ZYXEL
COMMUNICATIONS

User's Guide

EX3510-B1

AX5700 WiFi6 Gigabit Ethernet Gateway

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

Version 5.17 Edition 1, 10/2022
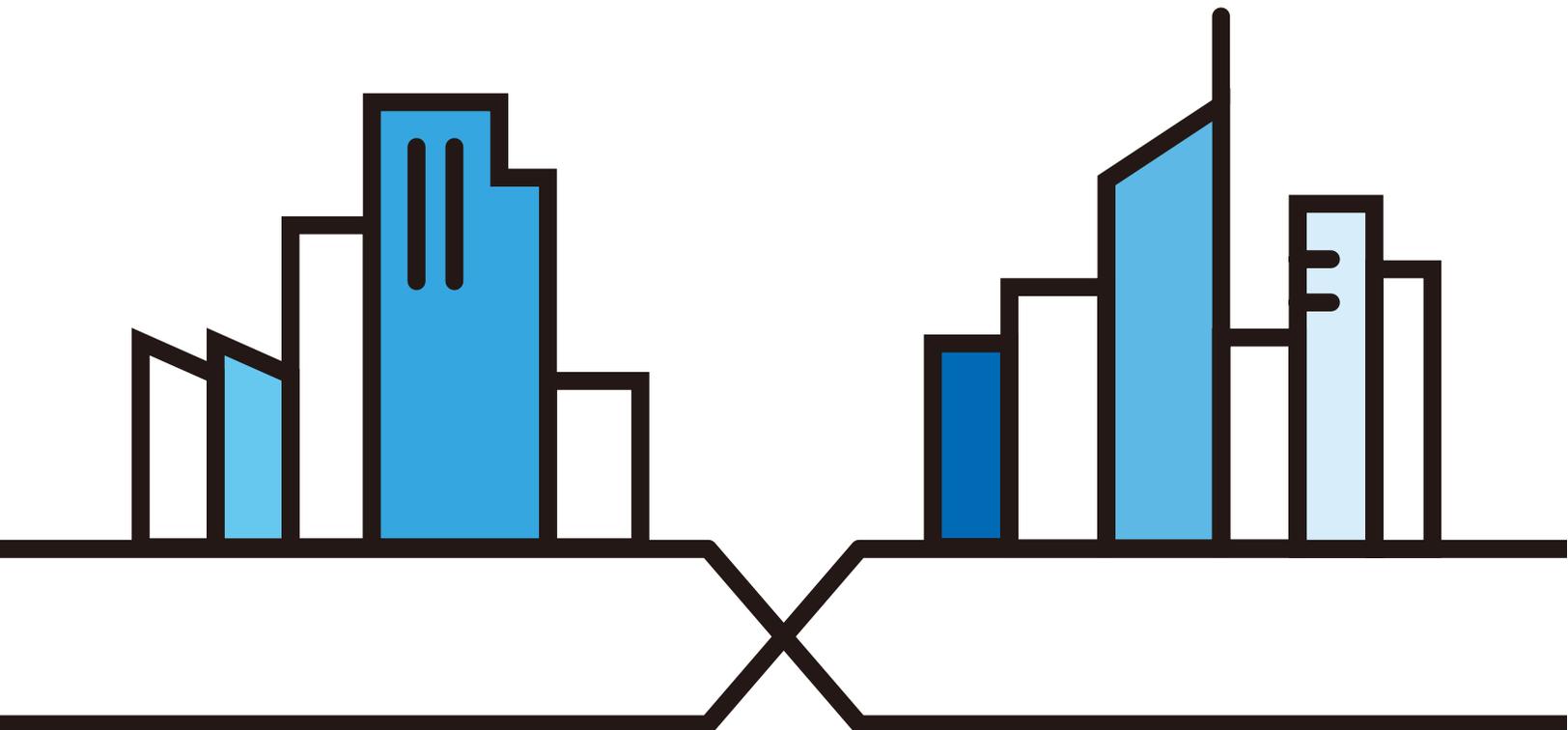
IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from what you see due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the Zyxel Device.

- More Information

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

Document Conventions

Warnings and Notes

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

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

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

Syntax Conventions

- The EX3510-B1 in this user's guide may be referred to as the "Zyxel Device" in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Network Setting** > **Routing** > **DNS Route** means you first click **Network Setting** in the navigation panel, then the **Routing** sub menu and finally the **DNS Route** tab to get to that screen.

Icons Used in Figures

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

Zyxel Device	Wireless Device	Laptop Computer
Switch	Firewall	Server
Internet	User	Smartphone

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Introducing the Zyxel Device

1.1 Overview

The Zyxel Device is an Ethernet gateway which provides fast Internet access. It has one 1 Gigabit Ethernet (GbE) WAN port that is backward compatible with standard 10/100 Mbps speeds. It also has four 1000 Mbps Ethernet LAN ports.

See the following table for the cables required and distance limitation to attain the corresponding speed.

Table 1   Ethernet Cable Types

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 5	100 Mbps	100 m	100 MHz
Category 5e	1 Gbps / 2.5 Gbps	100 m	100 MHz

It also supports dual-band 2.4G / 5G WiFi with WiFi6 that is most suitable in areas with a high concentration of users. You can schedule WiFi usage using Parental Control. See Section on page 89 for more information on WiFi6.

The Zyxel Device supports MPro Mesh that lets you easily extend WiFi in your home or office using a compatible WiFi Extender. See the Zyxel website for more information on MPro Mesh.

1.2 Example Applications

This section shows a few examples of using the Zyxel Device in various network environments. Note that the Zyxel Device in the figure is just an example Zyxel Device and not your actual Zyxel Device.

1.2.1 Internet Access

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

Figure 1 Zyxel Device's Internet Access Application
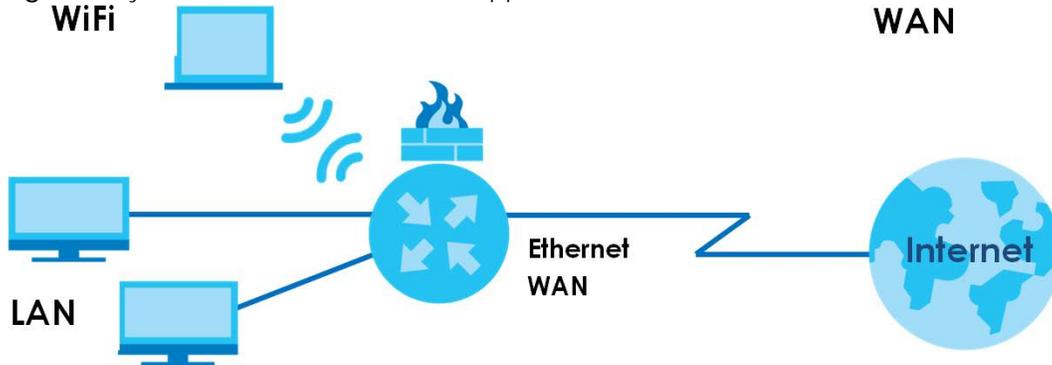
When the Firewall is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

Connect the WAN port to the broadband modem or router. This way, you can access the Internet through an Ethernet connection and use the QoS, Firewall and parental control functions on the Zyxel Device.

Figure 2 Zyxel Device's Internet Access Application: Ethernet WAN
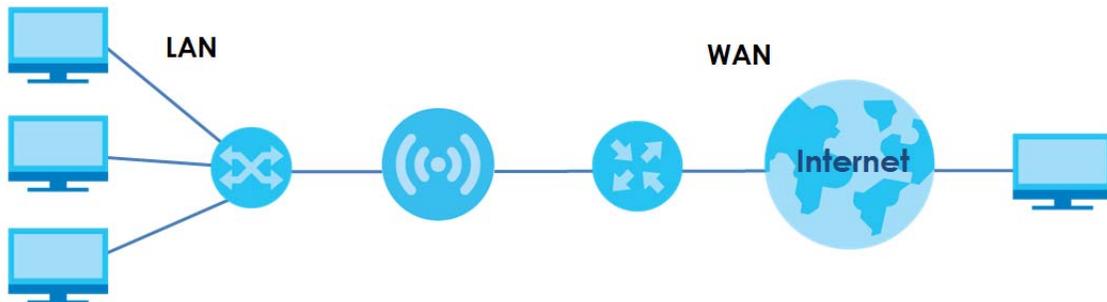
1.2.2 Dual-Band WiFi

By default, WiFi is enabled on the Zyxel Device. IEEE 802.11a/b/g/n/ac/ax compliant clients can wirelessly connect to the Zyxel Device to access network resources.

The Zyxel Device is a dual-band gateway that can use both 2.4G and 5G networks at the same time. You could use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz

band for time sensitive traffic like high-definition video, music, and gaming.

Figure 3   Dual-Band Application
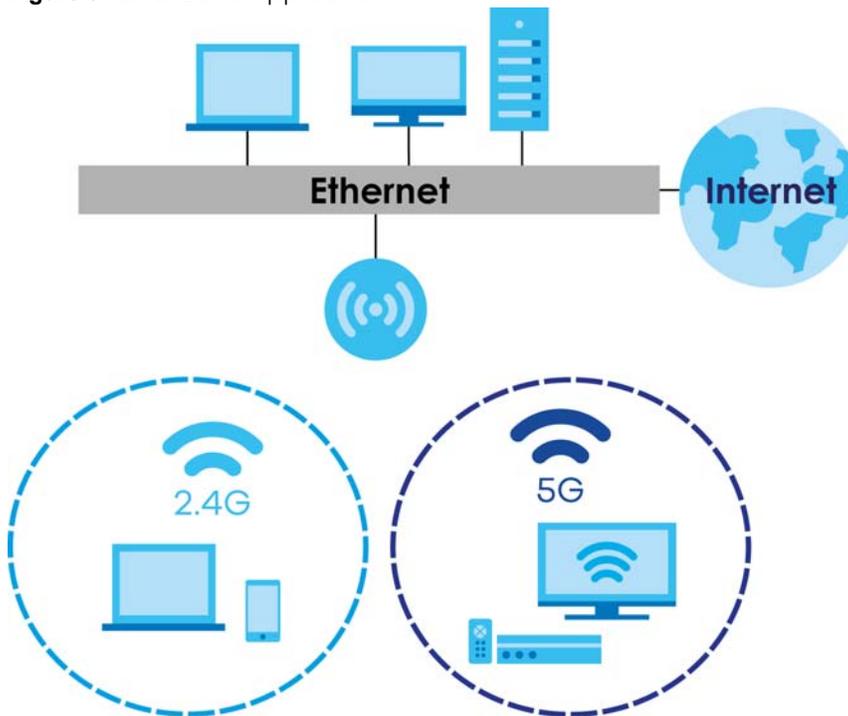
The Zyxel Device is a wireless Access Point (AP) for IEEE 802.11b/g/n/a/ac/ax wireless clients, such as notebook computers, iPads, smartphones, and so on. It allows them to connect to the Internet without having to rely on inconvenient Ethernet cables.

Your Zyxel Device supports WiFi Protected Setup (WPS), which allows you to quickly set up a wireless network with strong security.

Figure 4   Wireless Access Example
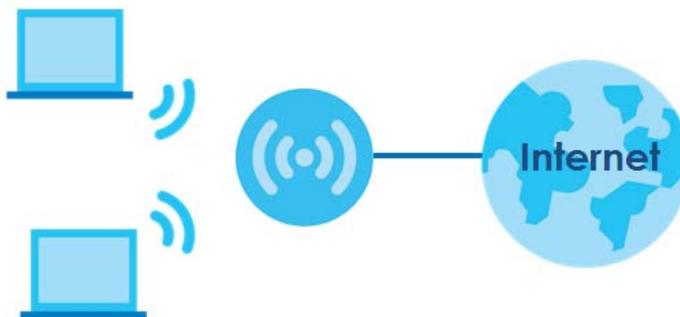
1.3 Ways to Manage the Zyxel Device

Use any of the following methods to manage the Zyxel Device.

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

- Simple Network Management Protocol (SNMP). Use to monitor and/or manage the Zyxel Device by an SNMP manager. See (Section 30.2 on page 250).
- Secure Shell (SSH), Telnet. Use for troubleshooting the Zyxel Device by qualified personnel.
- FTP. Use FTP for firmware upgrades and configuration backup/restore.

1.4 Good Habits for Managing the Zyxel Device

Do the following things regularly to make the Zyxel Device more secure and to manage the Zyxel Device more effectively.

- Change the WiFi and Web Configurator passwords. Use a password that is not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the passwords 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 Zyxel Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Zyxel Device. You could simply restore your last configuration.

1.5 Hardware

This section describes the front and rear panels.

1.5.1 Front Panel

The LED indicators are located on the front panel.

Figure 5   LED Indicators
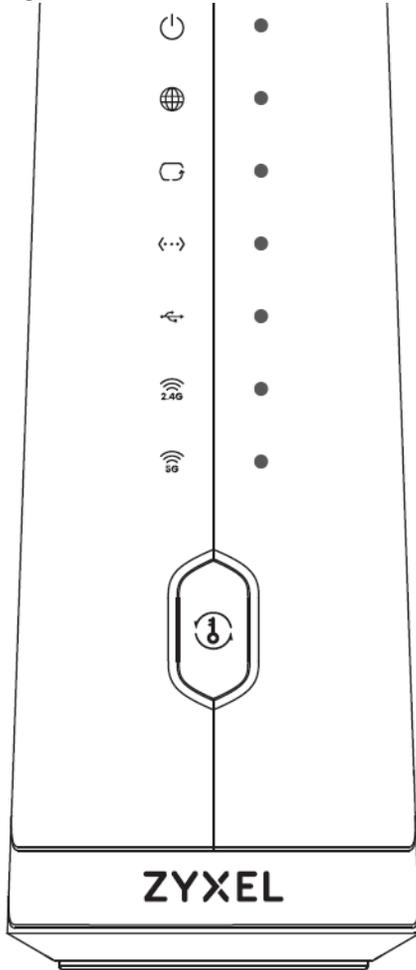
None of the LEDs are on if the Zyxel Device is not receiving power.

Table 2   LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The Zyxel Device is receiving power and ready for use.
		Blinking	The Zyxel Device is booting.
	Red	On	The Zyxel Device detected an error while self-testing, or there is a device malfunction.
		Blinking	The Zyxel Device is upgrading firmware.
		Off	The Zyxel Device is not receiving power.
INTERNET	Green	On	The Zyxel Device 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).
		Blinking	The Zyxel Device is sending or receiving IP traffic.
		Off	There is no Internet connection or the gateway is in bridged mode.
	Red	On	The Zyxel Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.

Table 2   LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
WAN	Green	On	The Zyxel Device has a successful 10M / 100M / 1Gbps Ethernet connection on the WAN.
		Off	The Zyxel Device does not have an Ethernet connection with the WAN.
LAN	Green	On	The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection with a device on the Local Area Network (LAN) via the ETHERNET1-4 ports.
		Blinking	The Zyxel Device is sending or receiving data to/from the LAN at 10/100/1000 Mbps via the ETHERNET1-4 ports.
		Off	The Zyxel Device does not have an Ethernet connection with the LAN via the ETHERNET1~4 ports.
USB	The USB LED is reserved for future development.		
2.4G WiFi	Green	On	The 2.4G wireless network is activated.
		Blinking	The Zyxel Device is communicating with 2.4G wireless clients.
		Off	The 2.4G wireless network is not activated.
5G WiFi	Green	On	The 5G wireless network is activated.
		Blinking	The Zyxel Device is communicating with 5G wireless clients.
		Off	The 5G wireless network is not activated.
WPS	Green	Blinking	The Zyxel Device is setting up a WPS connection with a wireless client.
		Off	The Zyxel Device has set up a WPS connection with a wireless client or WPS has not been enabled.
	Amber	Blinking	The Zyxel Device is pairing with IPTV SSID.

1.5.2 Rear Panel

The connection ports are located on the rear panel.

Figure 6   Rear Panel
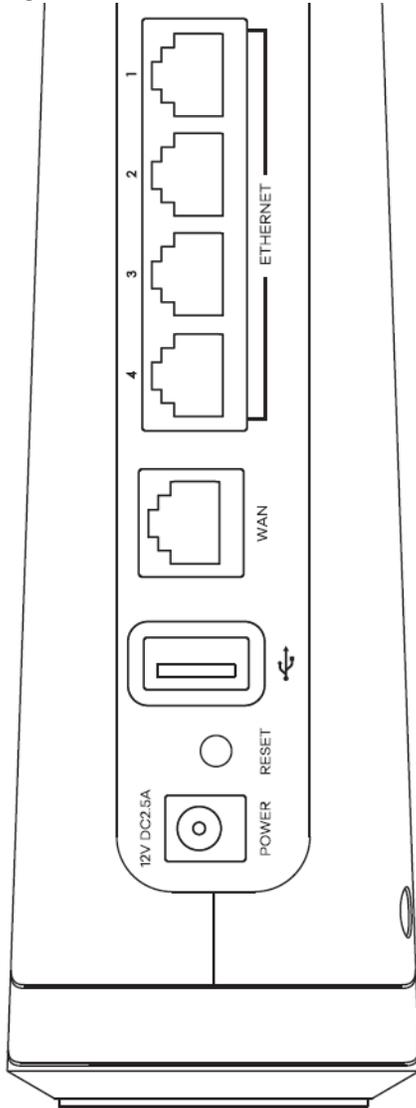
The following table describes the items on the rear panel.

