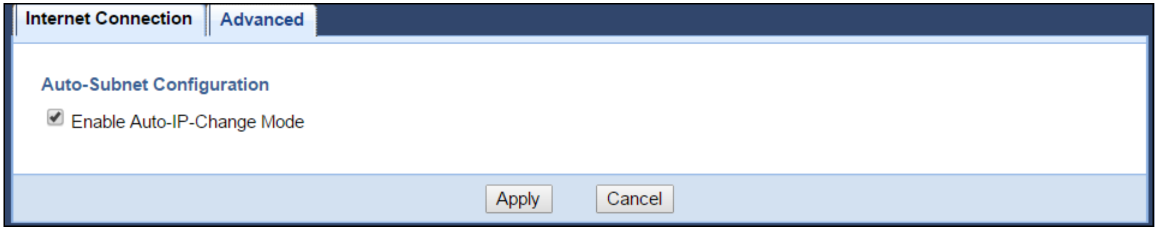
Table 17 Network > WAN > Internet Connection: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
IPv6 Tunneling	Enable **IPv6 Rapid Deployment** (**6rd**) to tunnel IPv6 traffic from the local network through the ISP's IPv4 network. The EMG6765-Q10A generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router to connect to the native IPv6 Internet. The local network can also use IPv4 services. The EMG6765-Q10A uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet. Enable **6to4** to enable IPv6 packets to cross IPv4 networks. the EMG6765-Q10A should get a public IPv4 address for the WAN. The EMG6765-Q10A adds an IPv4 IP header to an IPv6 packet when transmitting the packet to the Internet. In reverse, the EMG6765-Q10A removes the IPv4 header from an IPv6 packet when receiving it from the Internet. Enable **6in4** if the EMG6765-Q10A has a public IPv4 IP address given from your ISP and you want to transmit your Ipv6 packets to one and only one remote site whose LAN network is also an IPv6 network. This is available only when you select **IPv4 Only** in the **IPv6/IPv4** field.
Manually Configured	Select this if you have the IPv4 address of the relay server.
Border Relay IPv4 Address	Specify the relay server's IPv4 address.
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.
Service Provider IPv6 Prefix length	Enter the IPv6 prefix length. An IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address.
IPv4 mask length	Enter the subnet mask number (1~32) for the IPv4 network.
IPv6 DNS server This is not available when you select **IPv4 Only** in the **IPv6/IPv4** field.	
Obtain IPv6 DNS info Automatically	Select this to have the EMG6765-Q10A get the IPv6 DNS server addresses from the ISP automatically.
Use the following Static DNS IPv6 Address	Select this to have the EMG6765-Q10A use the IPv6 DNS server addresses you configure manually.
IPv6 DNS Server	Enter the IPv6 DNS server address assigned by the ISP.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.4.1.3 Add/Edit WAN Connection > Advanced

Click the **Add New WAN Entries** in the **Configuration** > **WAN** screen or the **Edit** icon next to the connection you want to configure. Then click the **Advanced** tab to view the following screen. Use this screen to enable the **Auto-IP Change Mode** to have the EMG6765-Q10A change it LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the EMG6765-Q10A gets a dynamic WAN IP address in the same subnet as the LAN IP address 192.168.1.1 or 10.0.0.1.

Figure 29 Add/Edit WAN Connection > Advanced



Auto-Subnet Configuration

☑ Enable Auto-IP-Change Mode

CHAPTER 9
Wireless LAN

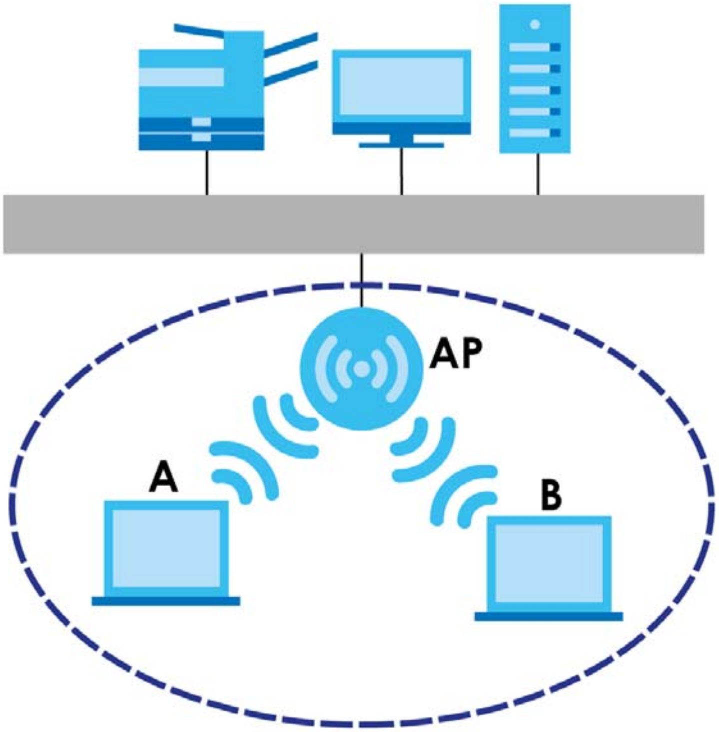
9.1 Overview

This chapter discusses how to configure the wireless network settings in your EMG6765-Q10A. The EMG6765-Q10A is able to function both 2.4GHz and 5GHz network at the same time. You can have different wireless and wireless security settings for 2.4GHz and 5GHz wireless LANs. Click **Configuration > Network > Wireless LAN 2.4G** or **Wireless LAN 5G** to configure to do so.

See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 30 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your EMG6765-Q10A is the AP.

9.1.1 What You Can Do

- Use the **General** screen to turn the wireless connection on or off, set up wireless security between the EMG6765-Q10A and the wireless clients, and make other basic configuration changes (Section 9.2 on page 76).
- Use the **More AP** screen to set up multiple wireless networks on your EMG6765-Q10A (Section 9.4 on page 81).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the EMG6765-Q10A (Section 9.5 on page 84).
- Use the **Advanced** screen to allow intra-BSS networking and set the RTS/CTS Threshold (Section 9.6 on page 86).
- Use the **QoS** screen to ensure Quality of Service (QoS) in your wireless network (Section 9.7 on page 87).
- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually (Section 9.8 on page 87).
- Use the **WPS Station** screen to add a wireless station using WPS (Section 9.9 on page 89).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off (Section 9.10 on page 89).
- Use the **Airtime Management** screen to assign available airtime and bandwidth to interfaces and hosts (Section 9.11 on page 90).

9.1.2 What You Should Know

Every wireless network must follow these basic guidelines.

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

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

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client 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.

Wireless Security Overview

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

SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP 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 devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

MAC Address Filter

Every wireless client 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 wireless client, see the appropriate User's Guide or other documentation.

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

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

User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized 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.

Local user databases also have an additional limitation that is explained in the next section.

Guest WLAN

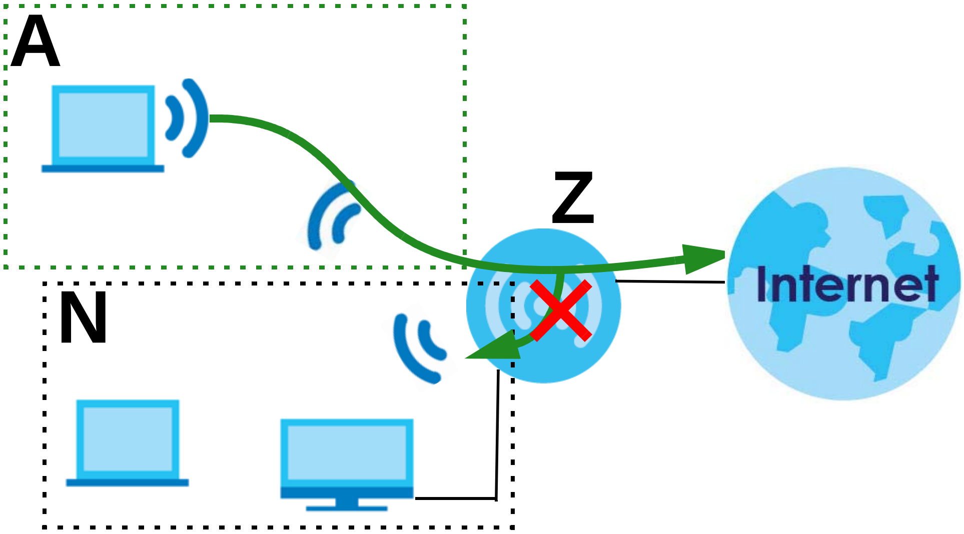
Guest WLAN allows you to set up a wireless network where users can access to Internet via the EMG6765-Q10A (**Z**), but not other networks connected to the **Z**. In the following figure, a guest user can access the Internet from the guest wireless network **A** via **Z** but not the home or company network **N**.

Note: The home or company network **N** and Guest WLAN network are independent networks.

[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.

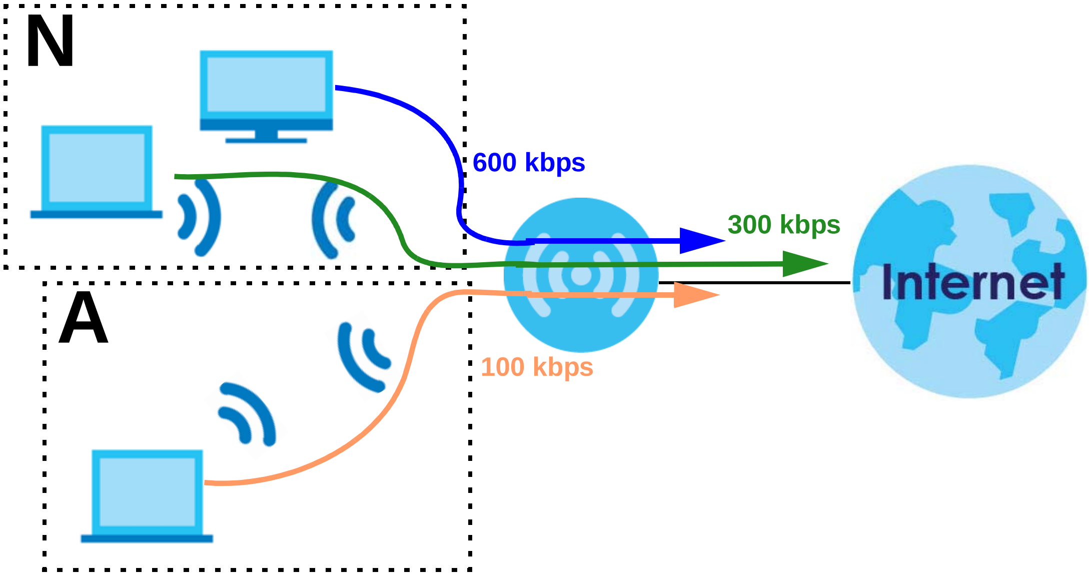
Figure 31 Guest Wireless LAN Network



Guest WLAN Bandwidth

The Guest WLAN Bandwidth function allows you to restrict the maximum bandwidth for the guest wireless network. Additionally, you can also define bandwidth for your home or office network. An example is shown next to define maximum bandwidth for your networks (**A** is Guest WLAN and **N** is home or company network.)

Figure 32 Example: Bandwidth for Different Networks



WPS

Wi-Fi Protected Setup (WPS) is an industry standard specification, defined by the Wi-Fi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices.

Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the Section 6.8 on page 48.

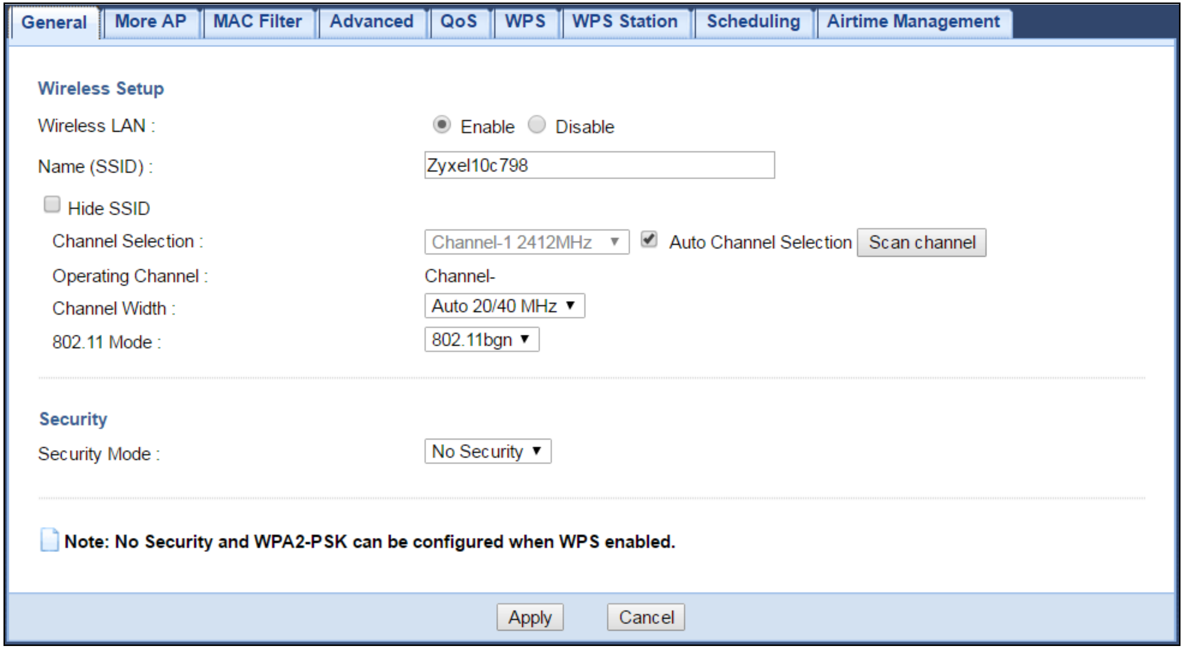
9.2 General Wireless LAN Screen

Use this screen to configure the SSID and wireless security of the wireless LAN.

Note: If you are configuring the EMG6765-Q10A from a computer connected to the wireless LAN and you change the EMG6765-Q10A's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the EMG6765-Q10A's new settings.

Click **Network** > **Wireless LAN 2.4G/5G** to open the **General** screen.

Figure 33 Network > Wireless LAN 2.4G/5G > General



Wireless Setup

Wireless LAN : ● Enable ○ Disable

Name (SSID) : Zyxel10c798

□ Hide SSID

Channel Selection : Channel-1 2412MHz ▼ ☑ Auto Channel Selection Scan channel

Operating Channel : Channel-

Channel Width : Auto 20/40 MHz ▼

802.11 Mode : 802.11bgn ▼

Security

Security Mode : No Security ▼

Note: No Security and WPA2-PSK can be configured when WPS enabled.

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

Table 18 Network > Wireless LAN 2.4G/5G > General

LABEL	DESCRIPTION
Wireless Setup	
Wireless LAN	Select **Enable** to activate the 2.4GHz and/or 5GHz wireless LAN. Select **Disable** to turn it off. Note: You can enable or disable both 2.4GHz and 5GHz wireless LANs by using the **WIFI** button located on the side panel of the EMG6765-Q10A.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.

Table 18 Network > Wireless LAN 2.4G/5G > General (continued)

LABEL	DESCRIPTION
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels. This option is only available if **Network Search** is disabled.
Network Search	Select this check box for the EMG6765-Q10A to automatically choose the channel with the least interference. Deselect this check box if you wish to manually select the channel using the **Channel Selection** field. Click **Scan channel** so the EMG6765-Q10A can scan for an available channel.
Operating Channel	This displays the channel the EMG6765-Q10A is currently using.
Channel Width	Select the wireless channel width used by EMG6765-Q10A. A standard 20 MHz channel offers transfer speeds of up to 144Mbps (2.4GHz) or 217Mbps (5GHZ) whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps (2.4GHz) or 450Mbps (5GHZ). An IEEE 802.11ac-specific 80MHz channel offers speeds of up to 1.3Gbps. Because not all devices support 40 MHz and/or 80 MHz channels, select **Auto 20/40 MHz** or **Auto 20/40/80 MHz** to allow the EMG6765-Q10A to adjust the channel bandwidth automatically. **40 MHz** (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. A **80 MHz** channel consists of two adjacent 40 MHz channels. The wireless clients must also support **40 MHz** or **80 MHz**. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. Select **20 MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.
802.11 Mode	If you are in the **Wireless LAN 2.4G > General** screen, you can select from the following: • **802.11b**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the EMG6765-Q10A. In this mode, all wireless devices can only transmit at the data rates supported by IEEE 802.11b. • **802.11g**: allows IEEE 802.11g compliant WLAN devices to associate with the Device. IEEE 802.11b compliant WLAN devices can associate with the EMG6765-Q10A only when they use the short preamble type. • **802.11bg**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the EMG6765-Q10A. The EMG6765-Q10A adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. • **802.11n**: allows IEEE 802.11n compliant WLAN devices to associate with the EMG6765-Q10A. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the EMG6765-Q10A. • **802.11gn**: allows either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the EMG6765-Q10A. The transmission rate of your EMG6765-Q10A might be reduced. • **802.11 bgn**: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the EMG6765-Q10A. The transmission rate of your EMG6765-Q10A might be reduced. If you are in the **Wireless LAN 5G > General** screen, you can select from the following: • **802.11a**: allows only IEEE 802.11a compliant WLAN devices to associate with the EMG6765-Q10A. • **802.11a/an**: allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the EMG6765-Q10A. The transmission rate of your EMG6765-Q10A might be reduced. • **802.11a/an/ac**: allows both IEEE802.11a, IEEE802.11n and IEEE802.11ac compliant WLAN devices to associate with the EMG6765-Q10A. The transmission rate of your EMG6765-Q10A might be reduced.
Security	

Table 18 Network > Wireless LAN 2.4G/5G > General (continued)

LABEL	DESCRIPTION
Security Mode	Select **WPA2-PSK** or **WPA2** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See Section 9.3 on page 78 for detailed information on different security modes. Or you can select **No Security** to allow any client to associate this network without authentication. Note: If the WPS function is enabled (default), only **No Security** and **WPA2-PSK** are available in this field.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

See the rest of this chapter for information on the other labels in this screen.

9.3 Wireless Security

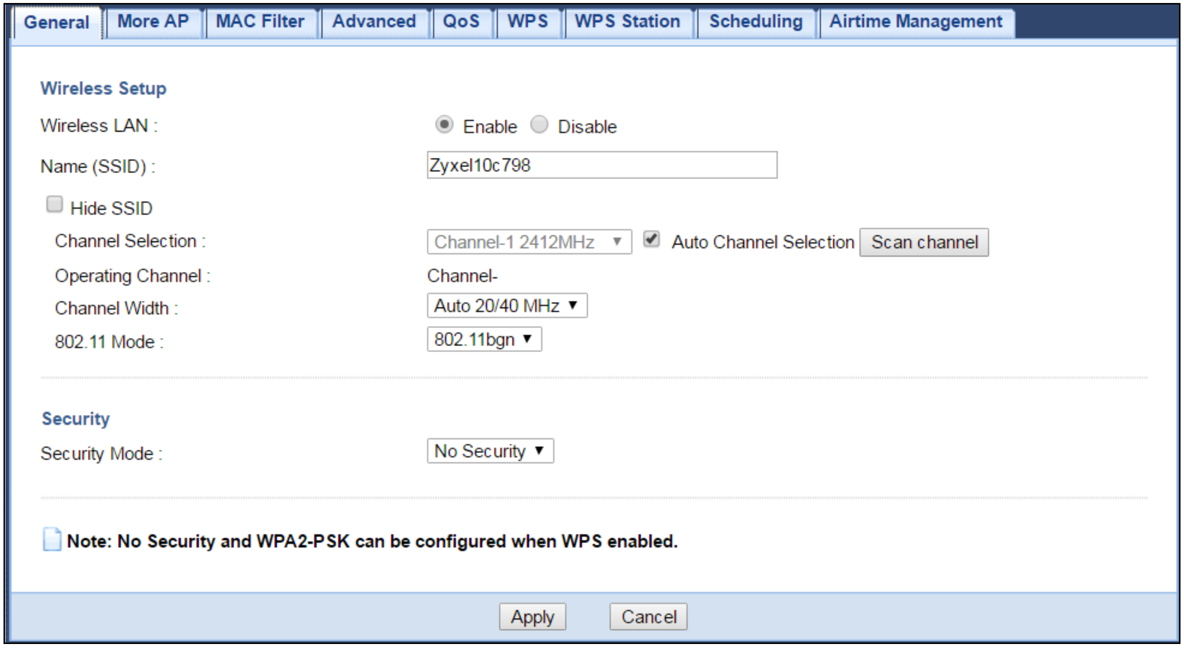
The screen varies depending on what you select in the **Security Mode** field.

9.3.1 No Security

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

Note: If you do not enable any wireless security on your EMG6765-Q10A, your network is accessible to any wireless networking device that is within range.

Figure 34 Network > Wireless LAN 2.4G/5G > General: No Security



Wireless Setup

Wireless LAN : ● Enable ○ Disable

Name (SSID) : Zyxel10c798

□ Hide SSID

Channel Selection : Channel-1 2412MHz ☑ Auto Channel Selection Scan channel

Operating Channel : Channel-

Channel Width : Auto 20/40 MHz

802.11 Mode : 802.11bgn

Security

Security Mode : No Security

Note: No Security and WPA2-PSK can be configured when WPS enabled.

The following table describes the labels in this screen.

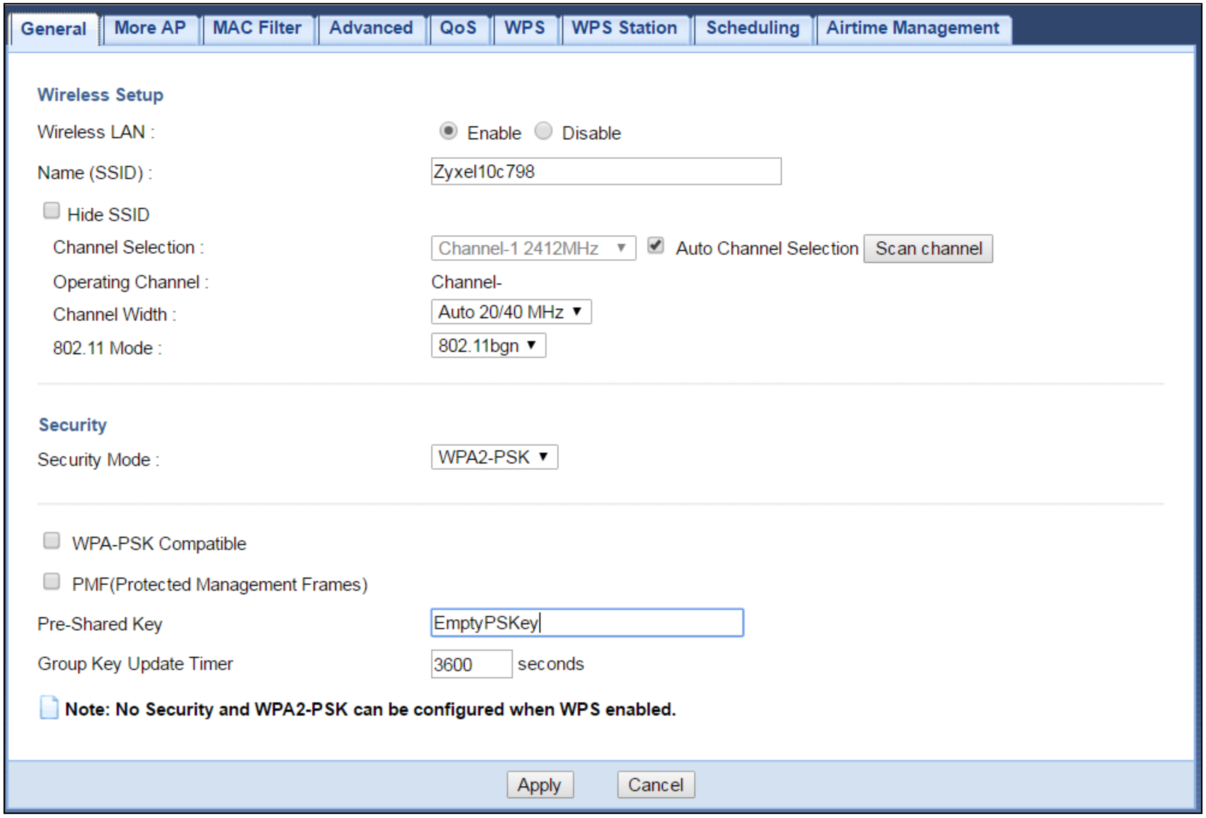
Table 19 Network > Wireless LAN 2.4G/5G > General: No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

9.3.2 WPA2-PSK

Select **WPA2-PSK** from the **Security Mode** list.

Figure 35 Network > Wireless LAN 2.4G/5G > General: WPA2-PSK



Wireless Setup

Wireless LAN : ● Enable ○ Disable

Name (SSID) : Zyxel10c798

□ Hide SSID

Channel Selection : Channel-1 2412MHz ☑ Auto Channel Selection Scan channel

Operating Channel : Channel-

Channel Width : Auto 20/40 MHz

802.11 Mode : 802.11bgn

Security

Security Mode : WPA2-PSK

□ WPA-PSK Compatible

□ PMF(Protected Management Frames)

Pre-Shared Key EmptyPSKey

Group Key Update Timer 3600 seconds

Note: No Security and WPA2-PSK can be configured when WPS enabled.

The following table describes the labels in this screen.

Table 20 Network > Wireless LAN 2.4G/5G > General: WPA2-PSK

LABEL	DESCRIPTION
Security Mode	Select **WPA2-PSK** to enable data encryption.
WPA-PSK Compatible	Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your EMG6765-Q10A even when the EMG6765-Q10A is using WPA2-PSK.
Pre-Shared Key	**WPA2-PSK** uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.

Table 20 Network > Wireless LAN 2.4G/5G > General: WPA2-PSK (continued)

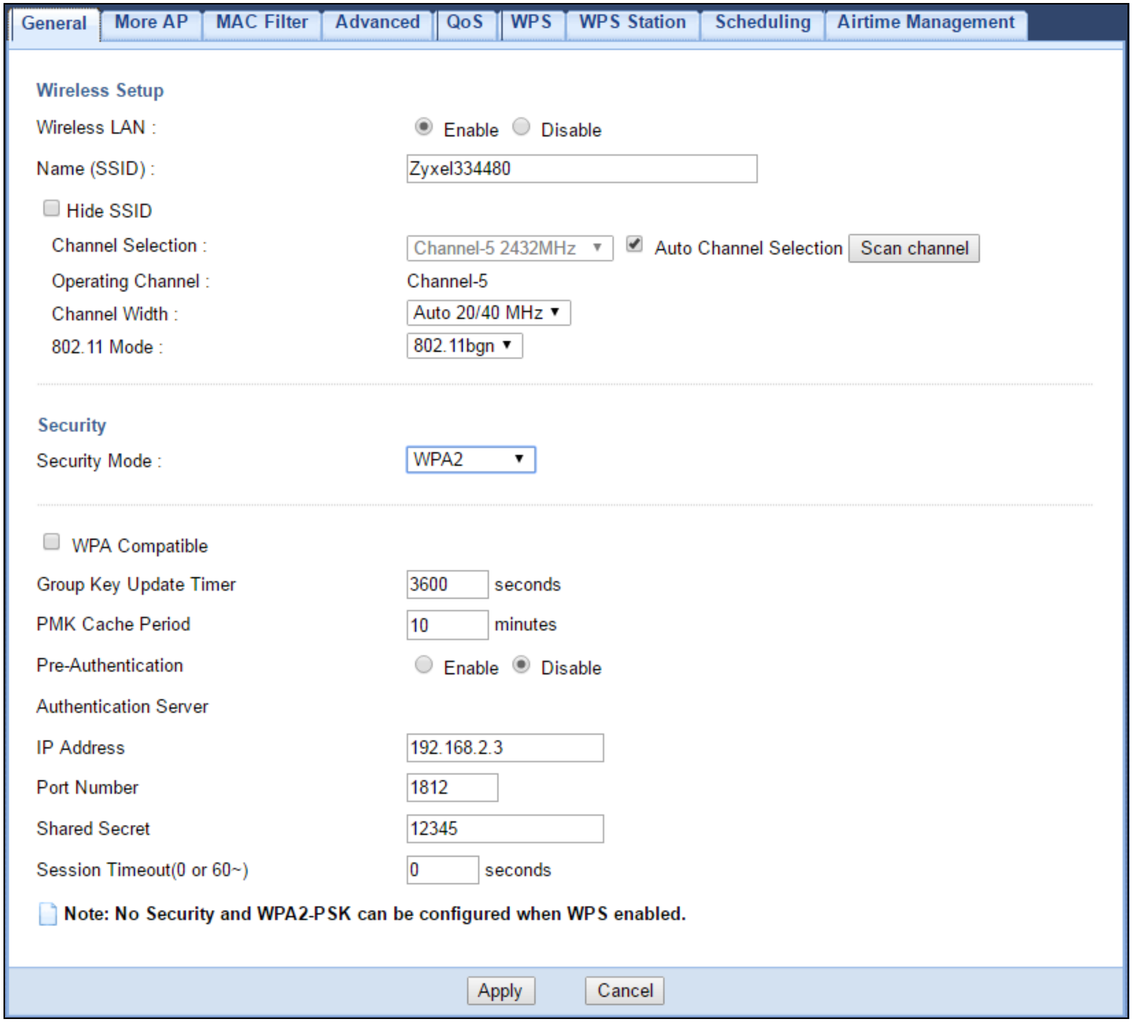
LABEL	DESCRIPTION
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The default is **3600** seconds (60 minutes).
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

9.3.3 WPA2

Select **WPA2** from the **Security Mode** list.

Note: WPA2 is not available if you enable WPS before you configure WPA2 in the **Wireless LAN 2.4G/5G > General** screen.

Figure 36 Network > Wireless LAN 2.4G/5G > General: WPA2



Wireless Setup

Wireless LAN : ● Enable ○ Disable

Name (SSID) : Zyxel334480

□ Hide SSID

Channel Selection : Channel-5 2432MHz ☑ Auto Channel Selection Scan channel

Operating Channel : Channel-5

Channel Width : Auto 20/40 MHz

802.11 Mode : 802.11bgn

Security

Security Mode : WPA2

□ WPA Compatible

Group Key Update Timer 3600 seconds

PMK Cache Period 10 minutes

Pre-Authentication ○ Enable ● Disable

Authentication Server

IP Address 192.168.2.3

Port Number 1812

Shared Secret 12345

Session Timeout(0 or 60~) 0 seconds

Note: No Security and WPA2-PSK can be configured when WPS enabled.

The following table describes the labels in this screen.

Table 21 Network > Wireless LAN 2.4G/5G > General: WPA2

LABEL	DESCRIPTION
Security Mode	Select **WPA** or **WPA2** to enable data encryption.
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the EMG6765-Q10A even when the EMG6765-Q10A is using WPA2-PSK or WPA2.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK/WPA2-PSK** key management) or RADIUS server (if using **WPA/WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA-PSK/WPA2-PSK** mode.
PMK Cache Period	This field is available only when you select **WPA2**. Specify how often wireless clients have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 999999 minutes. Note: If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Pre-Authentication	This field is available only when you select **WPA2**. Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it. Select **Enable** to turn on preauthentication in WAP2. Otherwise, select **Disable**.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 127 alphanumeric characters) as the key to be shared between the external authentication server and the EMG6765-Q10A. The key must be the same on the external authentication server and your EMG6765-Q10A. The key is not sent over the network.
Session Timeout	The EMG6765-Q10A automatically disconnects a wireless client from the wireless and wired networks after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless and wired networks again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. Enter the time in seconds from 0 to 999999.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

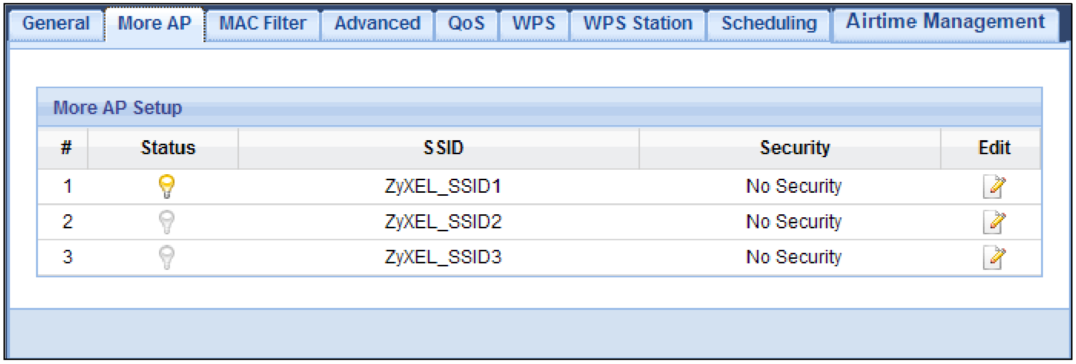
9.4 More AP Screen

This screen allows you to enable and configure multiple wireless networks and guest wireless network settings on the EMG6765-Q10A.

You can configure up to four SSIDs to enable multiple BSSs (Basic Service Sets) on the EMG6765-Q10A. This allows you to use one access point to provide several BSSs simultaneously. You can then assign varying security types to different SSIDs. Wireless clients can use different SSIDs to associate with the same access point.

Click **Network > Wireless LAN 2.4G/5G > More AP**. The following screen displays.

Figure 37 Network > Wireless LAN 2.4G/5G > More AP



More AP Setup

#	Status	SSID	Security	Edit
1	●	ZyXEL_SSID1	No Security	✎
2	○	ZyXEL_SSID2	No Security	✎
3	○	ZyXEL_SSID3	No Security	✎

The following table describes the labels in this screen.

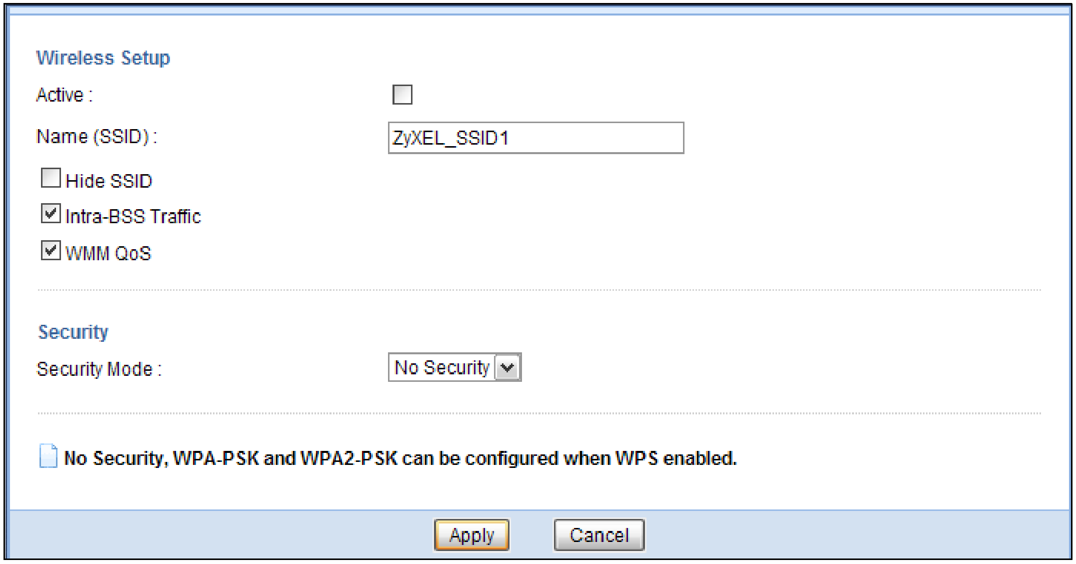
Table 22 Network > Wireless LAN 2.4G/5G > More AP

LABEL	DESCRIPTION
More AP Setup	
#	This is the index number of each SSID profile.
Status	This shows whether the SSID profile is active (a yellow bulb) or not (a gray bulb).
SSID	An SSID profile is the set of parameters relating to one of the EMG6765-Q10A's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Edit	Click the **Edit** icon to configure the SSID profile.