Table 3   Panel Ports and Buttons

LABEL	DESCRIPTION
WPS	Press the WPS button for more than one second to quickly set up a secure WiFi connection between the device and a WPS-compatible client.
Power	Connect the power adapter and press the power button to start the device.
Reset	Press the button to return the Zyxel Device to the factory defaults.
USB	The USB port is reserved for future development.
1G WAN	Connect an Ethernet cable to a modem for Internet access.
ETHERNET1 – ETHERNET4	Connect computers or other Ethernet devices to Ethernet ports for Internet access.

1.5.3 WPS Button

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

To activate WPS:

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

2 Press the **WPS** button for one second and release it.

3 Press the WPS button on another WPS-enabled device within range of the Zyxel Device within 120 seconds. The **WPS** LED flashes green while the Zyxel Device sets up a WPS connection with the other WiFi device.

4 Once the connection is successfully made, the **WPS** LED will turn off.

1.5.4 RESET Button

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

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

2 To set the device back to the factory default settings, press the **RESET** button for more than 5 seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

> **Do NOT turn off the Zyxel Device while it is restarting. If you must turn off the Zyxel Device, wait until it has fully restarted – the 2.4G and/or 5G WiFi LEDs should be blinking.**

1.5.5 Wall Mounting

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

Table 4   Wall Mounting Information

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

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

Figure 7   Screws and Screw Anchors Specifications
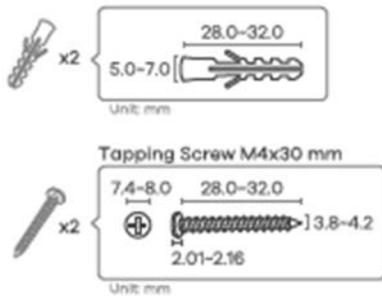
1   Select a position free of obstructions on a wall strong enough to hold the weight of the Zyxel Device.

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 Zyxel Device with the connection cables.

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

Figure 8   Wall Mounting Example
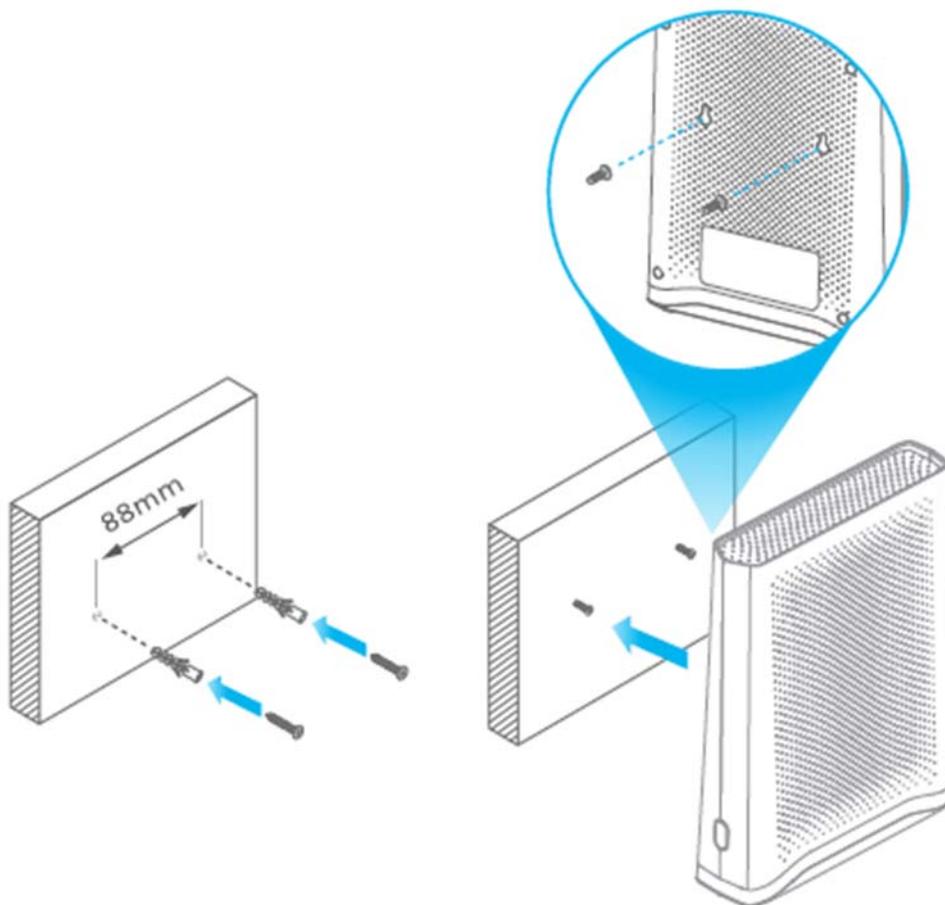
CHAPTER 2
Web Configurator

2.1 Overview

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

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

- Web browser pop-up windows from your Zyxel Device. Web pop-up blocking is enabled by default in Windows 10.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

2.1.1 Accessing the Web Configurator

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

2. Make sure your computer has an IP address in the same subnet as the Zyxel Device. Your computer should have an IP address from 192.168.1.2 to 192.168.1.254. See for details.

3. Launch your web browser. If the Zyxel Device does not automatically re-direct you to the login screen, go to http://192.168.1.1.

4. A login screen displays. Select the language you prefer.

5. To access the administrative Web Configurator and manage the Zyxel Device, type the default username **admin** and the randomly assigned default password (see the device label) in the login screen and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 9   Login Screen
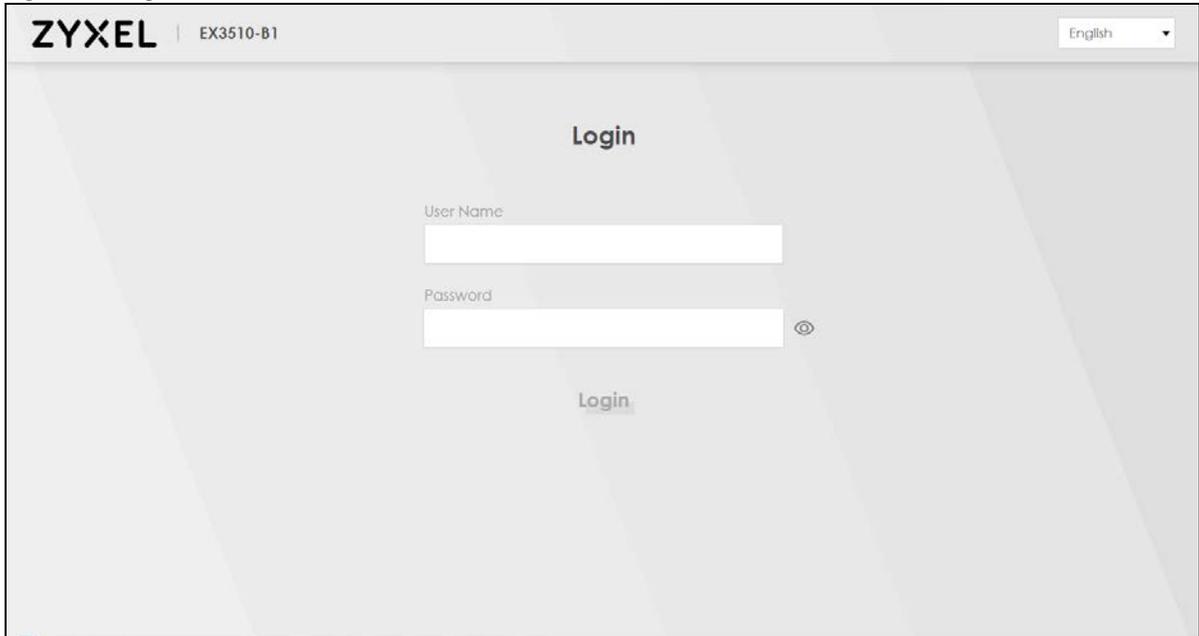
Note: The default allowable times that you can enter the **Password** is 3. If you entered the wrong password for the fourth time, by default the Web Configurator will lock itself for 5 minutes before you can try entering the correct **Password** again.

6   The following screen displays when you log into the Web Configurator for the first time. Enter a new password, retype it to confirm, and click **Change password**. If you prefer to use the default password, click **Skip**.

Figure 10   Change Password Screen

7   The **Wizard** screen displays when you log into the Web Configurator for the first time. Use the **Wizard** screens to configure the Zyxel Device's time zone, basic Internet access, and wireless settings. See for more information about the **Wizard** screens.

8 The **Connection Status** page appears. Use this screen to configure basic Internet access, wireless settings, and parental control settings (see Section 5.1 on page 61 for details).

Figure 11 Connection Status
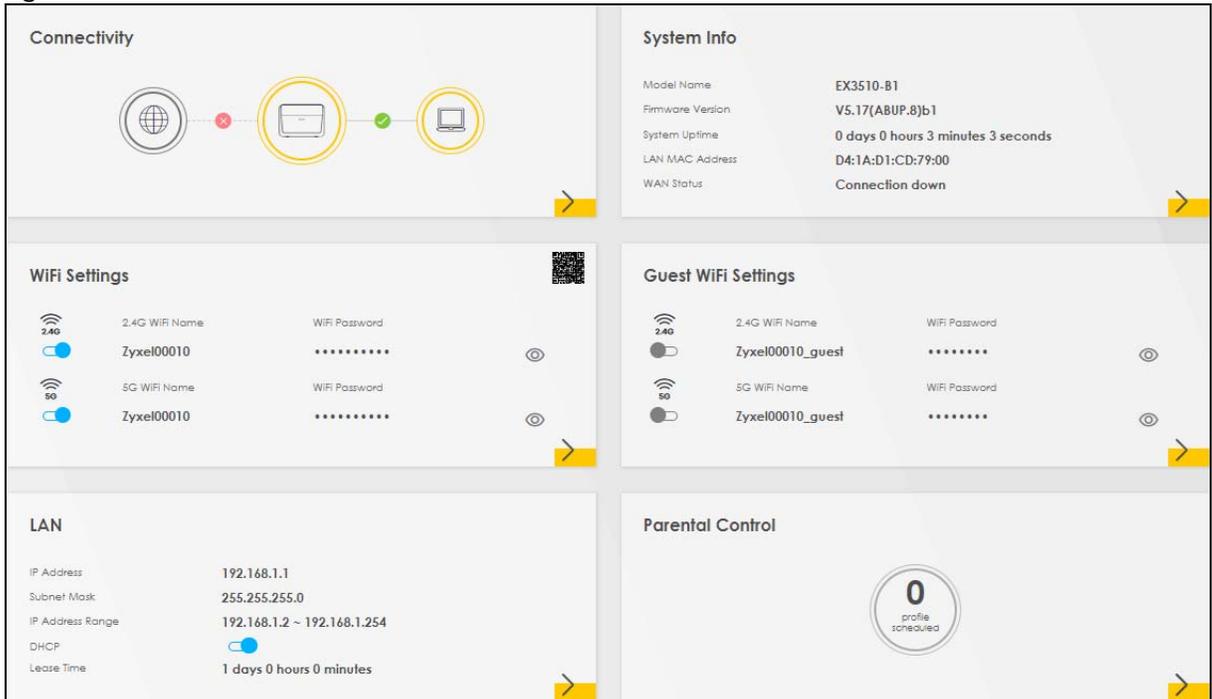
2.2 Web Configurator Layout

Figure 12 Screen Layout
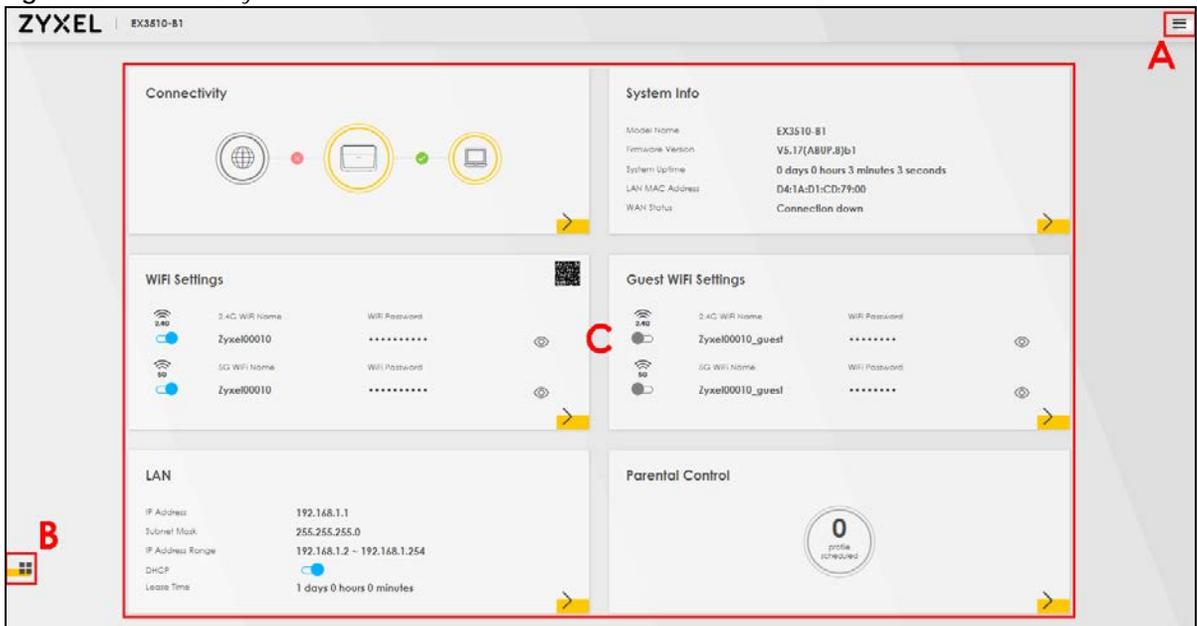
As illustrated above, the main screen is divided into these parts:

- **A** – Navigation Panel
- **B** – Layout Icon
- **C** – Main Window

2.2.1 Navigation Panel

Click the menu icon ( ) to display the navigation panel that contains configuration menus and icons (quick links). Click **X** to close the navigation panel.

Figure 13   Navigation Panel (Administrator Login)
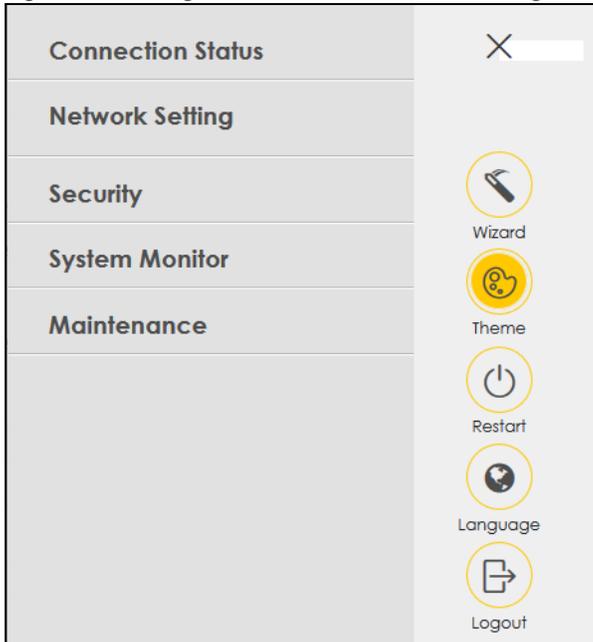
2.2.1.1 Configuration Menus

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

Table 5   Configuration Menus Summary

LINK	TAB	FUNCTION
Connection Status		Use this screen to configure basic Internet access, wireless settings, and parental control settings. This screen also shows the network status of the Zyxel Device and computers/devices connected to it.
Network Setting		
Broadband	Broadband	Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections.

Table 5   Configuration Menus Summary (continued)

LINK	TAB	FUNCTION
Wireless	General	Use this screen to configure the WiFi settings and wireless LAN authentication/security settings.
	Guest/More APGuest/More AP	Use this screen to configure multiple BSSs on the Zyxel Device.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the Zyxel Device.
	WPS	Use this screen to configure and view your WPS (WiFi Protected Setup) settings.
	WMM	Use this screen to enable or disable WiFi MultiMedia (WMM).
	Others	Use this screen to configure advanced wireless settings.
	Channel Status	Use this screen to scan WiFi channel noises and view the results.
	MESH	Use this screen to enable • AP steering which allows wireless clients to roam seamlessly between Mesh supported devices in your Mesh network by using the same SSID and WiFi password. Also, AP steering helps monitor wireless clients and drop their connections to optimize the Zyxel Device bandwidth when the clients are idle or have a low signal. When a wireless client is dropped, it has the opportunity to steer to a Mesh supported device with a strong signal, and • band steering which allows dual-band wireless client devices, to use the less-congested and higher capacity 5 GHz band, leaving the more crowded 2.4 GHz band available for legacy clients.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to turn UPnP and UPnP NAT-T on or off.
	Additional Subnet	Use this screen to configure IP alias and public static IP.
	STB Vendor ID	Use this screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the Zyxel Device automatically create static DHCP entries for the STB devices when they request IP addresses.
	Wake on LAN	Use this screen to remotely turn on a device on the local network.
	TFTP Server Name	Use DHCP option 66 to identify a TFTP server name.
Routing	Static Route	Use this screen to view and set up static routes on the Zyxel Device.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s).
	Policy Route	Use this screen to configure policy routing on the Zyxel Device.
	RIP	Use this screen to configure Routing Information Protocol to exchange routing information with other routers.
QoS	General	Use this screen to enable QoS and traffic prioritizing. You can also configure the QoS rules and actions.
	Queue Setup	Use this screen to configure QoS queues.
	Classification Setup	Use this screen to define a classifier.
	Shaper Setup	Use this screen to limit outgoing traffic rate on the selected interface.
	Policer Setup	Use this screen to configure QoS policers.
	Monitor	Use this screen to view statistics of QoS on WAN/LAN interface and the status of queues.

Table 5   Configuration Menus Summary (continued)

LINK	TAB	FUNCTION
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Port Triggering	Use this screen to change your Zyxel Device's port triggering settings.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the **Port Forwarding** screen.
	ALG	Use this screen to enable the ALGs (Application Layer Gateways) in the Zyxel Device to allow applications to operate through NAT.
	Address Mapping	Use this screen to change your Zyxel Device's address mapping settings.
	Sessions	Use this screen to configure the maximum number of NAT sessions each client host is allowed to have through the Zyxel Device.
DNS	DNS Entry	Use this screen to view and configure DNS routes.
	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
IGMP/MLD	IGMP/MLD	Use this screen to configure multicast settings (IGMP for IPv4 and MLD for IPv6 multicast groups) on the WAN.
Vlan Group	Vlan Group	Use this screen to group and tag VLAN IDs to outgoing traffic from the specified interface.
Interface Grouping	Interface Grouping	Use this screen to create multiple networks on the Zyxel Device.
Security		
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the Zyxel Device.
Parental Control	Parental Control	Use this screen to block web sites with the specific URL.
Scheduler Rule	Scheduler Rule	Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced.
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the Zyxel Device. You can export or email the logs.
	Security Log	Use this screen to view all security related events. You can select level and category of the security events in their proper drop-down list window.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Zyxel Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Zyxel Device.
	NAT	Use this screen to view NAT statistics for connected hosts.
ARP Table	ARP Table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.
Routing Table	Routing Table	Use this screen to view the routing table on the Zyxel Device.

Table 5   Configuration Menus Summary (continued)

LINK	TAB	FUNCTION
Multicast Status	IGMP Status	Use this screen to view the status of all IGMP settings on the Zyxel Device.
	MLD Status	Use this screen to view the status of all MLD settings on the Zyxel Device.
WLAN Station Status	WLAN Station Status	Use this screen to view the wireless stations that are currently associated with the Zyxel Device.
Steering Status	Steering Status	Use this screen to view the AP and band steering records.
Maintenance		
System	System	Use this screen to set Device name and Domain name.
User Account	User Account	Use this screen to change user password on the Zyxel Device.
Remote Management	MGMT Services	Use this screen to enable specific traffic directions for network services.
	Trust Domain	Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance** > **Remote Management** > **MGMT Services** screen.
SNMP	SNMP	Use this screen to configure SNMP (Simple Network Management Protocol) settings.
Time	Time	Use this screen to change your Zyxel Device's time and date.
E-mail Notification	E-mail Notification	Use this screen to configure up to two mail servers and sender addresses on the Zyxel Device.
Log Settings	Log Setting	Use this screen to change your Zyxel Device's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your Zyxel Device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your Zyxel Device's configuration (settings) or reset the factory default settings.
	ROM-D	Use this screen to save the current configuration as the defaults on the Zyxel Device.
Reboot	Reboot	Use this screen to reboot the Zyxel Device without turning the power off.
Diagnostic	Ping&Traceroute &Nslookup	Use this screen to identify problems with the Zyxel Device. You can use Ping, TraceRoute, or Nslookup to help you identify problems.
	802.1ag	Use this screen to configure CFM (Connectivity Fault Management) MD (maintenance domain) and MA (maintenance association), perform connectivity tests and view test reports.
	802.3ah	Use this screen to configure link OAM port parameters,

2.2.1.2 Icons

The navigation panel provides some icons on the right hand side.

Figure 14 Navigation Panel Icons (Administrator Login)

The icons provide the following functions.

Table 6   Web Configurator Icons

| ICON	DESCRIPTION
	Wizard: Click this icon to open the screens where you can configure the Zyxel Device's time zone Internet access, and wireless settings. See Chapter 3 on page 34 for more information about the **Wizard** screens.
	Theme: Click this icon to select a color that you prefer and apply it to the Web Configurator.
	Language: Select the language you prefer.
	Restart: Click this icon to reboot the Zyxel Device without turning the power off.
	Logout: Click this icon to log out of the Web Configurator.
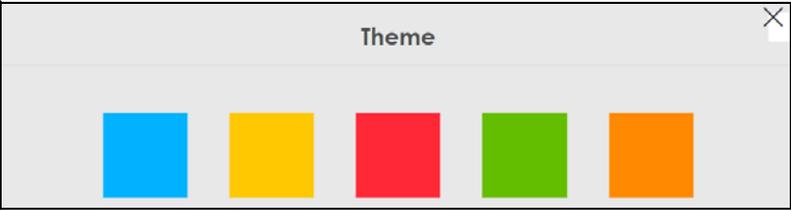
CHAPTER 3
Quick Start Wizard

3.1 Overview

Use the **Wizard** screens to configure the Zyxel Device's time zone, basic Internet access, and wireless settings.

Note: See the technical reference chapters (starting on Chapter 4 on page 39) for background information on the features in this chapter.

3.2 Wizard Setup

You can click the **Wizard** icon in the navigation panel to open the **Wizard** screens. See Section 2.2.1 on page 29 for more information about the navigation panel. After you click the **Wizard** icon, the following screen appears. Click **Let's Go** to proceed with settings on time zone, basic Internet access, and wireless networks. It will take you a few minutes to complete the settings on the **Wizard** screens. You can also click **Skip** to leave the **Wizard** screens.

Figure 15   Wizard - Home
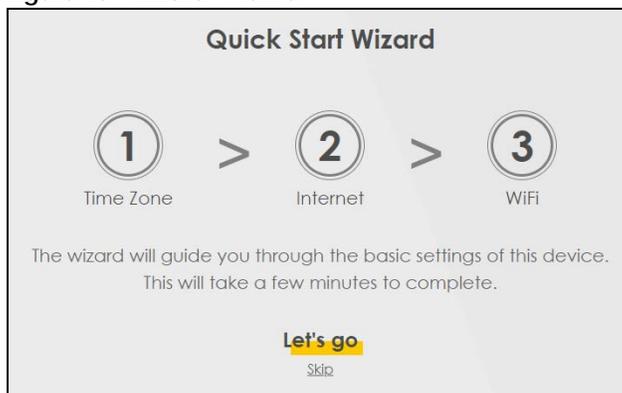
3.2.1 Time Zone

Select the time zone of your location. Click **Next**.

Figure 16 Wizard - Time Zone
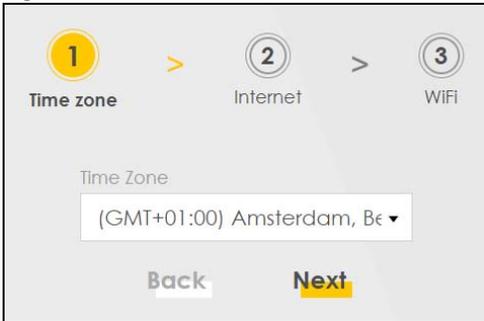
3.2.2 Internet

1 The Zyxel Device will check the Internet status automatically, and determine your connection type. Click **Next** to proceed. You can also click **Skip** to pass Internet settings in the **Wizard**.

Figure 17 Wizard - Internet
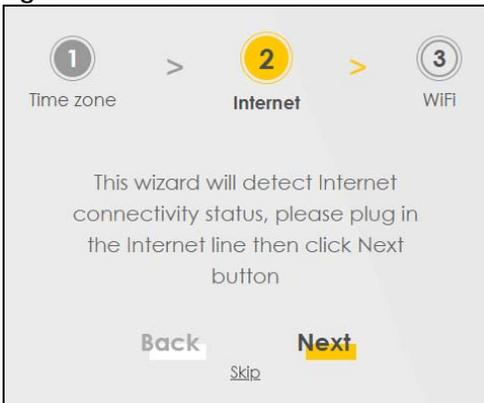
2 If the following screen displays, select the encapsulation type your ISP uses. Click **Next**.

Figure 18 Wizard - Incorrect Internet Information (IPoE)
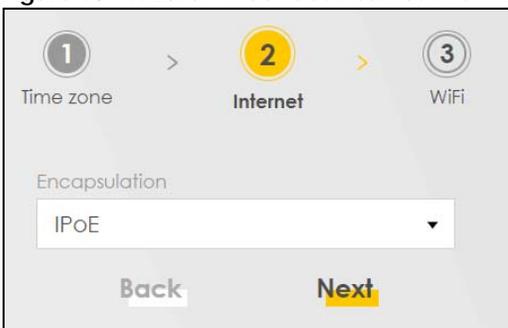
3 Enter your Internet connection information. The screen and fields to enter may vary depending on your current connection type. Click **Next**.

Figure 19 Wizard - Internet Connection Information (PPPoE)
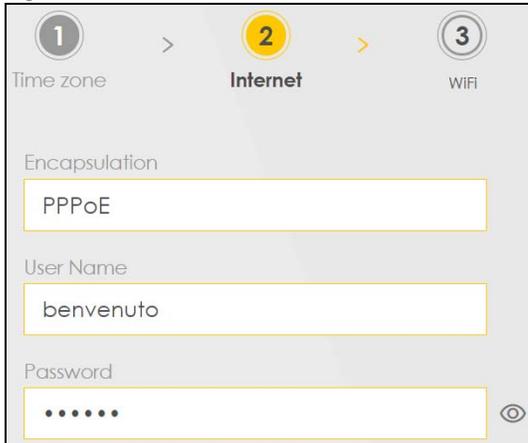
4 Click **Next** when the Zyxel Device has a successful Internet connection.

Figure 20 Wizard - Successful WAN Connection
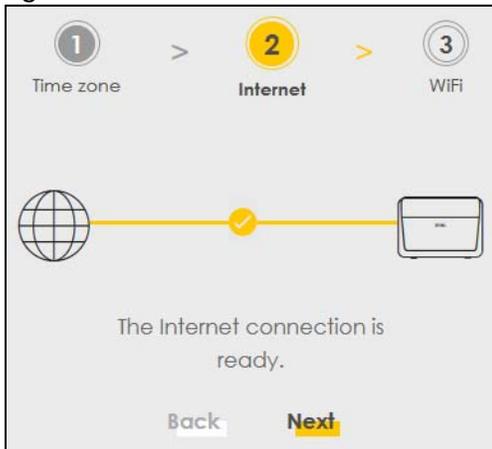
Unsuccessful Internet Connection

The following screen displays when the Zyxel Device did not detect a WAN connection. Connect the WAN port to a broadband modem or router for Internet access if you have not connected any. Click **Next**.

Figure 21   Wizard - WAN Connection is Down
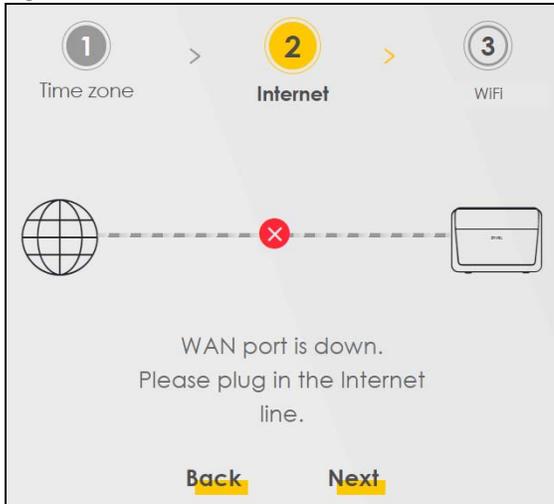
Incorrect Internet Information

If the following screen displays, click **Next** to configure the Internet settings.

Figure 22   Wizard - Incorrect Internet Information
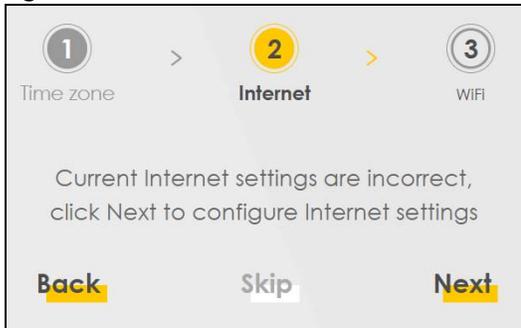
3.2.3 WiFi

Turn WiFi on or off. If you keep it on, record the security settings so you can configure your wireless clients to connect to the Zyxel Device.

Click the **Keep 2.4G and 5G the same** check box to use the same SSID for 2.4G and 5G wireless networks. Otherwise, deselect the check box to have two different SSIDs for 2.4G and 5G wireless networks. The screen and fields to enter may vary when you select or deselect the check box.

Click **Done** to complete the setup.

Figure 23 Wizard - WiFi

CHAPTER 4
Tutorials

4.1 Overview

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

- Setting Up a Secure Wireless Network, see page 39
- Setting Up Multiple Wireless Groups, see page 46
- Configuring Static Route for Routing to Another Network, see page 50
- Configuring QoS Queue and Class Setup, see page 52
- Access the Zyxel Device Using DDNS, see page 56
- Configuring the MAC Address Filter, see page 58

4.2 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 Zyxel Device serves as an access point (AP), and the notebook is the wireless client. The wireless client can access the Internet through the AP.
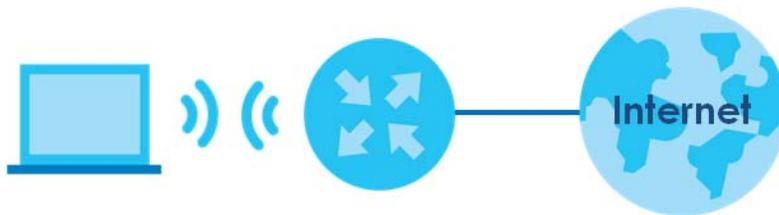
Thomas has to configure the wireless network settings on the Zyxel Device. Then he can set up a wireless network using WPS (Section 4.2.2 on page 41) or manual configuration (Section 4.2.3 on page 45).

4.2.1 Configuring the Wireless Network Settings

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

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

1 Click **Network Setting** > **Wireless** to open the **General** screen. Select **More Secure** as the security level and **WPA2-PSK** as the security mode. Configure the screen using the provided parameters (see page 39). Click **Apply**.

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. These are basic elements for starting a wireless service. It's recommended that you select **More Secure** to enable **WPA2-PSK** data encryption.

Wireless

| Wireless | ☑ Keep the same settings for 2.4G and 5G wireless networks |

Wireless Network Setup

Band	2.4GHz ▼	
Wireless	⬤	
Channel	Auto ▼	Current: 5 / 40 MHz
Bandwidth	20MHz ▼	
Control Sideband	None	

Wireless Network Settings

| Wireless Network Name | Example |
| Max Clients | 32 |

☐ Hide SSID   ⓘ   Hide SSID does not support WPS 2.0. You should disable WPS in WPS page.

☐ Blocking BSSID LAN Access

☑ Multicast Forwarding

| Max. Upstream Bandwidth | | Kbps |
| Max. Downstream Bandwidth | | Kbps |

Note

(1) If you are configuring the Zyxel Device from a computer connected to the wireless LAN and you change the Zyxel Device'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 Zyxel Device's new settings.

(2) If upstream/downstream bandwidth is empty, the Zyxel Device sets the value automatically. Setting a maximum upstream/downstream bandwidth will significantly decrease wireless performance.

BSSID   08:26:97:C4:CC:A3

Security Level

No Security   More Secure (Recommended)

| Security Mode | WPA2-PSK ▼ |

☐ Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

| Password | DoNotStealMyWirelessNetwork 👁 |
| Strength | strong |

| Encryption | AES ▼ |
| Timer | 3600 | sec |

Cancel   **Apply**

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

Use this screen to configure advanced wireless settings additional security settings, power saving, and data transmission settings.

RTS/CTS Threshold	2347
Fragmentation Threshold	2346
Output Power	100%
Beacon Interval	100 ms
DTIM Interval	1 ms
802.11 Mode	802.11b/g/n/ax Mixed
802.11 Protection	Auto
Preamble	Long
Protected Management Frames	Capable

Cancel   **Apply**

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the Zyxel Device (see Section 4.2.2 on page 41). He can also use the notebook's wireless client to search for the Zyxel Device (see Section 4.2.3 on page 45).