9.4.1 More AP Edit

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

Figure 38 Network > Wireless LAN 2.4G/5G > More AP: Edit



Wireless Setup

Active : □

Name (SSID) : ZyXEL_SSID1

□ Hide SSID

☑ Intra-BSS Traffic

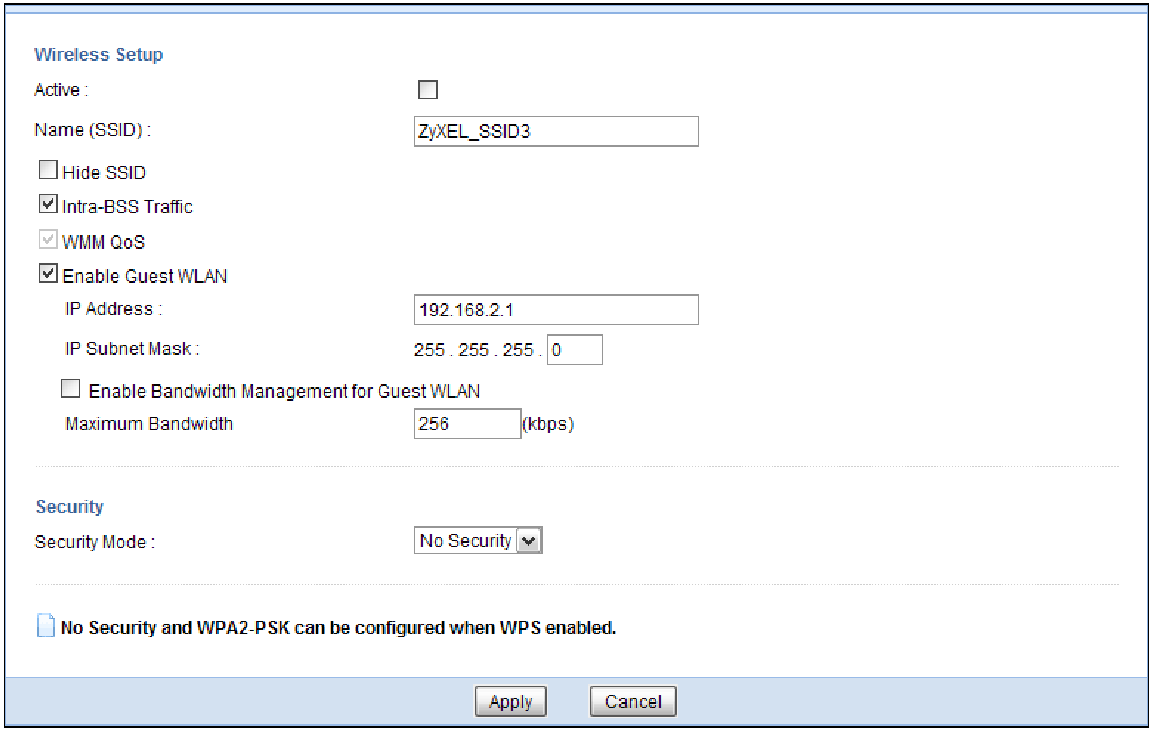
☑ WMM QoS

Security

Security Mode : No Security

No Security, WPA-PSK and WPA2-PSK can be configured when WPS enabled.

Figure 39 Network > Wireless LAN 2.4G/5G > More AP: Edit (the last SSID)



Wireless Setup

Active : □

Name (SSID) : ZyXEL_SSID3

□ Hide SSID

☑ Intra-BSS Traffic

☑ WMM QoS

☑ Enable Guest WLAN

IP Address : 192.168.2.1

IP Subnet Mask : 255 . 255 . 255 . 0

□ Enable Bandwidth Management for Guest WLAN

Maximum Bandwidth 256 (kbps)

Security

Security Mode : No Security

No Security and WPA2-PSK can be configured when WPS enabled.

The following table describes the labels in this screen.

Table 23 Network > Wireless LAN 2.4G/5G > More AP: Edit

LABEL	DESCRIPTION
Wireless Setup	
Active	Select this to activate the SSID profile.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.

Table 23 Network > Wireless LAN 2.4G/5G > More AP: Edit (continued)

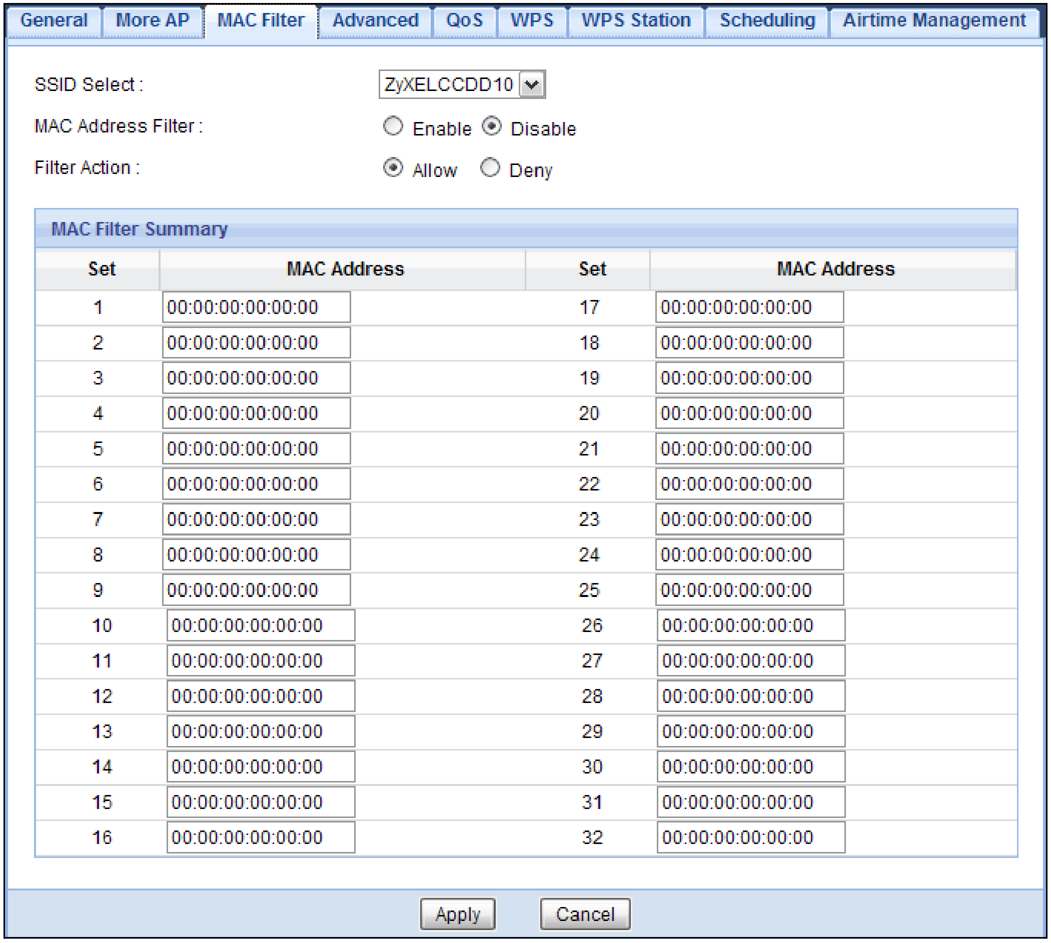
LABEL	DESCRIPTION
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client 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 clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other.
WMM QoS	Check this to have the EMG6765-Q10A automatically give a service 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.
Enable Guest WLAN	Select the check box to activate guest wireless LAN. This is available only for the last SSID on the EMG6765-Q10A.
IP Address	Type an IP address for the devices on the Guest WLAN using this as the gateway IP address.
IP Subnet Mask	Type the subnet mask for the guest wireless LAN.
Enable Bandwidth Management for Guest WLAN	Select this to turn on bandwidth management for the Guest WLAN network.
Maximum Bandwidth	Enter a number to specify maximum bandwidth the Guest WLAN network can use.
Security	
Security Mode	Select **WPA2-PSK** or **WPA2** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See Section 9.3 on page 78 for detailed information on different security modes. Or you can select **No Security** to allow any client to associate this network without authentication. Note: If the WPS function is enabled (default), only **No Security** and **WPA2-PSK** are available in this field.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

9.5 MAC Filter Screen

The MAC filter screen allows you to configure the EMG6765-Q10A to give exclusive access to devices (**Allow**) or exclude devices from accessing the EMG6765-Q10A (**Deny**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your EMG6765-Q10A's MAC filter settings, click **Network** > **Wireless LAN 2.4G/5G** > **MAC Filter**. The screen appears as shown.

Figure 40 Network > Wireless LAN 2.4G/5G > MAC Filter



SSID Select : ZyXELCCDD10

MAC Address Filter : ○ Enable ● Disable

Filter Action : ● Allow ○ Deny

MAC Filter Summary

Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
6	00:00:00:00:00:00	22	00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

The following table describes the labels in this menu.

Table 24 Network > Wireless LAN 2.4G/5G > MAC Filter

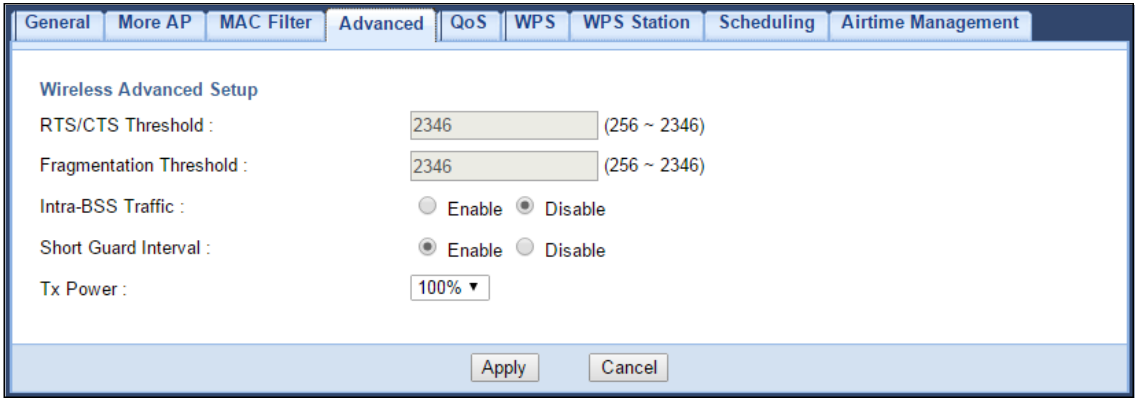
LABEL	DESCRIPTION
SSID Select	Select the SSID for which you want to configure MAC filtering.
MAC Address Filter	Select to turn on (**Enable**) or off (**Disable**) MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Filter Summary** table. Select **Allow** to permit access to the EMG6765-Q10A, MAC addresses not listed will be denied access to the EMG6765-Q10A. Select **Deny** to block access to the EMG6765-Q10A, MAC addresses not listed will be allowed to access the EMG6765-Q10A.
MAC Filter Summary	
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC address of the wireless station that are allowed or denied access to the EMG6765-Q10A.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

9.6 Wireless LAN Advanced Screen

Use this screen to allow wireless advanced features, such as the output power, RTS/CTS Threshold settings.

Click **Network** > **Wireless LAN 2.4G/5G** > **Advanced**. The screen appears as shown.

Figure 41 Network > Wireless LAN 2.4G/5G > Advanced



Wireless Advanced Setup

RTS/CTS Threshold : 2346 (256 ~ 2346)

Fragmentation Threshold : 2346 (256 ~ 2346)

Intra-BSS Traffic : ○ Enable ● Disable

Short Guard Interval : ● Enable ○ Disable

Tx Power : 100%

The following table describes the labels in this screen.

Table 25 Network > Wireless LAN 2.4G/5G > Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. This field is not configurable and the EMG6765-Q10A automatically changes to use the maximum value if you select **802.11a/an**, **802.11a/an/ac**, **802.11n**, **802.11gn** or **802.11bgn** in the **Wireless LAN 2.4G/5G > General** screen.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. This field is not configurable and the EMG6765-Q10A automatically changes to use the maximum value if you select **802.11a/an**, **802.11a/an/ac**, **802.11n**, **802.11gn** or **802.11bgn** in the **Wireless LAN 2.4G/5G > General** screen.
Intra-BSS Traffic Blocking	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 clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other. Select **Enable** to prevent crossover traffic from within the same SSID on the EMG6765-Q10A.
Short Guard Interval	Select **Enable** to use Short GI (Guard Interval). The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the interval increases data transfer rates but also increases interference. Increasing the interval reduces data transfer rates but also reduces interference.
Tx Power	Set the output power of the EMG6765-Q10A in this field. If there is a high density of APs in an area, decrease the output power of the EMG6765-Q10A to reduce interference with other APs. Select one of the following **100%**, **90%**, **75%**, **50%**, **25%** or **10%**.

Table 25 Network > Wireless LAN 2.4G/5G > Advanced (continued)

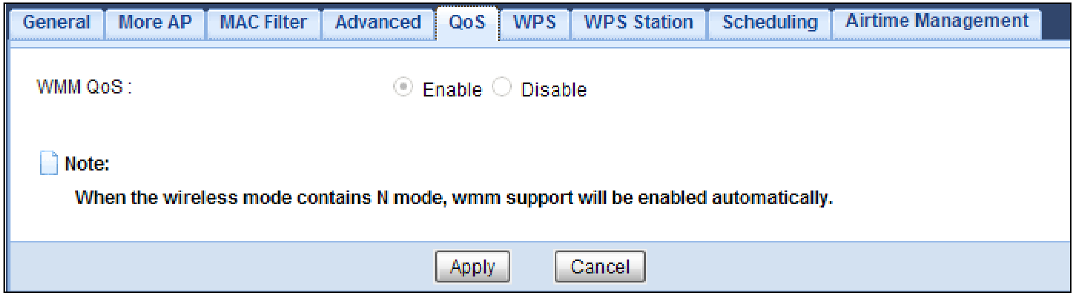
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

9.7 Quality of Service (QoS) Screen

The QoS screen allows you to automatically give a service (such as VoIP and video) a priority level.

Click **Network** > **Wireless LAN 2.4G/5G** > **QoS**. The following screen appears.

Figure 42 Network > Wireless LAN 2.4G/5G > QoS



WMM QoS : ● Enable ○ Disable

Note:

When the wireless mode contains N mode, wmm support will be enabled automatically.

The following table describes the labels in this screen.

Table 26 Network > Wireless LAN 2.4G/5G > QoS

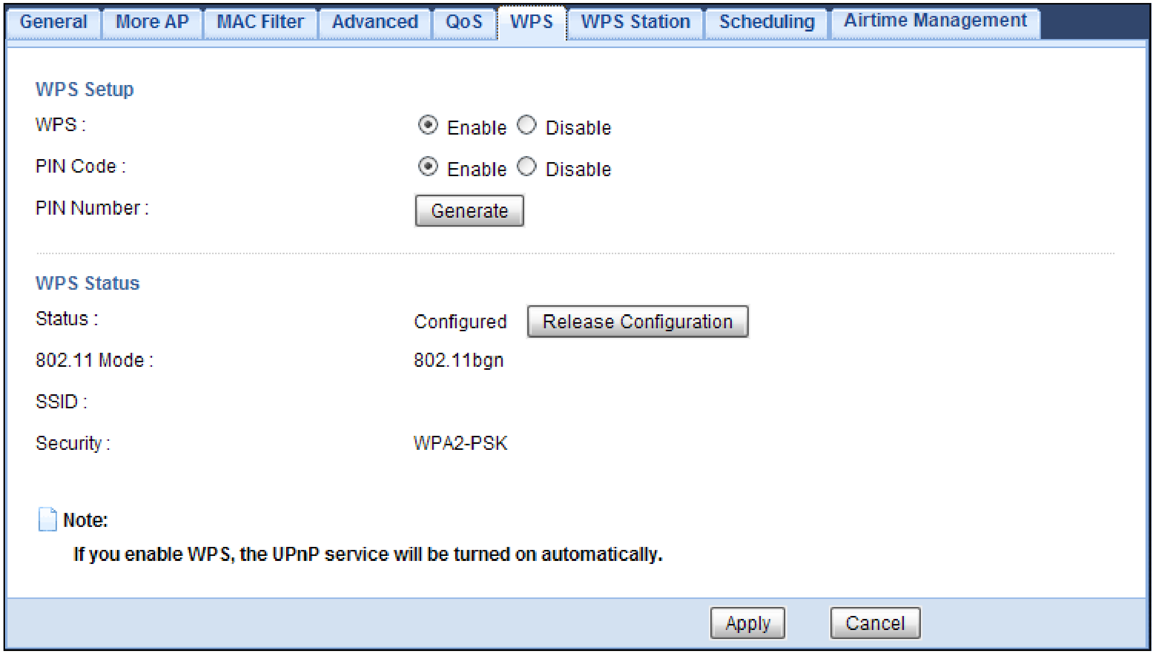
LABEL	DESCRIPTION
WMM QoS	Select **Enable** to have the EMG6765-Q10A automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. Note: This field is not configurable and the EMG6765-Q10A automatically enables WMM QoS if you select **802.11n**, **802.11an**, **802.11gn** or **802.11bgn** in the **Wireless LAN 24G/5G > General** screen.
Apply	Click **Apply** to save your changes to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

9.8 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Network** > **Wireless LAN 2.4G/5G** > **WPS**.

Note: With WPS, wireless clients can only connect to the wireless network using the first SSID on the EMG6765-Q10A.

Figure 43 Network > Wireless LAN 2.4G/5G > WPS



WPS Setup

WPS : ● Enable ○ Disable

PIN Code : ● Enable ○ Disable

PIN Number : Generate

WPS Status

Status : Configured Release Configuration

802.11 Mode : 802.11bgn

SSID :

Security : WPA2-PSK

Note:

If you enable WPS, the UPnP service will be turned on automatically.

The following table describes the labels in this screen.

Table 27 Network > Wireless LAN 2.4G/5G > WPS

LABEL	DESCRIPTION
WPS Setup	
WPS	Select **Enable** to turn on the WPS feature. Otherwise, select **Disable**.
PIN Code	Select **Enable** and click **Apply** to allow the PIN Configuration method. If you select **Disable**, you cannot create a new PIN number.
PIN Number	This is the WPS PIN (Personal Identification Number) of the EMG6765-Q10A. Enter this PIN in the configuration utility of the device you want to connect to the EMG6765-Q10A using WPS. The PIN is not necessary when you use WPS push-button method. Click **Generate** to generate a new PIN number.
WPS Status	
Status	This displays **Configured** when the EMG6765-Q10A has connected to a wireless network using WPS or when **WPS Enable** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the EMG6765-Q10A or you click **Release Configuration** to remove the configured wireless and wireless security settings.
Release Configuration	This button is only available when the WPS status displays **Configured**. Click this button to remove all configured wireless and wireless security settings for WPS connections on the EMG6765-Q10A.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the EMG6765-Q10A.
SSID	This is the name of the wireless network (the EMG6765-Q10A's first SSID).
Security	This is the type of wireless security employed by the network.

Table 27 Network > Wireless LAN 2.4G/5G > WPS (continued)

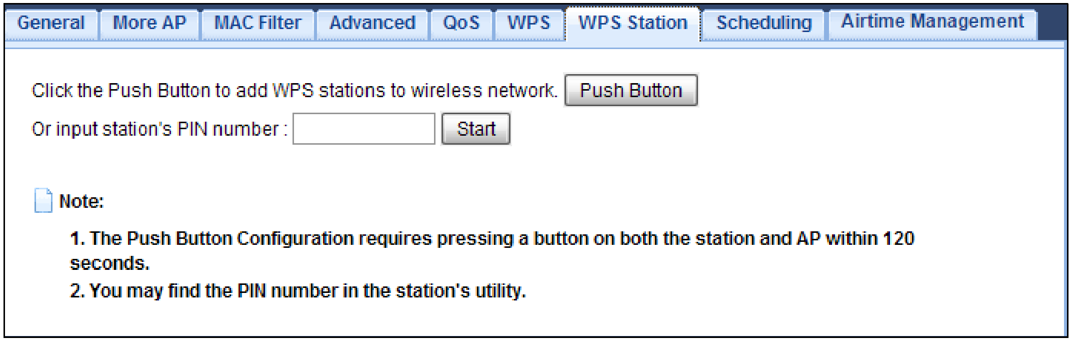
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

9.9 WPS Station Screen

Use this screen when you want to add a wireless station using WPS. To open this screen, click **Network** > **Wireless LAN 2.4G/5G** > **WPS Station**.

Note: After you click **Push Button** on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.

Figure 44 Network > Wireless LAN 2.4G/5G > WPS Station



Click the Push Button to add WPS stations to wireless network.

Or input station's PIN number :

Note:

1. The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2. You may find the PIN number in the station's utility.

The following table describes the labels in this screen.

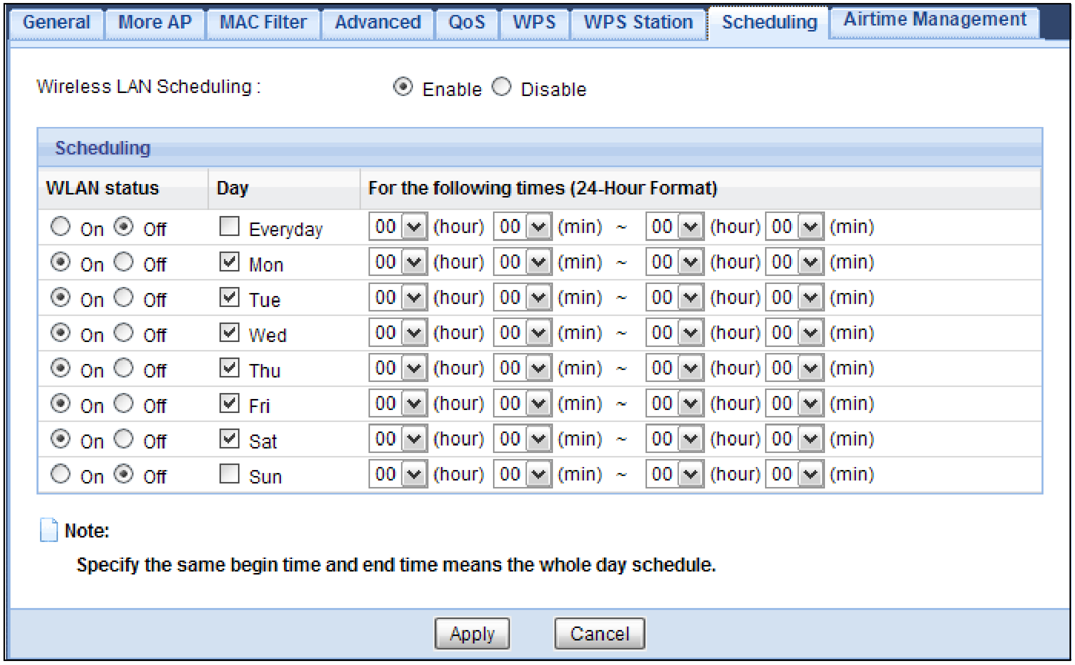
Table 28 Network > Wireless LAN 2.4G/5G > WPS Station

LABEL	DESCRIPTION
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless station's wireless settings. Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Or input station's PIN number	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings. Type the same PIN number generated in the wireless station's utility. Then click **Start** to associate to each other and perform the wireless security information synchronization.

9.10 Scheduling Screen

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn on or off on certain days and at certain times. To open this screen, click **Network** > **Wireless LAN 2.4G/5G** > **Scheduling** tab.

Figure 45 Network > Wireless LAN 2.4G/5G > Scheduling



Wireless LAN Scheduling : ● Enable ○ Disable

Scheduling

WLAN status	Day	For the following times (24-Hour Format)
○ On ● Off	□ Everyday	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
● On ○ Off	☑ Mon	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
● On ○ Off	☑ Tue	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
● On ○ Off	☑ Wed	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
● On ○ Off	☑ Thu	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
● On ○ Off	☑ Fri	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
● On ○ Off	☑ Sat	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Sun	00 (hour) 00 (min) ~ 00 (hour) 00 (min)

Note:

Specify the same begin time and end time means the whole day schedule.

The following table describes the labels in this screen.

Table 29 Network > Wireless LAN 2.4G/5G > Scheduling

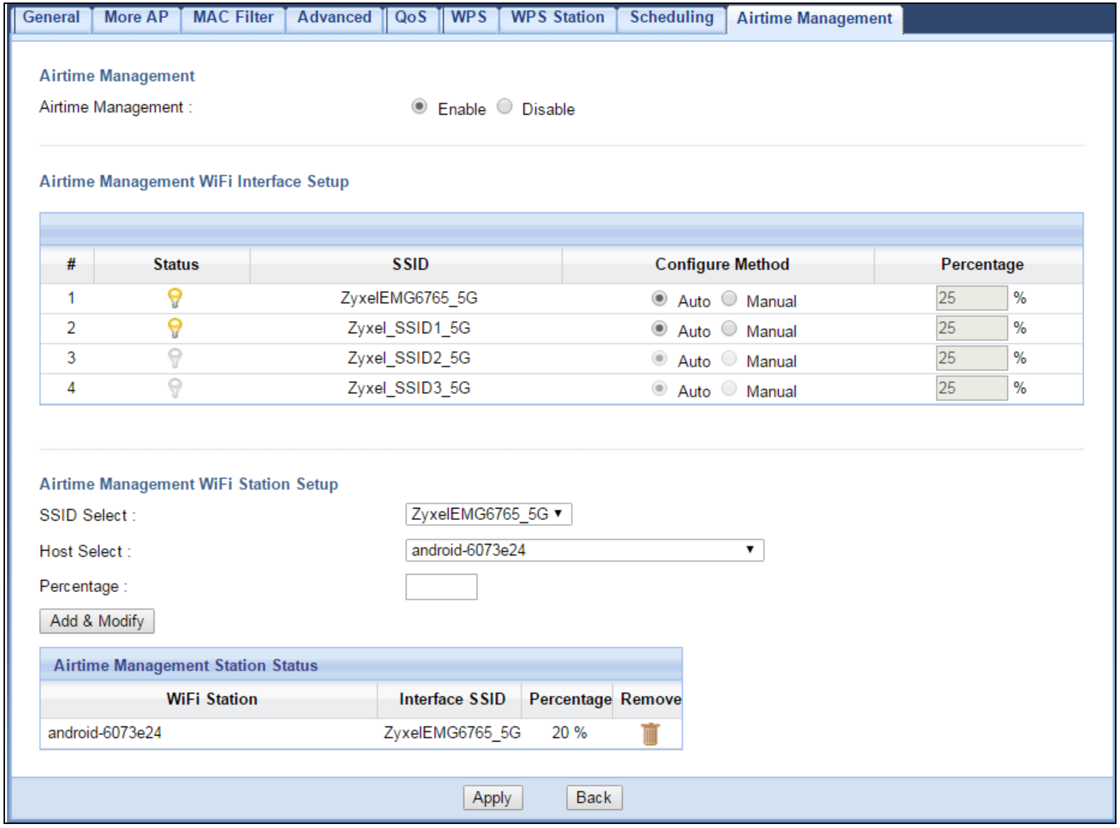
LABEL	DESCRIPTION
Wireless LAN Scheduling	
Wireless LAN Scheduling	Select **Enable** to activate the wireless LAN scheduling feature. Select **Disable** to turn it off.
Scheduling	
WLAN Status	Select **On** or **Off** to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the **Day** and **For the following times** fields.
Day	Select **Everyday** or the specific days to turn the Wireless LAN on or off. If you select **Everyday** you can not select any specific days. This field works in conjunction with the **For the following times** field.
For the following times (24-Hour Format)	Select a begin time using the first set of **hour** and minute (**min**) drop down boxes and select an end time using the second set of **hour** and minute (**min**) drop down boxes. If you have chosen **On** earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

9.11 Airtime Management Screen

Airtime is a period during which a Wi-Fi station transmits or receives data. Use this screen to manage the time for Wi-Fi transmission traffic and improve the EMG6765-Q10A's network performance. Airtime management contributes to a consistent transmission by preventing clients or SSIDs from hogging the Wi-Fi network, and affecting others throughput.

Use airtime management to allocate a percentage of available airtime to active SSID profiles in the EMG6765-Q10A. You can also allocate airtime to hosts connected to the network. To open this screen, click **Network > Wireless LAN 2.4G/5G > Airtime Management**.

Figure 46 Network > Wireless LAN 2.4G/5G > Airtime Management



Airtime Management

Airtime Management : ● Enable ○ Disable

Airtime Management WiFi Interface Setup

#	Status	SSID	Configure Method	Percentage
1	●	ZyxelEMG6765_5G	● Auto ○ Manual	25 %
2	●	Zyxel_SSID1_5G	● Auto ○ Manual	25 %
3	○	Zyxel_SSID2_5G	● Auto ○ Manual	25 %
4	○	Zyxel_SSID3_5G	● Auto ○ Manual	25 %

Airtime Management WiFi Station Setup

SSID Select : ZyxelEMG6765_5G ▾

Host Select : android-6073e24 ▾

Percentage :

Airtime Management Station Status

WiFi Station	Interface SSID	Percentage	Remove
android-6073e24	ZyxelEMG6765_5G	20 %	🗑

The following table describes the labels in this screen.

Table 30 Network > Wireless LAN 2.4G/5G > Airtime Management

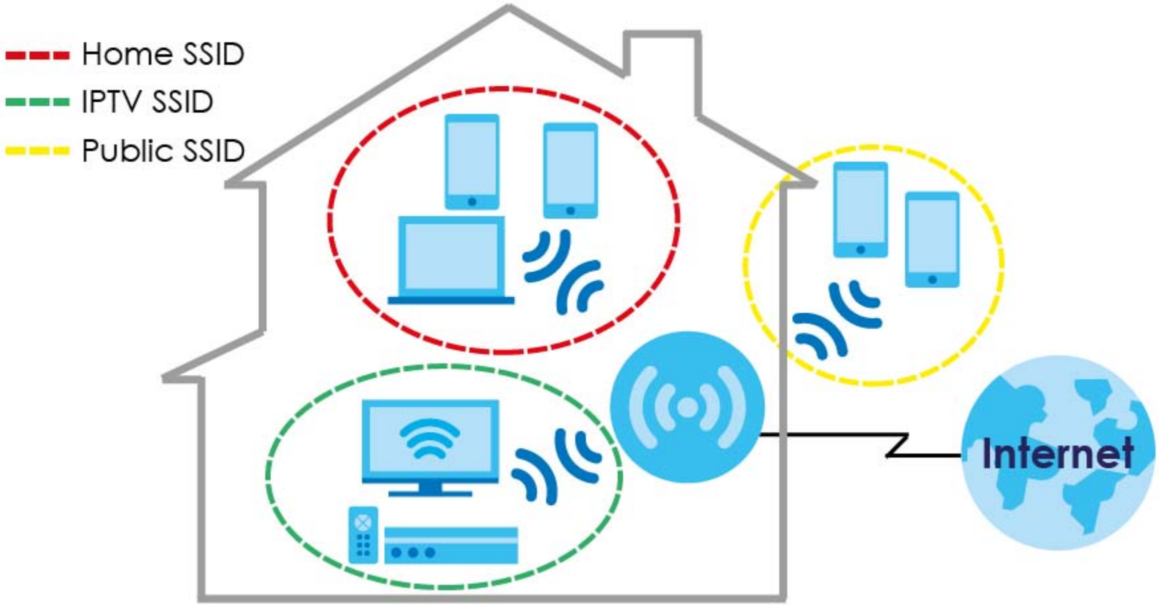
LABEL	DESCRIPTION
Airtime Management	Select **Enable** to activate the airtime management feature. Click **Disable** to turn it off.
Airtime Management WiFi Interface Setup	Use this to allocate a specific amount of time for an SSID's transmissions.
#	This is the index number of each SSID profile.
Status	This shows whether the SSID profile is active (a yellow bulb) or not (a gray bulb).
SSID	This field displays the name of the Wi-Fi network used in this SSID profile.
Configure Method	Select **Manual** to configure the percentage of airtime this SSID profile has. Otherwise select **Auto** for the EMG6765-Q10A to assign it automatically. Note: To allocate airtime, the SSID profile's status should be active in the **More AP** screen.
Percentage	Enter the percentage of time for the transmissions on this SSID profile.
Airtime Management WiFi Station Setup	Use this to allocate a specific amount of time for transmissions of a Wi-Fi station connected to the EMG6765-Q10A.
SSID Select	Select the SSID the Wi-Fi station is connected to.
Host Select	Select a Wi-Fi station to assign airtime.

Table 30 Network > Wireless LAN 2.4G/5G > Airtime Management

LABEL	DESCRIPTION
Percentage	Enter the percentage of time for the transmissions on this Wi-Fi station. Note: The airtime per Wi-Fi Station is proportional to the airtime of the SSID this station is connected to.
Add & Modify	Click this to add or modify a Wi-Fi station airtime rule to the EMG6765-Q10A.
Airtime Management Station Status	
WiFi Station	This displays the name and MAC address of the Wi-Fi station.
Interface SSID	This displays the SSID the Wi-Fi station is connected to.
Percentage	This displays the percentage of airtime this Wi-Fi station has been assigned.
Remove	Click this to remove the airtime rule.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Back	Click **Back** to begin configuring this screen afresh.

9.11.1 Airtime Management Scenarios

The figure below is used to explain some possible scenarios on how airtime management works in the EMG6765-Q10A.



- Scenario 1. All active SSIDs can use all of the EMG6765-Q10A's airtime. Make sure the airtime total is 100%. If you don't allocate all airtime to active SSIDs, the remaining airtime will be lost.

Table 31 Scenario 1

SSID	AIRTIME (%)	CONFIGURE METHOD
Home SSID	40%	Manual
IPTV SSID	50%	Manual
Public SSID	10%	Manual

- Scenario 2. If **Home SSID** and **IPTV SSID** take 100% of the airtime in **Manual**, no Airtime (0%) is allocated to **Public SSID**, whether this SSID is in **Auto** or **Manual**. In this cases **Manual** will have priority over **Auto**.

Table 32 Scenario 2

SSID	AIRTIME (%)	CONFIGURE METHOD
Home SSID	40%	Manual
IPTV SSID	60%	Manual
Public SSID	0%	Auto

- Scenario 3. If all active SSIDs are in **Auto**, the EMG6765-Q10A will assign equal percentages of airtime to all active SSIDs.

Table 33 Scenario 3

SSID	AIRTIME (%)	CONFIGURE METHOD
Home SSID	33.3%	Auto
IPTV SSID	33.3%	Auto
Public SSID	33.3%	Auto

- Scenario 4. Wi-Fi Stations airtime is proportional to the total airtime of the SSID they belong to. In this scenario Wi-Fi Station **A** will take up 50% of the 40% assigned to **Home SSID**, which would be 40%*50%= **20%**. Whereas Wi-Fi Station **B** will use 50% of the 10% assigned to **Public SSID**, which would be 10%*50%= **5%**.

Table 34 Scenario 4

SSID	SSID AIRTIME (%)	WI-FI STATION	WI-FI STATION AIRTIME (%)	CONFIGURE METHOD
Home SSID	40%	A	50%	Manual
IPTV SSID	50%			Manual
Public SSID	10%	B	50%	Manual

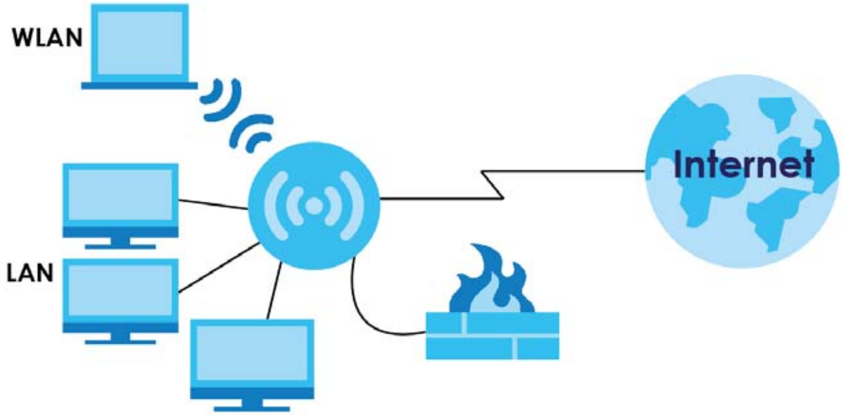
CHAPTER 10 LAN

10.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building.

Figure 47 LAN Example



The LAN screens can help you configure a manage IP address, and partition your physical network into logical networks.

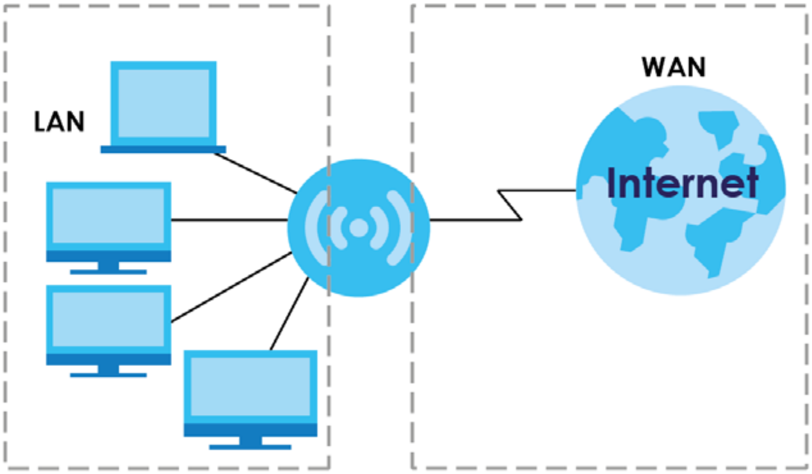
10.2 What You Can Do

- Use the **IP** screen to change the IP address for your EMG6765-Q10A (Section 10.4 on page 96).
- Use the **IP Alias** screen to have the EMG6765-Q10A apply IP alias to create LAN subnets (Section 10.5 on page 96).
- Use the **IPv6 LAN** screen to configure the IPv6 address for your EMG6765-Q10A on the LAN (Section 10.6 on page 97).
- Use the **IGMP Snooping** screen to enable IGMP Snooping and configure IGMP modes. (Section 10.7 on page 98).

10.3 What You Need To Know

The actual physical connection determines whether the EMG6765-Q10A 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 48 LAN and WAN IP Addresses



The LAN parameters of the EMG6765-Q10A are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded Web Configurator help regarding what fields need to be configured.