4.2.2 Using WPS

This section gives you an example of how to set up a wireless network using WPS. This example uses the Zyxel Device as the AP and a WPS-enabled Android 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 on page 41. 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 Zyxel Device's interface. See Section on page 43. This is the more secure method, since one device can authenticate the other.

Note: When using WPS in the Web Configurator, and depending on your **Band** selection (**2.4GHz** or **5GHz**), the secure connection will apply for the selected **Band** only.

Push Button Configuration (PBC)

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

2 Push and hold the **WPS** button located on the Zyxel Device's front panel for one second. Alternatively, you may log into the Zyxel Device's Web Configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function for method 1 and click **Apply**. Then click the **WPS** button.

WiFi Protected Setup (WPS) allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. To set up a WPS connection between two devices, both devices must support WPS. It is recommended to use the Push Button Configuration (**PBC**) method if your wireless client supports it.

General

WPS

Add a new device with WPS Method

Method 1 PBC   Method 2 PIN

Step1. Click WPS button   WPS   **Step1.** Enter the PIN of your new wireless client device and then click Register

Step2. Press the WPS button on your new wireless client device within 120 seconds   Register

Step2. Press the WPS button on your new wireless client device within 120 seconds

Note

(1) If WPS is Enabled, UPnP will automatically be turned on.

(2) The Zyxel Device applies the security settings of the main SSID (**SSID1**) profile.

(3) The WPS switch is grayed out when wireless LAN is disabled.

Cancel   Apply

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

Note: It does not matter which button is pressed first. You must press the second button within 2 minutes of pressing the first one.

The Zyxel Device sends the proper configuration settings to the wireless client. This may take up to 2 minutes. The wireless client is then able to communicate with the Zyxel Device securely.

The following figure shows you how to set up wireless network and security by pressing a button on both Zyxel Device and wireless client (the Android phone in this example).

Figure 24   Example WPS Process: PBC Method

Wireless Client

WITHIN 2 MINUTES

SECURITY INFO

COMMUNICATION
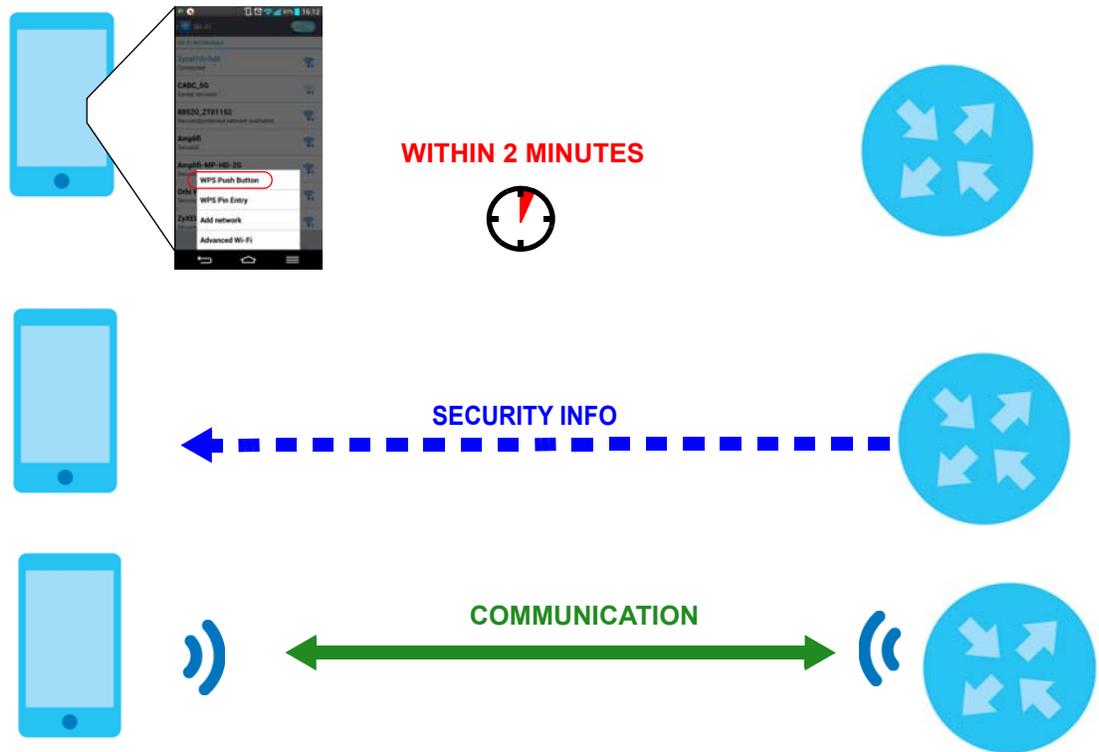
PIN Configuration

When you use the PIN configuration method, you need to check the client's PIN number and use the Zyxel Device's configuration interface.

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

2 Log into Zyxel Device's Web Configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function and click **Apply**.
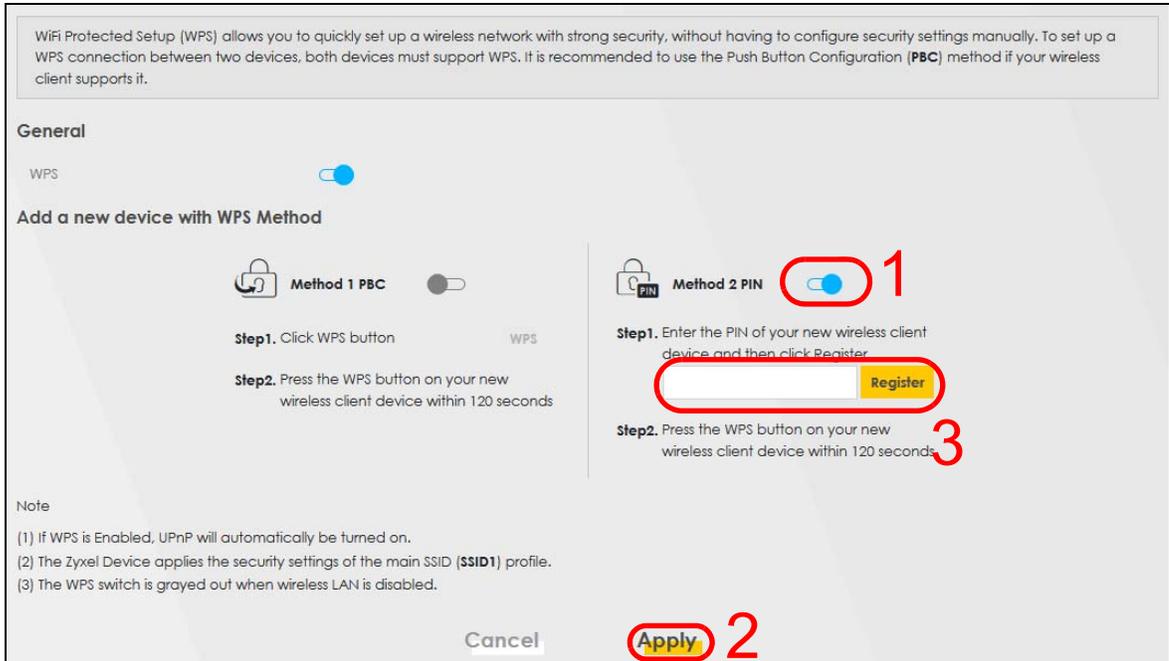
3 Enter the PIN number of the wireless client and click the **Register** button. Activate WPS function on the wireless client utility screen within two minutes.

The Zyxel Device 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 Zyxel Device securely.

The following figure shows you how to set up wireless network and security on Zyxel Device and wireless client (Android smartphone in this example) by using the PIN method.

Figure 25   Example WPS Process: PIN Method

Wireless Client
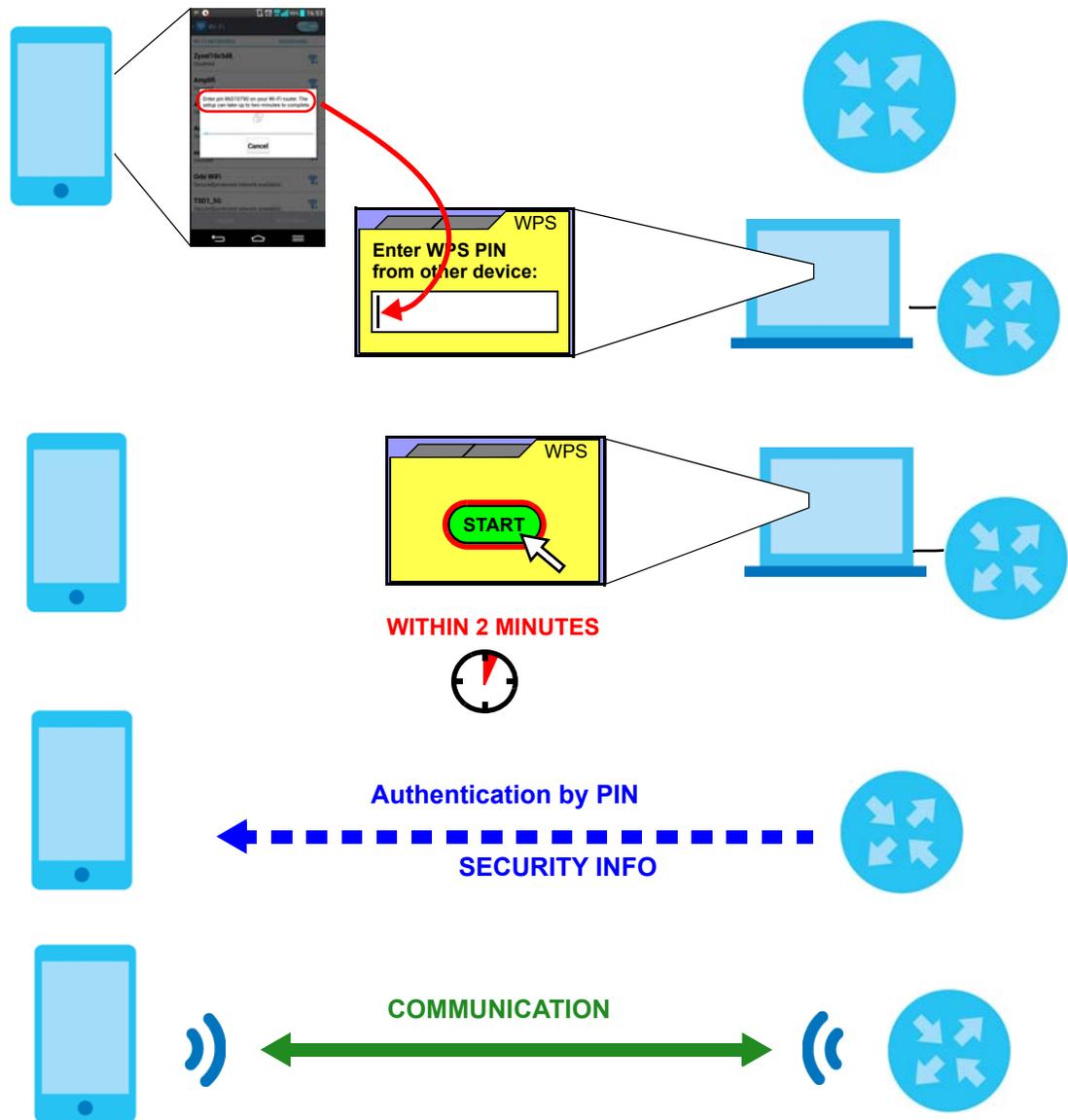
4.2.3 Without WPS

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

Note: The Zyxel Device supports IEEE 802.11a/b/g/n/ac/ax wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

4.3 Setting Up Multiple Wireless Groups

Company A wants to create different wireless network groups for different types of users as shown in the following figure. Each group has its own SSID and security mode.
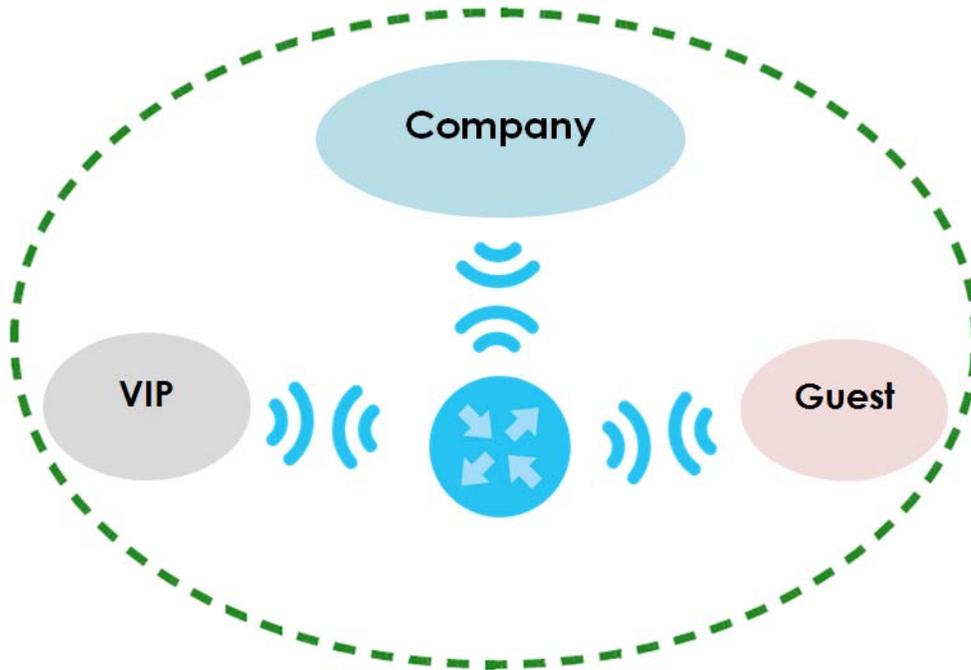
• Employees in Company A will use a general **Company** wireless network group.

• Higher management level and important visitors will use the **VIP** group.

• Visiting guests will use the **Guest** group, which has a different SSID and password.

Company A will use the following parameters to set up the wireless network groups.

	COMPANY	VIP	GUEST
SSID	Company	VIP	Guest
Security Level	More Secure	More Secure	More Secure
Security Mode	WPA2-PSK	WPA2-PSK	WPA2-PSK
Pre-Shared Key	ForCompanyOnly	123456789	guest123

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

2 Click **Network Setting > Wireless > Guest/More AP** to open the following screen. Click the **Edit** icon to configure the second wireless network group.

#	Status	SSID	Security	Guest WLAN	Modify
1	💡	Zyxel_9DE5_guest1	WPA2-Personal	External Guest	📝
2	💡	Zyxel_9DE5_guest2	WPA2-Personal	External Guest	📝
3	💡	Zyxel_9DE5_guest3	WPA2-Personal	External Guest	📝

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

Note: The Guest SSID (**Wireless Network Name**) depends on the state of the Main SSID. For example, when the 2.4GHz Main SSID is enabled, then the 2.4GHz Guest SSID can be enabled. But when the 2.4GHz Main SSID is disabled, then the 2.4GHz Guest SSID is automatically disabled (cannot be enabled by the user).

4 In the **Guest/More AP** screen, click the **Edit** icon to configure the third wireless network group. Configure the screen using the provided parameters and click **Apply**.

5 Check the status of **VIP** and **Guest** in the **Guest/More AP** screen. The yellow bulbs signify that the SSIDs are active and ready for wireless access.

#	Status	SSID	Security	Guest WLAN	Modify
1		Home&Life SuperWiFi-F0FD_guest1	WPA2-Personal	External Guest	
2		VIP	WPA2-Personal	External Guest	
3		Guest	WPA2-Personal	External Guest	

4.4 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the Zyxel Device'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 Zyxel Device'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 Zyxel Device's WAN default gateway by default. In this case, **B** will never receive the traffic.
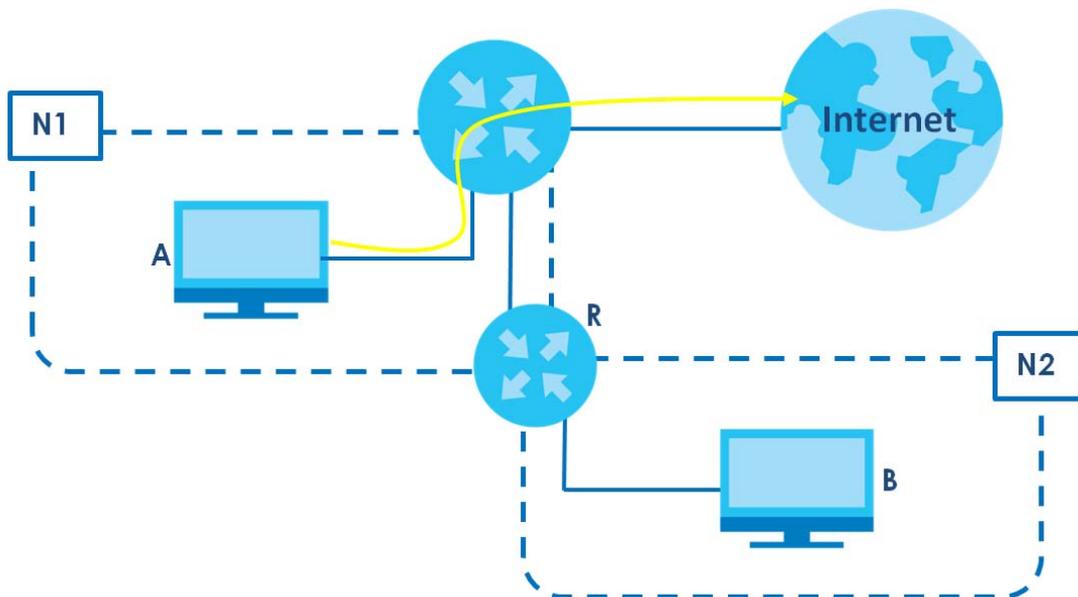
You need to specify a static routing rule on the Zyxel Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the Zyxel Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.
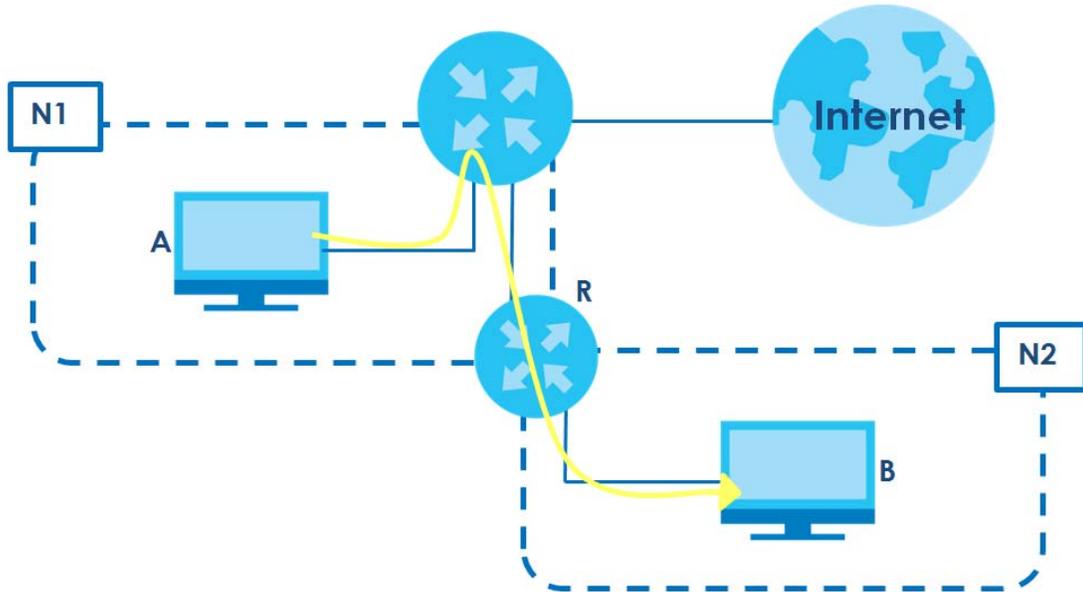
This tutorial uses the following example IP settings:

Table 7   IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The Zyxel Device's WAN	172.16.1.1
The Zyxel Device's LAN	192.168.1.1
IP Type	IPv4
Use Interface	Ethernet
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 Zyxel Device's Web Configurator in advanced mode.

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

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

4 Create a new static route using the following settings:

4a Click the **Active** button to enable this static route. When the switch goes to the right ( ), the function is enabled. Enter the **Route Name** as **R**.

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

4c Type the **Destination IP Address 192.168.10.0** and **IP Subnet Mask 255.255.255.0** for the destination, **N2**.

4d Click the **Use Gateway IP Address** button to enable this function. When the switch goes to the right ( ), the function is enabled. Type **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.

4e Select **ETHWAN** as the **Use Interface**.
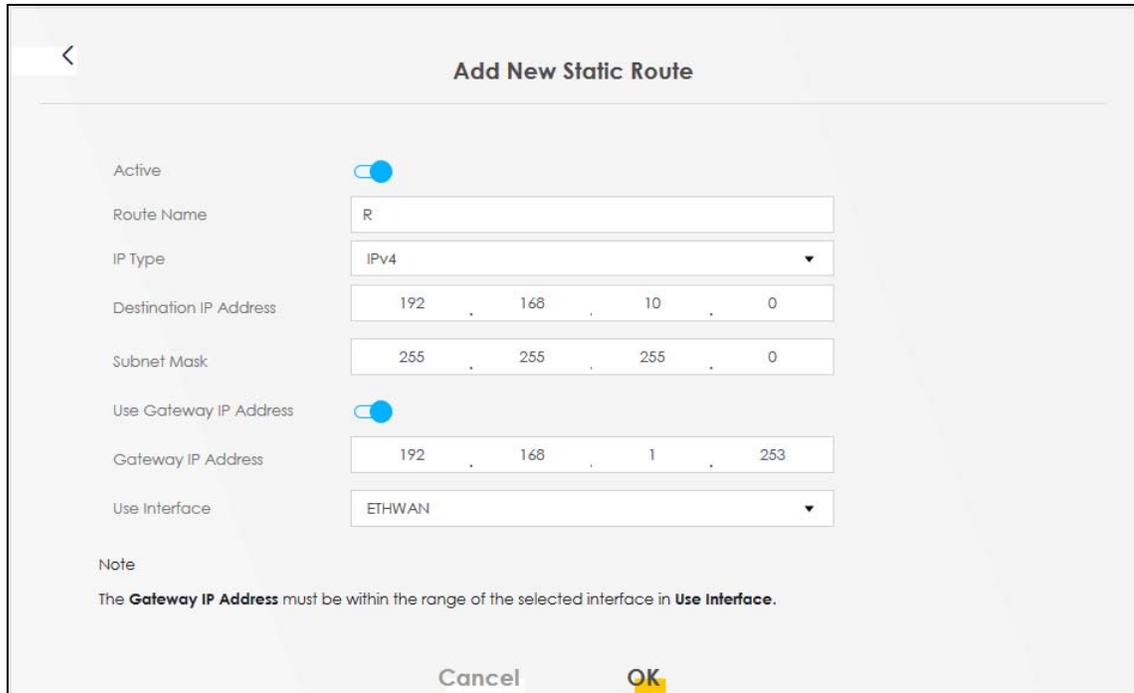
4a Click **OK**.

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

4.5 Configuring QoS Queue and Class Setup

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

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

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

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

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

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

Your computer
IP=192.168.1.23
and/or
MAC=AA:FF:AA:FF:AA:FF
E-mail traffic: Highest priority

A colleague's computer
Other traffic: Automatic classifier

10,000 kbps

Internet
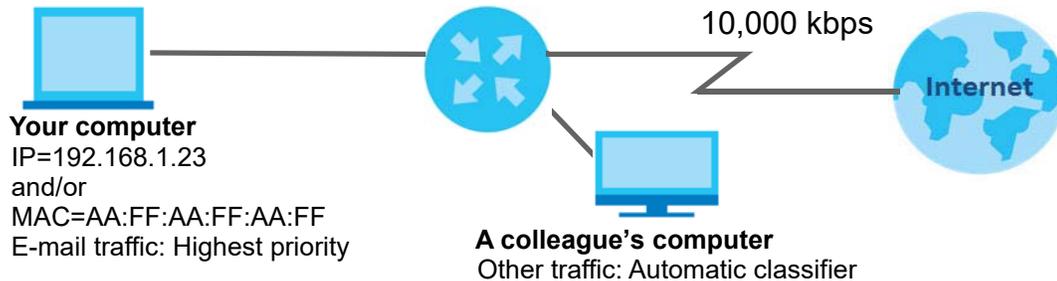
1 Click **Network Setting > QoS > General** and click the **QoS** button to enable. When the switch goes to the right ( ), the function is enabled. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the Zyxel Device automatically determine this figure). Click **Apply**.

Use this screen to enable or disable QoS and set the upstream bandwidth or assign traffic priority.

When one of the following situations happens, the current WAN linkup rate will be used instead:
1. **WAN Managed Upstream Bandwidth** is set to 0
2. **WAN Managed Upstream Bandwidth** is empty
3. **WAN Managed Upstream Bandwidth** is higher than the current WAN interface linkup rate

QoS

WAN Managed Upstream Bandwidth   10000   (kbps)

Upstream Traffic Priority Assigned by   None

Note
(1) Manually defined QoS is ignored when **Upstream Traffic Priority** is selected.
(2) **Upstream Traffic Priority** automatically assigns a traffic priority level based on the selected criteria.
(3) To have your QoS settings configured in other **QoS** screens take effect, select **None** in the **Upstream Traffic Priority** field.

Cancel   Apply

2 Click **Network** > **Queue Setup** > **Add new Queue** to create a new queue. In the screen that opens, click the **Active** field to enable. When the switch goes to the right ( ), the function is enabled. Enter or select the following values:

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

Add New Queue

Active	
Name	E-mail
Interface	WAN ▼
Priority	1 (highest) ▼
Weight	8 ▼
Buffer Management	Drop Tail(DT) ▼
Rate Limit	5000 (kbps)

Cancel   OK

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

Add New Classification   ✕

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

Step1: Class Configuration

Active	⬤
Class Name	Email
Classification Order	Last ▼

Step2: Criteria Configuration

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

Basic

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

Source

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

Destination

☐ Address		Subnet Mask		◼ Exclude
◼ Port Range		~		◼ Exclude
☐ MAC	- - - - -	MAC Mask		◼ Exclude

Others

☐ Service	RTSP Server ▼		◼ Exclude
☑ IP protocol	User Defined ▼	25	☐ Exclude
☐ DHCP	▼		◼ Exclude
☐ IP Packet Length		~	◼ Exclude
☐ DSCP		(0~63)	◼ Exclude
◼ 802.1P	0 BE ▼		◼ Exclude
◼ VLAN ID		(1~4094)	◼ Exclude
◼ TCP ACK			◼ Exclude

Step3: Packet Modification

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

DSCP Mark	Unchange ▼		(0~63)
VLAN ID Tag	Unchange ▼	0	(1~4094)
802.1P Mark	0 BE ▼		

Step4: Class Routing

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

Forward To Interface	Unchange ▼

Step5: Outgoing Queue Selection

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

To Queue Index	Email ▼

Cancel   OK

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

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

4.6 Access the Zyxel Device Using DDNS

If you connect your Zyxel Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The Zyxel Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the Zyxel Device using a domain name.
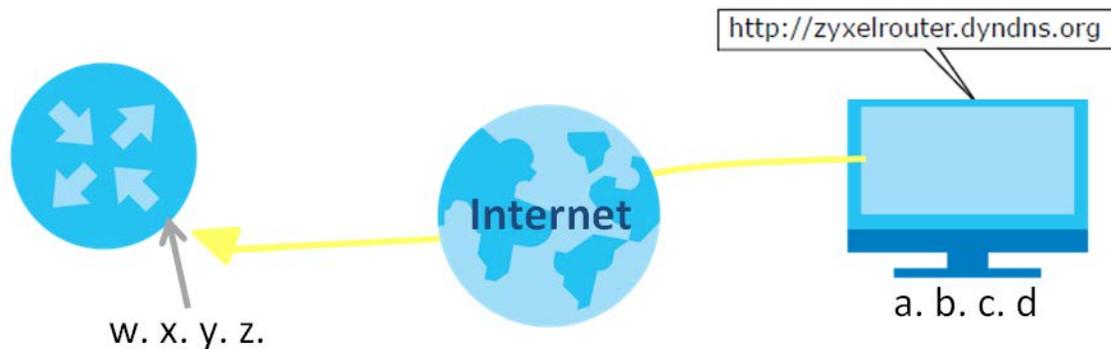
To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial covers:

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

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

4.6.1 Registering a DDNS Account on www.dyndns.org

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

2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.

3 Log into www.dyndns.org using your account.

4   Add a new DDNS host name. This tutorial uses the following settings as an example.

- Hostname: **zyxelrouter.dyndns.org**

- Service Type: **Host with IP address**

- IP Address: Enter the WAN IP address that your Zyxel Device is currently using. You can find the IP address on the Zyxel Device's Web Configurator **Status** page.

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

4.6.2 Configuring DDNS on Your Zyxel Device

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

- Select **Enable Dynamic DNS**.

- Select **www.DynDNS.com** as the service provider.

- Type **zyxelrouter.dyndns.org** in the **Host Name** field.

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

Click **Apply**.

4.6.3 Testing the DDNS Setting

Now you should be able to access the Zyxel Device 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 Zyxel Device's login page should appear. You can then log into the Zyxel Device and manage it.

4.7 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 Zyxel Device. Thomas decides to use the **Security > MAC Filter** screen to grant wireless network access to his computer but not to Josephine's computer.
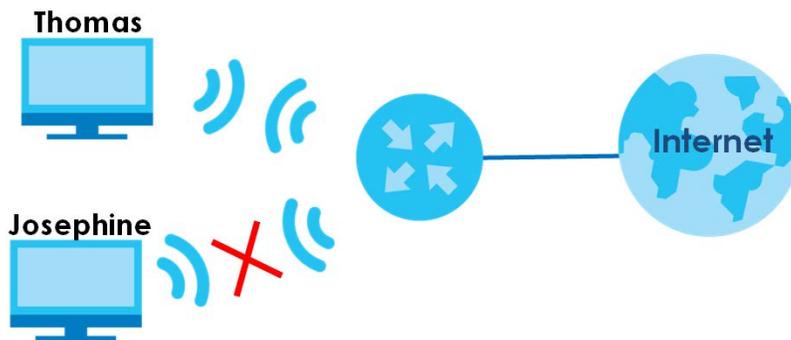
1   Click **Security** > **MAC Filter** to open the **MAC Filter** screen. Select the **Enable** check box to activate MAC filter function.

2   Select **Allow**. Click **Add a new setting** to add a new entry. Then enter the host name and MAC address of Thomas' computer in this screen. Click **Apply**.

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

PART II
Technical Reference

CHAPTER 5
Connection Status

5.1 Overview

After you log into the Web Configurator, the **Connection Status** screen appears. You can configure basic Internet access, wireless settings, and parental control settings in this screen. It also shows the network status of the Zyxel Device and computers/devices connected to it.

Figure 26 Connection Status
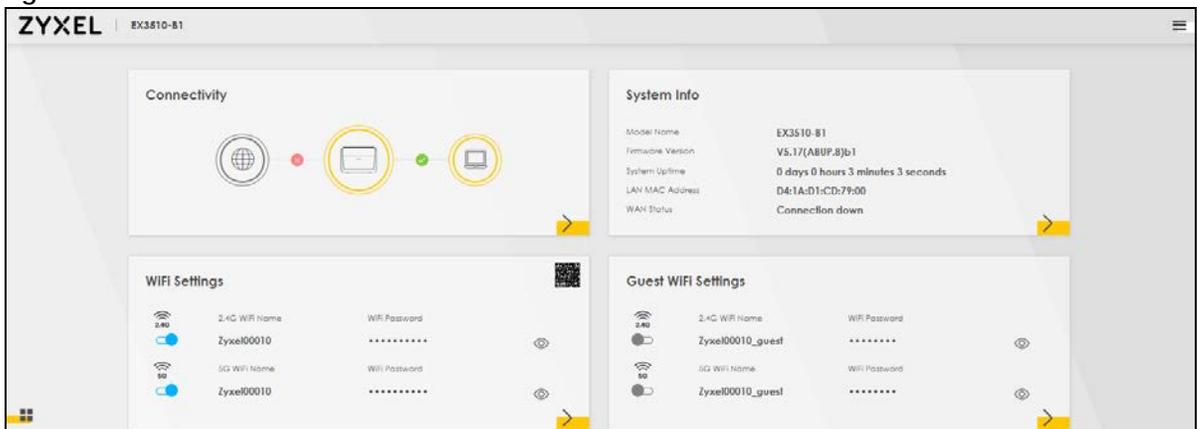
5.1.1 Layout Icon

Click this icon (⬛) to arrange the screen order. Select a block and hold it to move around. Click the Check icon (☑) in the lower left corner to save the changes.