10.3.1 IP Pool Setup

The EMG6765-Q10A is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the EMG6765-Q10A itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

10.3.2 LAN TCP/IP

The EMG6765-Q10A has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

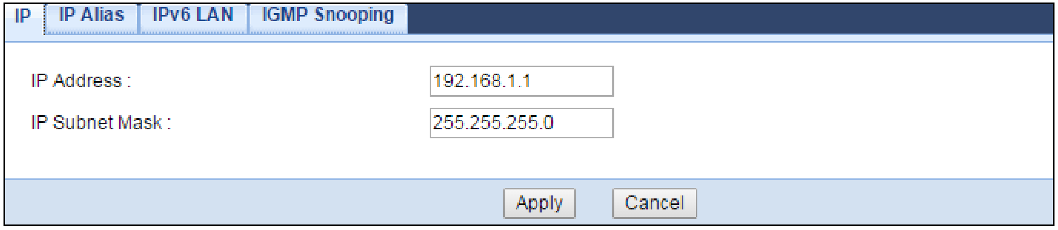
10.3.3 IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The EMG6765-Q10A supports three logical LAN interfaces via its single physical Ethernet interface with the EMG6765-Q10A itself as the gateway for each LAN network.

10.4 LAN IP Screen

Use this screen to change the IP address for your EMG6765-Q10A. Click **Network > LAN > IP**.

Figure 49 Network > LAN > IP



IP Address : 192.168.1.1

IP Subnet Mask : 255.255.255.0

The following table describes the labels in this screen.

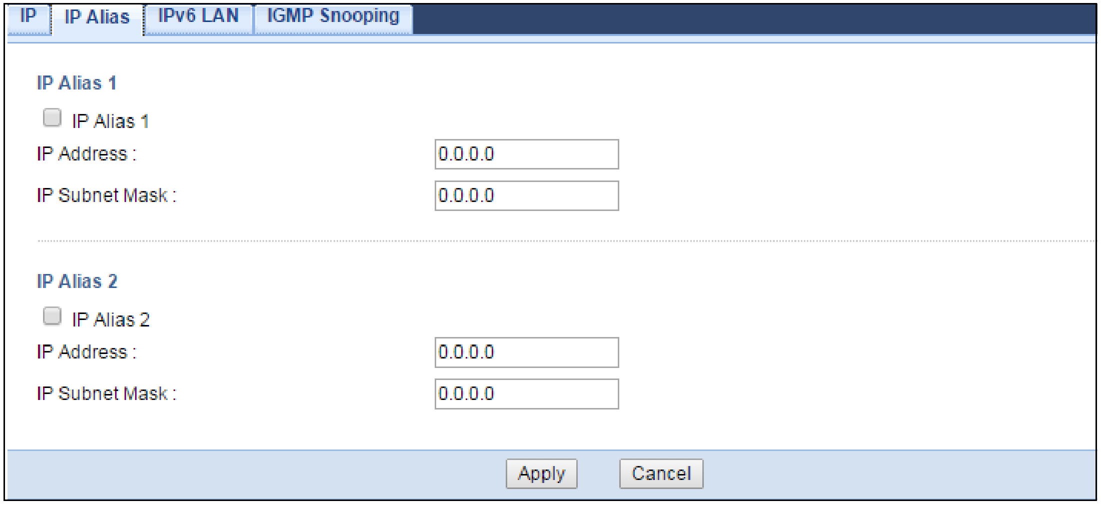
Table 35 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your EMG6765-Q10A in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your EMG6765-Q10A will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the EMG6765-Q10A.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.5 IP Alias Screen

Use this screen to have the EMG6765-Q10A apply IP alias to create LAN subnets. Click **LAN** > **IP Alias**.

Figure 50 Network > LAN > IP Alias



IP Alias 1

□ IP Alias 1

IP Address : 0.0.0.0

IP Subnet Mask : 0.0.0.0

IP Alias 2

□ IP Alias 2

IP Address : 0.0.0.0

IP Subnet Mask : 0.0.0.0

The following table describes the labels in this screen.

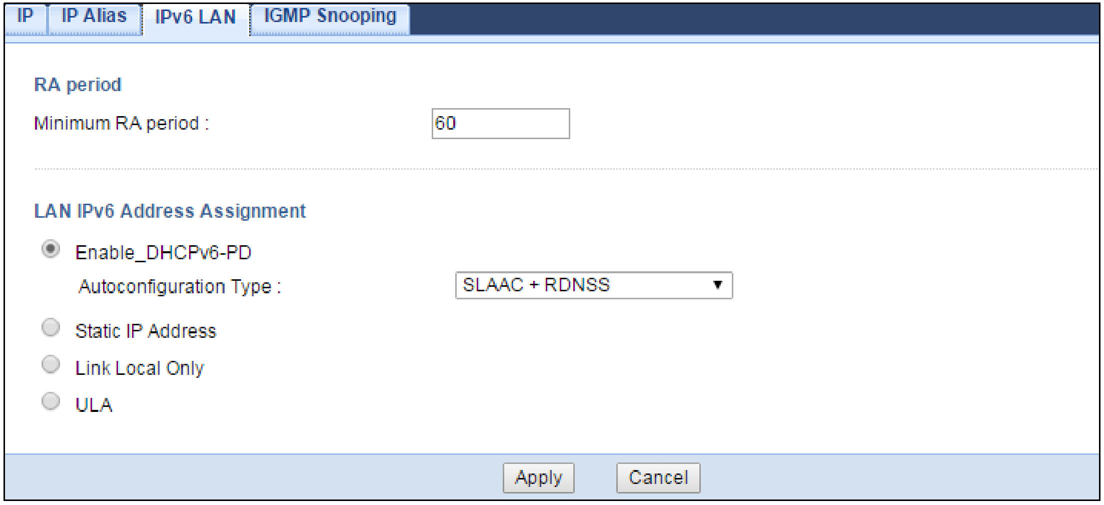
Table 36 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias 1, 2	Check this to enable IP alias to configure another LAN network for the EMG6765-Q10A.
IP Address	Type the IP alias address of your EMG6765-Q10A in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your EMG6765-Q10A will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the EMG6765-Q10A.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.6 IPv6 LAN Screen

Use this screen to configure the IPv6 address for your EMG6765-Q10A on the LAN. Click **Network > LAN > IPv6 LAN**.

Figure 51 Network > LAN > IPv6 LAN



RA period

Minimum RA period : 60

LAN IPv6 Address Assignment

● Enable_DHCPv6-PD

Autoconfiguration Type : SLAAC + RDNSS

○ Static IP Address

○ Link Local Only

○ ULA

The following table describes the labels on this screen.

Table 37 Network > LAN > IPv6 LAN

LABEL	DESCRIPTION
RA period	
Minimum RA period	Enter the minimum time in seconds between router advertisement messages.
LAN IPv6 Address Assignment	
Enable DHCPv6-PD Select this option to use DHCPv6 prefix delegation. The EMG6765-Q10A will obtain an IPv6 prefix from the ISP or a connected uplink router for the LAN.	

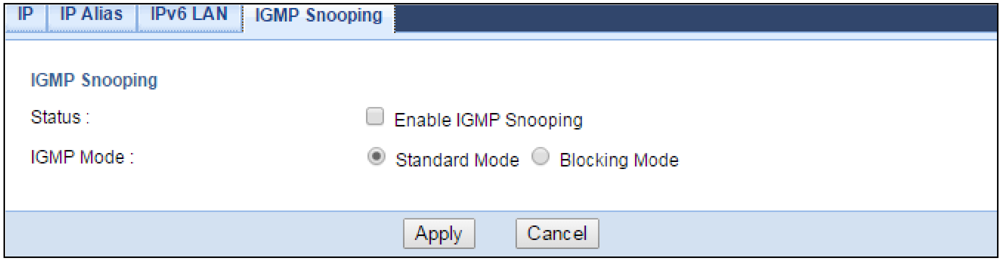
Table 37 Network > LAN > IPv6 LAN (continued)

LABEL	DESCRIPTION
Autoconfiguration Type	Select **SLAAC + RDNSS** to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network. Select **SLAAC + Stateless DHCPv6** to enable IPv6 stateless auto-configuration on this interface. The interface will get an IPv6 address from an IPv6 router and the DHCP server. The IP address information gets through DHCPv6. Select **Stateful DHCPv6** to allow a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients.
Static IP Address Select this option to manually enter an IPv6 address if you want to use a static IP address.	
LAN IPv6 Address	Enter the LAN IPv6 address you want to assign to your EMG6765-Q10A in hexadecimal notation.
LAN IPv6 Prefix Length (48~64)	Enter the 48 to 64 address prefix length to specify in an IPv6 address compose the network address.
Prefix Preferred Lifetime	Enter the preferred lifetime for the prefix.
Prefix Valid Lifetime	Enter the valid lifetime for the prefix.
Link Local Only Select this option to only use the link local address on the EMG6765-Q10A interfaces in the LAN.	
ULA Select this option to identify a unique local address of the EMG6765-Q10A in the LAN.	
Apply	Click **Apply** to save your changes with the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.7 IGMP Snooping Screen

Use this screen to enable IGMP Snooping and configure IGMP mode. Click **Network > LAN > IGMP Snooping**.

Figure 52 Network > LAN > IGMP Snooping



IGMP Snooping

Status : □ Enable IGMP Snooping

IGMP Mode : ● Standard Mode ○ Blocking Mode

The following table describes the labels on this screen.

Table 38 Network > LAN > IGMP Snooping

LABEL	DESCRIPTION
IGMP Snooping	

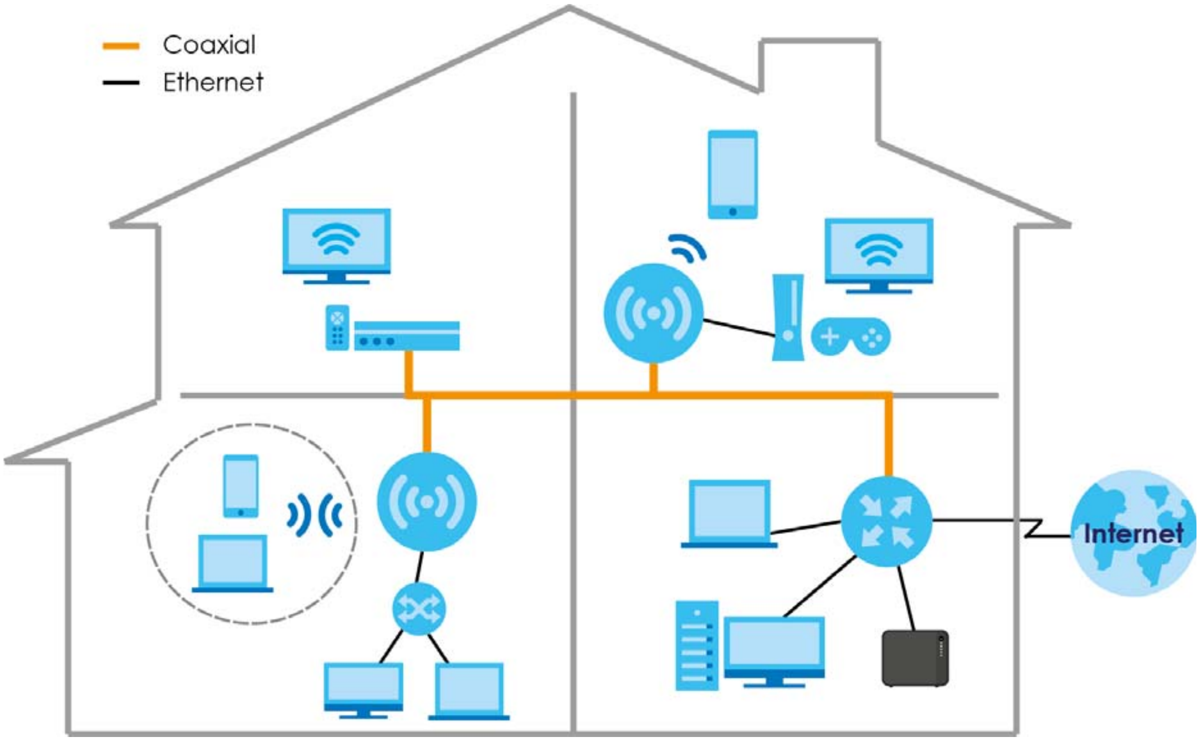
Table 38   Network > LAN > IGMP Snooping (continued)

LABEL	DESCRIPTION
Status	Select this option to activate IGMP snooping. This allows the EMG6765-Q10A to passively learn multicast group.
IGMP Mode	Select **Standard Mode** to have the EMG6765-Q10A 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 have the EMG6765-Q10A block all unknown multicast packets from the WAN.
Apply	Click **Apply** to save your changes with the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 11
MoCA

11.1 Overview

MoCA (Multimedia over Coax Alliance) is an industry standard organization, which created a standard for transferring data and multimedia content over the existing coaxial wires in your home. Data communication and audio/video streaming are allowed at the same time. The EMG6765-Q10A (A) automatically sets up a MoCA network when multiple MoCA devices (nodes) are powered on and connected with a coaxial cable.



The EMG6765-Q10A supports MoCA 2.0 and is backward compatible with MoCA 1.1. The MoCA 1.1 technology provides 175 Mbps net throughputs (270 Mbps PHY rate) and operates in the 500 to 1500 MHz frequency range. MoCA 2.0 in turbo mode offers actual data rates of up to 1 Gbps MAC throughputs and operates in the 500 to 1650 MHz operating frequency range. MoCA 2.0 also supports improved packet error rate (PER) and two new power saving modes: Standby (reduced power) and Sleep (minimum power).

The EMG6765-Q10A should be connected to the WAN via Ethernet, then the coaxial network in your home will only work as a LAN.

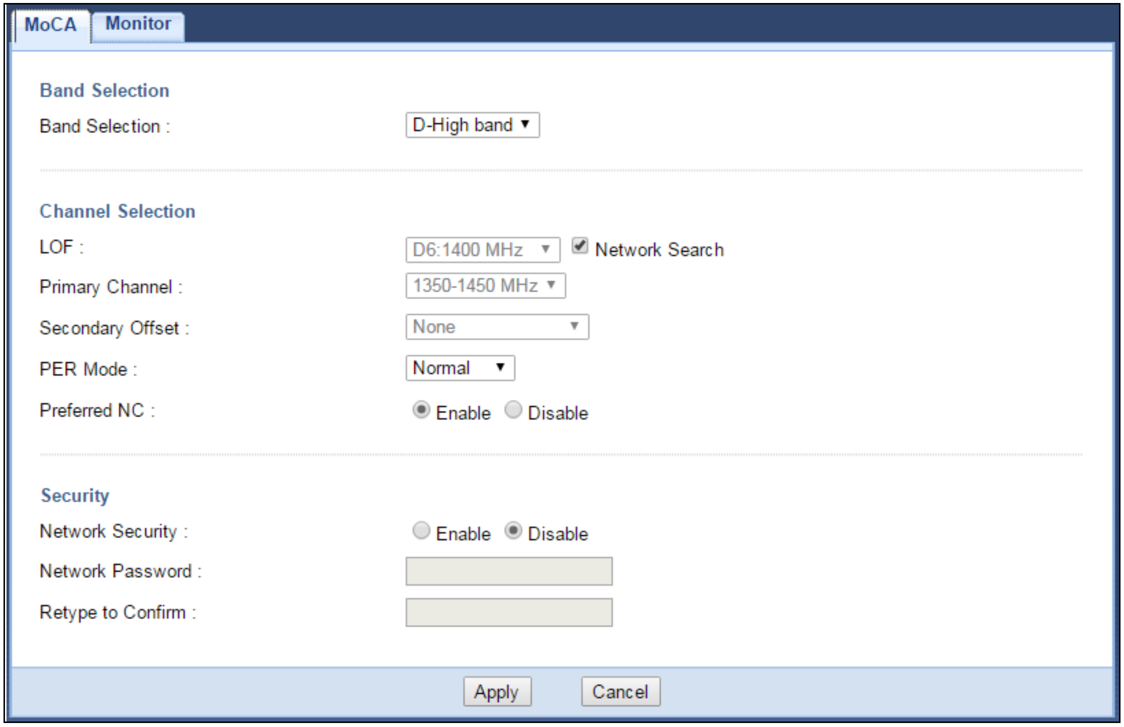
11.2 What You Can Do

- Use the **MoCA** screen (Section 11.3 on page 101) to set the MoCA Privacy, and enable multimedia and home networking over coaxial cabling.
- Use the **MoCA > Monitor** screen (Section 11.4 on page 103) to view the MoCA network status and information about the connected MoCA devices (nodes).

11.3 MoCA Screen

Use this screen to change the MoCA settings for your EMG6765-Q10A. Click **Network > MoCA**.

Figure 53 Network > MoCA



Band Selection

Band Selection : D-High band ▾

Channel Selection

LOF : D6:1400 MHz ▾ ☑ Network Search

Primary Channel : 1350-1450 MHz ▾

Secondary Offset : None ▾

PER Mode : Normal ▾

Preferred NC : ● Enable ○ Disable

Security

Network Security : ○ Enable ● Disable

Network Password :

Retype to Confirm :

The following table describes the labels in this screen.

Table 39 Network > MoCA

LABEL	DESCRIPTION
Band Selection	In MoCA frequency band plans, there are bands A, B, C1, C2, C3, C4, D, E, F, G, and H. The extended band D in MoCA 2.0 is between 1125 MHz and 1675 MHz. Two sub-bands (D-Low and D-High) are defined within the extended band D. • Sub-band D-Low (DL): 1125 to 1225 MHz edge to edge (100 MHz wide) • Sub-band D-High (DH): 1350 to 1675 MHz edge to edge (325 MHz wide) At the time of setting, the EMG6765-Q10A supports the sub-band D-High only.
Channel Selection	

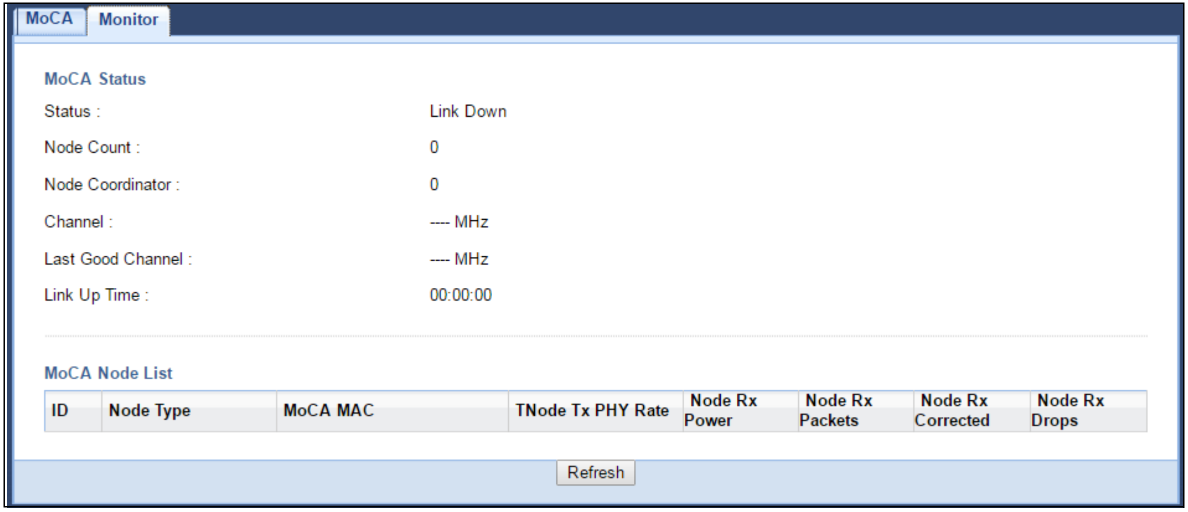
Table 39 Network > MoCA

LABEL	DESCRIPTION
LOF	Last Operational Frequency (LOF) is the last RF channel center frequency which a MoCA device (node) will automatically turn to when it is last in the linkup state, The center frequency of a channel is a central frequency in the middle of the upper cutoff and lower cutoff frequencies. If you clear the **Network Search** check box, manually select an operating frequency from the drop-down list.
Network Search	Select the check box to enable auto scan for the operating frequency.
Primary Channel	Select the first operating frequency range if you clear the **Network Search** check box. The field options vary depending on the center frequency you select in the **LOF** field.
Secondary Offset	Select the second operating frequency range if you clear the **Network Search** check box. Select **None** if you do not want to specify a second channel. Select **Above** to have the EMG6765-Q10A use a frequency higher than the upper edge of the selected primary channel. Select **Below** to have the EMG6765-Q10A use a frequency less than the lower edge of the selected primary channel.
PER Mode	The Packet Error Rate (PER) indicates the ratio between the total number of incorrectly received data packets and the total number of transmitted data packets. The total number of transmitted packets is at least 100,000,000 when the PER mode is NPER (Normal PER) and at least 10,000,000,000 when the PER mode is VLPER (Very Low PER). In very low PER mode, the physical data rate will be decreased in order to achieve a lower packet error rate. Select **Normal** to set the PER mode to NPER. Otherwise, select **Very Low** to set the PER mode to VLPER.
Preferred NC	The Network Coordinator (NC) is a node that performs the following functions in a MoCA network: beacon generation, MAP (Medium Allocation Plan) generation, admission of new MoCA nodes to the network, privacy key generation and distribution, and LMO (Link Maintenance Operation) scheduling. The NC is dynamically selected from all the MoCA nodes in the network. There is only one NC in a MoCA network and the rest of the MoCa nodes in the MoCA network are clients. Select **Enable** to configure the EMG6765-Q10A as a preferred network coordinator. The preferred NC has an advantage in the NC selection.
Security	
Network Security	Select **Enable** to turn on MoCA privacy. If this is enabled, all MoCA devices connected via coaxial cables must use the same password.
Network Password	Enter the password for the MoCA network. All packets in the MoCA network are encrypted except for beacons. The password should be 12 to 17 ASCII characters long.
Retype to Confirm	Enter the password again for confirmation.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

11.4 MoCA Monitor Screen

Use this screen to view the MoCA network status and information about the connected MoCA devices (nodes). Click **Network > MoCA > Monitor**.

Figure 54 Network > MoCA > Monitor



MoCA Status

Status : Link Down

Node Count : 0

Node Coordinator : 0

Channel : ---- MHz

Last Good Channel : ---- MHz

Link Up Time : 00:00:00

MoCA Node List

ID	Node Type	MoCA MAC	TNode Tx PHY Rate	Node Rx Power	Node Rx Packets	Node Rx Corrected	Node Rx Drops

The following table describes the labels in this screen.

Table 40 Network > MoCA > Monitor

LABEL	DESCRIPTION
MoCA Status	
Status	This shows the MoCA network status. It displays **Link Up** if the EMG6765-Q10A joins the MoCA network successfully. Otherwise, it displays **Link Down**.
Node Count	This shows the number of the nodes (including the EMG6765-Q10A) present in the MoCA network.
Node Coordinator	This shows the ID of the network coordinator in the MoCA network.
Channel	This shows the primary channel frequency at which the EMG6765-Q10A is operating.
Last Good Channel	This shows the last RF channel center frequency you configured in the MoCA screen.
Link Up Time	This displays how long the connection with other MoCA node(s) has been up.
MoCA Node List	
ID	This shows the node ID in the MoCA network.
Node Type	This shows whether the MoCA node is acting as a **Client** or an **NC** (Network Coordinator)
MoCA MAC	This shows the MAC address of the MoCA node.
TNode Tx PHY Rate	This shows the transmitted PHY rate in Mbps from the MoCA node.
Node Rx Power	This shows the MoCA node’s power consumption (in dBm) of receiving.
Node Rx Packets	This shows the number of packets received by the MoCA node.
Node Rx Corrected	This shows the number of packets corrected and received by the MoCA node.
Node Rx Drops	This shows the number of packets dropped by the MoCA node.
Refresh	Click this button to renew the screen.

CHAPTER 12 DHCP Server

12.1 Overview

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 EMG6765-Q10A's LAN as a DHCP server or disable it. When configured as a server, the EMG6765-Q10A provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

12.1.1 What You Can Do

- Use the **General** screen to enable the DHCP server (Section 12.2 on page 104).
- Use the **Advanced** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 12.3 on page 105).
- Use the **Client List** screen to view the current DHCP client information (Section 12.4 on page 107).

12.1.2 What You Need To Know

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

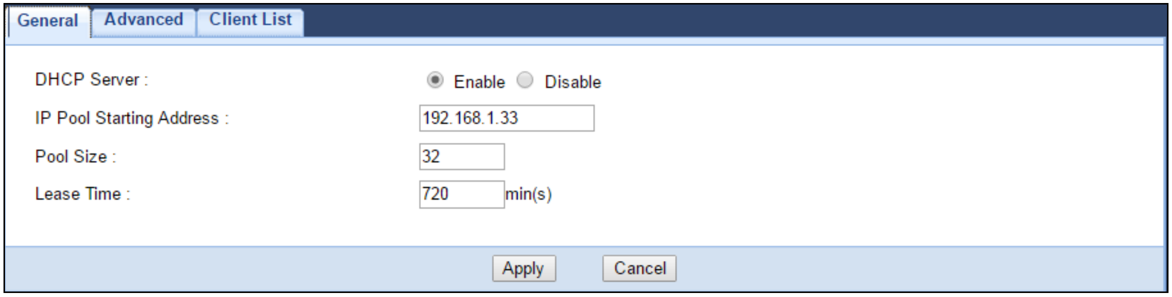
MAC Addresses

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

12.2 DHCP Server General Screen

Use this screen to enable the DHCP server. Click **Network** > **DHCP Server**. The following screen displays.

Figure 55 Network > DHCP Server > General



DHCP Server :	● Enable ○ Disable
IP Pool Starting Address :	192.168.1.33
Pool Size :	32
Lease Time :	720 min(s)

The following table describes the labels in this screen.

Table 41 Network > DHCP Server > General

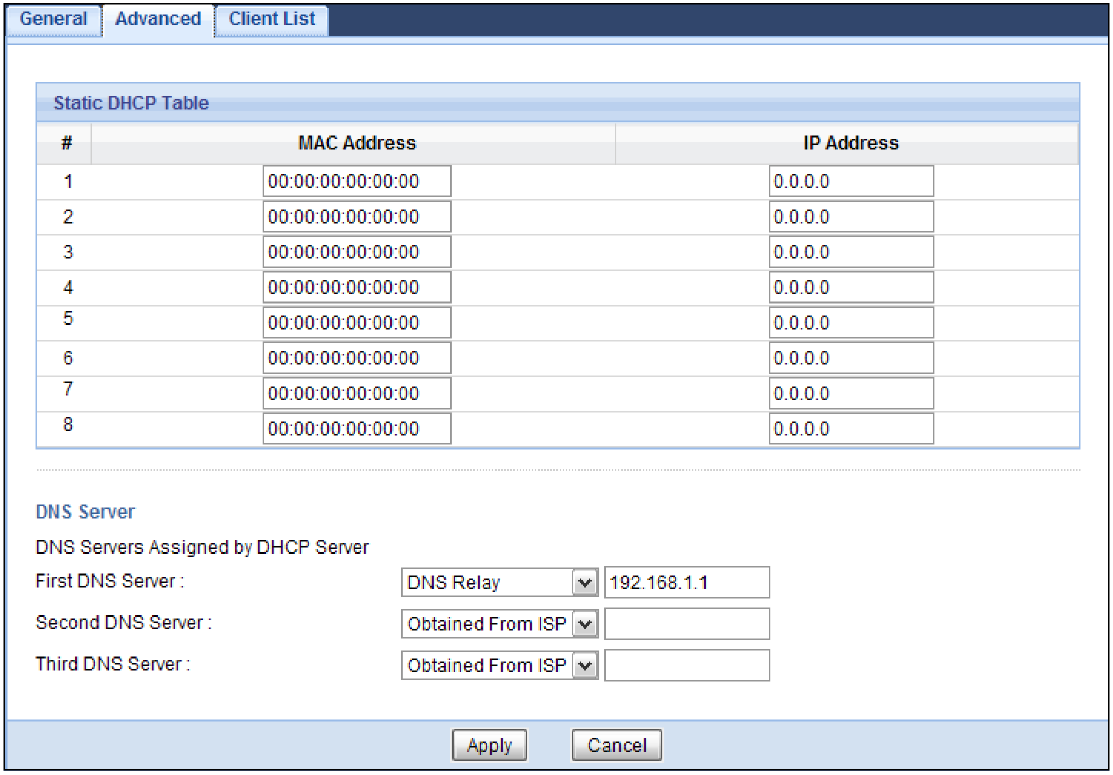
LABEL	DESCRIPTION
DHCP Server	Select **Enable** to activate DHCP for LAN. DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Enable the DHCP server unless your ISP instructs you to do otherwise. Select **Disable** to stop the EMG6765-Q10A acting as a DHCP server. When configured as a server, the EMG6765-Q10A provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool for LAN.
Pool Size	This field specifies the size, or count of the IP address pool for LAN.
Lease Time	This field specifies how long an individual client can use an IP address before it has to request a new one.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

12.3 DHCP Server Advanced Screen

This screen allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses. You can also use this screen to configure the DNS server information that the EMG6765-Q10A sends to the DHCP clients.

To change your EMG6765-Q10A's static DHCP settings, click **Network** > **DHCP Server** > **Advanced**. The following screen displays.

Figure 56 Network > DHCP Server > Advanced



Static DHCP Table

#	MAC Address	IP Address
1	00:00:00:00:00:00	0.0.0.0
2	00:00:00:00:00:00	0.0.0.0
3	00:00:00:00:00:00	0.0.0.0
4	00:00:00:00:00:00	0.0.0.0
5	00:00:00:00:00:00	0.0.0.0
6	00:00:00:00:00:00	0.0.0.0
7	00:00:00:00:00:00	0.0.0.0
8	00:00:00:00:00:00	0.0.0.0

DNS Server

DNS Servers Assigned by DHCP Server

First DNS Server : DNS Relay 192.168.1.1

Second DNS Server : Obtained From ISP

Third DNS Server : Obtained From ISP

The following table describes the labels in this screen.

Table 42 Network > DHCP Server > Advanced

LABEL	DESCRIPTION
Static DHCP Table	
#	This is the index number of the static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	Type the LAN IP address of a computer on your LAN.
DNS Server	
DNS Servers Assigned by DHCP Server	The EMG6765-Q10A passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The EMG6765-Q10A only passes this information to the LAN DHCP clients when you enable **DHCP Server**. When you disable **DHCP Server**, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.

Table 42 Network > DHCP Server > Advanced (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the EMG6765-Q10A's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **DNS Relay** to have the EMG6765-Q10A act as a DNS proxy. The EMG6765-Q10A's LAN IP address displays in the field to the right (read-only). The EMG6765-Q10A tells the DHCP clients on the LAN that the EMG6765-Q10A itself is the DNS server. When a computer on the LAN sends a DNS query to the EMG6765-Q10A, the EMG6765-Q10A forwards the query to the EMG6765-Q10A's system DNS server (configured in the **WAN** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

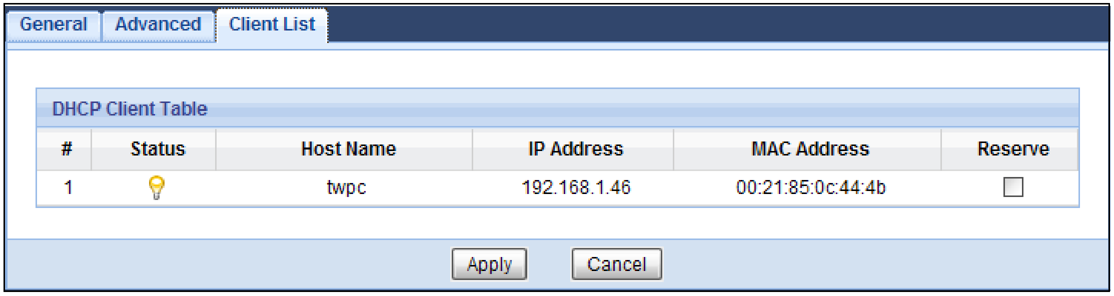
12.4 DHCP Client List Screen

The DHCP table shows current DHCP client information (including IP Address, Host Name and MAC Address) of network clients using the EMG6765-Q10A’s DHCP servers.

Configure this screen to always assign an IP address to a MAC address (and host name). Click **Network > DHCP Server > Client List**.

Note: You can also view a read-only client list by clicking **Monitor > DHCP Server**.

Figure 57 Network > DHCP Server > Client List



DHCP Client Table

#	Status	Host Name	IP Address	MAC Address	Reserve
1	💡	twpc	192.168.1.46	00:21:85:0c:44:4b	□

The following table describes the labels in this screen.

Table 43 Network > DHCP Server > Client List

LABEL	DESCRIPTION
DHCP Client Table	
#	This is the index number of the host computer.
Status	This field displays whether the connection to the host computer is up (a yellow bulb) or down (a gray bulb).
Host Name	This field displays the computer host name.

Table 43   Network > DHCP Server > Client List (continued)

LABEL	DESCRIPTION
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Reserve	Select this if you want to reserve the IP address for this specific MAC address.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

CHAPTER 13
NAT

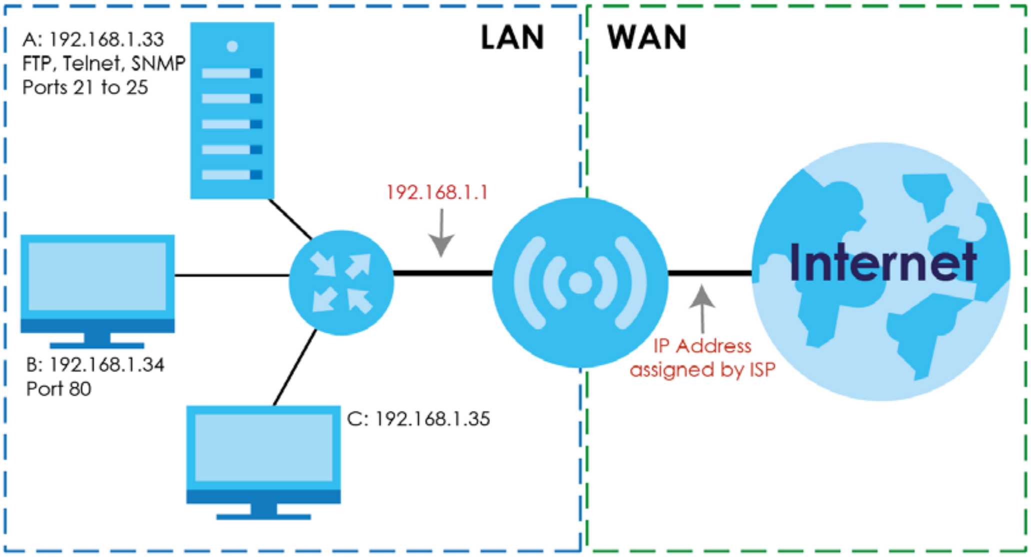
13.1 Overview

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 is changed to a different IP address known within another network.

The figure below is a simple illustration of a NAT network. 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 to the devices (**A** to **D**) connected to your EMG6765-Q10A. The ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet. All traffic coming from **A** to **D** going out to the Internet use the IP address of the EMG6765-Q10A, which is 192.168.1.1.

Figure 58 NAT Example



This chapter discusses how to configure NAT on the EMG6765-Q10A.

Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the EMG6765-Q10A.

13.1.1 What You Can Do

- Use the **General** screen to enable NAT (Section 13.2 on page 111).
- Use the **Port Forwarding** screen to set a default server and change your EMG6765-Q10A's port forwarding settings to forward incoming service requests to the server(s) on your local network (Section 13.3 on page 112).

- Use the **Port Trigger** screen to change your EMG6765-Q10A's trigger port settings (Section 13.5.3 on page 117).

13.1.2 What You Need To Know

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

Inside/Outside

This denotes where a host is located relative to the EMG6765-Q10A, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

This 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: Inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet.

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 44 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.

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

What NAT Does

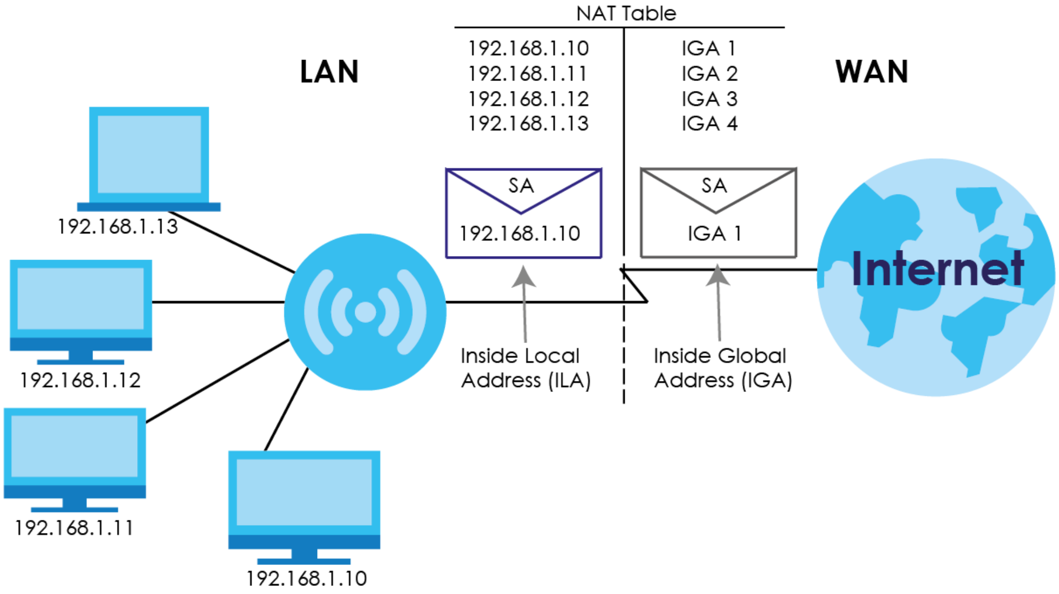
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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, NAT offers the additional benefit of firewall protection. With no servers defined, your EMG6765-Q10A 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)*.

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 in each packet and then forwards it to the Internet. The EMG6765-Q10A keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

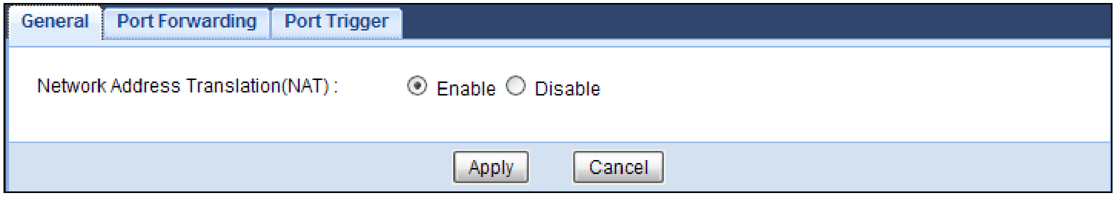
Figure 59 How NAT Works



13.2 General

Use this screen to enable NAT and set a default server. Click **Network > NAT** to open the **General** screen.

Figure 60 Network > NAT > General



Network Address Translation(NAT) : ● Enable ○ Disable

The following table describes the labels in this screen.

Table 45 Network > NAT > General

LABEL	DESCRIPTION
Network Address Translation (NAT)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select **Enable** to activate NAT. Select **Disable** to turn it off.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.3 Port Forwarding Screen

Use this screen to forward incoming service requests to the server(s) on your local network and set a default server. 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.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

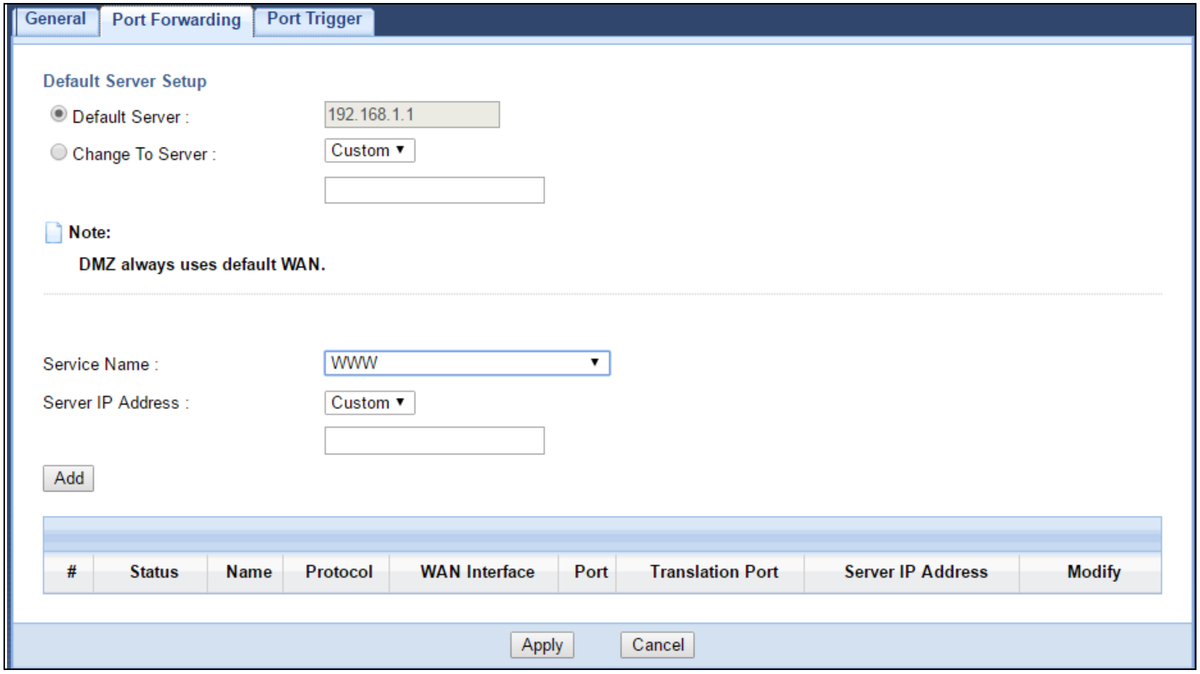
Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your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

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your EMG6765-Q10A's port forwarding settings, click **Network > NAT** > **Port Forwarding**. The screen appears as shown.

Note: If you do not assign a **Default Server**, the EMG6765-Q10A discards all packets received for ports that are not specified in this screen or remote management.

Refer to Appendix B on page 200 for port numbers commonly used for particular services.

Figure 61 Network > NAT > Port Forwarding



Default Server Setup

● Default Server : 192.168.1.1

○ Change To Server : Custom ▾

Note:

DMZ always uses default WAN.

Service Name : WWW ▾

Server IP Address : Custom ▾

#	Status	Name	Protocol	WAN Interface	Port	Translation Port	Server IP Address	Modify

The following table describes the labels in this screen.

Table 46 Network > NAT > Port Forwarding

LABEL	**DESCRIPTION**
Default Server Setup	
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in the **Port Forwarding** screen. You can decide whether you want to use the default server or specify a server manually. Select this to use the default server.
Change to Server	Select this and manually enter the server's IP address.
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will be displayed in the port forwarding summary table. Otherwise, select **User define** to manually enter the port number(s) and select the IP protocol.
Server IP Address	Enter the inside IP address of the virtual server here and click **Add** to add it in the port forwarding summary table.
Add	Click this to add a new port forwarding rule.
#	This is the number of an individual port forwarding server entry.
Status	This icon is turned on when the rule is enabled.
Name	This field displays a name to identify this rule.
Protocol	This is the transport layer protocol used for the service.
WAN Interface	This field displays the interface on which packets for the NAT entry are received.
Port	This field displays the external port number(s) that identifies a service.
Translation Port	This field displays the internal port number(s) that identifies a service.
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the **Edit** icon to open the edit screen where you can modify an existing rule. Click the **Delete** icon to remove a rule.

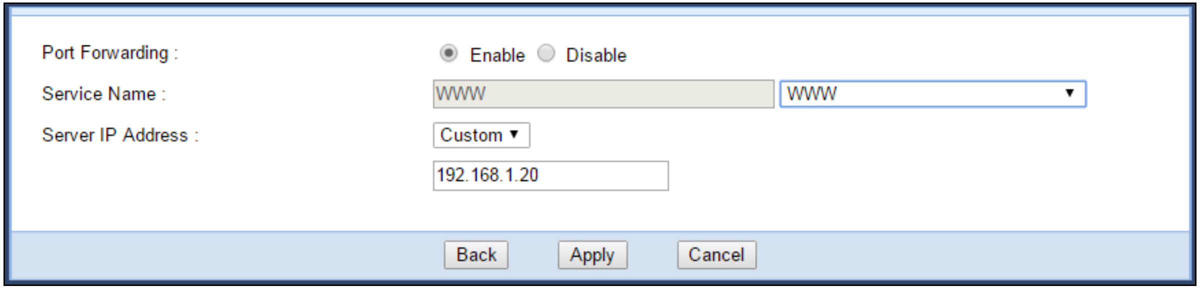
Table 46 Network > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.3.1 Port Forwarding Edit Screen

This screen lets you edit a port forwarding rule. Click a rule's **Edit** icon in the **Port Forwarding** screen to open the following screen.

Figure 62 Network > NAT > Port Forwarding Edit



Port Forwarding : ● Enable ○ Disable

Service Name : WWW | WWW ▾

Server IP Address : Custom ▾

192.168.1.20

The following table describes the labels in this screen.

Table 47 Network > NAT > Port Forwarding Edit

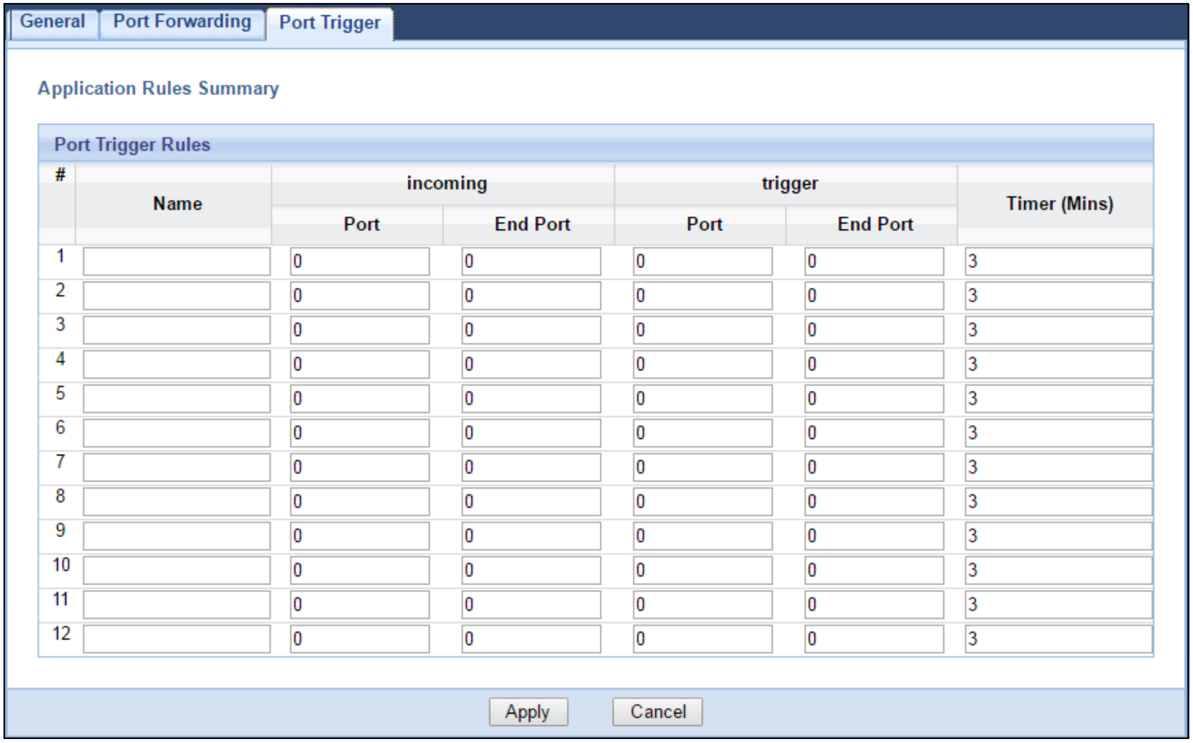
LABEL	DESCRIPTION
Port Forwarding	Select **Enable** to turn on this rule and the requested service can be forwarded to the host with a specified internal IP address. Select **Disable** to disallow forwarding of these ports to an inside server without having to delete the entry.
Service Name	Select **User define** and type a name (of up to 31 printable characters) to identify this rule in the first field next to **Service Name**. Otherwise, select a predefined service in the second field next to **Service Name**.
Protocol	Select the transport layer protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP_UDP**. If you have chosen a pre-defined service in the **Service Name** field, the protocol will be configured automatically.
Port	Type a port number(s) to define the service to be forwarded to the specified server. To specify a range of ports, enter a hyphen (-) between the first port and the last port, such as 10-.
Server IP Address	Type the IP address of the server on your LAN that receives packets from the port(s) specified in the **Port** field.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.4 Port Trigger Screen

To change your EMG6765-Q10A’s trigger port settings, click **Network > NAT > Port Trigger**. The screen appears as shown.

Note: Only one LAN computer can use a trigger port (range) at a time.

Figure 63 Network > NAT > Port Trigger



Application Rules Summary

Port Trigger Rules

#	Name	incoming		trigger		Timer (Mins)
		Port	End Port	Port	End Port	
1		0	0	0	0	3
2		0	0	0	0	3
3		0	0	0	0	3
4		0	0	0	0	3
5		0	0	0	0	3
6		0	0	0	0	3
7		0	0	0	0	3
8		0	0	0	0	3
9		0	0	0	0	3
10		0	0	0	0	3
11		0	0	0	0	3
12		0	0	0	0	3

The following table describes the labels in this screen.

Table 48 Network > NAT > Port Trigger

LABEL	DESCRIPTION
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The EMG6765-Q10A forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the EMG6765-Q10A to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Timer (Mins)	Enter the interval (in minutes) a trigger port records an IP address of the client requesting the service.

Table 48 Network > NAT > Port Trigger (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.5 Technical Reference

The following section contains additional technical information about the EMG6765-Q10A features described in this chapter.

13.5.1 NATPort Forwarding: Services and Port Numbers

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

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.

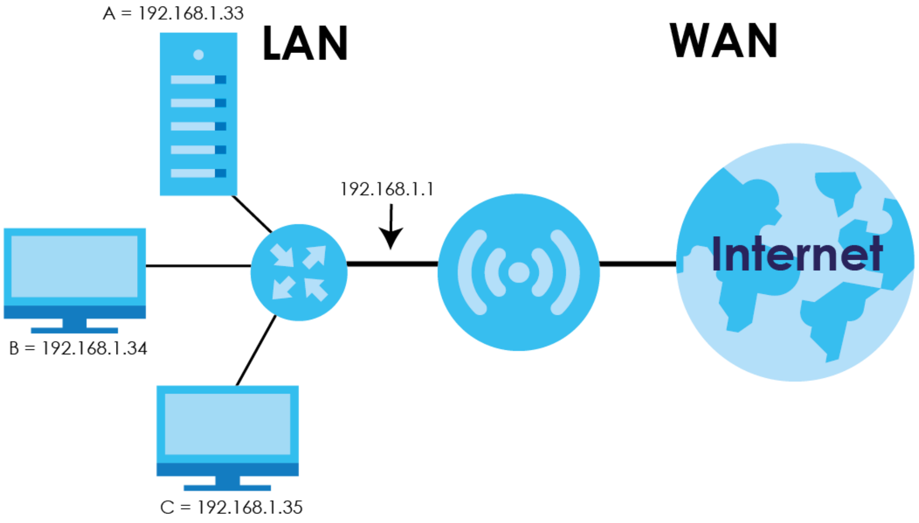
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

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.

13.5.2 NAT 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 64 Multiple Servers Behind NAT Example



13.5.3 Trigger Port Forwarding

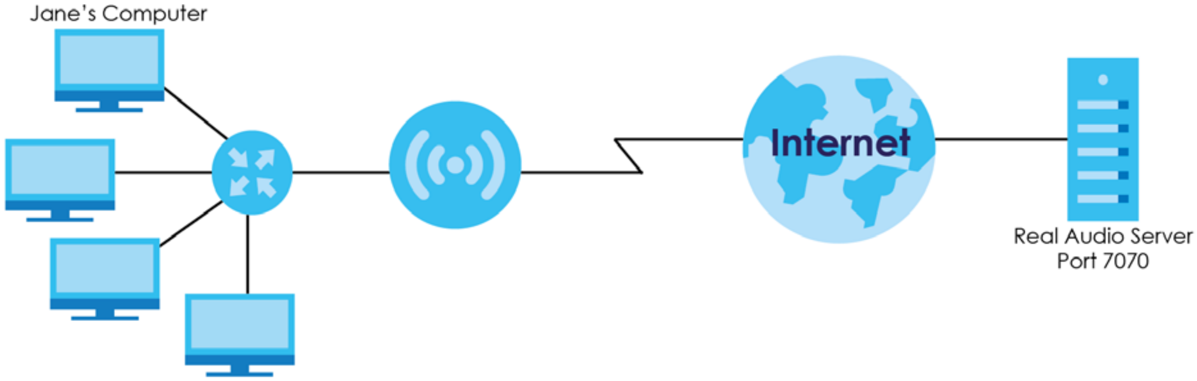
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem 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 EMG6765-Q10A 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 EMG6765-Q10A's WAN port receives a response with a specific port number and protocol ("incoming" port), the EMG6765-Q10A 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.

13.5.4 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 65 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 EMG6765-Q10A to record Jane’s computer IP address. The EMG6765-Q10A associates Jane's computer IP address with the "incoming" port range of 6970-7170.

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

4 The EMG6765-Q10A 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 EMG6765-Q10A times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

13.5.5 Two Points To Remember About Trigger Ports

1 Trigger events only happen on data that is coming from inside the EMG6765-Q10A and going to the outside.

2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can’t trigger it.

CHAPTER 14
DDNS

14.1 Overview

DDNS services let you use a domain name with a dynamic IP address.

14.1.1 What You Need To Know

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

What is DDNS?

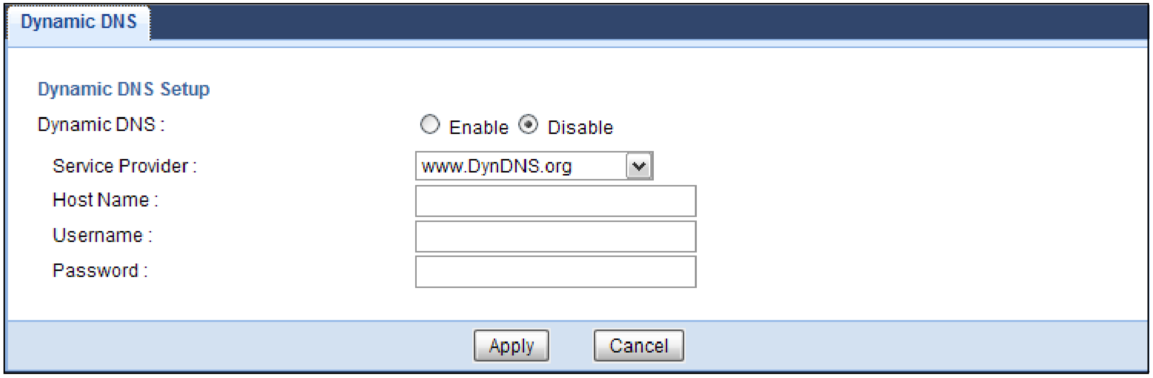
Dynamic Domain Name Service (DDNS) services let you use a fixed domain name with a dynamic IP address. Users can always use the same domain name instead of a different dynamic IP address that changes each time to connect to the EMG6765-Q10A or a server in your network.

Note: The EMG6765-Q10A must have a public global IP address and you should have your registered DDNS account information on hand.

14.2 General

To change your EMG6765-Q10A's DDNS, click **Network > DDNS**. The screen appears as shown.

Figure 66 Dynamic DNS



Dynamic DNS

Dynamic DNS Setup

Dynamic DNS : ○ Enable ● Disable

Service Provider : www.DynDNS.org

Host Name :

Username :

Password :

The following table describes the labels in this screen.

Table 49 Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS	Select **Enable** to use dynamic DNS. Select **Disable** to turn this feature off.
Service Provider	Select the name of your Dynamic DNS service provider.

Table 49 Dynamic DNS (continued)

LABEL	DESCRIPTION
Host Name	Enter a host names in the field provided. You can specify up to two host names in the field separated by a comma (",").
Username	Enter your user name.
Password	Enter the password assigned to you.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 15
Static Route

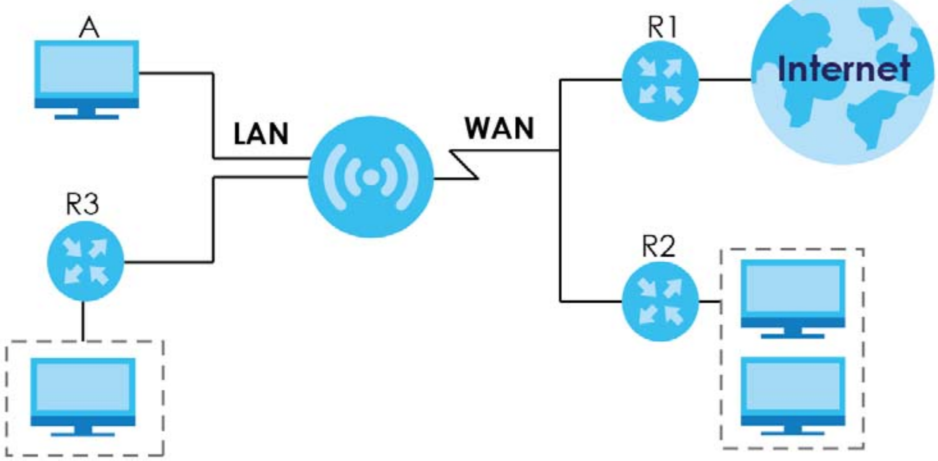
15.1 Overview

This chapter shows you how to configure static routes for your EMG6765-Q10A.

The EMG6765-Q10A usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the EMG6765-Q10A 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 EMG6765-Q10A's LAN interface. The EMG6765-Q10A routes most traffic from **A** to the Internet through the EMG6765-Q10A'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.

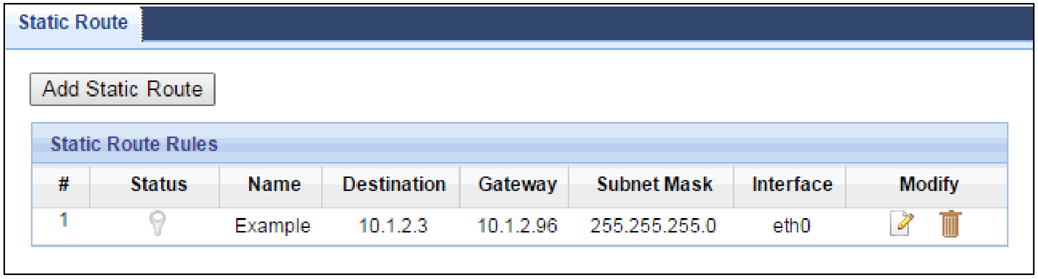
Figure 67 Example of Static Routing Topology



15.2 IP Static Route Screen

Click **Network > Static Route** to open the **Static Route** screen.

Figure 68 Network > Static Route



Static Route Rules

#	Status	Name	Destination	Gateway	Subnet Mask	Interface	Modify
1	💡	Example	10.1.2.3	10.1.2.96	255.255.255.0	eth0	✎ 🗑

The following table describes the labels in this screen.

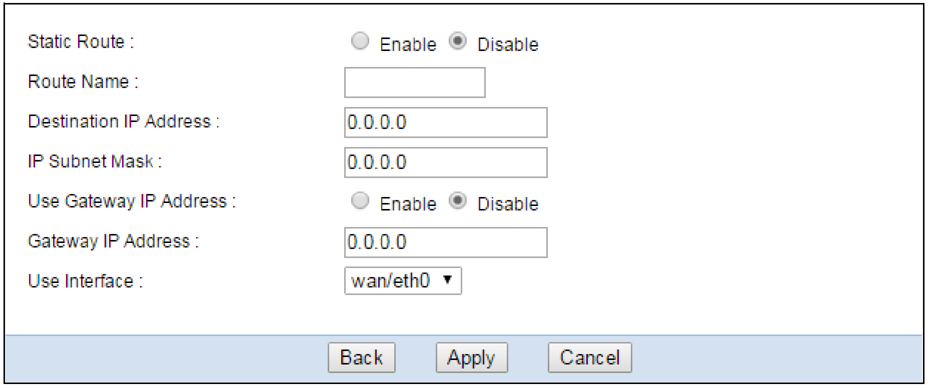
Table 50 Network > Static Route

LABEL	DESCRIPTION
Add Static Route	Click this to create a new rule.
Static Route Rules	
#	This is the number of an individual static route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Name	This field displays a name to identify this rule.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
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.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the **Edit** icon to open a screen where you can modify an existing rule. Click the **Delete** icon to remove a rule from the EMG6765-Q10A.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.2.1 Add/Edit Static Route

Click the **Add Static Route** button or a rule’s **Edit** icon in the **Static Route** screen. Use this screen to configure the required information for a static route.

Figure 69 Network > Static Route: Add/Edit



Static Route :	○ Enable ● Disable
Route Name :	
Destination IP Address :	0.0.0.0
IP Subnet Mask :	0.0.0.0
Use Gateway IP Address :	○ Enable ● Disable
Gateway IP Address :	0.0.0.0
Use Interface :	wan/eth0 ▼

The following table describes the labels in this screen.

Table 51 Network > Static Route: Add/Edit

LABEL	DESCRIPTION
Static Route	Select to enable or disable this rule.
Route Name	Type a name to identify this rule. You can use up to 31 printable English keyboard characters, including spaces.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you 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.
IP Subnet Mask	Enter the IP subnet mask here.
Use Gateway IP Address	Select to enable or disable this rule.
Gateway IP Address	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your EMG6765-Q10A's interface(s). The gateway helps forward packets to their destinations.
Use Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **WAN** screens.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to set every field in this screen to its last-saved value.

CHAPTER 16
Interface Group

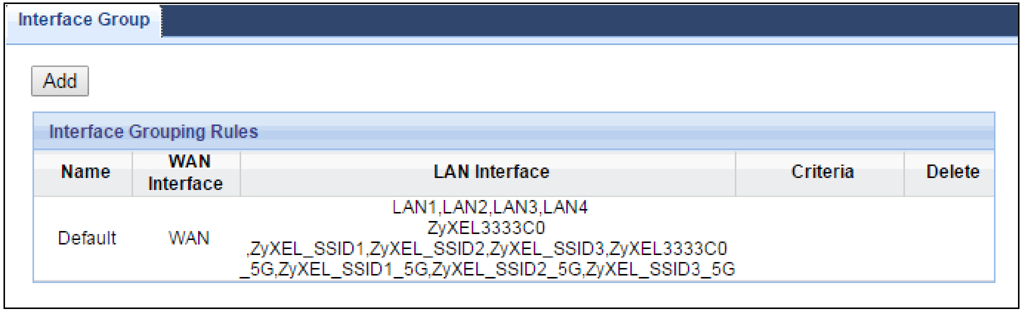
16.1 Overview

By default, all LAN and WAN interfaces on the EMG6765-Q10A are in the same group and can communicate with each other. Each group acts as an independent network on the EMG6765-Q10A.

16.2 The Interface Group Screen

You can manually add a LAN and/or WLAN interface to a new group. Click **Network > Interface Group** to open the following screen.

Figure 70 Network > Interface Group



Interface Grouping Rules

Name	WAN Interface	LAN Interface	Criteria	Delete
Default	WAN	LAN1,LAN2,LAN3,LAN4 ZyXEL3333C0 ,ZyXEL_SSID1,ZyXEL_SSID2,ZyXEL_SSID3,ZyXEL3333C0 _5G,ZyXEL_SSID1_5G,ZyXEL_SSID2_5G,ZyXEL_SSID3_5G		

The following table describes the fields in this screen.

Table 52 Network > Interface Group

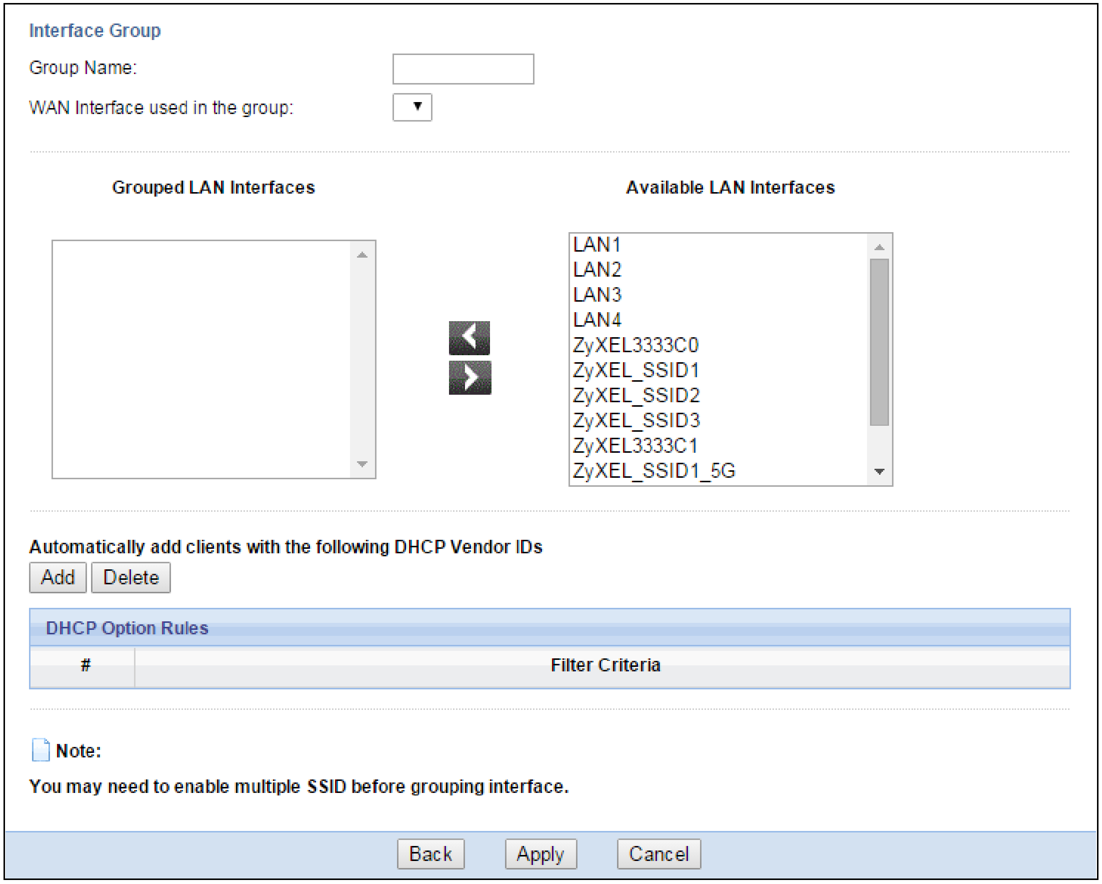
LABEL	DESCRIPTION
Add	Click this to add a new interface grouping rule. You must configure a WAN connection before you can add a new interface grouping rule. See Chapter 8 on page 60 for more information.
Interface Grouping Rules	
Name	This shows the descriptive name of the group.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN and/or WLAN interfaces in the group.
Criteria	This shows the filtering criteria for the group.
Delete	Click the **Delete** icon to remove the group.

16.2.1 Add Interface Group

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

Note: An interface can belong to a group only.

Figure 71 Interface Group > Add New Group



Interface Group

Group Name:

WAN Interface used in the group:

Grouped LAN Interfaces

Available LAN Interfaces

LAN1
LAN2
LAN3
LAN4
ZyXEL3333C0
ZyXEL_SSID1
ZyXEL_SSID2
ZyXEL_SSID3
ZyXEL3333C1
ZyXEL_SSID1_5G

Automatically add clients with the following DHCP Vendor IDs

Add Delete

DHCP Option Rules

#	Filter Criteria

Note:

You may need to enable multiple SSID before grouping interface.

The following table describes the fields in this screen.

Table 53 Interface Group > Add New Group

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group.
WAN Interfaces used in the group	Select a WAN interface to be used in this group. Select **None** to not add a WAN interface to this group.
Grouped LAN Interfaces Available LAN Interfaces	Select a LAN or wireless LAN interface in the **Available LAN Interfaces** and use the left-facing arrow to move it to the **Grouped LAN Interfaces** to add the interface to this group. To remove a LAN or wireless LAN interface from the **Grouped LAN Interfaces**, use the right-facing arrow.
Add	Click this button to create a new rule.
Delete	Click the **Delete** icon to remove this rule from the EMG6765-Q10A.
DHCP Option Rules	
#	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.
Back	Click this button to return to the previous screen without saving any changes.

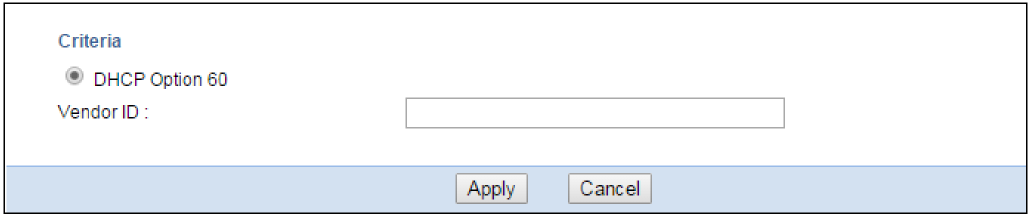
Table 53 Interface Group > Add New Group

LABEL	DESCRIPTION
Apply	Click this button to save your settings back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16.2.2 Add Interface Group Criteria

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

Figure 72 Interface Group > Add New Group > Add Interface Group Criteria



Criteria

● DHCP Option 60

Vendor ID :

The following table describes the fields in this screen.

Table 54 Interface Group > Add New Group > Add Interface Group Criteria

LABEL	DESCRIPTION
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.
Vendor ID	Enter the identification number assigned to the company by the IANA (Internet Assigned Numbers Authority).
Apply	Click this button to save your settings back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 17
Firewall

17.1 Overview

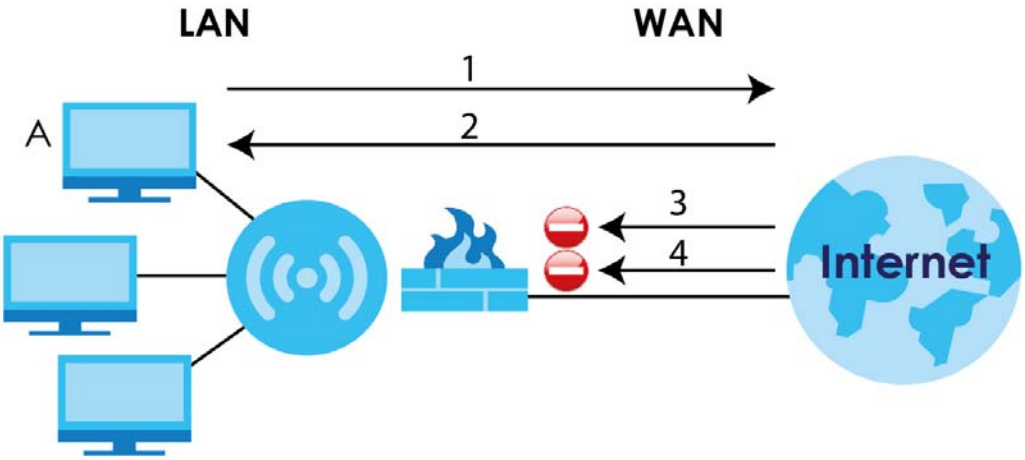
Use these screens to enable and configure the firewall that protects your EMG6765-Q10A and your LAN from unwanted or malicious traffic.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the 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 73 Default Firewall Action



17.1.1 What You Can Do

- Use the **General** screen to enable or disable the EMG6765-Q10A's firewall (Section 17.2 on page 129).
- Use the **Services** screen enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them (Section 17.3 on page 129).

17.1.2 What You Need To Know

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

What is a Firewall?

Originally, the term “firewall” referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from a network that is not trusted. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

Stateful Inspection Firewall

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

About the EMG6765-Q10A Firewall

The EMG6765-Q10A’s firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The EMG6765-Q10A's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The EMG6765-Q10A can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The EMG6765-Q10A is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The EMG6765-Q10A has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

Guidelines For Enhancing Security With Your Firewall

1. Change the default password via Web Configurator.

2. Think about access control before you connect to the network in any way, including attaching a modem to the port.

3. Limit who can access your router.

4 Don't enable any local service (such as NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.

5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.

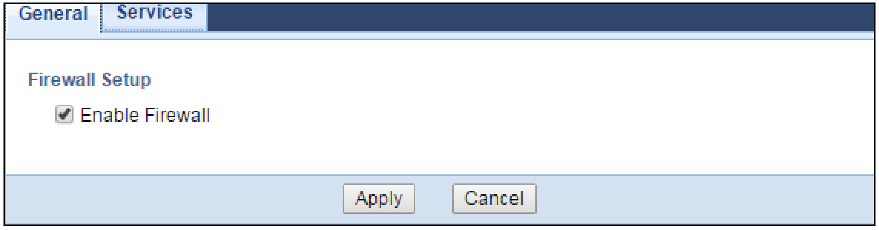
6 Protect against IP spoofing by making sure the firewall is active.

7 Keep the firewall in a secured (locked) room.

17.2 General Screen

Use this screen to enable or disable the EMG6765-Q10A's firewall, and set up firewall logs. Click **Security** > **Firewall** to open the **General** screen.

Figure 74 Security > Firewall > General I



☑ Enable Firewall

The following table describes the labels in this screen.

Table 55 Security > Firewall > General

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The EMG6765-Q10A performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to start configuring this screen again.