Figure 27 Change Screen Order
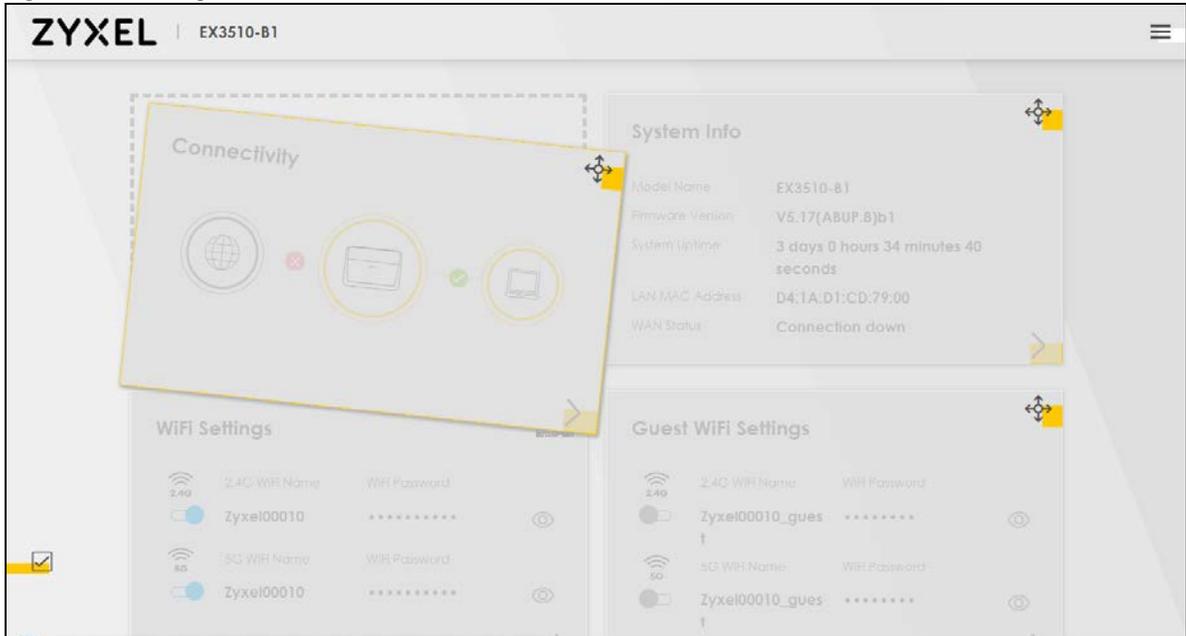
5.1.2 Connectivity

Use this screen to view the network connection status of the Zyxel Device and its clients.

Figure 28 Connectivity
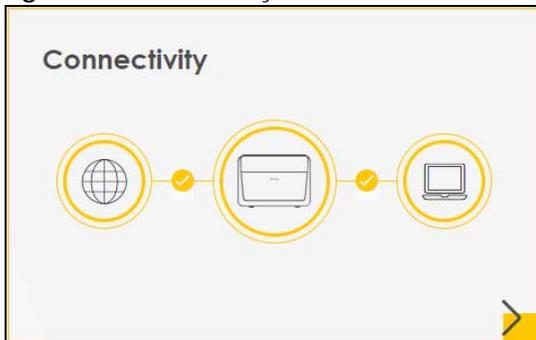
Click the Arrow icon ( ) to open the following screen. Use this screen to view IP addresses and MAC addresses of the wireless and wired devices connected to the Zyxel Device.

Place your mouse within the device block, and an Edit icon ( ) will appear. Click the Edit icon to change the icon and name of a connected device.

Figure 29   Connectivity: Connected Devices

Icon and Device Name

You can change the icon and name of a connected device by clicking the device's Edit icon. Select an icon and/or enter a name in the **Device Name** field for a connected device. Click **Save** to save your changes.

Figure 30   Connectivity: Edit
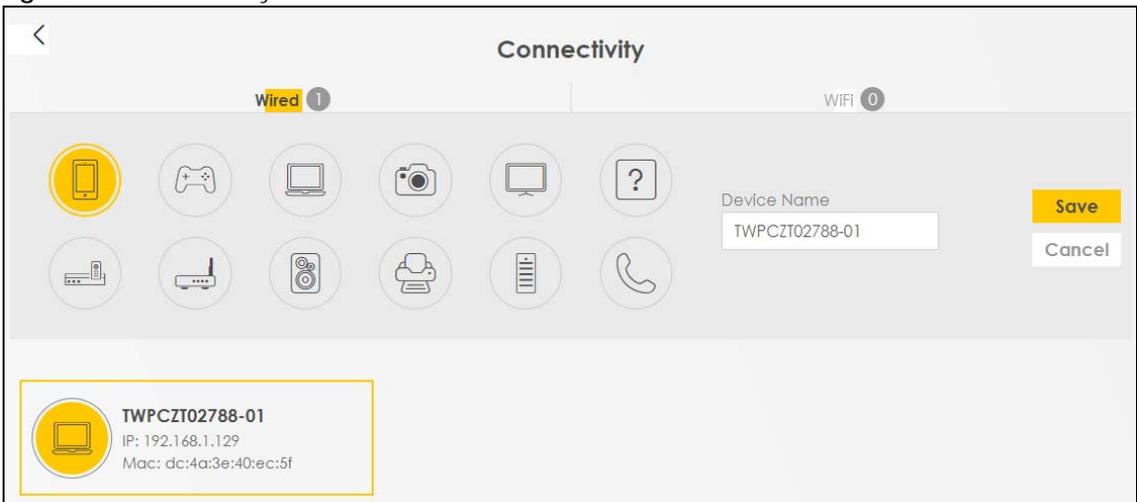
5.1.3 System Information

Use this screen to view the basic system information of the Zyxel Device.

Figure 31   System Information

Click the Arrow icon ( ) to open the following screen. Use this screen to view more information on the status of your firewall and interfaces (WAN, LAN, and WiFi).

Figure 32 System Information: Detailed Information

Each field is described in the following table.

Table 8   System Info: Detailed Information

LABEL	DESCRIPTION
Host Name	This field displays the Zyxel Device system name. It is used for identification.
Model Name	This shows the model number of your Zyxel Device.
Serial Number	This field displays the serial number of the Zyxel Device.
Firmware Version	This is the current version of the firmware on the Zyxel Device.
System Up Time	This field displays how long the Zyxel Device has been running since it last started up. The Zyxel Device starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it.
Interface Status Virtual ports are shown here. You can see whether the ports are in use and their transmission rate.	
WAN Information (These fields display when you have an Internet connection.)	
Name	This field displays the name given to the Internet connection.
Encapsulation	This field displays the current encapsulation method.
IP Address	This field displays the current IPv4 address of the Zyxel Device. Click the **Release** button to release the IP address provided by a DHCP server. Click the **Renew** button to renew the IP address. Click the **Disconnect** button to disconnect the PPP WAN when PPP WAN has an IPv4 address. Click the **Connect** button to connect the PPP WAN. The Web Configurator will display the loading panel until the IP address has been released/renewed/disconnected/connected.
IP Subnet Mask	This field displays the current subnet mask in the WAN.

Table 8   System Info: Detailed Information (continued)

LABEL	DESCRIPTION
IPv6 Address	This field displays the current IPv6 address of the Zyxel Device.
MAC Address	This field displays the WAN Ethernet adapter MAC (Media Access Control) address of your Zyxel Device.
Primary DNS server	This field displays the first DNS server address assigned by the ISP.
Secondary DNS server	This field displays the second DNS server address assigned by the ISP.
LAN Information (These fields display information about the LAN ports.)	
IP Address	This is the current IPv4 address of the Zyxel Device in the LAN.
Subnet Mask	This is the current subnet mask in the LAN.
IPv6 Address	This is the current IPv6 address of the Zyxel Device in the LAN.
IPv6 Link Local Address	This field displays the current link-local address of the Zyxel Device for the LAN interface.
DHCP	This field displays what DHCP services the Zyxel Device is providing to the LAN. The possible values are: **Server** - The Zyxel Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The Zyxel Device is not providing any DHCP services to the LAN.
MAC Address	This field displays the LAN Ethernet adapter MAC (Media Access Control) address of your Zyxel Device.
Security	
Firewall	This displays the firewall's current security level.
WLAN Information 2.4GHz/5GHz	
MAC Address	This shows the wireless adapter MAC (Media Access Control) address of the wireless interface.
Status	This displays whether WiFi is activated.
SSID	This is the descriptive name used to identify the Zyxel Device in a wireless LAN.
Channel	This is the channel number used by the wireless interface now.
Security	This displays the type of security mode the wireless interface is using in the wireless LAN.
802.11 Mode	This displays the type of 802.11 mode the wireless interface is using in the wireless LAN.
WPS	This displays whether WPS is activated on the wireless interface.

5.2 WiFi Settings

Use this screen to enable or disable the main 2.4G and/or 5G wireless networks. When the switch goes to the right (⬤), the function is enabled. Otherwise, it is not. You can use this screen or the QR code on the upper right corner to check the SSIDs (WiFi network name) and passwords of the main wireless networks. If you want to show or hide your WiFi passwords, click the Eye icon (∅).

Figure 33   WiFi Settings
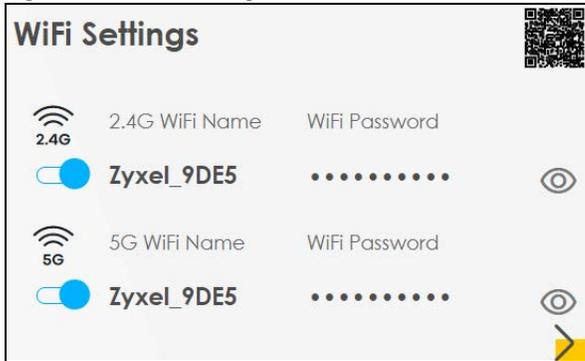
Click the Arrow icon ( ) to open the following screen. Use this screen to configure the SSIDs and/or passwords for your main wireless networks. Select **Keep 2.4G and 5G the same** to use the same SSID for 2.4 GHz and 5 GHz bands.

Figure 34   WiFi Settings: Configuration
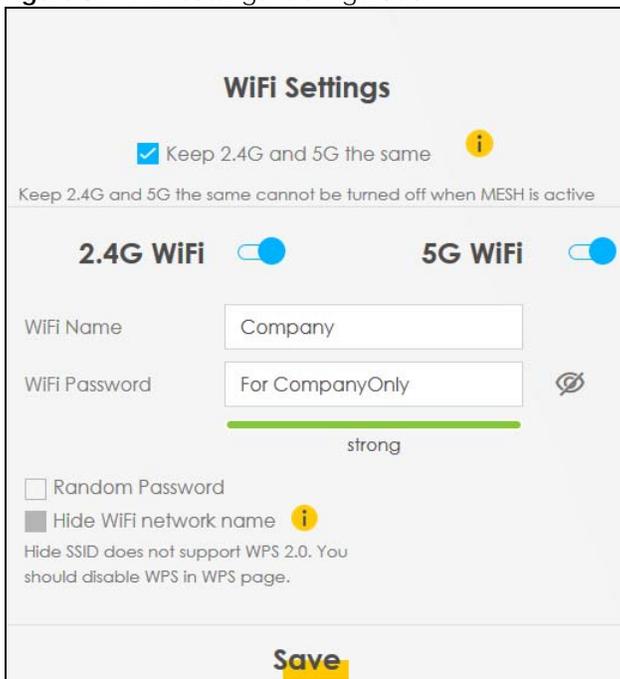
Each field is described in the following table.

Table 9   WiFi Settings: Configuration

LABEL	DESCRIPTION
Keep 2.4G and 5G the same	Select this and the 2.4G and 5G wireless networks will use the same SSID.
	If you deselect this, the screen will change. You need to assign different SSIDs for the 2.4G and 5G wireless networks.
2.4G/5G WiFi	Click this switch to enable or disable the 2.4G and/or 5G wireless networks. When the switch goes to the right , the function is enabled. Otherwise, it is not.
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.
	Enter a descriptive name (up to 32 English keyboard characters) for WiFi.

Table 9   WiFi Settings: Configuration (continued)

LABEL	DESCRIPTION
WiFi Password	If you selected **Random Password**, this field displays a pre-shared key generated by the Zyxel Device.
	If you did not select **Random Password**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
	Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed ⊘ , you will see the password in plain text. Otherwise, it is hidden.
Random Password	Select this option to have the Zyxel Device automatically generate a password. The **WiFi Password** field will not be configurable when you select this option.
Hide WiFi Name	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.
	Note: Disable WPS in the **Network Setting** > **Wireless** > **WPS** screen to hide the SSID.
Save	Click **Save** to save your changes.

5.3 Guest WiFi Settings

Use this screen to enable or disable the guest 2.4G and/or 5G wireless networks. When the switch goes to the right (⬤━), the function is enabled. Otherwise, it is not. You can check their SSIDs (WiFi network name) and passwords from this screen. If you want to show or hide your WiFi passwords, click the Eye icon.

Figure 35   Guest WiFi Settings
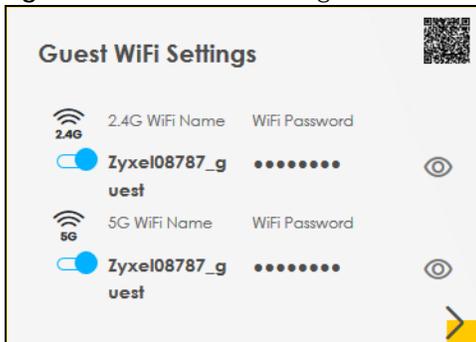
Click the Arrow icon (>) to open the following screen. Use this screen to configure the 2.4G and 5G SSIDs and/or passwords for your guest wireless networks.

Figure 36 Guest WiFi Settings: Configuration

To assign different SSIDs to the 2.4G and 5G guest wireless networks, clear the **Keep 2.4G and 5G the same** check box in the **WiFi Settings** screen, and the **Guest WiFi Settings** screen will change.

Figure 37 Guest WiFi Settings: Different SSIDs

Each field is described in the following table.

Table 10 WiFi Settings: Configuration

LABEL	DESCRIPTION
WiFi 2.4G/5G WiFi	Click this switch to enable or disable the 2.4G and/or 5G wireless networks. When the switch goes to the right, the function is enabled. Otherwise, it is not.
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
WiFi Password	If you selected **Random Password**, this field displays a pre-shared key generated by the Zyxel Device. If you did not select **Random Password**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
	Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed, you'll see the password in plain text. Otherwise, it is hidden.

Table 10   WiFi Settings: Configuration (continued)

LABEL	DESCRIPTION
Random Password	Select this option to have the Zyxel Device automatically generate a password. The **WiFi Password** field will not be configurable when you select this option.
Hide WiFi Name	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. Note: Disable WPS in the **Network Setting** > **Wireless** > **WPS** screen to hide the SSID.
Save	Click **Save** to save your changes.

5.4 LAN Settings

Use this screen to view the LAN IP address, subnet mask, and DHCP settings of your Zyxel Device.

Figure 38   LAN

Click the Arrow icon ( ) to open the following screen. Use this screen to configure the LAN IP address and DHCP setting for your Zyxel Device.

Figure 39   LAN Setup

Each field is described in the following table.

Table 11   Status Screen

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IPv4 address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
IP Addressing Values	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
DHCP Server State	
DHCP Server Lease Time	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems.
Days/Hours/ Minutes	Enter the lease time of the DHCP server.
Save	Click **Save** to save your changes.

5.5 Parental Control

Use this screen to view the number of profiles that were created for parental control.

Figure 40   Parental Control

Click the Arrow icon (➤) to open the following screen. Use this screen to enable parental control and add more profiles. Add a profile to create restricted access schedules. Go to the **Security** > **Parental Control** > **Add New PCP/Edit** screen to configure URL filtering settings to block the users on your network from accessing certain web sites.

Figure 41 Parental Control: Scheduled Profile (no profile)
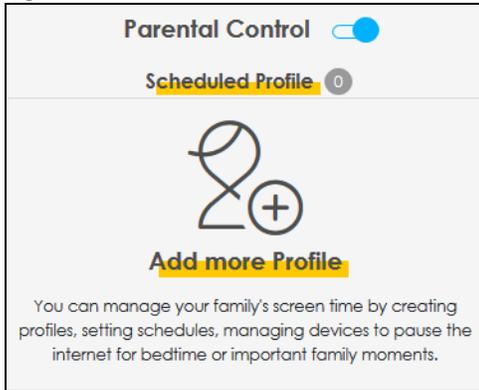
Figure 42 Parental Control: Scheduled Profile
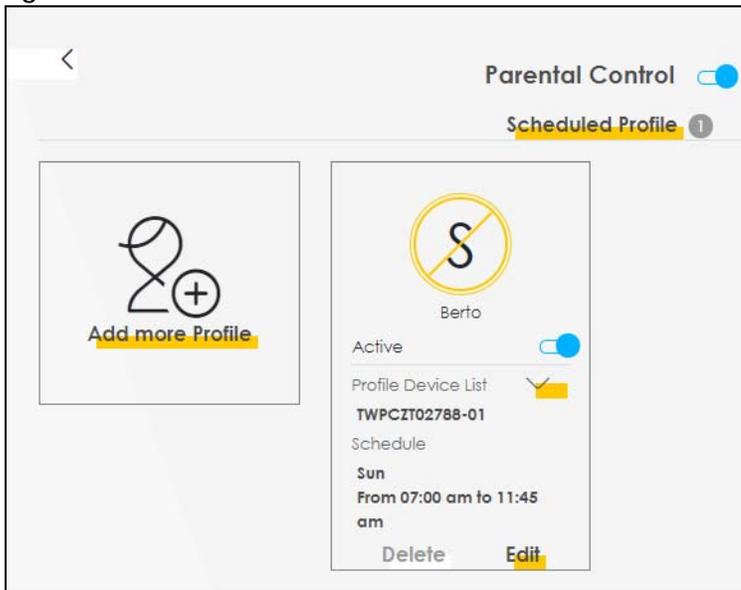
Each field is described in the following table.