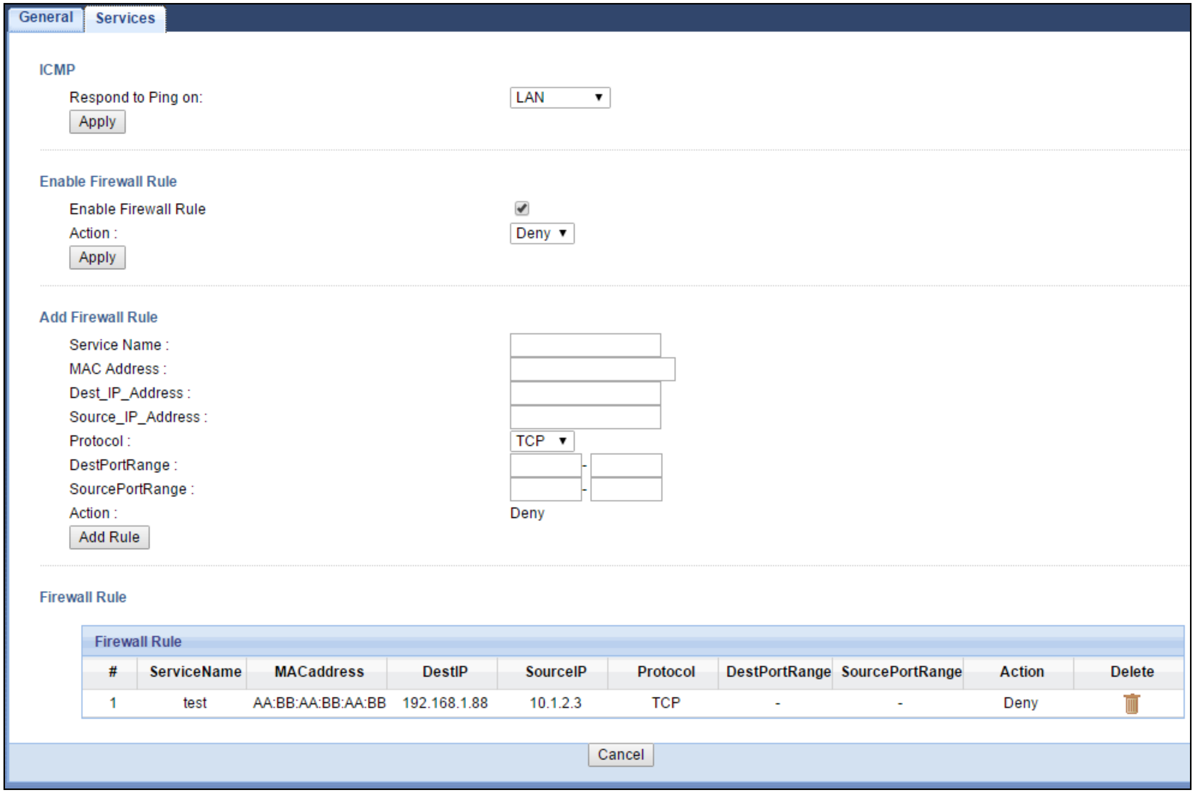
17.3 Services Screen

If an outside user attempts to probe an unsupported port on your EMG6765-Q10A, an ICMP response packet is automatically returned. This allows the outside user to know the EMG6765-Q10A exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your EMG6765-Q10A when unsupported ports are probed.

You can also use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

Click **Security** > **Firewall** > **Services**. The screen appears as shown next.

Figure 75 Security > Firewall > Services I



ICMP

Respond to Ping on: LAN

Enable Firewall Rule

Enable Firewall Rule ☑

Action : Deny

Add Firewall Rule

Service Name :

MAC Address :

Dest_IP_Address :

Source_IP_Address :

Protocol : TCP

DestPortRange : -

SourcePortRange : -

Action : Deny

Firewall Rule

Firewall Rule

#	ServiceName	MACaddress	DestIP	SourceIP	Protocol	DestPortRange	SourcePortRange	Action	Delete
1	test	AA:BB:AA:BB:AA:BB	192.168.1.88	10.1.2.3	TCP	-	-	Deny	🗑

The following table describes the labels in this screen.

Table 56 Security > Firewall > Services

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The EMG6765-Q10A will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN&WAN** to reply to all incoming LAN and WAN Ping requests.
Apply	Click **Apply** to save the settings.
Enable Firewall Rule	
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see **Add Firewall Rule** below).
Action	Select which action the firewall rule applies to the packets, select **Deny** to drop the packets and **Allow** to accept the packets.
Apply	Click **Apply** to save the settings.
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest IP Address	Enter the IP address of the computer to which traffic for the application or service is entering. The EMG6765-Q10A applies the firewall rule to traffic initiating from this computer.
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service. The EMG6765-Q10A applies the firewall rule to traffic initiating from this computer.

Table 56 Security > Firewall > Services (continued)

LABEL	DESCRIPTION
Protocol	Select the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Action	This field displays whether the firewall silently discards packets (**Deny**), or permits the passage of packets (**Allow**).
Add Rule	Click **Add** to save the firewall rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Service Name	This is a name that identifies or describes the firewall rule.
MAC address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP	This is the IP address of the computer from which traffic for the application or service is initialized.
Protocol	This is the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Action	**Deny** - Traffic matching the conditions of the firewall rule are stopped.
Delete	Click **Delete** to remove the firewall rule.
Cancel	Click **Cancel** to start configuring this screen again.

See Appendix B on page 200 for commonly used services and port numbers.

CHAPTER 18
Content Filtering

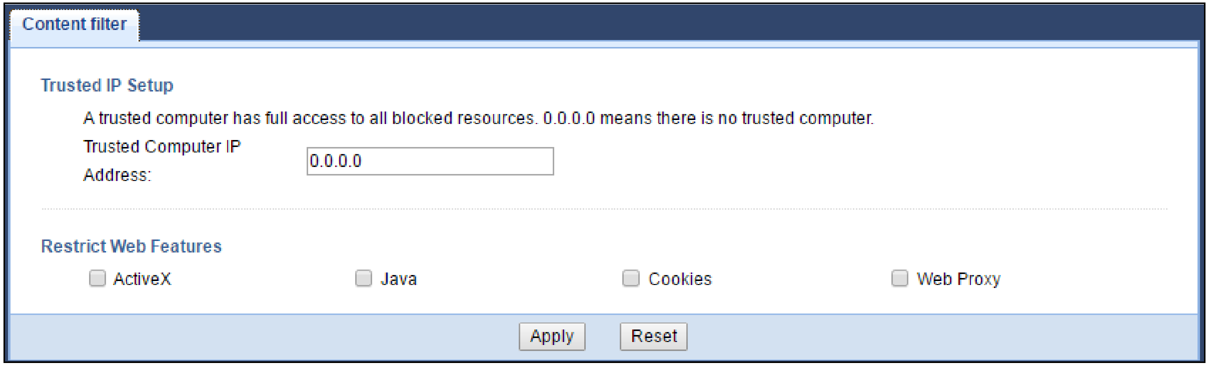
18.1 Overview

This chapter shows you how to configure content filtering. Content filtering is the ability to block certain web features.

18.2 Content Filter

Use this screen to restrict web features, and designate a trusted computer. Click **Security** > **Content Filter** to open the **Content Filter** screen.

Figure 76 Security > Content Filter



Trusted IP Setup

A trusted computer has full access to all blocked resources. 0.0.0.0 means there is no trusted computer.

Trusted Computer IP Address: 0.0.0.0

Restrict Web Features

□ ActiveX □ Java □ Cookies □ Web Proxy

The following table describes the labels in this screen.

Table 57 Security > Content Filter

LABEL	DESCRIPTION
Trusted IP Setup	To enable this feature, type an IP address of any one of the computers in your network that you want to have as a trusted computer. This allows the trusted computer to have full access to all features that are configured to be blocked by content filtering. Leave this field blank to have no trusted computers.
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.

Table 57 Security > Content Filter (continued)

LABEL	DESCRIPTION
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh

CHAPTER 19
IPv6 Firewall

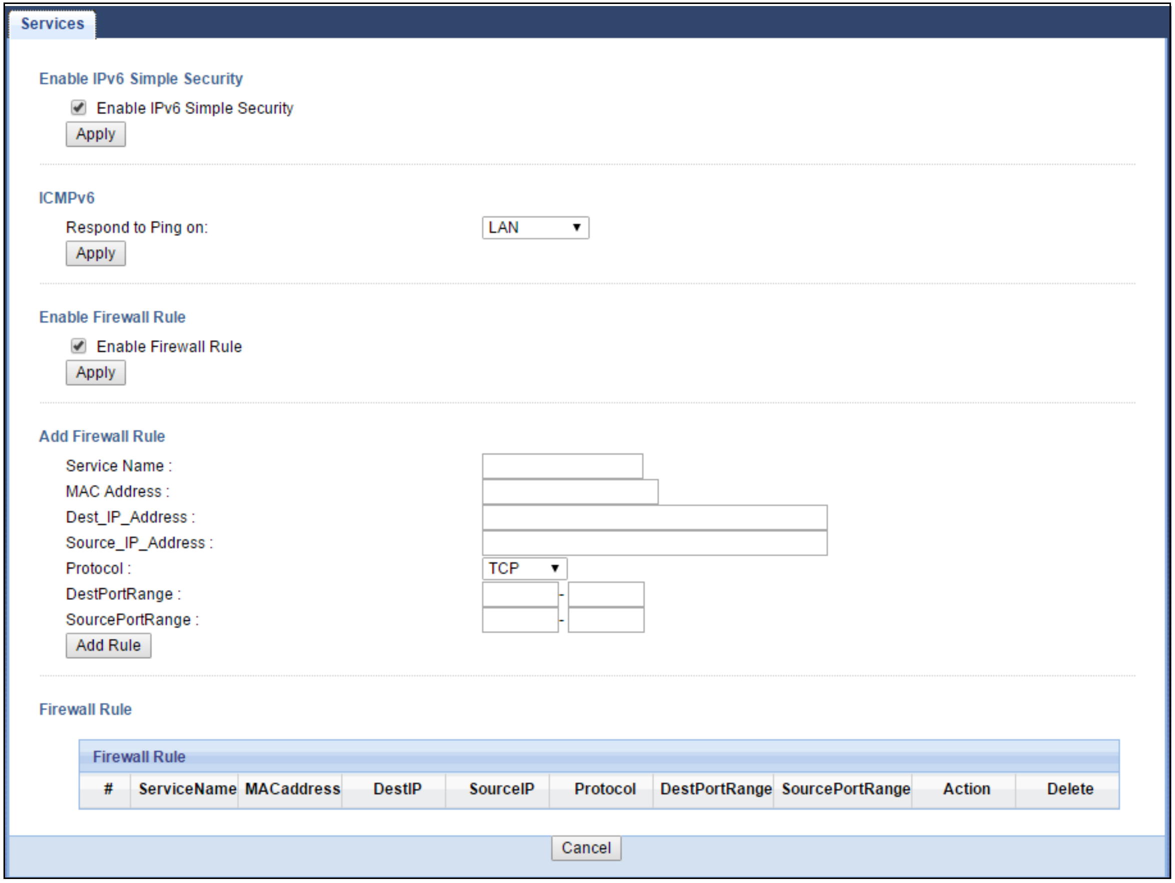
19.1 Overview

This chapter shows you how to enable and create IPv6 firewall rules to block unwanted IPv6 traffic.

19.2 IPv6 Firewall Screen

Click **Configuration** > **Security** > **IPv6 Firewall**. The **Service** screen appears as shown.

Figure 77 Configuration > Security > IPv6 Firewall



Services

Enable IPv6 Simple Security

☑ Enable IPv6 Simple Security

Apply

ICMPv6

Respond to Ping on: LAN

Apply

Enable Firewall Rule

☑ Enable Firewall Rule

Apply

Add Firewall Rule

Service Name :	
MAC Address :	
Dest_IP_Address :	
Source_IP_Address :	
Protocol :	TCP
DestPortRange :	-
SourcePortRange :	-

Add Rule

Firewall Rule

Firewall Rule

#	ServiceName	MACaddress	DestIP	SourceIP	Protocol	DestPortRange	SourcePortRange	Action	Delete

Cancel

The following table describes the labels in this screen.

Table 58 Configuration > Security > IPv6 Firewall

LABEL	DESCRIPTION
Enable IPv6 Simple Security	Select this to enable IPv6 Simple Security. IPv6 Simple Security is defined in RFC 6092. This security discards certain packets (such as packets with multicast source and/or destination address) to secure local networks and Internet.
Apply	Click **Apply** to save the settings.
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".
Respond to Ping on	The EMG6765-Q10A will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN&WAN** to reply to all incoming LAN and WAN Ping requests.
Apply	Click **Apply** to save the settings.
Enable Firewall Rule	
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see **Add Firewall Rule** below).
Apply	Click **Apply** to save the settings.
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest_IP_Address	Enter the IPv6 address of the computer to which traffic for the application or service is entering. The EMG6765-Q10A applies the firewall rule to traffic destined for this computer.
Source_IP_Address	Enter the IPv6 address of the computer that initializes traffic for the application or service. The EMG6765-Q10A applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	Enter the port number/range of the destination that defines the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	Enter the port number/range of the source that defines the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click **Add Rule** to save the firewall rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
ServiceName	This is a name that identifies or describes the firewall rule.
MACaddress	This is the MAC address of the computer for which the firewall rule applies.
DestIP	This is the IP address of the computer to which traffic for the application or service is entering.
SourceIP	This is the IP address of the computer to which traffic for the application or service is initialized.
Protocol	This is the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
DestPortRange	This is the port number/range of the destination that defines the traffic type, for example TCP port 80 defines web traffic.

Table 58 Configuration > Security > IPv6 Firewall (continued)

LABEL	DESCRIPTION
SourcePortRange	This is the port number/range of the source that defines the traffic type, for example TCP port 80 defines web traffic.
Action	**DROP** - Traffic matching the conditions of the firewall rule is stopped.
Delete	Click **Delete** to remove the firewall rule.
Cancel	Click **Cancel** to restore your previously saved settings.

CHAPTER 20
Parental Control

20.1 Overview

Parental controls allow you to block specific URLs. You can also define time periods and days during which the EMG6765-Q10A performs parental control on a specific user.

20.1.1 What You Need To Know

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

Keyword Blocking URL Checking

The EMG6765-Q10A checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

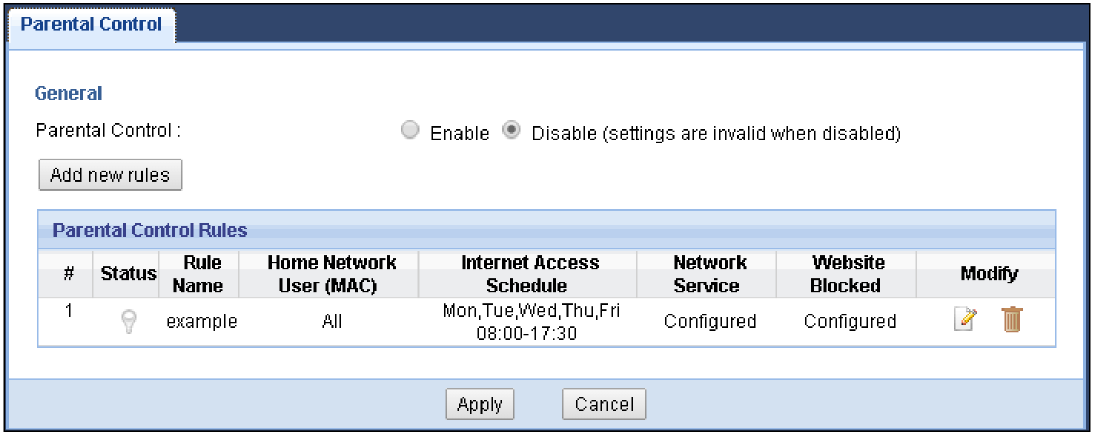
Since the EMG6765-Q10A checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the EMG6765-Q10A would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

20.2 Parental Control Screen

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

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

Figure 78 Security > Parental Control



General

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

Parental Control Rules

#	Status	Rule Name	Home Network User (MAC)	Internet Access Schedule	Network Service	Website Blocked	Modify
1	💡	example	All	Mon,Tue,Wed,Thu,Fri 08:00-17:30	Configured	Configured	✎ 🗑

The following table describes the fields in this screen.

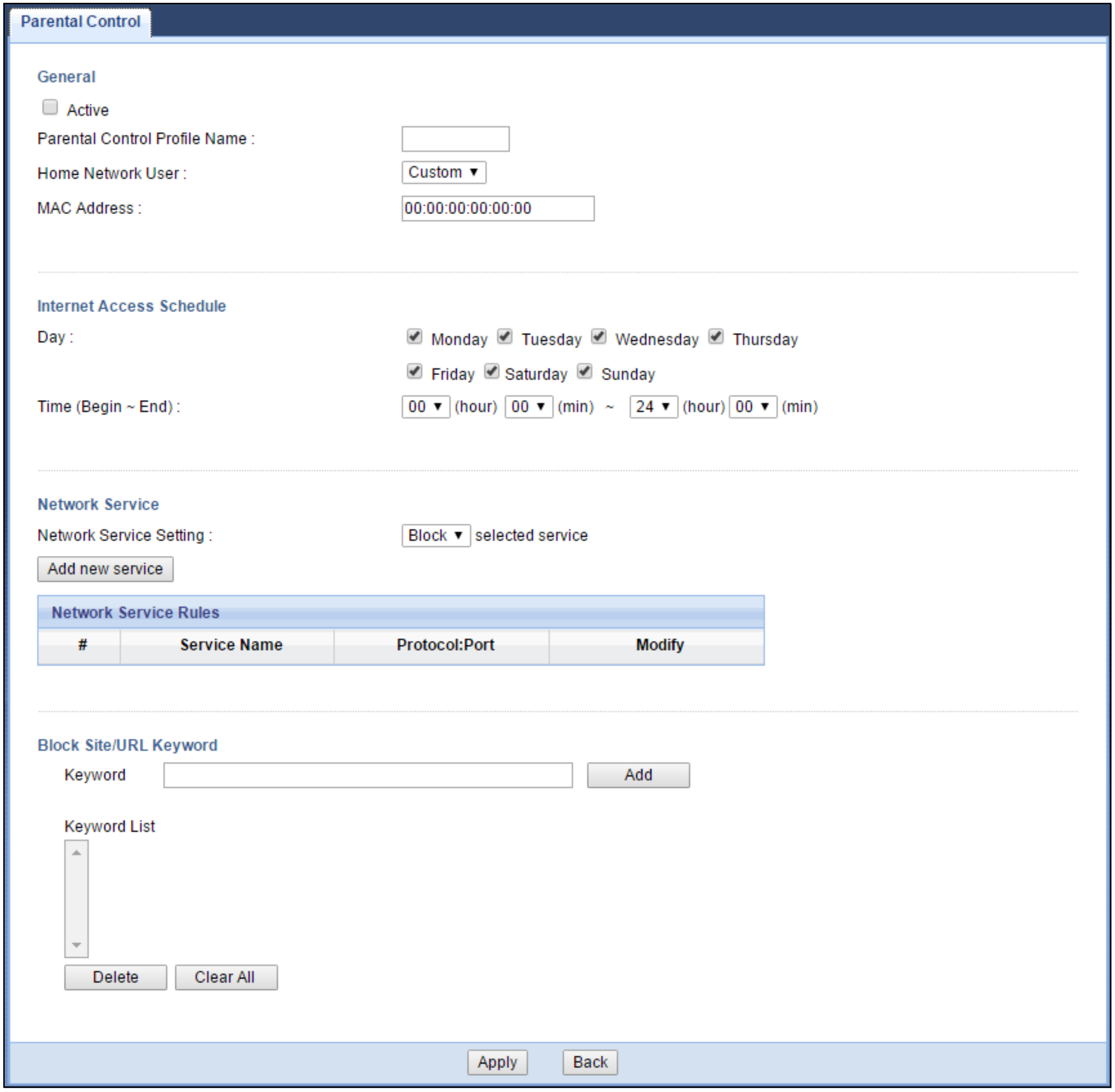
Table 59 Security > Parental Control

LABEL	DESCRIPTION
General	
Parental Control	Select **Enable** to activate parental control.
Add new rules	Click this if you want to configure a new parental control rule.
Parental Control Rules	
#	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.
Rule Name	This shows the name of the rule.
Home Network User (MAC)	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the day(s) and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, **None** will be shown.
Website Blocked	This shows whether the website block is configured. If not, **None** will be shown.
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.

20.2.1 Add/Edit a Parental Control Rule

Click **Add new rules** 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 79 Security > Parental Control: Add/Edit new rules



Parental Control

General

□ Active

Parental Control Profile Name :	
Home Network User :	Custom ▾
MAC Address :	00:00:00:00:00:00

Internet Access Schedule

Day : ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Time (Begin ~ End) : 00 ▾ (hour) 00 ▾ (min) ~ 24 ▾ (hour) 00 ▾ (min)

Network Service

Network Service Setting : Block ▾ selected service

Add new service

Network Service Rules

#	Service Name	Protocol:Port	Modify

Block Site/URL Keyword

Keyword [ ] Add

Keyword List

Delete Clear All

Apply Back

The following table describes the fields in this screen.

Table 60 Security > Parental Control: Add/Edit new rules

LABEL	DESCRIPTION
General	
Active	Select the check box to activate 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 in the **MAC Address** field. If you select **All**, the rule applies to all LAN users.
Internet Access Schedule	
Day	Select check boxes for the days that you want the EMG6765-Q10A to perform parental control.
Time	Drag the time bar to define the time that the LAN user is allowed access.

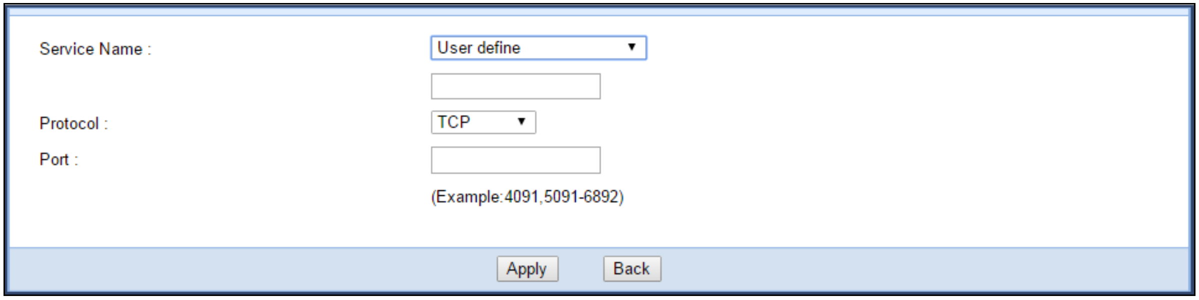
Table 60 Security > Parental Control: Add/Edit new rules (continued)

LABEL	DESCRIPTION
Network Service	
Network Service Setting	If you select **Block**, the EMG6765-Q10A prohibits the users from using the services listed below. If you select **Allow**, the EMG6765-Q10A blocks all 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.
Network Service Rules	
#	This shows the index number of the rule. Select the check box next to the rule to activate it.
Service Name	This shows the name of the service.
Protocol:Port	This shows the protocol and the port of the service.
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.
Blocked Site/URL Keyword	
Keyword	Use this field to enter the website URL or URL keyword to which the EMG6765-Q10A blocks access and click **Add**. Click **Delete** to remove it. Click **Clear All** to remove all keywords entered.
Apply	Click **Apply** to save your settings back to the EMG6765-Q10A.
Back	Click **Back** to return to the previous screen.

20.2.2 Add/Edit a Service

Click **Add new service** in the **Parental Control > Add/Edit new rules** screen to add a new entry or click the **Edit** icon next to an existing entry to edit it. Use this screen to configure a service rule.

Figure 80 Security > Parental Control > Add/Edit new rules > Add/Edit new service



Service Name : User define

Protocol : TCP

Port :

(Example:4091,5091-6892)

The following table describes the fields in this screen.

Table 61 Security > Parental Control > Add/Edit new rules > Add/Edit new service

LABEL	DESCRIPTION
Service Name	Select the name of the service. Otherwise, select **User define** and manually specify the name, protocol and the port of the service.
Protocol	Select the transport layer protocol used for the service. Choices are **TCP**, **UDP**, or **TCP/UDP**. If you have chosen a pre-defined service in the **Service Name** field, this field will not be configurable.
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.

Table 61 Security > Parental Control > Add/Edit new rules > Add/Edit new service (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your settings with the EMG6765-Q10A.
Back	Click **Back** to return to the previous screen.

20.3 Technical Reference

The following section contains additional technical information about the EMG6765-Q10A features described in this chapter.

20.3.1 Customizing Keyword Blocking URL Checking

You can use commands to set how much of a website’s URL the content filter is to check for keyword blocking. See the appendices for information on how to access and use the command interpreter.

Domain Name or IP Address URL Checking

By default, the EMG6765-Q10A checks the URL’s domain name or IP address when performing keyword blocking.

This means that the EMG6765-Q10A checks the characters that come before the first slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, content filtering only searches for keywords within www.zyxel.com.tw.

Full Path URL Checking

Full path URL checking has the EMG6765-Q10A check the characters that come before the last slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, full path URL checking searches for keywords within www.zyxel.com.tw/news/.

Use the `ip urlfilter customize actionFlags 6 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's full path.

File Name URL Checking

Filename URL checking has the EMG6765-Q10A check all of the characters in the URL.

For example, filename URL checking searches for keywords within the URL www.zyxel.com.tw/news/pressroom.php.

Use the `ip urlfilter customize actionFlags 8 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's complete filename.

CHAPTER 21 Bandwidth Management

21.1 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 EMG6765-Q10A 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 EMG6765-Q10A 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.

21.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth (Section 21.3 on page 144).
- The **Queue Setup** screen lets you configure QoS queue assignment (Section 21.4 on page 145).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers (Section 21.5 on page 147).

21.2 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.

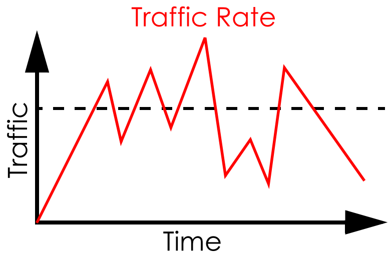
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

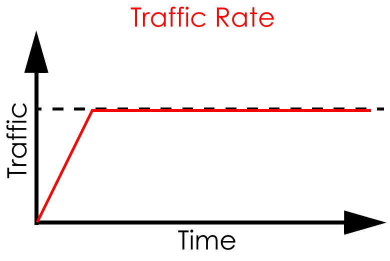
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or 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 EMG6765-Q10A uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



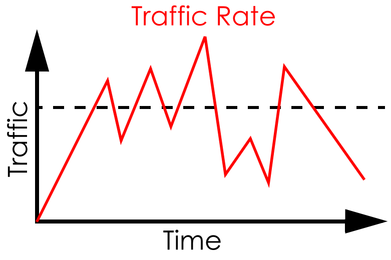
(Before Traffic Shaping)



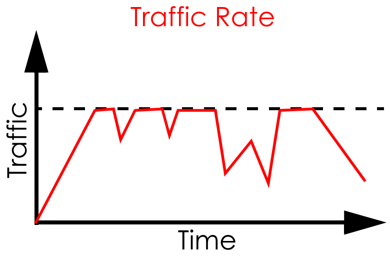
(After Traffic Shaping)

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)

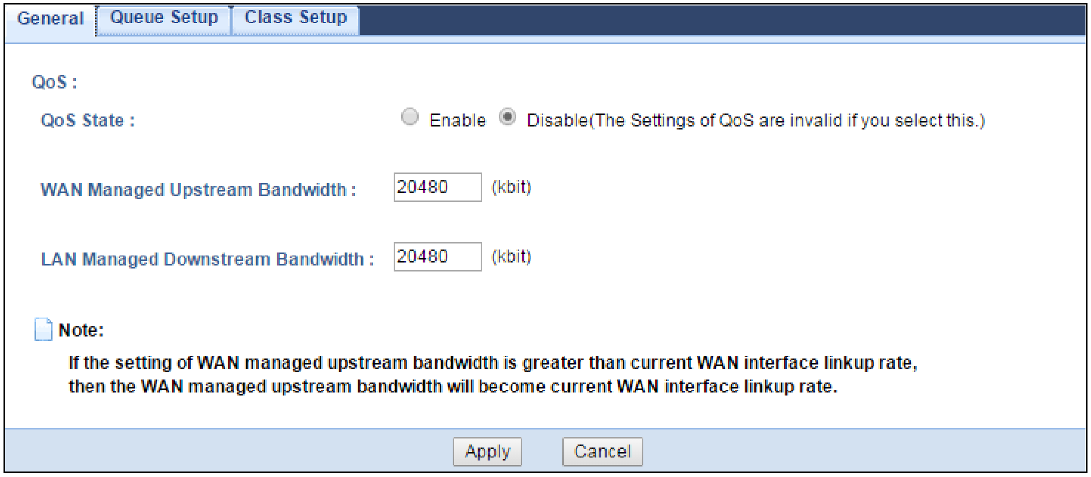
The EMG6765-Q10A supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Maker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See Section 21.6 on page 150 for more information on each metering algorithm.

21.3 Bandwidth MGMT General Screen

Click **Management > Bandwidth MGMT > General** to open the screen as shown next.

Use this screen to enable or disable QoS and set the upstream bandwidth. See Section 21.1 on page 142 for more information.

Figure 81 Management > Bandwidth MGMT > General



QoS :

QoS State : ○ Enable ● Disable(The Settings of QoS are invalid if you select this.)

WAN Managed Upstream Bandwidth : 20480 (kbit)

LAN Managed Downstream Bandwidth : 20480 (kbit)

Note:

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 62 Management > Bandwidth MGMT > General

LABEL	DESCRIPTION
QoS	
QoS State	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 set this number higher than the interfaces' actual transmission speed. The EMG6765-Q10A uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed. You can also set this number lower than the interfaces' actual transmission speed. This will cause the EMG6765-Q10A to not use some of the interfaces' available bandwidth. If you leave this field blank, the EMG6765-Q10A 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 EMG6765-Q10A to not use some of the interfaces' available bandwidth. If you leave this field blank, the EMG6765-Q10A automatically sets this to the LAN interfaces' maximum supported connection speed.

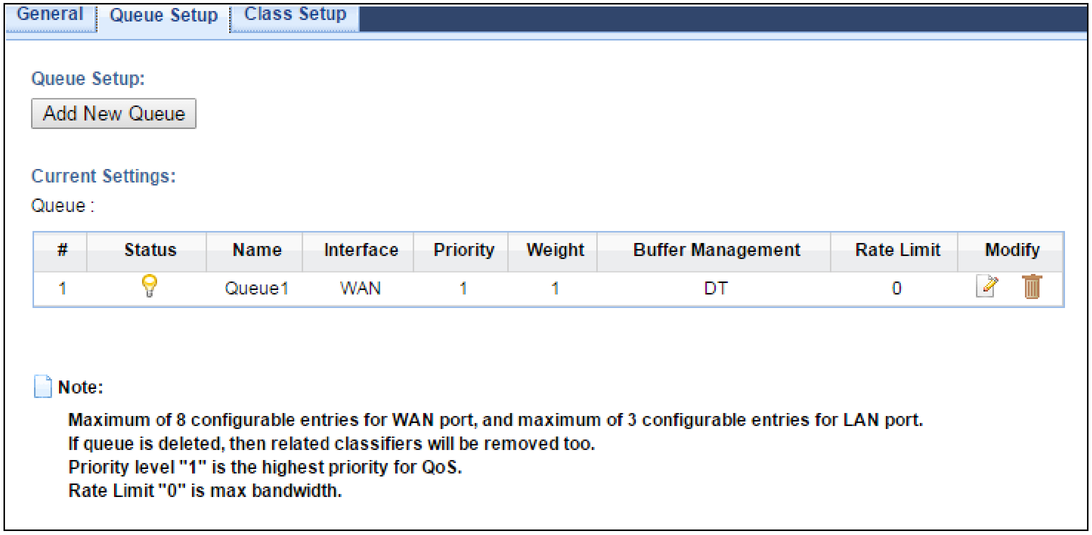
Table 62 Management > Bandwidth MGMT > General (continued) (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

21.4 The Queue Setup Screen

Use this screen to configure QoS queue assignment. Click **Management > Bandwidth MGMT > Queue Setup** to open the screen as shown next.

Figure 82 Management > Bandwidth MGMT > Queue Setup



#	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit	Modify
1	💡	Queue1	WAN	1	1	DT	0	✎ 🗑

Note:

Maximum of 8 configurable entries for WAN port, and maximum of 3 configurable entries for LAN port.
If queue is deleted, then related classifiers will be removed too.
Priority level "1" is the highest priority for QoS.
Rate Limit "0" is max bandwidth.

The following table describes the labels in this screen.

Table 63 Management > Bandwidth MGMT > Queue Setup

LABEL	DESCRIPTION
Queue Setup	
Add new Queue	Click this button to create a new queue entry.
Current Settings	
Queue	
#	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 EMG6765-Q10A'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 EMG6765-Q10A should handle packets when it receives too many (network congestion).

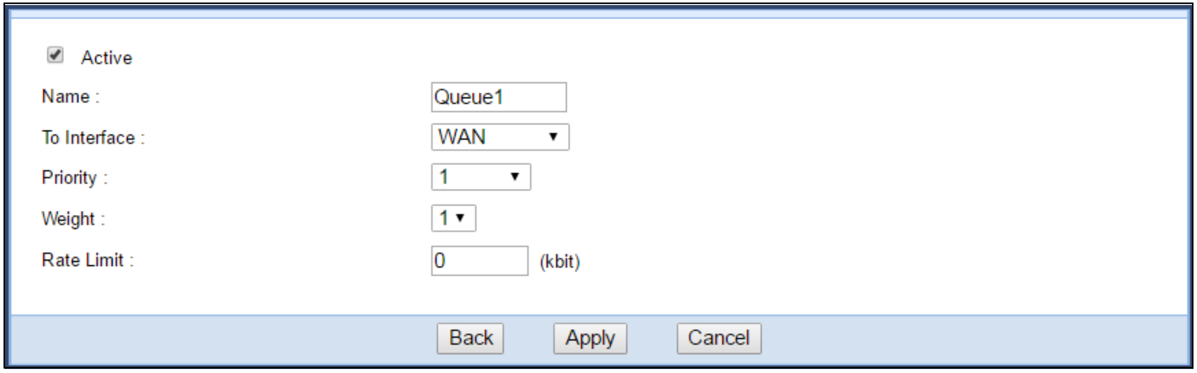
Table 63 Management > Bandwidth MGMT > Queue Setup (continued)

LABEL	DESCRIPTION
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.

21.4.1 Add/Edit a Queue

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

Figure 83 Management > Bandwidth MGMT > Queue Setup: Add/Edit new queue



☑ Active

Name :	Queue1
To Interface :	WAN
Priority :	1
Weight :	1
Rate Limit :	0 (kbit)

The following table describes the labels in this screen.

Table 64 Management > Bandwidth MGMT > Queue Setup: Add/Edit new queue

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue. Note that \"<>%\\^[]`\+\$\,='#&@.:() are not allowed.
To Interface	Select the interface to which this queue is applied.
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 EMG6765-Q10A divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
Back	Click this to return to the previous screen.
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

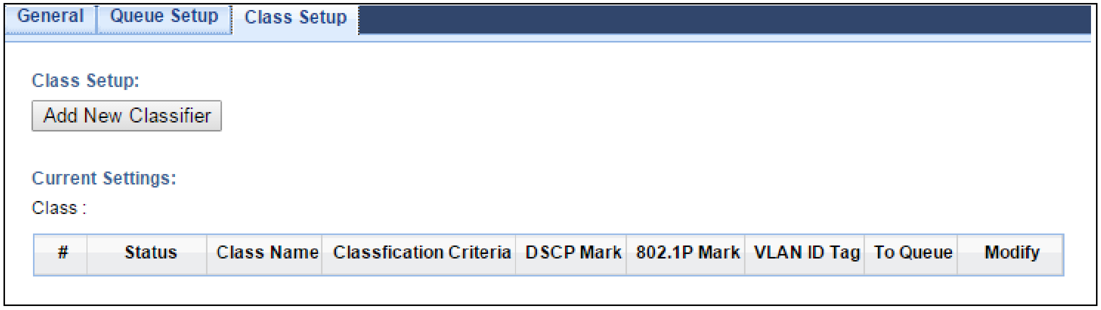
21.5 The Class Setup Screen

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 EMG6765-Q10A 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 **Management > Bandwidth MGMT > Class Setup** to open the following screen.

Figure 84 Management > Bandwidth MGMT > Class Setup



#	Status	Class Name	Classfication Criteria	DSCP Mark	802.1P Mark	VLAN ID Tag	To Queue	Modify

The following table describes the labels in this screen.

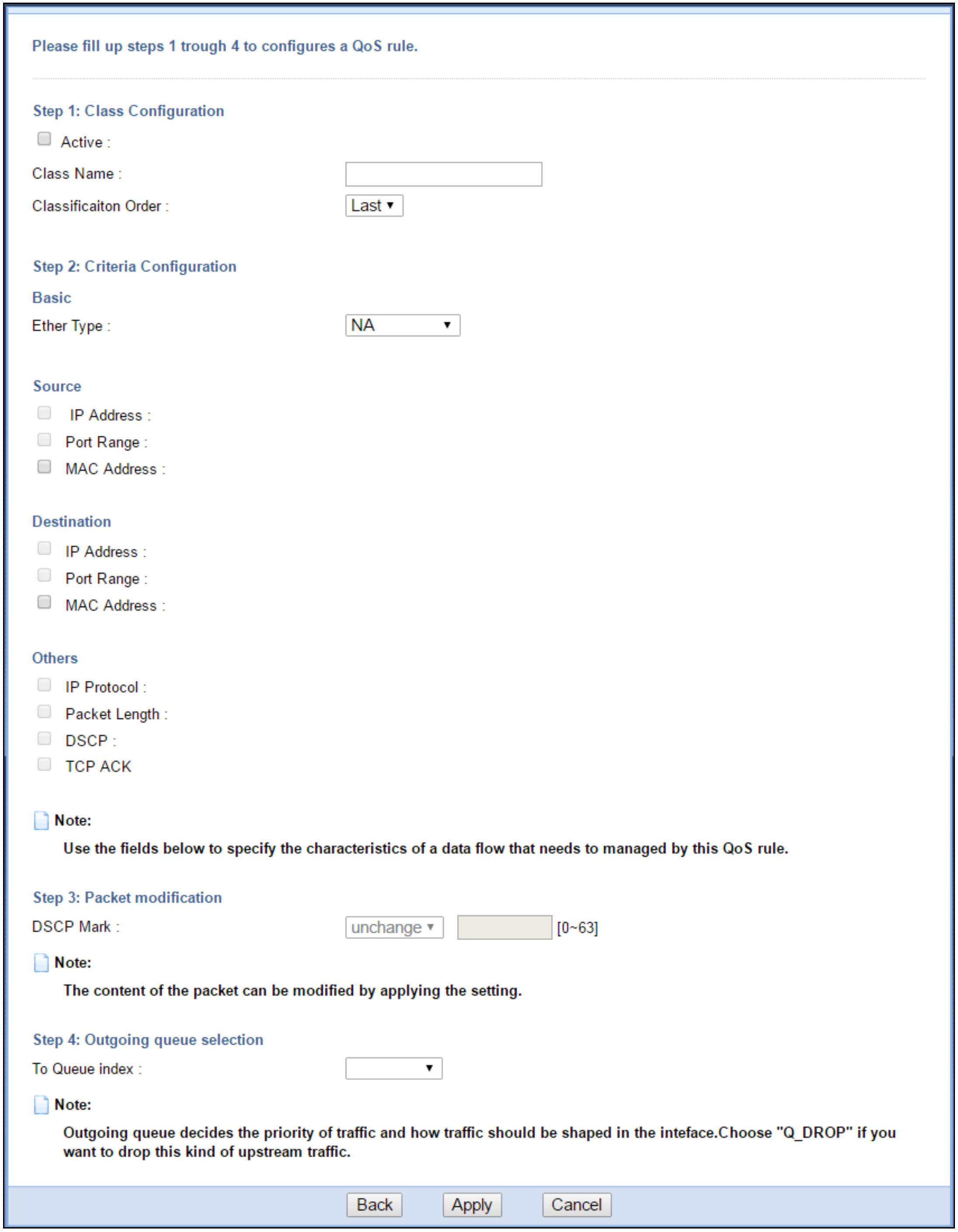
Table 65 Management > Bandwidth MGMT > Class Setup

LABEL	DESCRIPTION
Class Setup	
Add new Classifier	Click this to create a new classifier.
Current Settings	
Class	
#	This is the index number of the entry.
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.

21.5.1 Add/Edit a Classifier

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

Figure 85 Management > Bandwidth MGMT > Class Setup: Add/Edit new class



Please fill up steps 1 trough 4 to configures a QoS rule.

Step 1: Class Configuration

□ Active :

Class Name :

Classificaiton Order : Last ▾

Step 2: Criteria Configuration

Basic

Ether Type : NA ▾

Source

□ IP Address :

□ Port Range :

□ MAC Address :

Destination

□ IP Address :

□ Port Range :

□ MAC Address :

Others

□ IP Protocol :

□ Packet Length :

□ DSCP :

□ TCP ACK

Note:

Use the fields below to specify the characteristics of a data flow that needs to managed by this QoS rule.

Step 3: Packet modification

DSCP Mark : unchange ▾ [0~63]

Note:

The content of the packet can be modified by applying the setting.

Step 4: Outgoing queue selection

To Queue index : ▾

Note:

Outgoing queue decides the priority of traffic and how traffic should be shaped in the inteface.Choose "Q_DROP" if you want to drop this kind of upstream traffic.

The following table describes the labels in this screen.

Table 66 Management > Bandwidth MGMT > Class Setup: Add/Edit new class

LABEL	DESCRIPTION
Step 1: Class Configuration	
Active	Select this to enable 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.
Step 2: Criteria Configuration	
Basic	
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select **ARP**, you also need to configure source or destination MAC address. If you select **802.1Q**, you can configure an 802.1p priority level.
Source	
IP 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 Netmask	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 Address	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	
IP 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 Netmask	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 Address	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.

Table 66 Management > Bandwidth MGMT > Class Setup: Add/Edit new class

LABEL	DESCRIPTION
Others	
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.
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.
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.
Step 3: Packet modification	
DSCP Mark	This field is available only when you select **IP** in the **Ether Type** field. If you select **Mark**, enter a DSCP value with which the EMG6765-Q10A replaces the DSCP field in the packets. If you select **Unchange**, the EMG6765-Q10A keep the DSCP field in the packets.
Step 4: 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.
Back	Click this to return to the previous screen.
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

21.6 Technical Reference

The following section contains additional technical information about the EMG6765-Q10A 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 67 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 EMG6765-Q10A, the EMG6765-Q10A 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 EMG6765-Q10A. On the EMG6765-Q10A, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 68 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 EMG6765-Q10A stops transmitting until enough tokens are generated.
- If not enough tokens are available, the EMG6765-Q10A 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 EMG6765-Q10A 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 EMG6765-Q10A 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 EMG6765-Q10A 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 22
Universal Plug-and-Play (UPnP)

22.1 Overview

This chapter introduces the UPnP feature in the web configurator.

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.

22.2 What You Need to Know

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.

22.2.1 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 NAT chapter for more information on NAT.

22.2.2 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 EMG6765-Q10A allows multicast messages on the LAN only.

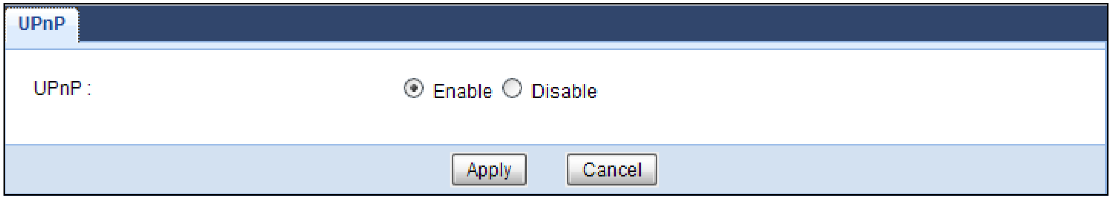
All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

22.3 UPnP Screen

Use this screen to enable UPnP on your EMG6765-Q10A.

Click **Management > UPnP** to display the screen shown next.

Figure 86 Management > UPnP



UPnP

UPnP : ● Enable ○ Disable

The following table describes the fields in this screen.

Table 69 Management > 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 EMG6765-Q10A's IP address (although you must still enter the password to access the web configurator).
Apply	Click **Apply** to save the setting to the EMG6765-Q10A.
Cancel	Click **Cancel** to return to the previously saved settings.

22.4 Technical Reference

The sections show examples of using UPnP.

22.4.1 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the EMG6765-Q10A.

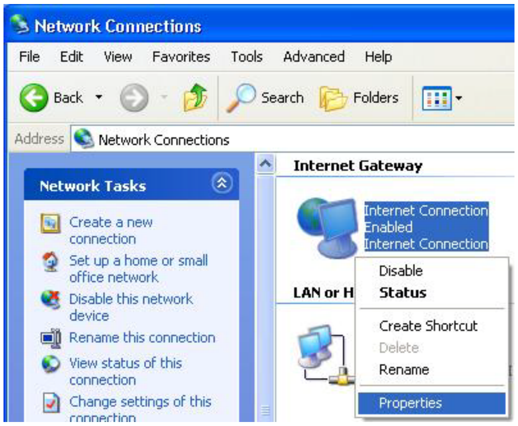
Make sure the computer is connected to a LAN port of the EMG6765-Q10A. Turn on your computer and the EMG6765-Q10A.

22.4.1.1 Auto-discover Your UPnP-enabled Network Device

1 Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

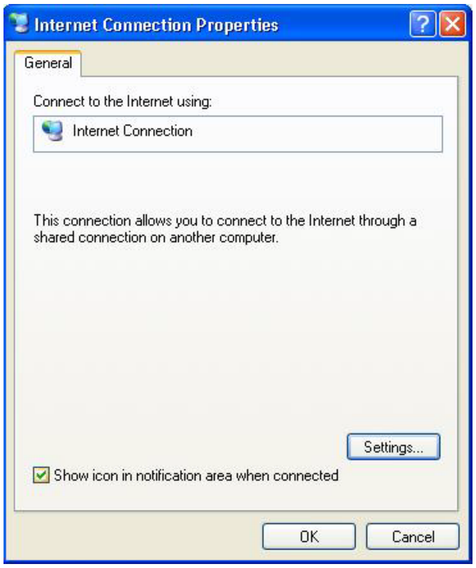
2 Right-click the icon and select **Properties**.

Figure 87 Network Connections



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 88 Internet Connection Properties



Connect to the Internet using:

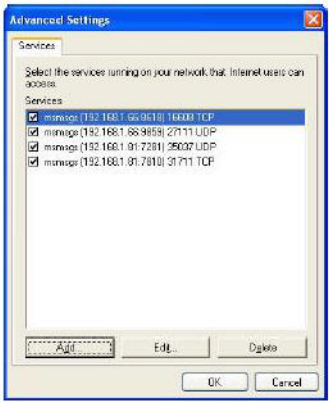
Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 89 Internet Connection Properties: Advanced Settings

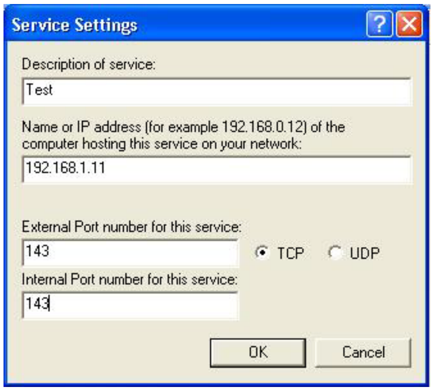


Select the services running on your network that Internet users can access.

Services

☑ msmsgs (192.168.1.66:9618) 16608 TCP
☑ msmsgs (192.168.1.66:9859) 27111 UDP
☑ msmsgs (192.168.1.81:7281) 35037 UDP
☑ msmsgs (192.168.1.81:7810) 31711 TCP

Figure 90 Internet Connection Properties: Advanced Settings: Add



Service Settings

Description of service: Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network: 192.168.1.11

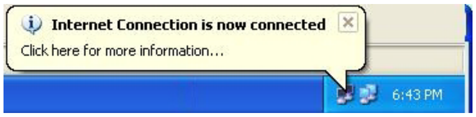
External Port number for this service: 143 ● TCP ○ UDP

Internal Port number for this service: 143

Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

5 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 91 System Tray Icon

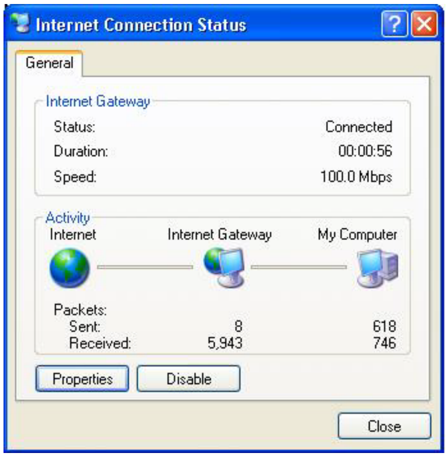


Internet Connection is now connected

Click here for more information...

6 Double-click on the icon to display your current Internet connection status.

Figure 92 Internet Connection Status



Internet Connection Status

General

Internet Gateway

Status:	Connected
Duration:	00:00:56
Speed:	100.0 Mbps

Activity

Packets:		
Sent:	8	618
Received:	5,943	746

22.4.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the EMG6765-Q10A without finding out the IP address of the EMG6765-Q10A first. This comes helpful if you do not know the IP address of the EMG6765-Q10A.

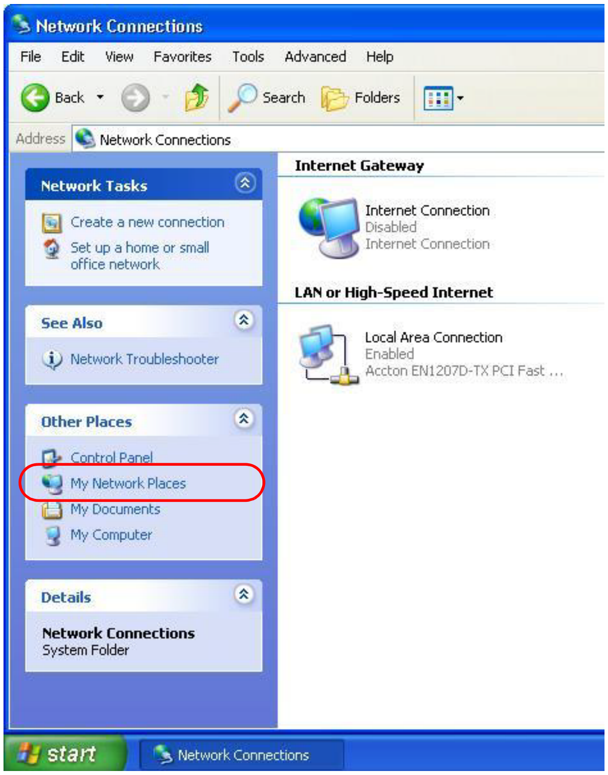
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

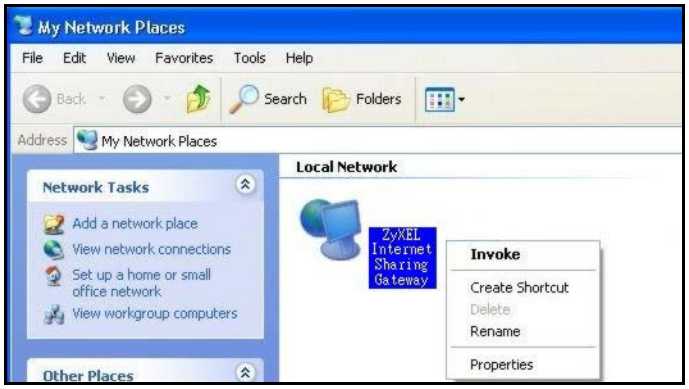
Figure 93 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

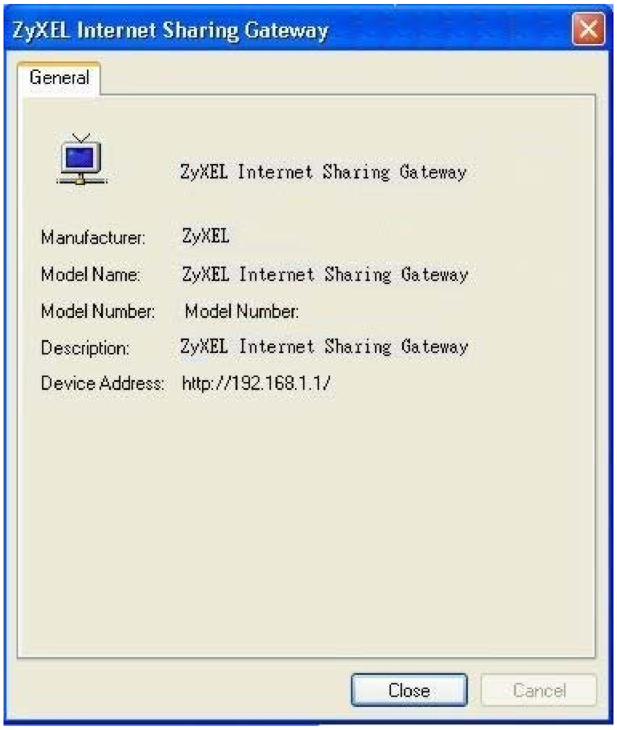
5 Right-click on the icon for your EMG6765-Q10A and select **Invoke**. The web configurator login screen displays.

Figure 94 Network Connections: My Network Places



6 Right-click on the icon for your EMG6765-Q10A and select **Properties**. A properties window displays with basic information about the EMG6765-Q10A.

Figure 95 Network Connections: My Network Places: Properties: Example



ZyXEL Internet Sharing Gateway

ZyXEL Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number: Model Number:

Description: ZyXEL Internet Sharing Gateway

Device Address: http://192.168.1.1/

CHAPTER 23
USB Media Sharing

23.1 Overview

This chapter describes how to configure the media sharing settings on the EMG6765-Q10A.

Note: The read and write performance may be affected by amount of file-sharing traffic on your network, type of connected USB device and your USB version (1.1 or 2.0).

Media Server

You can set up your EMG6765-Q10A to act as a media server to provide media (like video) to DLNA-compliant players, such as Windows Media Player, Zyxel DMAs (Digital Media Adapters), Xboxes or PS3s. The media server and clients must have IP addresses in the same subnet.

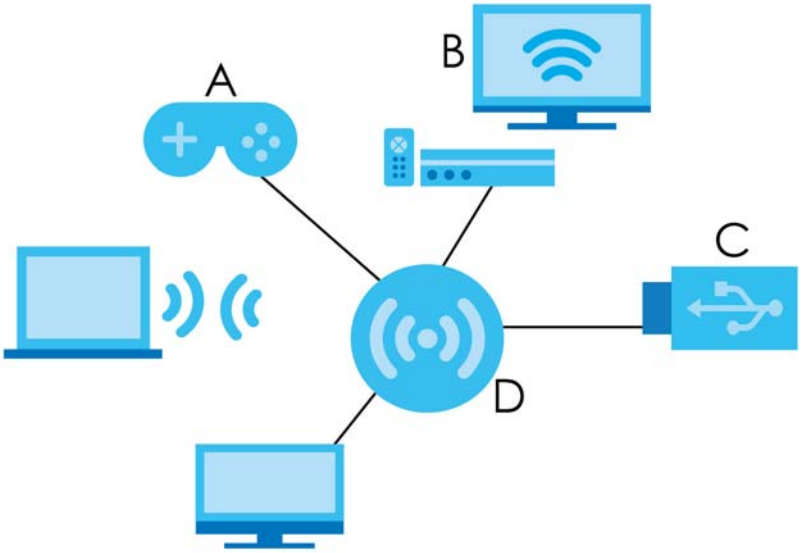
The EMG6765-Q10A media server enables you to:

- Publish all folders for everyone to play media files in the USB storage device connected to the EMG6765-Q10A.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published folders. No user name and password nor other form of security is required.

The following figure is an overview of the EMG6765-Q10A's media server feature. DLNA devices **A** and **B** can access and play files on a USB device (**C**) which is connected to the EMG6765-Q10A (**D**).

Figure 96 Media Server Overview

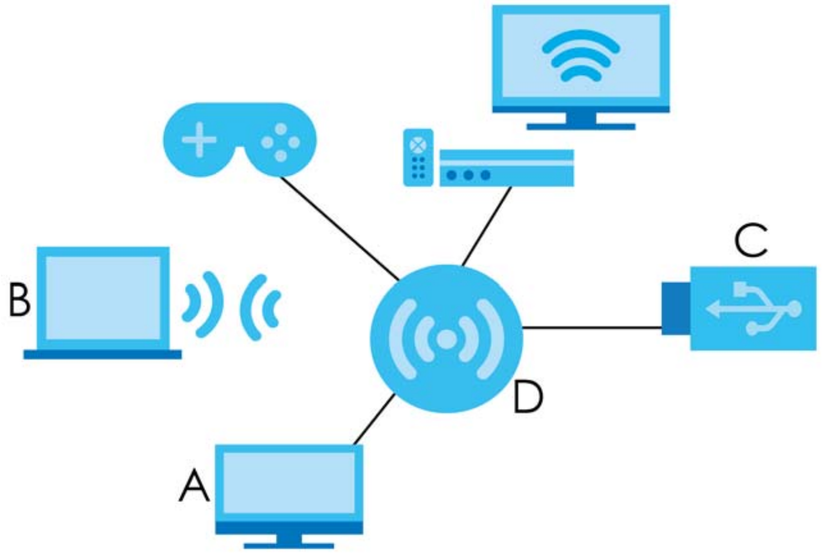


File-Sharing Server

You can also share files on a USB memory stick or hard drive connected to your EMG6765-Q10A with users on your network.

The following figure is an overview of the EMG6765-Q10A's file-sharing server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the EMG6765-Q10A (**D**).

Figure 97 File Sharing Overview



23.2 What You Can Do

- Use the **DLNA** screen to use the EMG6765-Q10A as a media server and allow DLNA-compliant devices to play media files stored in the attached USB device (Section 23.5 on page 164).
- Use the **SAMBA** screen to enable file-sharing via the EMG6765-Q10A using Windows Explorer or the workgroup name. This screen also allow you to configure the workgroup name and create user accounts (Section 23.6 on page 164).
- Use the **FTP** screen to allow file sharing via the EMG6765-Q10A using FTP and create user accounts (Section 23.7 on page 166).

23.3 What You Need To Know

DLNA

The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network. DLNA clients play files stored on DLNA servers. The EMG6765-Q10A can function as a DLNA-compliant media server and stream files to DLNA-compliant media clients without any configuration.

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file-sharing feature on your EMG6765-Q10A supports New Technology File System (NTFS), File Allocation Table (FAT) and FAT32 file systems.

Windows/CIFS

Common Internet File System (CIFS) is a standard protocol supported by most operating systems in order to share files across the network.

CIFS runs over TCP/IP but uses the SMB (Server Message Block) protocol found in Microsoft Windows for file and printer access; therefore, CIFS will allow all applications, not just Web browsers, to open and share files across the Internet.

The EMG6765-Q10A uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the EMG6765-Q10A. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

Samba

SMB is a client-server protocol used by Microsoft Windows systems for sharing files, printers, and so on.

Samba is a free SMB server that runs on most Unix and Unix-like systems. It provides an implementation of an SMB client and server for use with non-Microsoft operating systems.

File Transfer Protocol

This is a method of transferring data from one computer to another over a network such as the Internet.

23.4 Before You Begin

Make sure the EMG6765-Q10A is connected to your network and turned on.

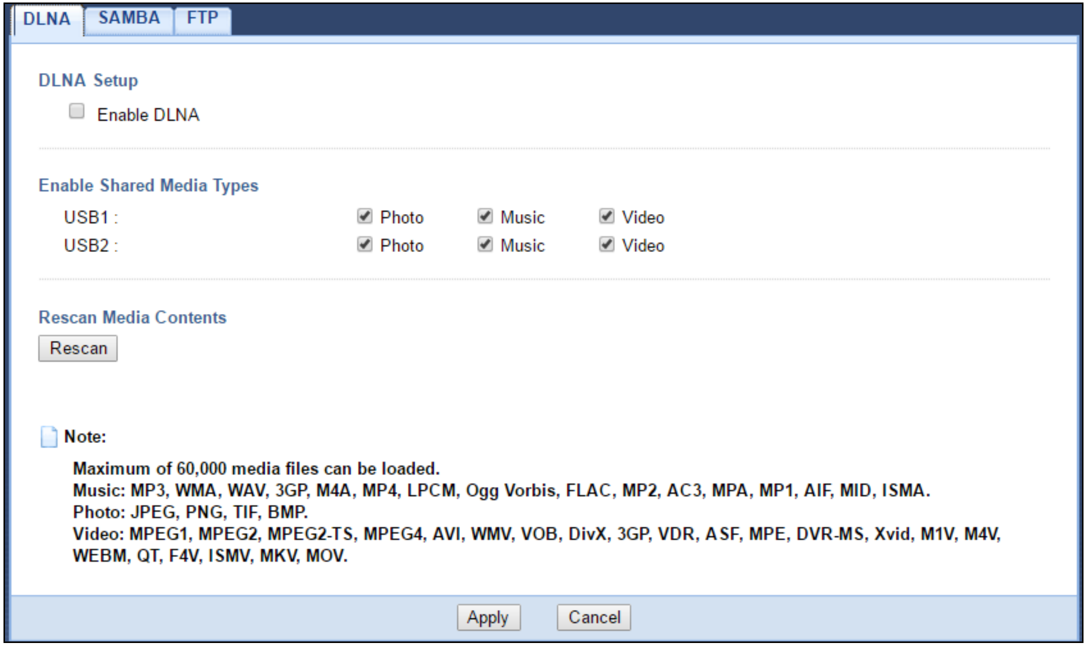
1. Connect the USB device to one of the EMG6765-Q10A's USB ports.
2. The EMG6765-Q10A detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the EMG6765-Q10A, see the troubleshooting for suggestions.

23.5 DLNA Screen

Use this screen to have the EMG6765-Q10A act as a DLNA-compliant media server that lets DLNA-compliant media clients on your network play video, music, and photos from the EMG6765-Q10A (without having to copy them to another computer). Click **Management > USB Media Sharing > DLNA**.

Figure 98 Management > USB Media Sharing > DLNA



DLNA Setup

□ Enable DLNA

Enable Shared Media Types

USB1 : ☑ Photo ☑ Music ☑ Video

USB2 : ☑ Photo ☑ Music ☑ Video

Rescan Media Contents

Note:

Maximum of 60,000 media files can be loaded.
Music: MP3, WMA, WAV, 3GP, M4A, MP4, LPCM, Ogg Vorbis, FLAC, MP2, AC3, MPA, MP1, AIF, MID, ISMA.
Photo: JPEG, PNG, TIF, BMP.
Video: MPEG1, MPEG2, MPEG2-TS, MPEG4, AVI, WMV, VOB, DivX, 3GP, VDR, ASF, MPE, DVR-MS, Xvid, M1V, M4V, WEBM, QT, F4V, ISMV, MKV, MOV.

The following table describes the labels in this screen.

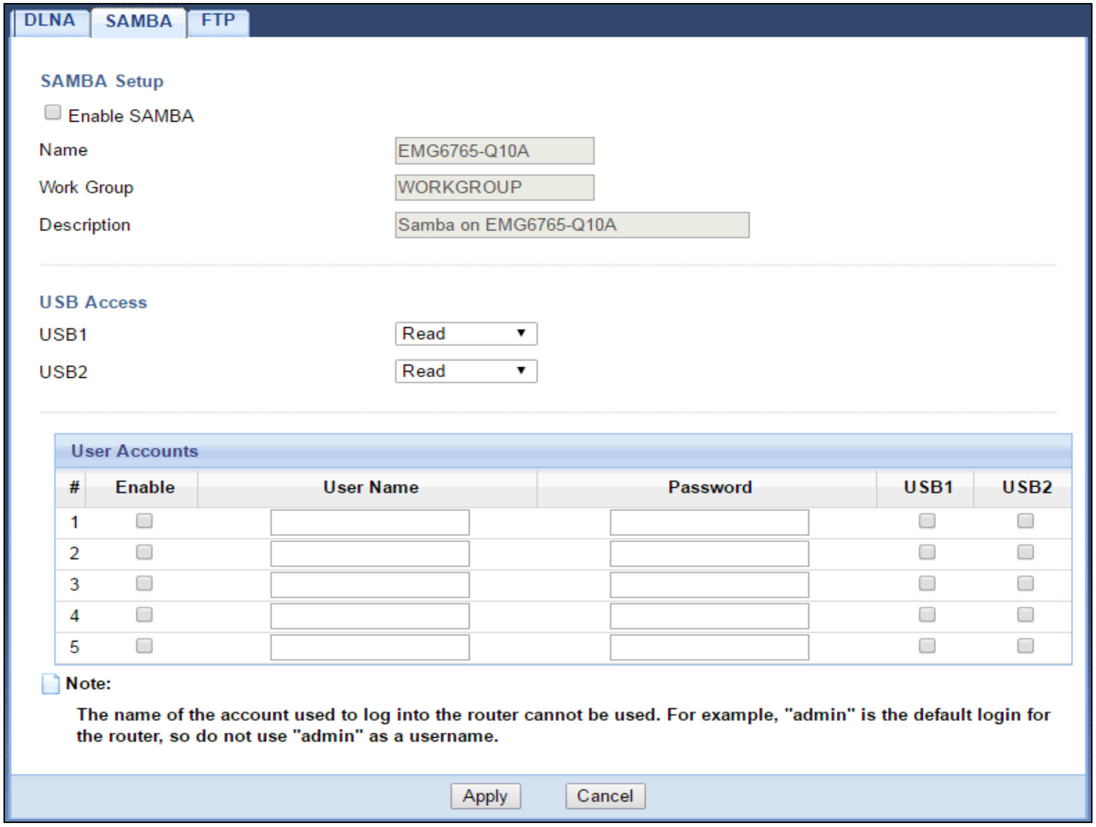
Table 70 Management > USB Media Sharing > DLNA

LABEL	DESCRIPTION
DLNA Setup	
Enable DLNA	Select this to have the EMG6765-Q10A function as a DLNA-compliant media server.
Enable Shared Media Types	
USB1/2	Select the media type that you want to share on the USB device connected to the EMG6765-Q10A's USB port.
Rescan Media Contents	
Rescan	Click this button to have the EMG6765-Q10A scan the media files on the connected USB device and do indexing of the file list again so that DLNA clients can find the new files if any.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.6 SAMBA Screen

Use this screen to set up file-sharing via the EMG6765-Q10A using Windows Explorer or the workgroup name. You can also configure the work group name and create file-sharing user accounts. Click **Management > USB Media Sharing > SAMBA**.

Figure 99 Management > USB Media Sharing > SAMBA



SAMBA Setup

☐ Enable SAMBA

Name	EMG6765-Q10A
Work Group	WORKGROUP
Description	Samba on EMG6765-Q10A

USB Access

USB1	Read ▾
USB2	Read ▾

User Accounts

#	Enable	User Name	Password	USB1	USB2
1	☐			☐	☐
2	☐			☐	☐
3	☐			☐	☐
4	☐			☐	☐
5	☐			☐	☐

Note:

The name of the account used to log into the router cannot be used. For example, "admin" is the default login for the router, so do not use "admin" as a username.

The following table describes the labels in this screen.

Table 71 Management > USB Media Sharing > SAMBA

LABEL	DESCRIPTION
Samba Setup	
Enable SAMBA	Select this to enable file sharing through the EMG6765-Q10A using Windows Explorer or by browsing to your work group.
Name	Specify the name to identify the EMG6765-Q10A in a work group.
Work Group	You can add the EMG6765-Q10A to an existing or a new workgroup on your network. Enter the name of the workgroup which your EMG6765-Q10A automatically joins. You can set the EMG6765-Q10A's workgroup name to be exactly the same as the workgroup name to which your computer belongs to. Note: The EMG6765-Q10A will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.
Description	Enter the description of the EMG6765-Q10A in a work group.
USB Access	
USB1/2	Specify the user's access rights to the USB storage device which is connected to the EMG6765-Q10A's USB port. **Read & Write** - The user has read and write rights, meaning that the user can create and edit the files on the connected USB device. **Read** - The user has read rights only and can not create or edit the files on the connected USB device.

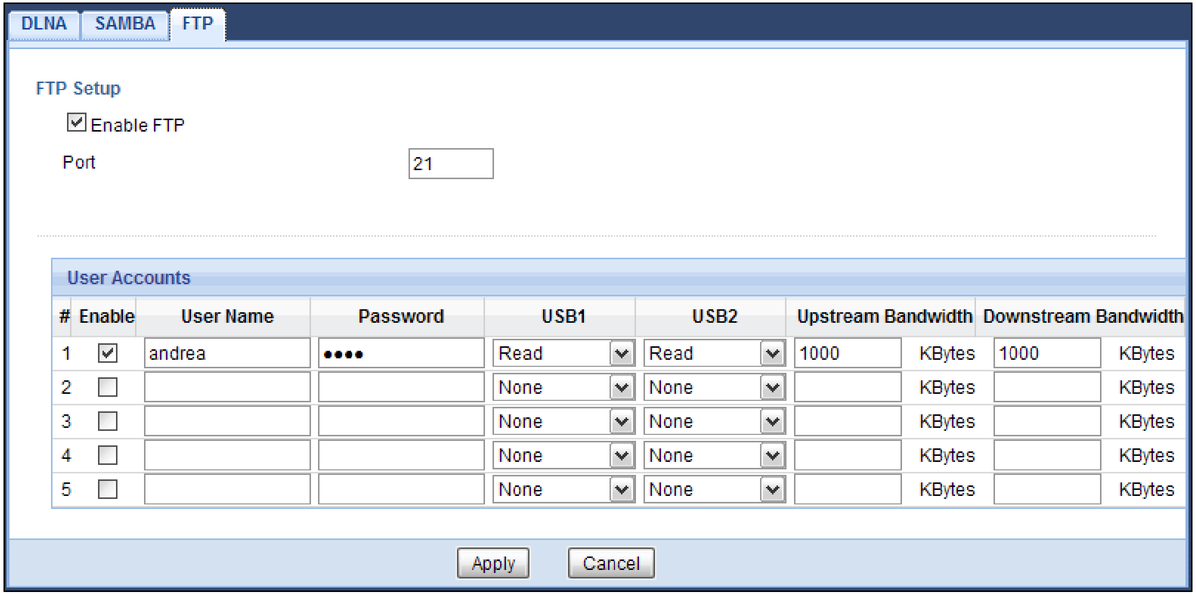
Table 71 Management > USB Media Sharing > SAMBA (continued)

LABEL	DESCRIPTION
User Accounts	Before you can share files you need a user account. Configure the following fields to set up a file-sharing account.
#	This is the index number of the user account.
Enable	This field displays whether a user account is activated or not. Select the check box to enable the account. Clear the check box to disable the account.
User Name	Enter a user name that will be allowed to access the shared files. You can enter up to 20 characters. Only letters and numbers allowed.
Password	Enter the password used to access the shared files. You can enter up to 20 characters. Only letters and numbers are allowed. The password is case sensitive.
USB1/2	Select the USB port(s) of the EMG6765-Q10A. The configured user can access the files on the USB device(s) connected to the selected USB port(s) only.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.7 FTP Screen

Use this screen to set up file sharing via the EMG6765-Q10A using FTP and create user accounts. Click **Management > USB Media Sharing > FTP**.

Figure 100 Management > USB Media Sharing > FTP



FTP Setup

☑ Enable FTP

Port 21

User Accounts

#	Enable	User Name	Password	USB1	USB2	Upstream Bandwidth		Downstream Bandwidth	
1	☑	andrea	••••	Read	Read	1000	KBytes	1000	KBytes
2	☐			None	None		KBytes		KBytes
3	☐			None	None		KBytes		KBytes
4	☐			None	None		KBytes		KBytes
5	☐			None	None		KBytes		KBytes

The following table describes the labels in this screen.

Table 72 Management > USB Media Sharing > FTP

LABEL	DESCRIPTION
FTP Setup	
Enable FTP	Select this to enable the FTP server on the EMG6765-Q10A for file sharing using FTP.
Port	You may change the server port number for FTP if needed, however you must use the same port number in order to use that service for file sharing.

Table 72 Management > USB Media Sharing > FTP (continued)

LABEL	DESCRIPTION
User Accounts	Before you can share files you need a user account. Configure the following fields to set up a file-sharing account.
#	This is the index number of the user account.
Enable	This field displays whether a user account is activated or not. Select the check box to enable the account. Clear the check box to disable the account.
User Name	Enter a user name that will be allowed to access the shared files. You can enter up to 20 characters. Only letters and numbers allowed.
Password	Enter the password used to access the shared files. You can enter up to 20 characters. Only letters and numbers are allowed. The password is case sensitive.
USB1/2	Specify the user's access rights to the USB storage device which is connected to the EMG6765-Q10A's USB port. **Read & Write** - The user has read and write rights, meaning that the user can create and edit the files on the connected USB device. **Read** - The user has read rights only and can not create or edit the files on the connected USB device. **None** - The user cannot access the files on the USB device(s) connected to the USB port.
Upstream Bandwidth	Enter the maximum bandwidth (in Kbps) allowed for incoming FTP traffic.
Downstream Bandwidth	Enter the maximum bandwidth (in Kbps) allowed for outgoing FTP traffic.
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.8 Example of Accessing Your Shared Files From a Computer

You can use Windows Explorer or FTP to access the USB storage devices connected to the EMG6765-Q10A.

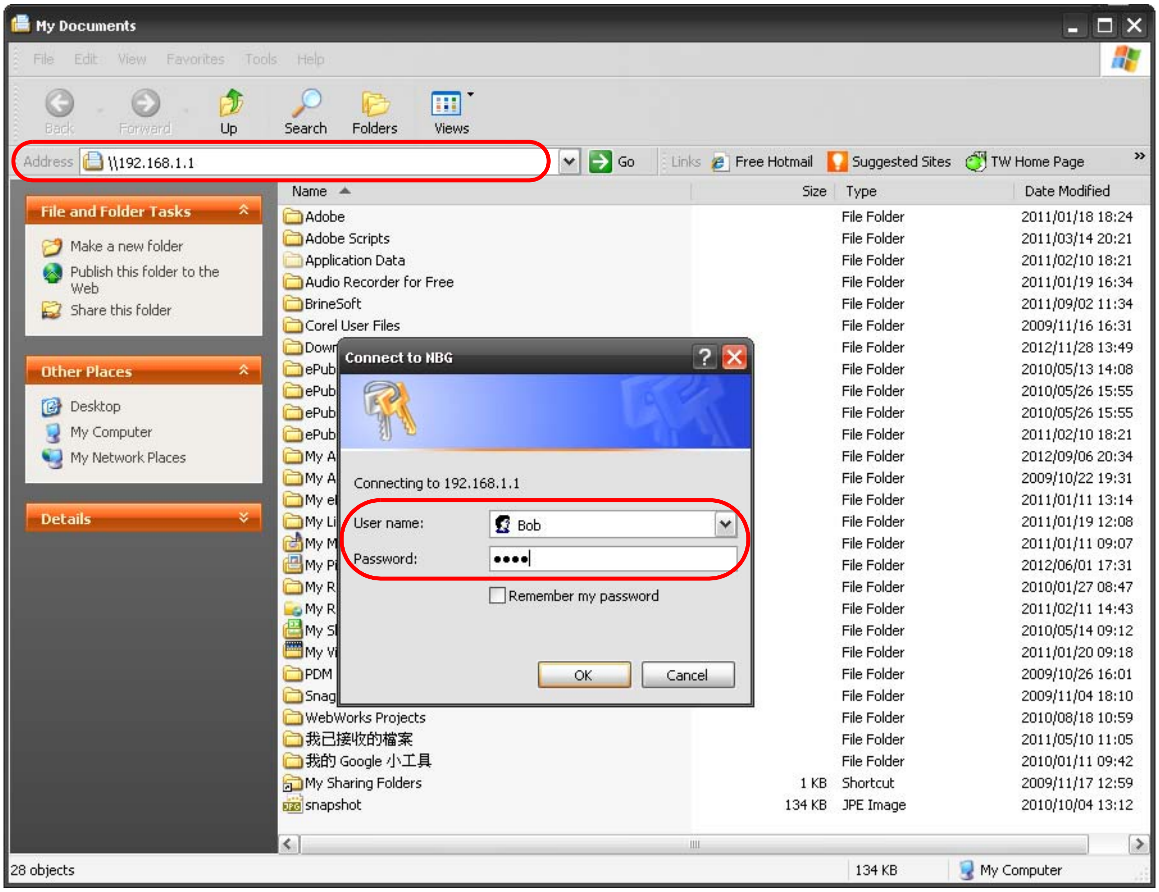
This example shows you how to use Microsoft's Windows XP to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

23.8.1 Use Windows Explorer to Share Files

You should have enabled file sharing and create a user account (Bob/1234 for example) with read and write access to USB 1 in the **USB Media Sharing > SAMBA** screen.

Open Windows Explorer to access the connected USB device using either Windows Explorer browser or by browsing to your workgroup.

1 In Windows Explorer’s Address bar type a double backslash “\\” followed by the IP address of the EMG6765-Q10A (the default IP address of the EMG6765-Q10A in router mode is 192.168.1.1) and press [ENTER]. A screen asking for password authentication appears. Type the user name and password (Bob and 1234 in this example) and click **OK**.



Address \\192.168.1.1

Name	Size	Type	Date Modified
Adobe		File Folder	2011/01/18 18:24
Adobe Scripts		File Folder	2011/03/14 20:21
Application Data		File Folder	2011/02/10 18:21
Audio Recorder for Free		File Folder	2011/01/19 16:34
BrineSoft		File Folder	2011/09/02 11:34
Corel User Files		File Folder	2009/11/16 16:31
Down		File Folder	2012/11/28 13:49
ePub		File Folder	2010/05/13 14:08
ePub		File Folder	2010/05/26 15:55
ePub		File Folder	2010/05/26 15:55
ePub		File Folder	2011/02/10 18:21
My A		File Folder	2012/09/06 20:34
My A		File Folder	2009/10/22 19:31
My e		File Folder	2011/01/11 13:14
My Li		File Folder	2011/01/19 12:08
My M		File Folder	2011/01/11 09:07
My Pi		File Folder	2012/06/01 17:31
My R		File Folder	2010/01/27 08:47
My R		File Folder	2011/02/11 14:43
My S		File Folder	2010/05/14 09:12
My Vi		File Folder	2011/01/20 09:18
PDM		File Folder	2009/10/26 16:01
Snag		File Folder	2009/11/04 18:10
WebWorks Projects		File Folder	2010/08/18 10:59
我已接收的檔案		File Folder	2011/05/10 11:05
我的 Google 小工具		File Folder	2010/01/11 09:42
My Sharing Folders	1 KB	Shortcut	2009/11/17 12:59
snapshot	134 KB	JPE Image	2010/10/04 13:12

Connecting to 192.168.1.1

User name: Bob

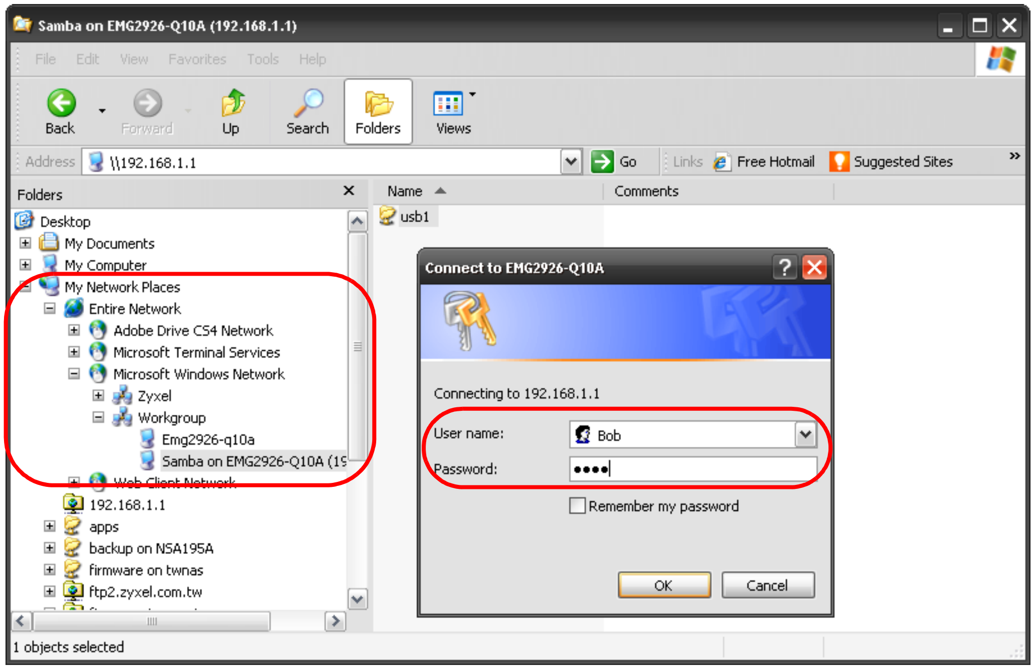
Password: ●●●●

□ Remember my password

28 objects 134 KB My Computer

Note: Once you log into the shared folder via your EMG6765-Q10A, you do not have to relogin unless you restart your computer.

2 You can also use the workgroup name to access files by browsing to the workgroup folder using the folder tree on the left side of the screen. It is located under **My Network Places**. In this example the workgroup name is the default “Workgroup”.



Samba on EMG2926-Q10A (192.168.1.1)

Address \\192.168.1.1

Connect to EMG2926-Q10A

Connecting to 192.168.1.1

User name: Bob

Password: ••••

□ Remember my password

1 objects selected

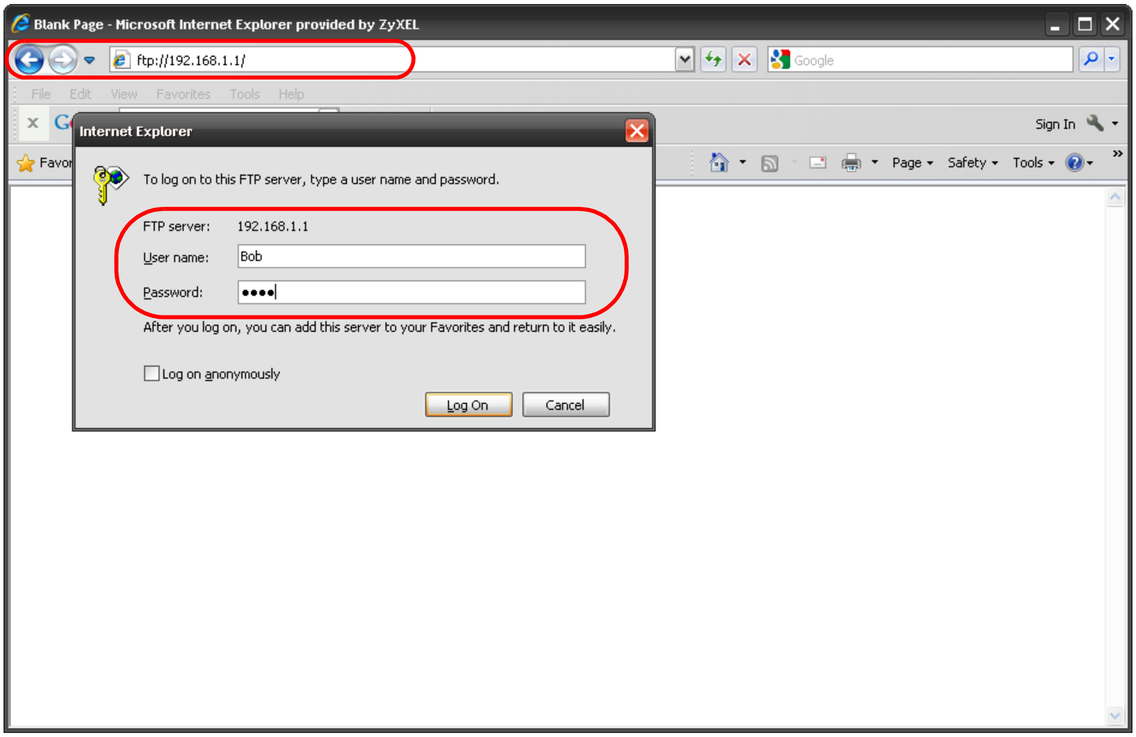
23.8.2 Use FTP to Share Files

You can use FTP to access the USB storage devices connected to the EMG6765-Q10A. In this example, we use the web browser to share files via FTP from the LAN. The way or screen you log into the FTP server (on the EMG6765-Q10A) varies depending on your FTP client. See your FTP client documentation for more information.

You should have enabled file sharing and create a user account (Bob/1234 for example) with read and write access to USB 1 in the **USB Media Sharing > FTP** screen.

1 In your web browser’s address or URL bar type “ftp://” followed by the IP address of the EMG6765-Q10A (the default LAN IP address of the EMG6765-Q10A in router mode is 192.168.1.1) and click **Go** or press [ENTER].

2 A screen asking for password authentication appears. Enter the user name and password (you configured in the **USB Media Sharing > FTP** screen) and click **Log On**.



To log on to this FTP server, type a user name and password.

FTP server: 192.168.1.1

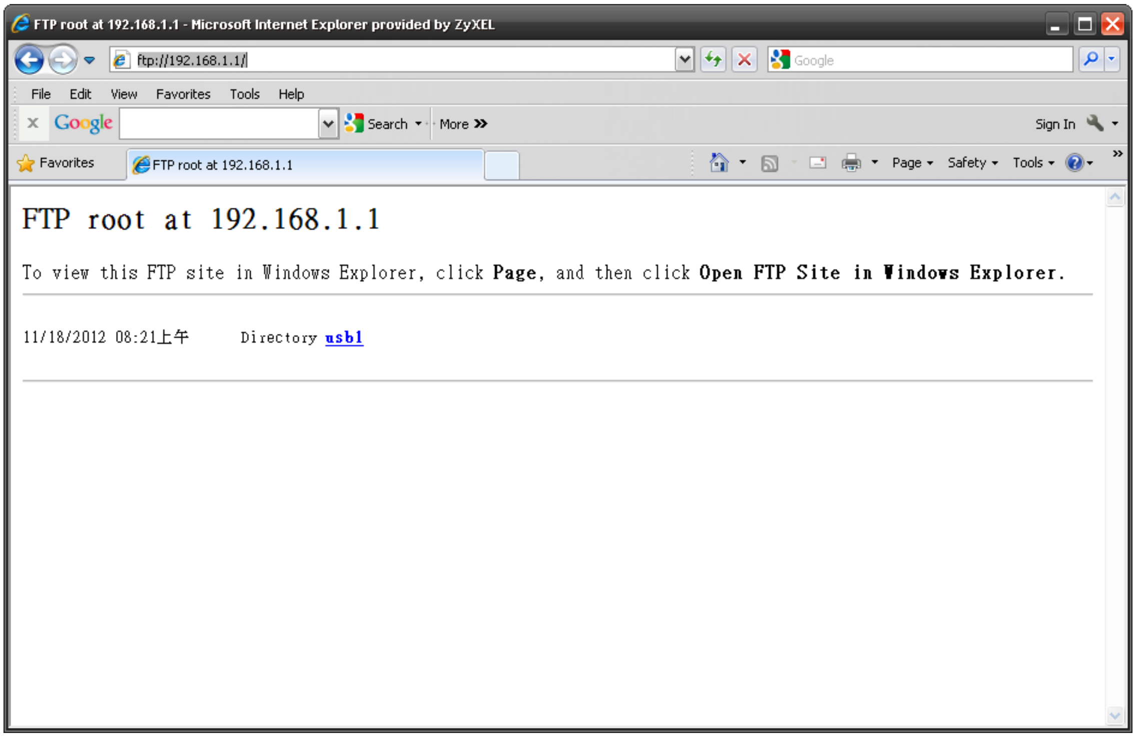
User name: Bob

Password: ••••

After you log on, you can add this server to your Favorites and return to it easily.

□ Log on anonymously

3 The screen changes and shows you the folder for the USB storage device connected to your EMG6765-Q10A. Double-click the folder to display the contents in it.



FTP root at 192.168.1.1

To view this FTP site in Windows Explorer, click **Page**, and then click **Open FTP Site in Windows Explorer**.

11/18/2012 08:21上午 Directory usb1

CHAPTER 24
Port Configuration

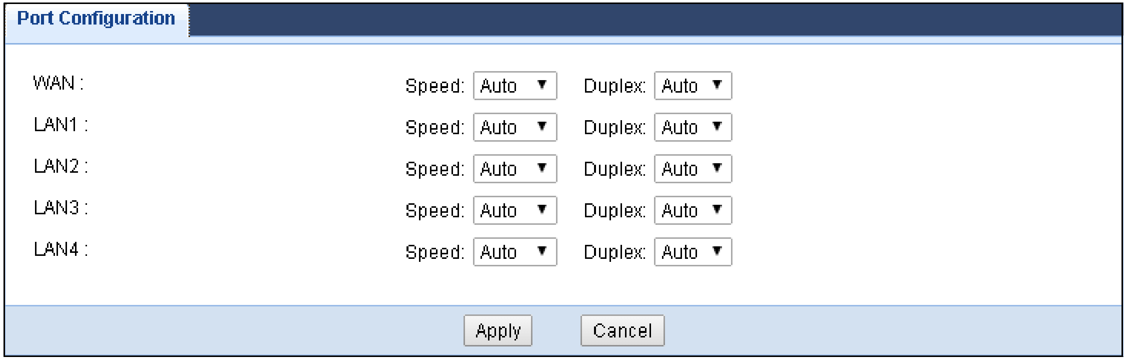
24.1 Overview

The EMG6765-Q10A has 1000Base-T auto-negotiating Ethernet ports. In 10/100/1000 Mbps Gigabit Ethernet, the speed can be 10 Mbps, 100 Mbps or 1000 Mbps. The duplex mode can be both half or full duplex. An auto-negotiating port can detect and adjust to the optimum Ethernet speed (10/100/1000 Mbps) and duplex mode (full duplex or half duplex) of the connected device.

24.2 Port Configuration Screen

Use this screen to configure the EMG6765-Q10A port speed and duplex settings. Click **Configuration** > **Management > Port Configuration**.

Figure 101 Management > Port Configuration



WAN : Speed: Auto Duplex: Auto

LAN1 : Speed: Auto Duplex: Auto

LAN2 : Speed: Auto Duplex: Auto

LAN3 : Speed: Auto Duplex: Auto

LAN4 : Speed: Auto Duplex: Auto

The following table describes the labels on this screen.

Table 73 Management > Port Configuration

LABEL	DESCRIPTION
WAN/LAN1~4	This field displays the Ethernet port of the EMG6765-Q10A.
Speed	Select the speed of the Ethernet connection on this port. The choices are **Auto**, **1000**, **100** and **10**. Selecting **Auto** (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed that both ends support. If the peer port does not support auto-negotiation or turns off this feature, the EMG6765-Q10A determines the connection speed by detecting the signal on the cable and using half duplex mode.
Duplex	Select the duplex mode of the Ethernet connection on this port. The choices are **Auto**, **Full** and **Half**. Selecting **Auto** (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the duplex mode that both ends support. If the peer port does not support auto-negotiation or turns off this feature, the EMG6765-Q10A determines the connection speed by detecting the signal on the cable and using half duplex mode.

Table 73   Management > Port Configuration (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes with the EMG6765-Q10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 25 Maintenance

25.1 Overview

This chapter provides information on the **Maintenance** screens.

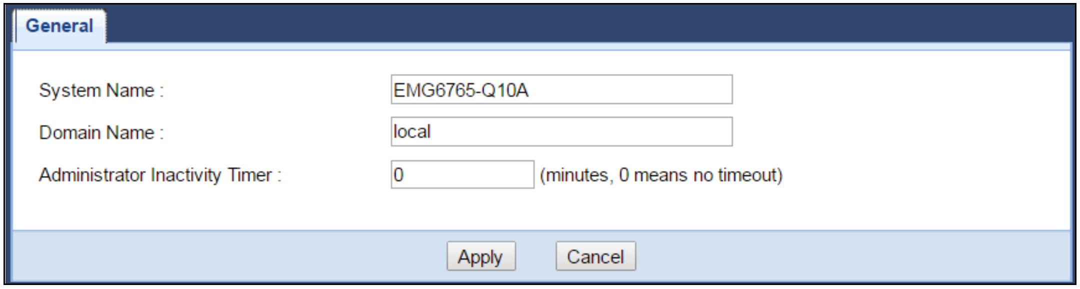
25.2 What You Can Do

- Use the **General** screen to set the system name, the domain name and the timeout period of the management session (Section 25.3 on page 173).
- Use the **Account** screen to change your EMG6765-Q10A's system password (Section 25.4 on page 174).
- Use the **Time** screen to change your EMG6765-Q10A's time and date (Section 25.5 on page 175).
- Use the **Firmware Upgrade** screen to upload firmware to your EMG6765-Q10A (Section 25.6 on page 177).
- Use the **Backup/Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration (Section 25.8 on page 180).
- Use the **Restart** screen to reboot the EMG6765-Q10A without turning the power off (Section 25.8 on page 180).
- Use the **Language** screen to change the language for the Web Configurator (Section 25.9 on page 180).
- Use the **Diagnostic** screens to identify problems with the EMG6765-Q10A (Section 25.10 on page 180).

25.3 General Screen

Use this screen to set the system and domain names and the timeout period of the management session. Click **Maintenance** > **General**. The following screen displays.

Figure 102 Maintenance > General



System Name : EMG6765-Q10A

Domain Name : local

Administrator Inactivity Timer : 0 (minutes, 0 means no timeout)

The following table describes the labels in this screen.

Table 74 Maintenance > General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the EMG6765-Q10A in an Ethernet network.
Domain Name	Enter the domain name you want to give to the EMG6765-Q10A.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to exit this screen without saving.

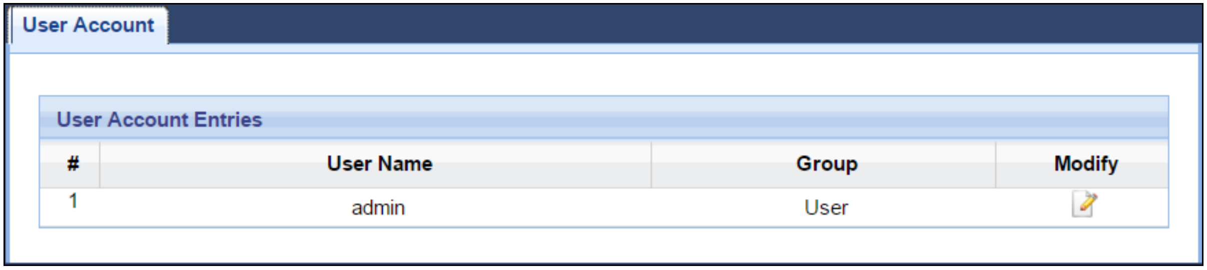
25.4 Account Screen

It is strongly recommended that you change the password of the user account.

If you forget your login account password (or IP address), you will need to reset the device. See Section 1.5 on page 14 and Section 25.8 on page 180 for details.

Click **Maintenance** > **Account**. The screen appears as shown.

Figure 103 Maintenance > Account



User Account Entries

#	User Name	Group	Modify
1	admin	User	✎

The following table describes the labels in this screen.

Table 75 Maintenance > Account

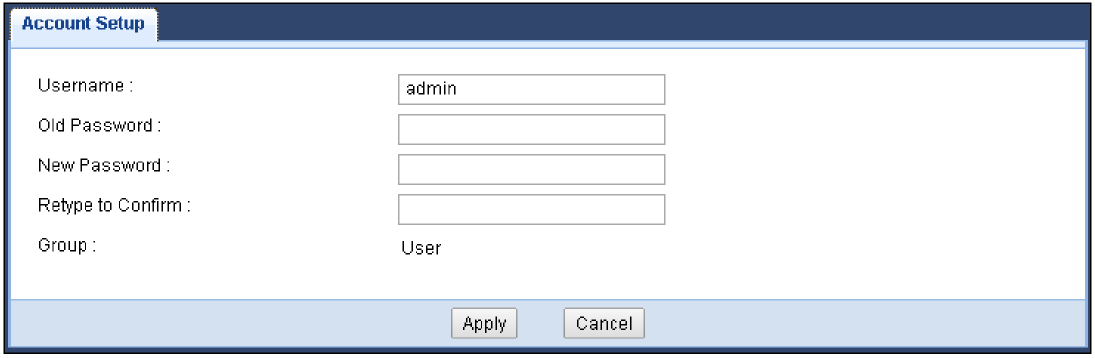
LABEL	DESCRIPTION
User Account Entries	
#	This is the index number of a user account.
User Name	The EMG6765-Q10A's user account name.
Group	The belonging of the user account. Different login account types have different privilege levels. The web configurator screens and privileges will vary depending on which account type you use to log in.
Modify	Click the **Edit** icon to open the Account Setup screen. **Account Setup** screen allows to change the user account password.

25.4.1 Account Setup Screen

This screen allows you to change a user account password.

In the **Maintenance** > **Account** screen, click an **Edit** icon under **Modify**. The screen appears as shown.

Figure 104 Maintenance > Account: Edit



Username : admin

Old Password :

New Password :

Retype to Confirm :

Group : User

The following table describes the labels in this screen.

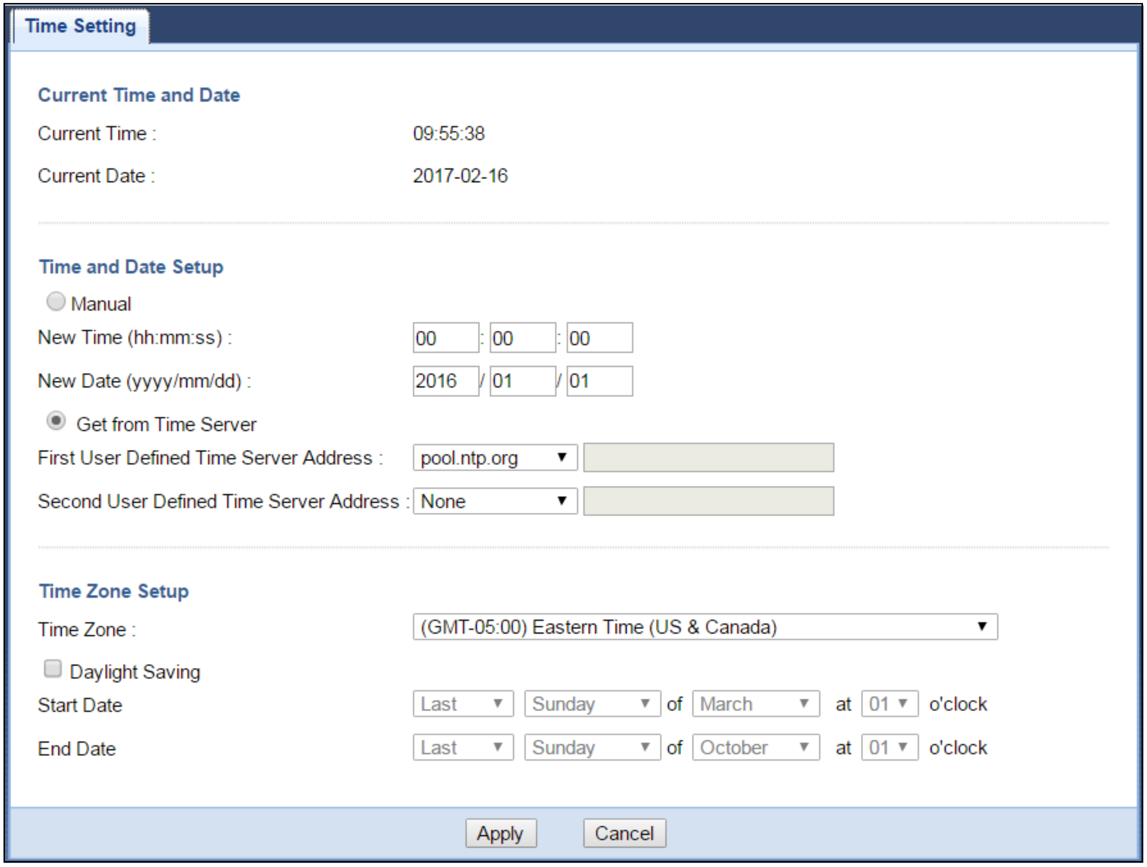
Table 76 Maintenance >

LABEL	DESCRIPTION
Username	The user account name.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays as asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Group	This shows the group belonging of the user account (read-only).
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to exit this screen without saving.

25.5 Time Setting Screen

Use this screen to configure the EMG6765-Q10A's time based on your local time zone. To change your EMG6765-Q10A's time and date, click **Maintenance** > **Time**. The screen appears as shown.

Figure 105 Maintenance > Time



Time Setting

Current Time and Date

Current Time : 09:55:38

Current Date : 2017-02-16

Time and Date Setup

○ Manual

New Time (hh:mm:ss) : 00 : 00 : 00

New Date (yyyy/mm/dd) : 2016 / 01 / 01

● Get from Time Server

First User Defined Time Server Address : pool.ntp.org

Second User Defined Time Server Address : None

Time Zone Setup

Time Zone : (GMT-05:00) Eastern Time (US & Canada)

□ Daylight Saving

Start Date: Last Sunday of March at 01 o'clock

End Date: Last Sunday of October at 01 o'clock

The following table describes the labels in this screen.

Table 77 Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your EMG6765-Q10A. Each time you reload this page, the EMG6765-Q10A synchronizes the time with the time server.
Current Date	This field displays the date of your EMG6765-Q10A. Each time you reload this page, the EMG6765-Q10A synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you select **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you select **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the EMG6765-Q10A get the time and date from the time server you specified below.

Table 77 Maintenance > Time (continued)

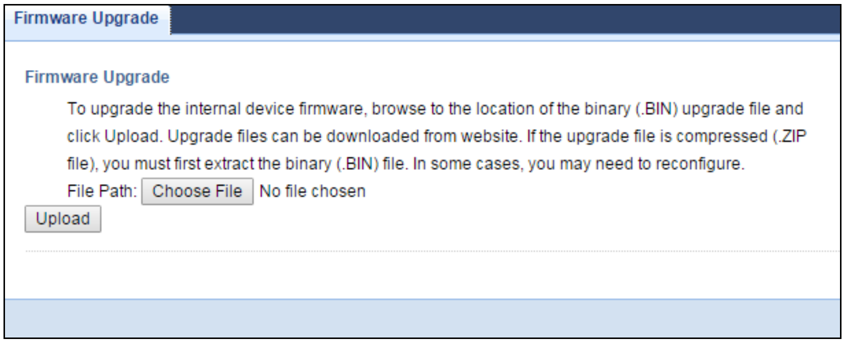
LABEL	DESCRIPTION
First / Second User Defined Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight saving 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. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** 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 first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M local time. So in the United States you would select **First**, **Sunday**, **April** and type 2 in the **o'clock** 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 select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples. Daylight Saving Time ends in the United States on the last Sunday of October. 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 select **Last, Sunday, October** and type 2 in the **o'clock** 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 select **Last, Sunday, October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT + 1).
Apply	Click **Apply** to save your changes back to the EMG6765-Q10A.
Cancel	Click **Cancel** to exit this screen without saving.

25.6 Firmware Upgrade Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "EMG6765-Q10A.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your EMG6765-Q10A.

Figure 106 Maintenance > Firmware Upgrade



Firmware Upgrade

Firmware Upgrade

To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure.

File Path: Choose File No file chosen

Upload

The following table describes the labels in this screen.

Table 78 Maintenance > Firmware Upgrade

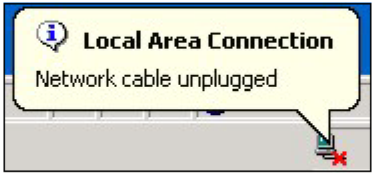
LABEL	DESCRIPTION
Firmware Upgrade	
File Path	Type in the location of the file you want to upload in this field or click to find it.
	Click to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Do not turn off the EMG6765-Q10A while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the EMG6765-Q10A again.

The EMG6765-Q10A automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 107 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.

If the upload was not successful, an error message appears.

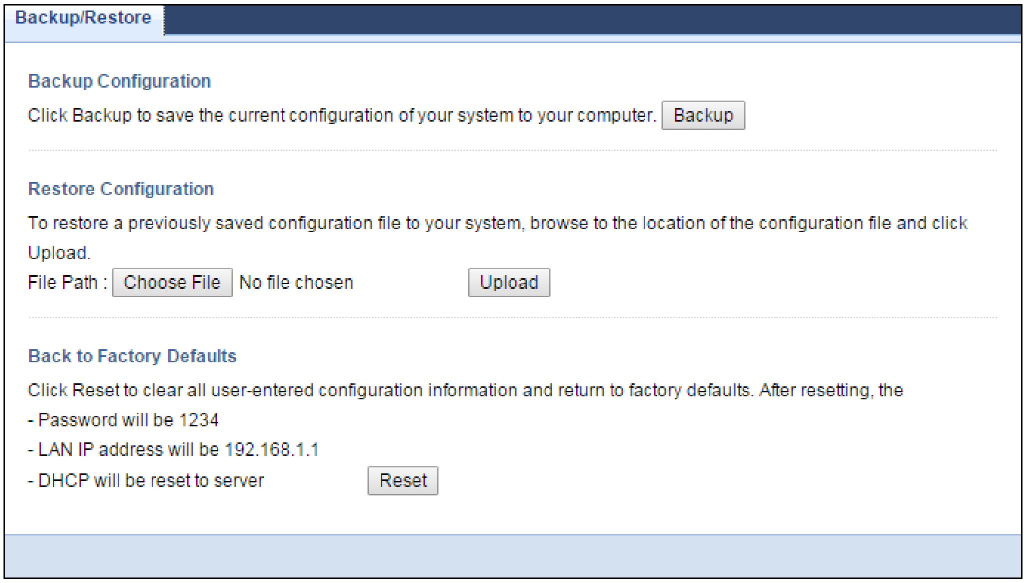
25.7 Configuration Backup/Restore Screen

Backup configuration allows you to back up (save) the EMG6765-Q10A's current configuration to a file on your computer. Once your EMG6765-Q10A 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.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your EMG6765-Q10A.

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

Figure 108 Maintenance > Backup/Restore



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 : No file chosen

Back to Factory Defaults

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

- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

The following table describes the labels in this screen.

Table 79 Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup Configuration	
Backup	Click **Backup** to save the EMG6765-Q10A's current configuration to your computer.
Restore Configuration	
File Path	Click **Choose File** to browse to the location of the configuration file in your computer.
Upload	Click **Upload** to begin the upload process. Note: Do not turn off the EMG6765-Q10A while configuration file upload is in progress. After you see a "configuration upload successful" screen, you must then wait one minute before logging into the EMG6765-Q10A again. The EMG6765-Q10A automatically restarts in this time causing a temporary network disconnect. If you see an error screen, click Back to return to the Backup/Restore screen.
Reset	Pressing the **Reset** button in this section clears all user-entered configuration information and returns the EMG6765-Q10A to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your EMG6765-Q10A. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button.

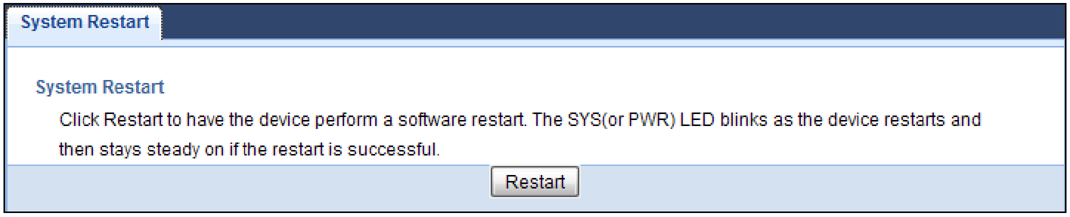
Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default EMG6765-Q10A IP address (192.168.1.1). See Appendix B on page 200 for details on how to set up your computer's IP address.

25.8 Restart Screen

System restart allows you to reboot the EMG6765-Q10A without turning the power off.

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

Figure 109 Maintenance > Restart



Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful.

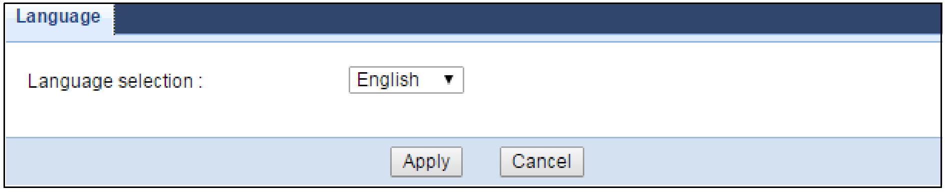
Click **Restart** to have the EMG6765-Q10A reboot. This does not affect the EMG6765-Q10A's configuration.

25.9 Language Screen

Use this screen to change the language for the Web Configurator.

Select the language you prefer and click **Apply**. The Web Configurator language changes after a while without restarting the EMG6765-Q10A.

Figure 110 Maintenance > Language



Language selection : English

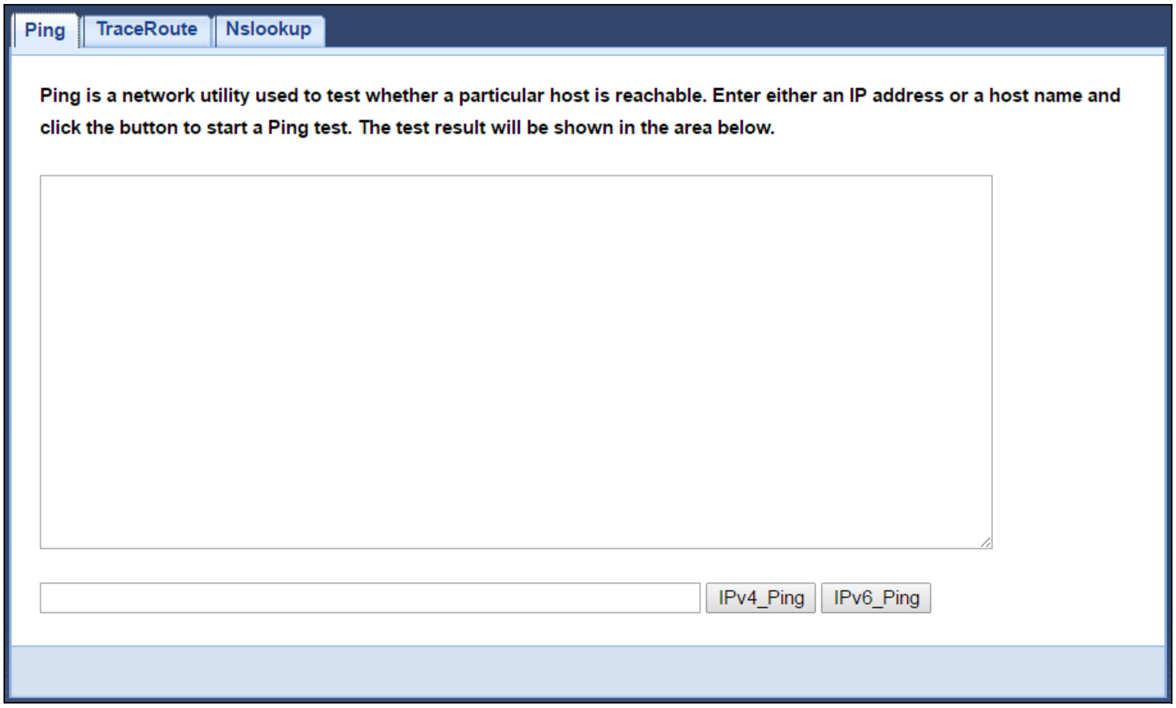
25.10 Diagnostic Screens

The **Diagnostic** screens display information to help you identify problems with the EMG6765-Q10A.

25.10.1 Ping Screen

Use this screen to ping an IP address. Click **Maintenance > Diagnostic > Ping** to open the following screen.

Figure 111 Maintenance > Diagnostic > Ping



Ping is a network utility used to test whether a particular host is reachable. Enter either an IP address or a host name and click the button to start a Ping test. The test result will be shown in the area below.

The following table describes the labels in the **Sys OP Mode** screen.

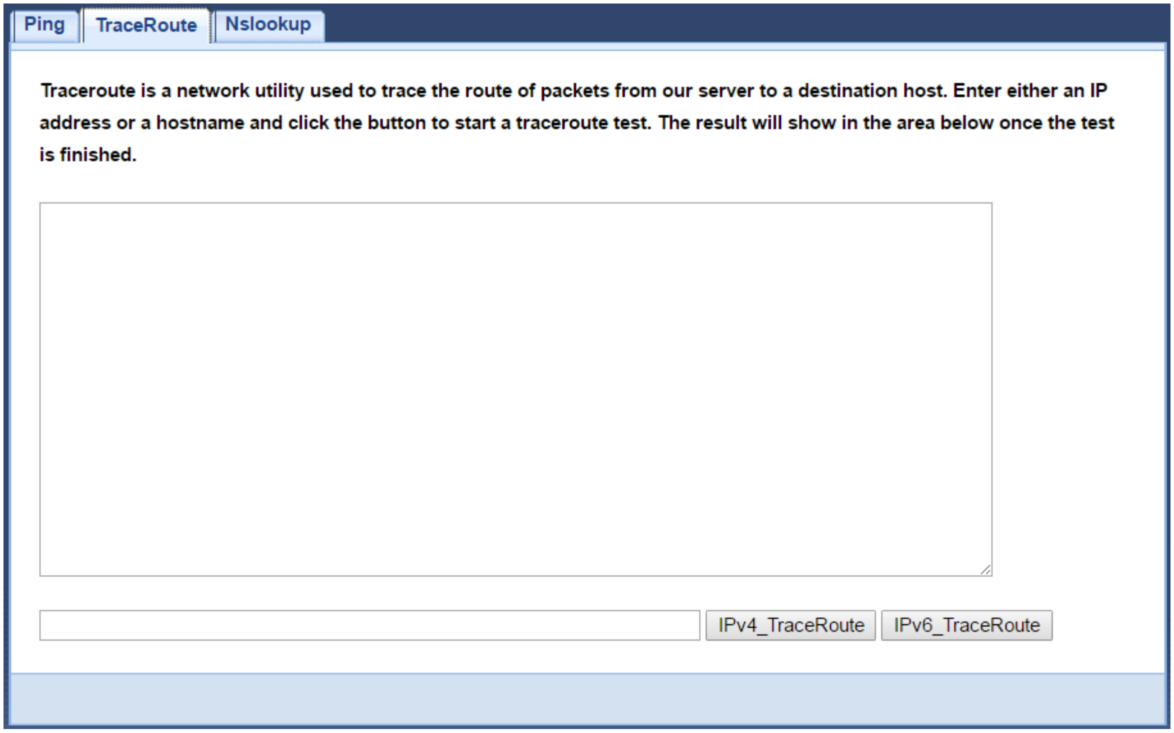
Table 80 Maintenance > Sys OP Mode

LABEL	DESCRIPTION
	Type the IP address of a computer that you want to perform ping in order to test a connection.
IPv4_Ping IPv6_Ping	Click this to ping the IP address that you entered.

25.10.2 Trace Route Screen

Use this screen to trace the route packets take to a host. Click **Maintenance > Diagnostic > TraceRoute** to open the following screen.

Figure 112 Maintenance > Diagnostic > TraceRoute



Traceroute is a network utility used to trace the route of packets from our server to a destination host. Enter either an IP address or a hostname and click the button to start a traceroute test. The result will show in the area below once the test is finished.

The following table describes the labels in this screen.

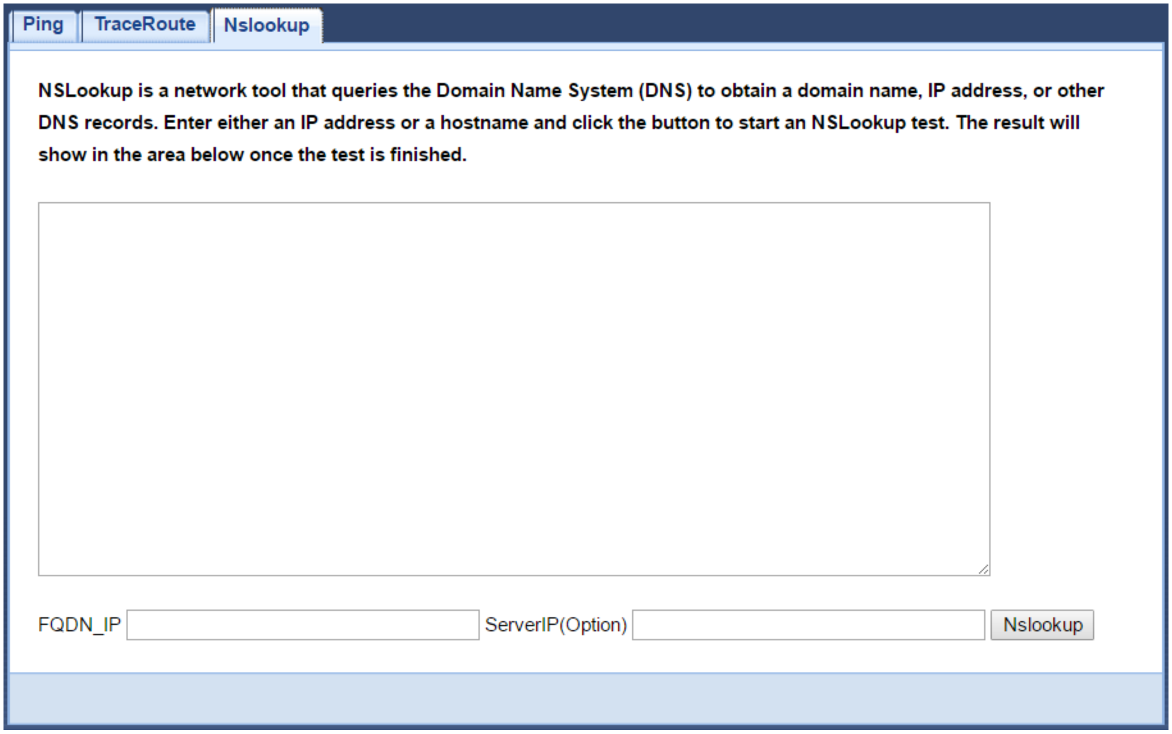
Table 81 Maintenance > Diagnostic > TraceRoute

LABEL	DESCRIPTION
	Type the URL or IP address of a computer for which you want to perform traceroute in order to test a connection.
IPv4 TraceRoute IPv6 TraceRoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified computer

25.10.3 NsLookup Screen

Use this screen to perform an Nslookup (Name server lookup). Nslookup queries the DNS to resolve an IP address into a host name and vice-versa. Click **Maintenance > Diagnostic > Nslookup** to open the following screen.

Figure 113 Maintenance > Diagnostic > Nslookup



NSLookup is a network tool that queries the Domain Name System (DNS) to obtain a domain name, IP address, or other DNS records. Enter either an IP address or a hostname and click the button to start an NSLookup test. The result will show in the area below once the test is finished.

The following table describes the labels in this screen.

Table 82 Maintenance > Diagnostic > Nslookup

LABEL	DESCRIPTION
FQDN_IP	Type a domain name or IP address in this field for the name server lookup.
ServerIP(Option)	Enter the IP address of the server the EMG6765-Q10A uses to translate the specified domain name or IP address.
Nslookup	Click this button to perform a DNS lookup on the IP address or domain name you entered.

CHAPTER 26
Troubleshooting

26.1 Overview

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
- EMG6765-Q10A Access and Login
- Internet Access
- Resetting the EMG6765-Q10A to Its Factory Defaults
- Wireless Connections
- USB Device Problems
- MoCA Network

26.2 Power, Hardware Connections, and LEDs

The EMG6765-Q10A does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the EMG6765-Q10A.
2. Make sure the power adaptor or cord is connected to the EMG6765-Q10A and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the EMG6765-Q10A.
4. 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 1.6 on page 15.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Disconnect and re-connect the power adaptor to the EMG6765-Q10A.

5 If the problem continues, contact the vendor.

26.3 EMG6765-Q10A Access and Login

I don't know the IP address of my EMG6765-Q10A.

1 The default IP address of the EMG6765-Q10A in **Router Mode** is **192.168.1.1**. The default IP address of the EMG6765-Q10A in **Access Point Mode** is **192.168.1.2**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the EMG6765-Q10A in **Router Mode** 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 EMG6765-Q10A (it depends on the network), so enter this IP address in your Internet browser.

3 If your EMG6765-Q10A in **Access Point Mode** is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.

4 Reset your EMG6765-Q10A to change all settings back to their default. This means your current settings are lost. See Section 26.5 on page 188 in the **Troubleshooting** for information on resetting your EMG6765-Q10A.

I forgot the password.

1 The default password is in the back label of your EMG6765-Q10A.

2 If this does not work, you have to reset the device to its factory defaults. See Section 26.5 on page 188.

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 of the EMG6765-Q10A in **Router Mode** is **192.168.1.1**. The default IP address of the EMG6765-Q10A in **Access Point Mode** is **192.168.1.2**.
- If you changed the IP address (Section 10.4 on page 96), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I don't know the IP address of my EMG6765-Q10A.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix A on page 191.

4 Make sure your computer is in the same subnet as the EMG6765-Q10A. (If you know that there are routers between your computer and the EMG6765-Q10A, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 10.4 on page 96.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the EMG6765-Q10A. See Section 10.4 on page 96.

5 Reset the device to its factory defaults, and try to access the EMG6765-Q10A with the default IP address. See Section 1.5 on page 14.

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

Advanced Suggestions

- Try to access the EMG6765-Q10A using another service, such as Telnet. If you can access the EMG6765-Q10A, check the remote management settings and firewall rules to find out why the EMG6765-Q10A does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN/ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the EMG6765-Q10A.

1 Make sure you have entered the password correctly. The default password is in the back label of your EMG6765-Q10A. This field is case-sensitive, so make sure [Caps Lock] is not on.

2 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.

3 Disconnect and re-connect the power adaptor or cord to the EMG6765-Q10A.

4 If this does not work, you have to reset the device to its factory defaults. See Section 26.5 on page 188.

26.4 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.

2 Go to **Maintenance > Sys OP Mode**. Check your System Operation Mode setting.

- If the EMG6765-Q10A is in **Router Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access. Your computer and the EMG6765-Q10A should be in the same subnet.
- If the EMG6765-Q10A is in **Access Point Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access and your computer is set to obtain an dynamic IP address.

3 If the EMG6765-Q10A is in **Router Mode**, make sure you entered your ISP account information correctly in the wizard or the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.

4 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.

5 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the EMG6765-Q10A), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.6 on page 15.

2 Reboot the EMG6765-Q10A.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.6 on page 15. If the EMG6765-Q10A is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Check the signal strength. If the signal strength is low, try moving the EMG6765-Q10A closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3 Reboot the EMG6765-Q10A.

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

Advanced Suggestion

- Check the settings for QoS. If it is disabled, you might consider activating it.

26.5 Resetting the EMG6765-Q10A to Its Factory Defaults

If you reset the EMG6765-Q10A, you lose all of the changes you have made. The EMG6765-Q10A reloads its default settings, and the password resets to the back-label default key. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the EMG6765-Q10A:

1. Make sure the power LED is on.
2. Press the **RESET** button for one to four seconds to restart/reboot the EMG6765-Q10A.
3. Press the **RESET** button for more than five seconds to set the EMG6765-Q10A back to its factory-default configurations.

   If the EMG6765-Q10A restarts automatically, wait for the EMG6765-Q10A to finish restarting, and log in to the Web Configurator. The password is in the back label of your EMG6765-Q10A.

   If the EMG6765-Q10A does not restart automatically, disconnect and reconnect the EMG6765-Q10A's power. Then, follow the directions above again.

26.6 Wireless Connections

I cannot access the EMG6765-Q10A or ping any computer from the WLAN.

1. Make sure the wireless LAN is enabled on the EMG6765-Q10A.
2. Make sure the wireless adapter on your computer is working properly.
3. Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the EMG6765-Q10A.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the EMG6765-Q10A.
5. Check that both the EMG6765-Q10A and the wireless adapter on your computer are using the same wireless and wireless security settings.
6. Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the EMG6765-Q10A.
7. Make sure you allow the EMG6765-Q10A to be remotely accessed through the WLAN interface. Check your remote management settings.

- See the chapter on Wireless LAN in the User's Guide for more information.

I set up URL keyword blocking, but I can still access a website that should be blocked.

Make sure that you enable parental control in the **Parental Control** screen, set up rules and turn on the rules. Make sure that the keywords that you type are listed in the rule's **Keyword List**.

If a keyword that is listed in the **Keyword List** is not blocked when it is found in a URL, customize the keyword blocking using commands. See the Customizing Keyword Blocking URL Checking section in the IPv6 Firewall chapter.

I cannot access the Web Configurator after I switched to AP mode.

When you change from router mode to AP mode, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

Refer to Appendix B on page 200 for instructions on how to change your computer's IP address.

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.
- Position the antennas for best reception. If the AP is placed on a table or floor, point the antennas upwards. If the AP is placed at a high position, point the antennas downwards. Try pointing the antennas in different directions and check which provides the strongest signal to the wireless clients.

26.7 USB Device Problems

I cannot access or see a USB device that is connected to the EMG6765-Q10A.

1. Disconnect the problematic USB device, then reconnect it to the EMG6765-Q10A.
2. Ensure that the USB device has power.
3. Check your cable connections.
4. Restart the EMG6765-Q10A by disconnecting the power and then reconnecting it.
5. If the USB device requires a special driver, install the driver from the installation disc that came with the device. After driver installation, reconnect the USB device to the EMG6765-Q10A and try to connect to it again with your computer.
6. If the problem persists, contact your vendor.

What kind of USB devices do the EMG6765-Q10A support?

1. It is strongly recommended to use version 2.0 or lower USB storage devices (such as memory sticks, USB hard drives) and/or USB devices. Other USB products are not guaranteed to function properly with the EMG6765-Q10A.

26.8 MoCA Network

The EMG6765-Q10A cannot set up a MoCA network with other MoCA devices.

1. Make sure all the MoCA devices are turned on and connected using the same coaxial wiring.
2. Make sure all the MoCA devices are operating at the same channel frequency.
3. If you enable MoCA network security on the EMG6765-Q10A, make sure other MoCA devices also use the same password.

APPENDIX A
Pop-up Windows, JavaScript and Java Permissions

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

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

Note: The screens used below belong to Internet Explorer version 6, 7 and 8. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

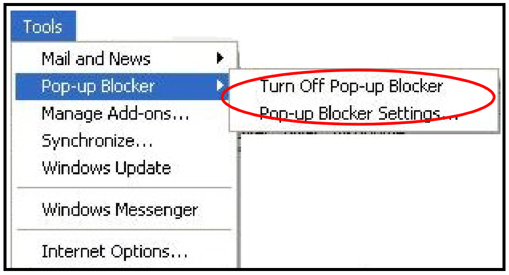
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 114 Pop-up Blocker

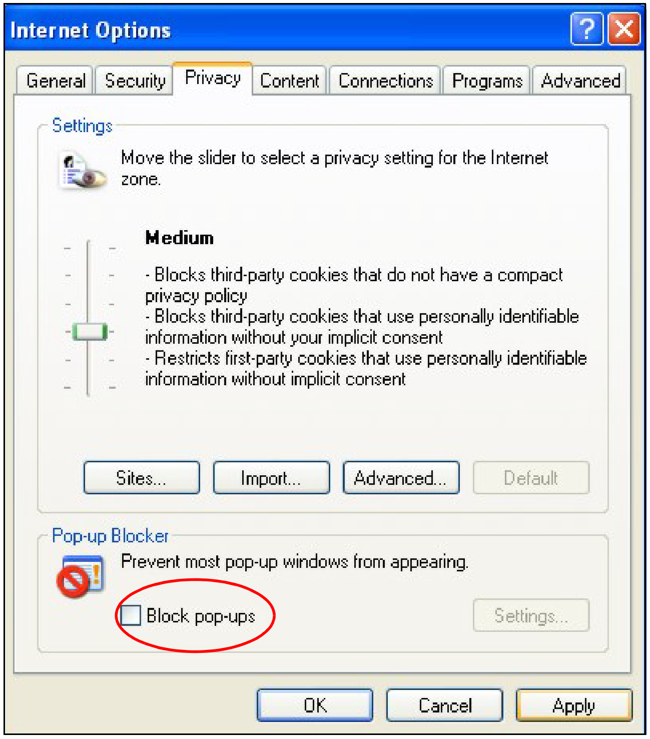


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 115 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

□ Block pop-ups

3 Click **Apply** to save this setting.

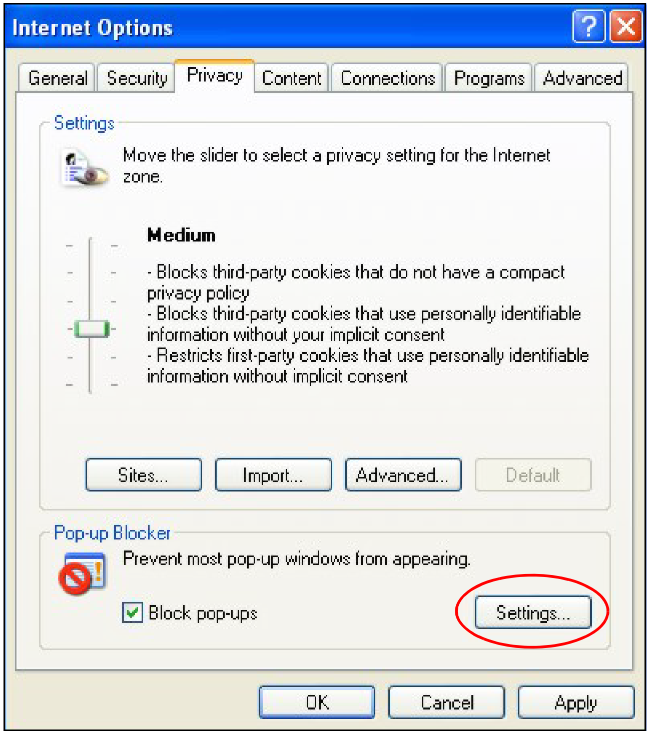
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 116 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

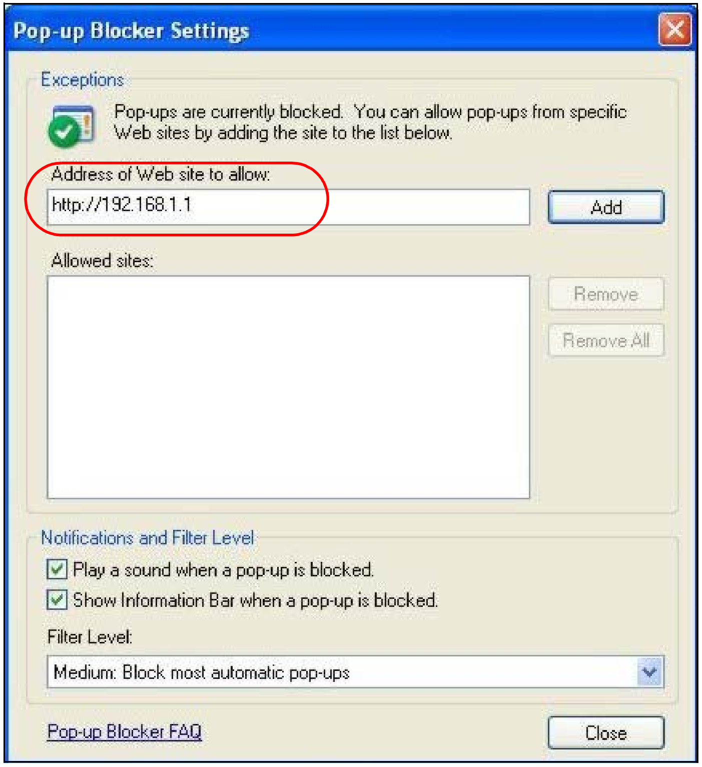
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 117 Pop-up Blocker Settings



Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow:
http://192.168.1.1

Allowed sites:

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level:
Medium: Block most automatic pop-ups

5 Click **Close** to return to the **Privacy** screen.

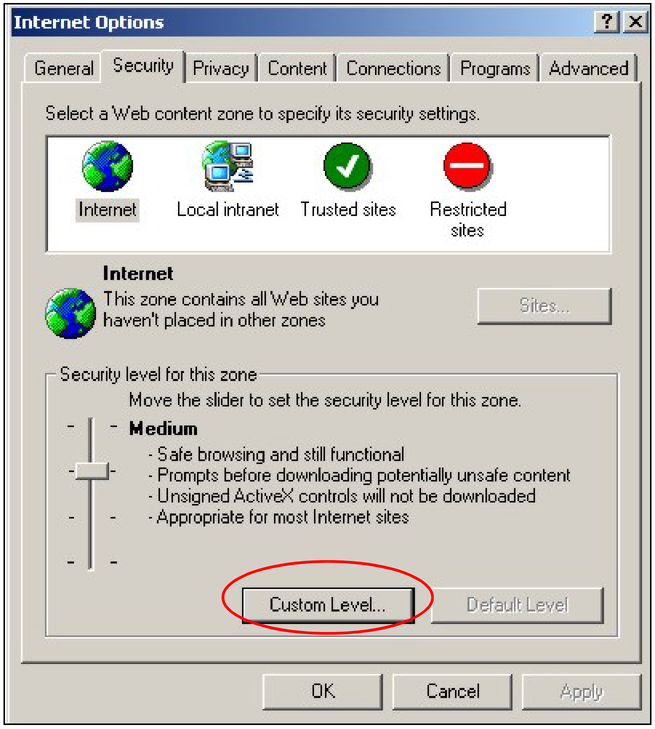
6 Click **Apply** to save this setting.

JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 118 Internet Options: Security



Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Move the slider to set the security level for this zone.

Medium
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.

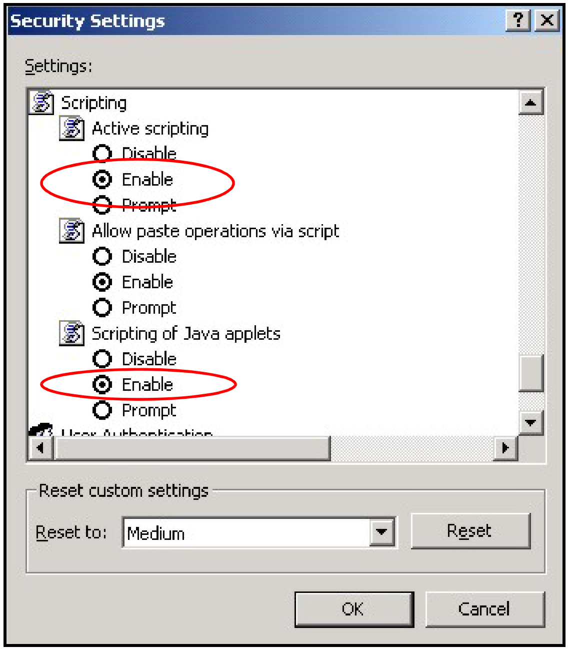
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 119 Security Settings - Java Scripting



Security Settings

Settings:

- Scripting
  - Active scripting
    - ○ Disable
    - ● Enable
    - ○ Prompt
  - Allow paste operations via script
    - ○ Disable
    - ● Enable
    - ○ Prompt
  - Scripting of Java applets
    - ○ Disable
    - ● Enable
    - ○ Prompt
- User Authentication

Reset custom settings

Reset to: Medium

Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

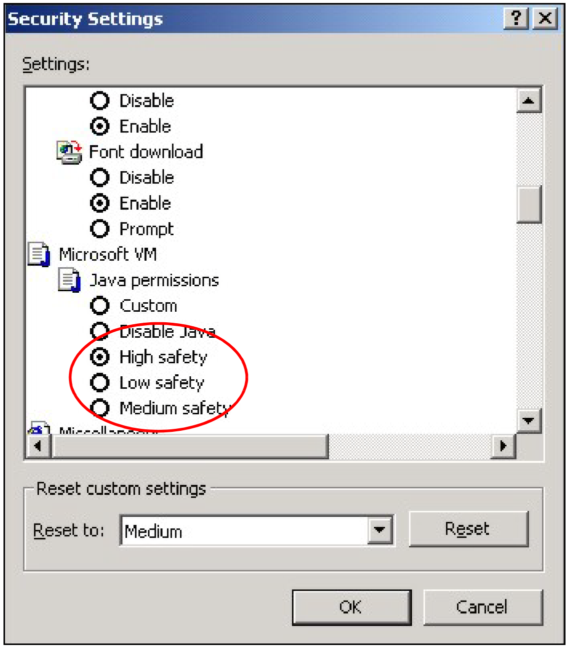
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 120 Security Settings - Java



Security Settings

Settings:

- ○ Disable
- ● Enable
- Font download
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Microsoft VM
  - Java permissions
    - ○ Custom
    - ○ Disable Java
    - ● High safety
    - ○ Low safety
    - ○ Medium safety

Reset custom settings

Reset to: Medium

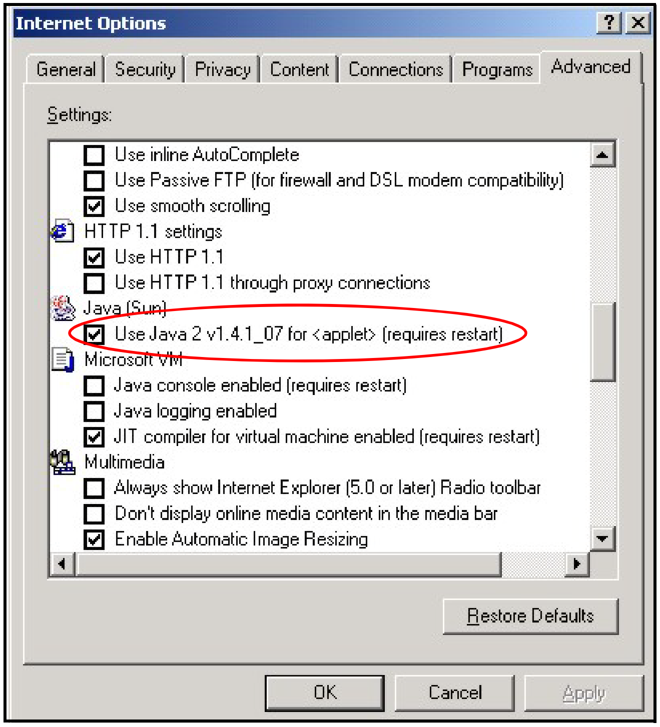
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 121 Java (Sun)



Internet Options

Settings:

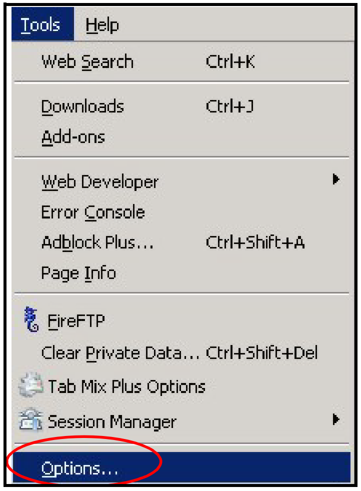
- ☐ Use inline AutoComplete
- ☐ Use Passive FTP (for firewall and DSL modem compatibility)
- ☑ Use smooth scrolling
- HTTP 1.1 settings
  - ☑ Use HTTP 1.1
  - ☐ Use HTTP 1.1 through proxy connections
- Java (Sun)
  - ☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
- Microsoft VM
  - ☐ Java console enabled (requires restart)
  - ☐ Java logging enabled
  - ☑ JIT compiler for virtual machine enabled (requires restart)
- Multimedia
  - ☐ Always show Internet Explorer (5.0 or later) Radio toolbar
  - ☐ Don't display online media content in the media bar
  - ☑ Enable Automatic Image Resizing

Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

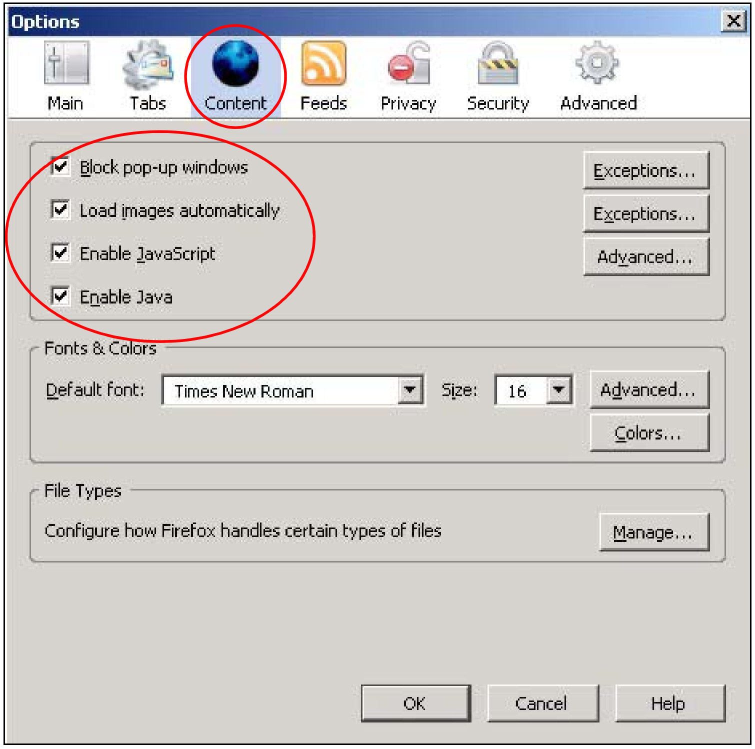
You can enable Java, Javascript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 122 Mozilla Firefox: TOOLS > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 123 Mozilla Firefox Content Security



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

Fonts & Colors

Default font: Times New Roman

Size: 16

File Types

Configure how Firefox handles certain types of files

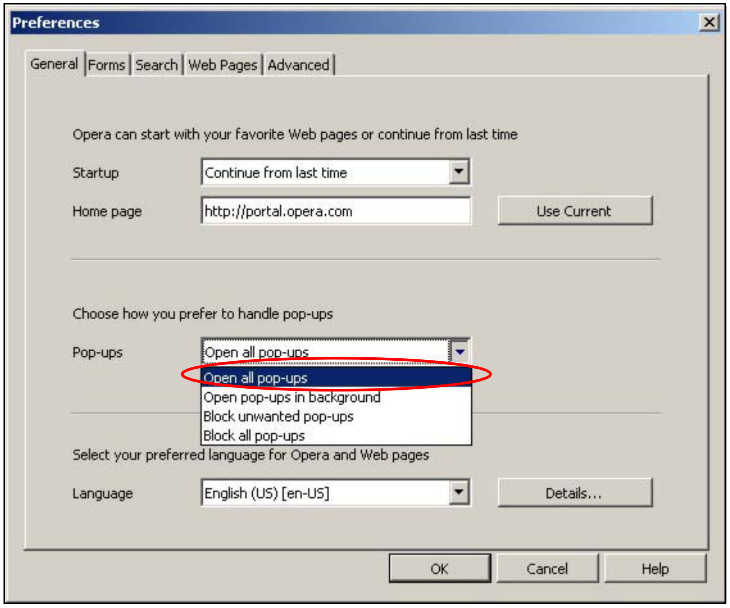
Opera

Opera 10 screens are used here. Screens for other versions may vary slightly.

Allowing Pop-Ups

From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

Figure 124 Opera: Allowing Pop-Ups



Opera can start with your favorite Web pages or continue from last time

Startup: Continue from last time

Home page: http://portal.opera.com

Choose how you prefer to handle pop-ups

Pop-ups: Open all pop-ups

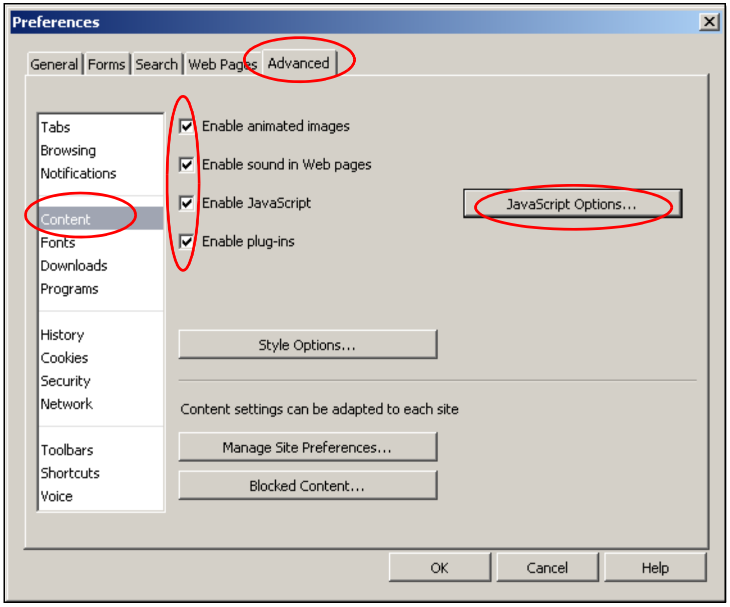
Select your preferred language for Opera and Web pages

Language: English (US) [en-US]

Enabling Java

From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 125 Opera: Enabling Java



☑ Enable animated images

☑ Enable sound in Web pages

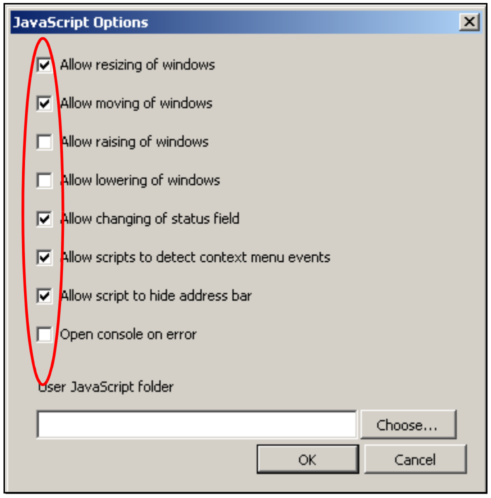
☑ Enable JavaScript

☑ Enable plug-ins

Content settings can be adapted to each site

To customize JavaScript behavior in the Opera browser, click **JavaScript Options**.

Figure 126 Opera: JavaScript Options



☑ Allow resizing of windows

☑ Allow moving of windows

☐ Allow raising of windows

☐ Allow lowering of windows

☑ Allow changing of status field

☑ Allow scripts to detect context menu events

☑ Allow script to hide address bar

☐ Open console on error

User JavaScript folder

Select the items you want Opera’s JavaScript to apply.

APPENDIX B
Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **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**. Please refer to RFC 1700 for further information about port numbers.
  - 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 83 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
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	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example 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 Program, 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.

Table 83 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management 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.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
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).
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.
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	Simple File Transfer Protocol.
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.
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.

Table 83 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

APPENDIX C
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 *http://www.zyxel.com/homepage.shtml* and also *http://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.
- http://www.zyxel.cn

India

- Zyxel Technology India Pvt Ltd
- http://www.zyxel.in

Kazakhstan

- Zyxel Kazakhstan
- http://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
- http://www.zyxel.com/tw/zh/

Thailand

- Zyxel Thailand Co., Ltd
- http://www.zyxel.co.th

Vietnam

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

Europe

Austria

- Zyxel Deutschland GmbH
- http://www.zyxel.de

Belarus

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

Belgium

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

Bulgaria

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

Czech Republic

- Zyxel Communications Czech s.r.o
- http://www.zyxel.cz

Denmark

- Zyxel Communications A/S
- http://www.zyxel.dk

Estonia

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

Finland

- Zyxel Communications
- http://www.zyxel.fi

France

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

Germany

- Zyxel Deutschland GmbH
- http://www.zyxel.de

Hungary

- Zyxel Hungary & SEE
- http://www.zyxel.hu

Italy

- Zyxel Communications Italy
- http://www.zyxel.it/

Latvia

- Zyxel Latvia
- http://www.zyxel.com/lv/lv/homepage.shtml

Lithuania

- Zyxel Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

Netherlands

- Zyxel Benelux
- http://www.zyxel.nl

Norway

- Zyxel Communications
- http://www.zyxel.no

Poland

- Zyxel Communications Poland
- http://www.zyxel.pl

Romania

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

Russia

- Zyxel Russia
- http://www.zyxel.ru

Slovakia

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

Spain

- Zyxel Communications ES Ltd
- http://www.zyxel.es

Sweden

- Zyxel Communications
- http://www.zyxel.se

Switzerland

- Studerus AG

- http://www.zyxel.ch/

Turkey

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

UK

- Zyxel Communications UK Ltd.
- http://www.zyxel.co.uk

Ukraine

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

Latin America

Argentina

- Zyxel Communication Corporation
- http://www.zyxel.com/ec/es/

Brazil

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

Ecuador

- Zyxel Communication Corporation
- http://www.zyxel.com/ec/es/

Middle East

Israel

- Zyxel Communication Corporation
- http://il.zyxel.com/homepage.shtml

Middle East

- Zyxel Communication Corporation
- http://www.zyxel.com/me/en/

North America

USA

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

Oceania

Australia

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

Africa

South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

APPENDIX D
Legal Information

Copyright

Copyright © 2017 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 28 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

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-EMG6765Q10A)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

TYPE	MANUFACTURER	GAIN	CONNECTOR
Dipole Antenna 2.4G*1	HONGBO	< 3.5dBi @ 2.4-GHz	I-PEX
Dipole Antenna 5G*4	HONGBO	< 5.1 dBi @ 5-GHz	I-PEX
Couple Antenna 2.4G*2	PEGATRON	< 3.5 dBI @ 2.4-GHz	I-PEX

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-EMG6765Q10A) 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

TYPE	FABRICANT	GAIN	CONNECTEUR
Dipole Antenna 2.4G*1	HONGBO	< 3.5dBi @ 2.4-GHz	I-PEX
Dipole Antenna 5G*4	HONGBO	< 5.1 dBi @ 5-GHz	I-PEX
Couple Antenna 2.4G*2	PEGATRON	< 3.5 dBI @ 2.4-GHz	I-PEX

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 34 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 34 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.

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС. **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/EÜ 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/EU.
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/EU.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/EU.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/EU.
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/EU. **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/EU 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/EU 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/EU.
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/EU.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale şi alte prevederi relevante ale Directivei 2014/53/EU.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU.
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:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

2. 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.

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.

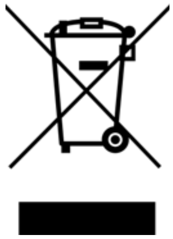
Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung 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

以下訊息僅適用於產品操作於 5.25-5.35 秭赫頻帶內並銷售至台灣地區

- 在 5.25-5.35 秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

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