Table 12 Parental Control: Schedule

LABEL	DESCRIPTION
Parental Control	Click this switch to enable or disable parental control. When the switch goes to the right ( ), the function is enabled. Otherwise, it is not.
Active	Click this switch to enable or disable a created profile. When the switch goes to the right ( ), this profile is active. Otherwise, it is not.
Scheduled Profile	This screen shows all the created profile(s). Click beside **Profile Device List** to view more information about the profile. You can click **Delete** to remove the profile or click **Edit** to change the profile settings. Only the **Add more Profile** button displays if there is no profile created.
Add more Profile	Click this button to create a new profile.

5.5.1 Create/Edit a Parental Control Profile

Click **Add more Profile** to create a profile or click **Edit** of an existing profile to change its settings. Use this screen to add a device(s) in a profile and block Internet access on the profile device(s).

Figure 43 Parental Control: Select Device

Each field is described in the following table.

Table 13   Parental Control: Select Device

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile.
Profile Active	Click this switch to enable or disable the profile. When the switch goes to the right 🔵 , the profile is enabled. Otherwise, it is disabled.
Profile Device List	This field shows the devices selected on the right for this profile.
Allowing Schedule	This field shows the time during which Internet access is blocked on the profile device(s).
	Select the device(s) on your network for this profile and click **Next**.

5.5.2 Define a Schedule

This screen allows you to define time periods and days during which Internet access is blocked on the profile device(s).

Figure 44   Parental Control > Add More Profile: Schedule

Each field is described in the following table.

Table 14   Parental Control: Time Limit

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile.
Profile Active	Click this switch to enable or disable the profile. When the switch goes to the right , the profile is enabled. Otherwise, it is disabled.
Profile Device List	This field shows the devices selected on the right for this profile.
Allowing Schedule	This field shows the time during which Internet access is blocked on the profile device(s).
Schedule	
Add New Schedule	Click this to add a new block for scheduling.
Start/End blocking	Select the time period when Internet access is blocked on the profile device(s). Select **Whole Day** and the scheduler rule will be activated 24 hours of the day. Select **Whole Week** and the scheduler rule will be activated everyday of the week.
Repeat On	Select the days when Internet access is blocked on the profile device(s).
Back	Click **Back** to return to the previous screen.
Save	Click **Save** to save your changes.

CHAPTER 6
Broadband

6.1 Overview

This chapter discusses the Zyxel Device's **Broadband** screens. Use these screens to configure your Zyxel Device 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 45 LAN and WAN
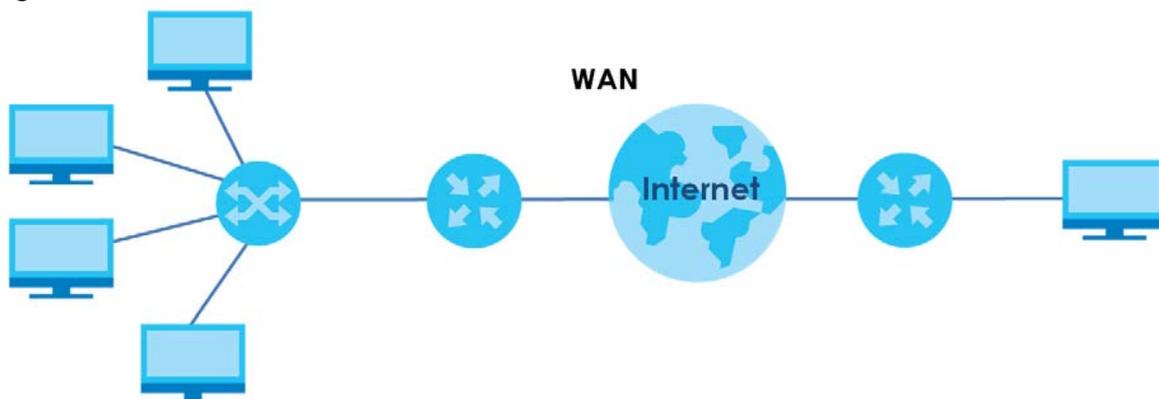
6.1.1 What You Can Do in this Chapter

Use the **Broadband** screen to view, remove or add a WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access (Section 6.2 on page 77).

Table 15   WAN Setup Overview

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

6.1.2 What You Need to Know

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

WAN IP Address

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

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

IPv6 Introduction

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

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

IPv6 Prefix and Prefix Length

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

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

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

IPv6 Subnet Masking

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

IPv6 Rapid Deployment

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

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

Figure 46 IPv6 Rapid Deployment
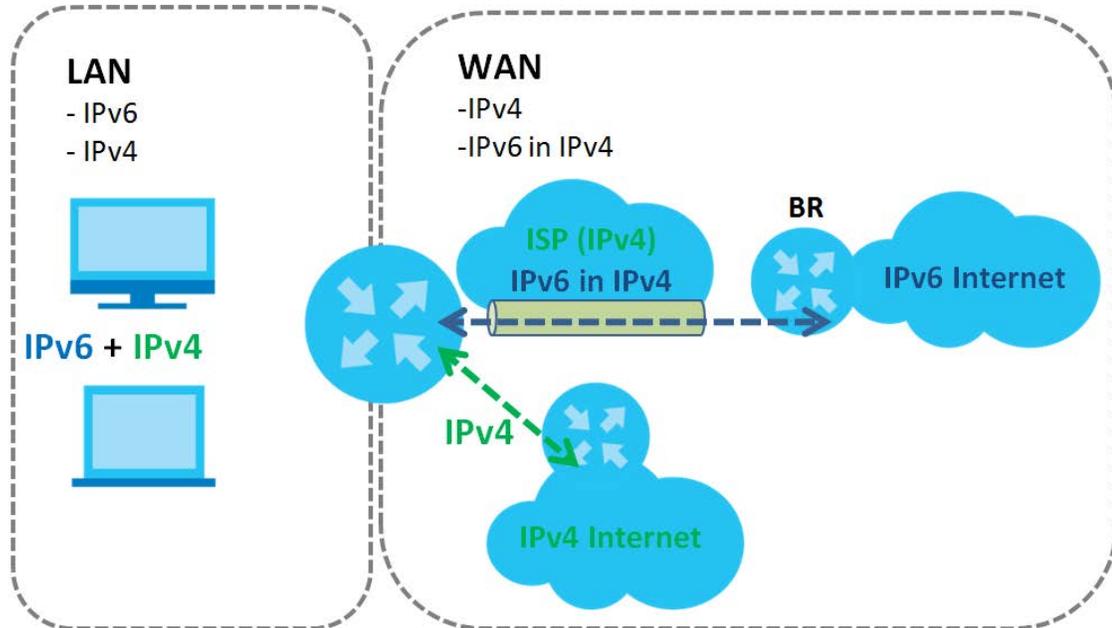
Dual Stack Lite

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

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

Figure 47   Dual Stack Lite
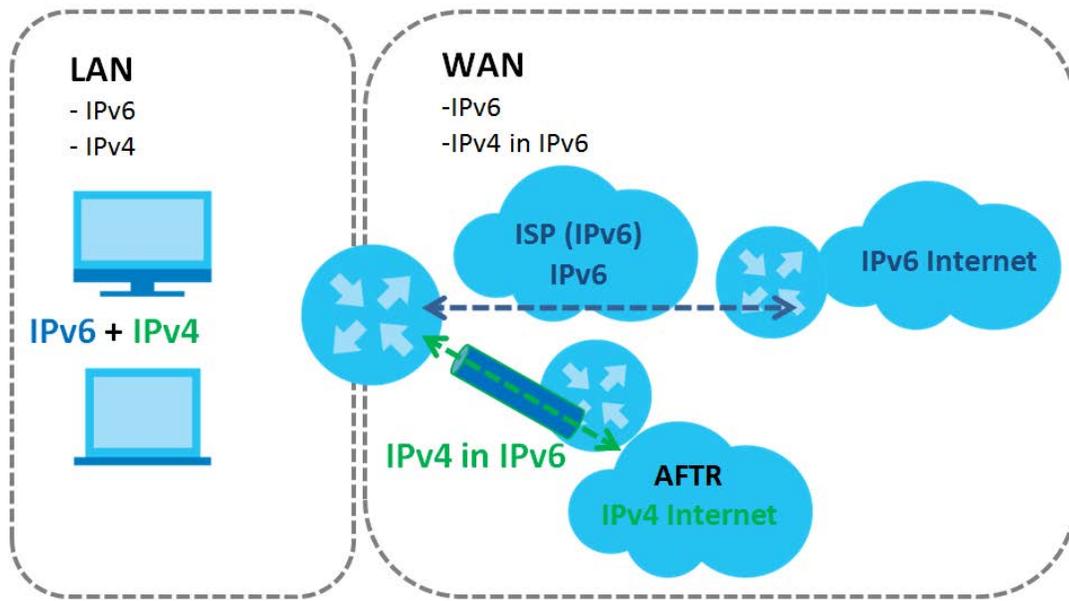
6.1.3 Before You Begin

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

6.2 Broadband Settings

Use this screen to change your Zyxel Device's Internet access settings. The summary table shows you the configured WAN services (connections) on the Zyxel Device. Use information provided by your ISP to configure WAN settings.

Click **Network Setting** > **Broadband** to access this screen.

Figure 48   Network Setting > Broadband

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

The following table describes the labels in this screen.

Table 16   Network Setting > Broadband

LABEL	DESCRIPTION
Add New WAN Interface	Click this button to create a new connection.
#	This is the index number of the entry.
Name	This is the service name of the connection.
Type	This shows it is an Ethernet connection.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.
802.1p	This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
802.1q	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
IGMP Proxy	This shows whether the Zyxel Device act as an IGMP proxy on this connection.
NAT	This shows whether NAT is activated or not for this connection.
Default Gateway	This shows whether the Zyxel Device use the WAN interface of this connection as the system default gateway.
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service.
MLD Proxy	This shows whether Multicast Listener Discovery (MLD) is activated or not for this connection. MLD is not available when the connection uses the bridging service.
Modify	Click the **Edit** icon to configure the WAN connection. Click the **Delete** icon to remove the WAN connection.

6.2.1 Add/Edit Internet Connection

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

Routing Mode

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

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

Figure 49 Network Setting > Broadband > Add/Edit New WAN Interface (Routing Mode)

The following table describes the labels in this screen.

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

LABEL	DESCRIPTION
General	Click this switch to enable or disable the interface. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Name	Specify a descriptive name for this connection.
Type	This field shows an Ethernet connection.
Mode	Select **Routing** if your ISP give you one IP address only and you want multiple computers to share an Internet account.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select **Routing** in the **Mode** field. The choices are **PPPoE** and **IPoE**.
IPv4/IPv6 Mode	Select **IPv4 Only** if you want the Zyxel Device to run IPv4 only. Select **IPv4 IPv6 DualStack** to allow the Zyxel Device to run IPv4 and IPv6 at the same time. Select **IPv6 Only** if you want the Zyxel Device to run IPv6 only.
PPP Information (This is available only when you select **Routing** in the **Mode** field.)	
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above. Select **password unmask** to show your entered password in plain text.
PPP Connection Trigger	Select when to have the Zyxel Device establish the PPP connection. **Auto Connect** - select this to not let the connection time out. **On Demand** - select this to automatically bring up the connection when the Zyxel Device receives packets destined for the Internet.
Idle Timeout	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server. This field is not available if you select **Auto Connect** in the **PPP Connection Trigger** field.
PPPoE Passthrough	This field is available when you select **PPPoE** encapsulation. In addition to the Zyxel Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Zyxel Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
VLAN	Click this switch to enable or disable VLAN on this WAN interface. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
MTU	
MTU	Enter the MTU (Maximum Transfer Unit) size for traffic through this connection.
IP Address (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	

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

LABEL	DESCRIPTION
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP. This is available only when you set the **Encapsulation** to **IPoE**.
Gateway IP Address	Enter the gateway IP address provided by your ISP. This is available only when you set the **Encapsulation** to **IPoE**.
DNS Server (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
	Select **Obtain DNS Info Automically** if you want the Zyxel Device to use the DNS server addresses assigned by your ISP. Select **Use Following Static DNS Address** if you want the Zyxel Device to use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
Routing Feature (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
NAT	Click this switch to activate or deactivate NAT on this connection. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
IGMP Proxy	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. Click this switch to have the Zyxel Device act as an IGMP proxy on this connection. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not. This allows the Zyxel Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Click this switch to have the Zyxel Device use the WAN interface of this connection as the system default gateway. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Fullcone NAT Enable	Click this switch to enable or disable full cone NAT on this connection. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not. This field is available only when you activate **NAT**. In full cone NAT, the Zyxel Device maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The Zyxel Device also maps packets coming to that external IP address and port to the internal IP address and port.
DHCPC Options (This is available only when you set the **Encapsulation** to **IPoE** and select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
Request Options	Select **Option 43** to have the Zyxel Device automatically add vendor specific information in the DHCP packets to request the vendor specific options from the DHCP server. Select **Option 121** to have the Zyxel Device push static routes to clients.
Sent Options	
option 60	Select this and enter the device identity you want the Zyxel Device to add in the DHCP discovery packets that go to the DHCP server.
Vendor ID	Enter the Vendor Class Identifier, such as the type of the hardware or firmware.
option 61	Select this and enter any string that identifies the device.

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

LABEL	DESCRIPTION
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DUID	Enter the hardware type, a time value and the MAC address of the device.
option 125	Select this to have the Zyxel Device automatically generate and add vendor specific parameters in the DHCP discovery packets that go to the DHCP server.
IPv6 Address (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field.)	
Obtain an IPv6 Address Automatically	Select **Obtain an IPv6 Address Automatically** if you want to have the Zyxel Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Static IPv6 Address	Select **Static IPv6 Address** if you have a fixed IPv6 address assigned by your ISP. When you select this, the following fields appear.
IPv6 Address	Enter an IPv6 IP address that your ISP gave to you for this WAN interface.
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
IPv6 Default Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your Zyxel Device's interface(s). The gateway helps forward packets to their destinations.
IPv6 DNS Server (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field. Configure the IPv6 DNS server in the following section.)	
Obtain IPv6 DNS Info Automatically	Select **Obtain IPv6 DNS Info Automatically** to have the Zyxel Device get the IPv6 DNS server addresses from the ISP automatically.
Use Following Static IPv6 DNS Address	Select **Use Following Static IPv6 DNS Address** to have the Zyxel Device use the IPv6 DNS server addresses you configure manually.
Primary DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.
IPv6 Routing Feature (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field. You can enable IPv6 routing features in the following section.)	
MLD Proxy Enable	Select this check box to have the Zyxel Device act as an MLD proxy on this connection. This allows the Zyxel Device to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the Zyxel Device use the WAN interface of this connection as the system default gateway.
DS-Lite	This is available only when you select **IPv6 Only** in the **IPv4/IPv6 Mode** field. Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network. See Dual Stack Lite on page 76 for more information. Click this switch to let local computers use IPv4 through an ISP's IPv6 network. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
DS-Lite Relay Server IP	Specify the transition router's IPv6 address.
6RD	The 6RD (IPv6 rapid deployment) fields display when you set the **IPv6/IPv4 Mode** field to **IPv4 Only**. See IPv6 Rapid Deployment on page 75 for more information. Click this switch to tunnel IPv6 traffic from the local network through the ISP's IPv4 network. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.

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

LABEL	DESCRIPTION
	Select **Manually Configured** if you have the IPv4 address of the relay server. Otherwise, select **Automatically configured by DHCPC** to have the Zyxel Device detect it automatically through DHCP. The **Automatically configured by DHCPC** option is configurable only when you set the method of encapsulation to **IPoE**.
Service Provider IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet.
IPv4 Mask Length	Enter the subnet mask number (1~32) for the IPv4 network.
Border Relay IPv4 Address	When you select **Manually Configured**, specify the relay server's IPv4 address in this field.
IPv6 IA_PD and IA_NA (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field.)	
Prefix Delegation	Click this switch to use DHCP PD (Prefix Delegation) which enables the Zyxel Device to pass the IPv6 prefix information to its LAN hosts. The hosts can then use the prefix to generate their IPv6 addresses. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
IPv6 Address From DHCPv6 Server	Click this switch to obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the Zyxel Device using the IPv6 prefix from a Router Advertisement (RA). When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
WAN MAC Address (You can set the WAN MAC address in the following section.)	
Factory Default	Select **Factory Default** to use the factory assigned default MAC address.
Clone LAN Host's MAC Address	Select this option to clone the MAC address of the computer (displaying in the screen) from which you are configuring the Zyxel Device. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
IP Address	Enter the IP address of the computer on the LAN whose MAC address you are cloning.
Set WAN MAC Address	Select this option to enter the MAC address you want to use.
MAC Address	Enter the MAC address you want to use.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

Bridge Mode

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. The following example screen displays when you select **Bridge** mode.

Figure 50 Network Setting > Broadband > Add/Edit New WAN Interface (Bridge Mode)

The following table describes the fields in this screen.

Table 18   Network Setting > Broadband > Add/Edit New WAN Interface (Bridge Mode)

LABEL	DESCRIPTION
General	Click this switch to enable or disable the interface. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Name	Enter a service name of the connection.
Type	This field shows an Ethernet connection.
Mode	Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
VLAN	Click this switch to enable or disable VLAN on this WAN interface. When the switch goes to the right, the function is enabled. Otherwise, it is not.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.

Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. |
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
WAN MAC Address (You can set the WAN MAC address in the following section.)	
Factory Default	Select **Factory Default** to use the factory assigned default MAC address.
Clone LAN Host's MAC Address	Select this option to clone the MAC address of the computer (displaying in the screen) from which you are configuring the Zyxel Device. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
IP Address	Enter the IP address of the computer on the LAN whose MAC address you are cloning.

Table 18   Network Setting > Broadband > Add/Edit New WAN Interface (Bridge Mode) (continued)

LABEL	DESCRIPTION
Set WAN MAC Address	Select this option to enter the MAC address you want to use.
MAC Address	Enter the MAC address you want to use.
Cancel	Click **Cancel** to exit this screen without saving any changes.
Apply	Click **Apply** to save your changes.

6.3 Technical Reference

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

Encapsulation

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

IP over Ethernet

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

PPP over Ethernet (PPPoE)

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

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

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

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

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

IP Address Assignment

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

Introduction to VLANs

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

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

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

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges – they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is 4 bytes longer than an untagged frame and contains 2 bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and 2 bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

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

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

Multicast

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

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

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

DNS Server Address Assignment

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

The Zyxel Device 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 Zyxel Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

IPv6 Prefix and Prefix Length

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

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

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

7.1 Wireless Overview

This chapter describes the Zyxel Device's **Network Setting** > **Wireless** screens. Use these screens to set up your Zyxel Device's WiFi connection and security settings.

7.1.1 What You Can Do in this Chapter

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

- Use the **General** screen to enable WiFi, enter the SSID and select the wireless security mode (Section 7.2 on page 89).
- Use the **Guest/More AP** screen to set up multiple wireless networks on your Zyxel Device (Section 7.3 on page 94).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Zyxel Device (Section 7.4 on page 97).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 7.5 on page 98).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications (Section 7.6 on page 100).
- Use the **Others** screen to configure wireless advanced features, such as the RTS/CTS Threshold (Section 7.7 on page 101).
- Use the **Channel Status** screen to scan WiFi channel noises and view the results (Section 7.8 on page 103).
- Use the **MESH** screen to allow wireless clients to roam seamlessly between Mesh supported devices in your Mesh network by using the same SSID and WiFi password as well as allow dual-band wireless client devices, to use the less-congested and higher capacity 5 GHz band, leaving the more crowded 2.4 GHz band available for legacy clients. (Section 7.9 on page 104).

7.1.2 What You Need to Know

Wireless Basics

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

WiFi6 / IEEE 802.11ax

WiFi6 is backwards compatible with IEEE 802.11a/b/g/n/ac and is most suitable in areas with a high concentration of users. WiFi6 devices support Target Wakeup Time (TWT) allowing them to automatically power down when they are inactive.

The following table displays the comparison of the different WiFi standards.

WIFI STANDARD	MAXIMUM LINK RATE *	BAND	SIMULTANEOUS CONNECTIONS
802.11b	11 Mbps	2.4 GHz	1
802.11a/g	54 Mbps	2.4 GHz and 5 GHz	1
802.11n	600 Mbps	2.4 GHz and 5 GHz	1
802.11ac	6.93 Gbps	5 GHz	4
802.11ax	2.4 Gbps	2.4 GHz	128
	9.61 Gbps	5 GHz and 6 GHz	

* The maximum link rate is for reference under ideal conditions only.

Finding Out More

See Section 7.10.1 on page 105 for advanced technical information on wireless networks.

7.2 Wireless General Settings

Use this screen to enable WiFi, enter the SSID and select the wireless security mode. These are basic elements for starting a wireless service. It is recommended that you select **More Secure** to enable **WPA2-PSK** data encryption.

Note: If you are configuring the Zyxel Device from a computer connected to WiFi and you change the Zyxel Device'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 Zyxel Device's new settings.

Note: If upstream/downstream bandwidth is empty, the Zyxel Device sets the value automatically.

Note: Setting a maximum upstream/downstream bandwidth will significantly decrease wireless performance.

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

Figure 51 Network Setting > Wireless > General

The following table describes the general WiFi labels in this screen.

Table 19   Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless	
Wireless	Select **Keep the same settings for 2.4G and 5G wireless networks** and the 2.4 GHz and 5 GHz wireless networks will use the same SSID and wireless security settings.
Wireless Network Setup	
Band	This shows the wireless band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n/ax wireless clients while **5GHz** is used by IEEE 802.11a/n/ac/ax wireless clients.
Wireless	Click this switch to enable or disable WiFi in this field. When the switch turns blue ⬤, the function is enabled. Otherwise, it is not.
Channel	Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Use **Auto** to have the Zyxel Device automatically determine a channel to use.
Bandwidth	Select whether the Zyxel Device uses a wireless channel width of **20MHz**, **40MHz, 20/40MHz** or **20/40/80MHz**. Note: **20/40/80MHz** is only available if you select the **5GHz Band**. A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. An 80 MHz channel groups adjacent 40 MHz channels into pairs to increase bandwidth even higher. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. Because not all devices support 40 MHz channels, select **20/40MHz** or **20/40/80MHz** to allow the Zyxel Device to adjust the channel bandwidth
Control Sideband	This is available for some regions when you select a specific channel and set the **Bandwidth** field to **40MHz** or **20/40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
Wireless Network Settings	
Wireless Network Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. This check box is grayed out if the WPS function is enabled in the **Network Setting** > **Wireless** > **WPS** screen.
Blocking BSSID LAN Access	Select this check box so that the wireless client's access to all devices on the LAN will be blocked.
Multicast Forwarding	Select this check box to allow the Zyxel Device to convert wireless multicast traffic into wireless unicast traffic.
Max. Upstream Bandwidth	Max. Upstream Bandwidth allows you to specify the maximum rate for upstream wireless traffic to the WAN from this wireless LAN in kilobits per second (Kbps).

Table 19   Network Setting > Wireless > General (continued)

LABEL	DESCRIPTION
Max. Downstream Bandwidth	Max. Upstream Bandwidth allows you to specify the maximum rate for downstream wireless traffic to this wireless LAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when WiFi is enabled.
Security Level	
Security Mode	Select **More Secure (Recommended)** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

7.2.1 No Security

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

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

Figure 52   Wireless > General: No Security
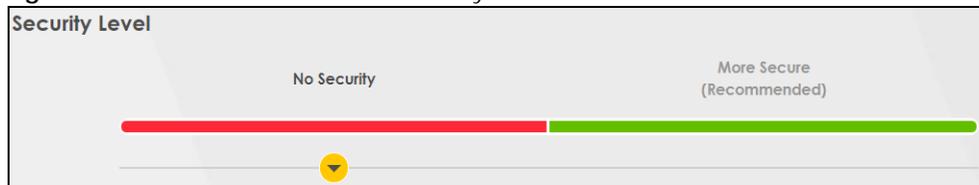
The following table describes the labels in this screen.

Table 20   Wireless > General: No Security

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

7.2.2 More Secure (Recommended)

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

Click **Network Setting** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. The default **WPA2-PSK** is shown in the **Security Mode** field.

Figure 53 Wireless > General: More Secure: WPA2-PSK

The following table describes the labels in this screen.

Table 21   Wireless > General: More Secure: WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA2-PSK data encryption.
Security Mode	This field shows the **WPA2-PSK** type of security mode.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	Select **Generate password automatically** or enter a **Password**. The password has two uses. 1. Manual. Manually enter the same password on the Zyxel Device and the client. Enter 8-63 ASCII characters or exactly 64 hexadecimal ('0-9', 'a-f') characters. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed ⦰ , you'll see the password in plain text. Otherwise, it is hidden.
	Click this ▸ to show more fields in this section. Click again to hide them.
Encryption	This field shows the **AES** type of data encryption.
Timer	The **Timer** is the rate at which the RADIUS server sends a new group key out to all clients.

7.3 Guest/More AP

This screen allows you to configure a guest wireless network that allows access to the Internet only through the Zyxel Device. You can also configure additional wireless networks, each with different security settings, in this screen.

Click **Network Setting > Wireless** > **Guest/More AP**. The following screen displays.

The following table introduces the supported wireless networks.

Table 22   Supported Wireless Networks

WIRELESS NETWORKS	WHERE TO CONFIGURE
Main/1	Network Setting > Wireless > General screen
Guest/3	Network Setting > Wireless > Guest/More AP screen

Figure 54   Network Setting > Wireless > Guest/More AP

The following table describes the labels in this screen.

Table 23   Network Setting > Wireless > Guest/More AP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active, while a gray bulb signifies that this SSID is not active.
SSID	An SSID profile is the set of parameters relating to one of the Zyxel Device'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.
Guest WLAN	This displays if the guest WiFi function has been enabled for this wireless LAN. If **Home Guest** displays, clients can connect to each other directly. If **External Guest** displays, clients are blocked from connecting to each other directly. **N/A** displays if guest wireless LAN is disabled.
Modify	Click the **Edit** icon to configure the SSID profile.

7.3.1 Edit Guest/More AP Settings

Use this screen to create Guest and additional wireless networks with different security settings.

Note: If upstream/downstream bandwidth is empty, the Zyxel Device sets the value automatically. Setting a maximum upstream/downstream bandwidth will significantly decrease wireless performance.

Click the **Edit** icon next to an SSID in the **Guest/More AP** screen. The following screen displays.

Figure 55   Network Setting > Wireless > Guest/More AP > Edit

The following table describes the fields in this screen.

Table 24   Network Setting > Wireless > Guest/More AP > Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Click this switch to enable or disable WiFi in this field. When the switch turns blue ⬤, the function is enabled; otherwise, it is not.

Table 24   Network Setting > Wireless > Guest/More AP > Edit (continued)

LABEL	DESCRIPTION
Security Level	
Wireless Network Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
Guest WLAN	Select this to create Guest WiFis for home and external clients. Select the WiFi type in the **Access Scenario** field.
Access Scenario	If you select **Home Guest**, clients can connect to each other directly. If you select **External Guest**, clients are blocked from connecting to each other directly.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this wireless LAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this wireless LAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when WiFi is enabled.
SSID Subnet	Click on this switch to **Enable** this function if you want the wireless network interface to assign DHCP IP addresses to the associated wireless clients. This option cannot be used if the WPS function is enabled in the **Network Setting** > **Wireless** > **WPS** screen or if the **Keep the same settings for 2.4G and 5G wireless networks** check box is selected in **Network Setting > Wireless > General**.
DHCP Start Address	Specify the first of the contiguous addresses in the DHCP IP address pool. The Zyxel Device assigns IP addresses from this DHCP pool to wireless clients connecting to the SSID.
DHCP End Address	Specify the last of the contiguous addresses in the DHCP IP address pool.
SSID Subnet Mask	Specify the subnet mask of the Zyxel Device for the SSID subnet.
LAN IP Address	Specify the IP address of the Zyxel Device for the SSID subnet.
Security Level	Select **More Secure (Recommended)** to add security on this wireless network. The wireless clients which want to associate to this network must have the same wireless security settings as the Zyxel Device. After you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See Section 7.2.1 on page 92 for more details about this field.
Security Mode	This field shows the **WPA2-PSK** type of security mode.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	WPA2-PSK uses a simple common password, instead of user-specific credentials. If you did not select **Generate password automatically**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters. Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed 🚫, you'll see the password in plain text. Otherwise, it is hidden.
	Click this 🔽 to show more fields in this section. Click again to hide them.
Encryption	This field shows the **AES** type of data encryption.
Timer	The **Timer** is the rate at which the RADIUS server sends a new group key out to all clients.

Table 24   Network Setting > Wireless > Guest/More AP > Edit (continued)

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

7.4 MAC Authentication

This screen allows you to configure the Zyxel Device to give exclusive access to specific devices **(Allow)** or exclude specific devices from accessing the Zyxel Device **(Deny)** based on the device(s) MAC address. Every Ethernet device has a unique MAC (Media Access Control) address. It is assigned at the factory and consists of six pairs of hexadecimal characters; for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the device(s) you want to allow/deny to configure this screen.

Note: You can have up to 25 MAC authentication rules.

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

Figure 56   Network Setting> Wireless > MAC Authentication

The following table describes the labels in this screen.

Table 25   Network Setting > Wireless > MAC Authentication

LABEL	DESCRIPTION
General	
SSID	Select the SSID for which you want to configure MAC filter settings.

Table 25   Network Setting > Wireless > MAC Authentication (continued)

LABEL	DESCRIPTION
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the **MAC Address** table.
	Select **Disable** to turn off MAC filtering.
	Select **Deny** to block access to the Zyxel Device. MAC addresses not listed will be allowed to access the Zyxel Device.
	Select **Allow** to permit access to the Zyxel Device. MAC addresses not listed will be denied access to the Zyxel Device.
MAC Address List	
Add New MAC Address	This field is available when you select **Deny** or **Allow** in the **MAC Restrict Mode** field.
	Click this if you want to add a new MAC address entry to the MAC filter list below.
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the Zyxel Device.
Modify	Click the **Edit** icon and type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc).
	Click the **Delete** icon to delete the entry.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

7.4.1 Add/Edit MAC Addresses

Click **Add new MAC address** in the **Network Setting** > **Wireless** > **MAC Authentication** screen to add a new MAC address. You can also click the Edit icon next to a MAC authentication rule to edit the rule.

Enter the MAC addresses of the wireless devices that are allowed or denied access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.

Figure 57   Network Setting> Wireless > MAC Authentication > Add/Edit

7.5 WPS Settings

WiFi Protected Setup (WPS) allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. To set up a WPS connection between two devices, both

devices must support WPS. It is recommended to use the Push Button Configuration (**PBC**) method if your wireless client supports it. See Section 7.10.8.3 on page 113 for more information about WPS.

Note: The Zyxel Device applies the security settings of the main SSID (**SSID1**) profile (see Section 7.2 on page 89).

Note: If WPS is enabled, UPnP will automatically be turned on.

Note: The WPS switch is grayed out when WiFi is disabled.

Click **Network Setting > Wireless > WPS**. The following screen displays. Click this switch and makes it turn blue. Click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 58   Network Setting > Wireless > WPS
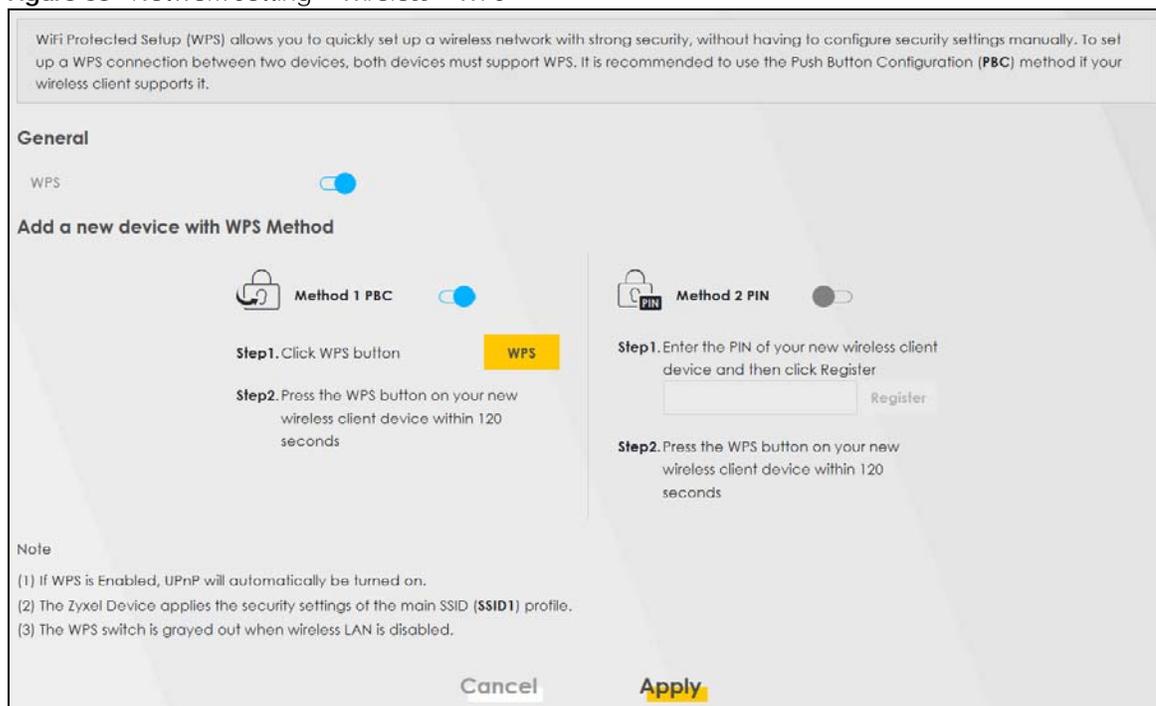
The following table describes the labels in this screen.

Table 26   Network Setting > Wireless > WPS

LABEL	DESCRIPTION
General	
WPS	Click this switch to activate or deactivate WPS on this Zyxel Device. When the switch turns blue , the function is enabled. Otherwise, it is not.
Add a new device with WPS Method	
Method 1	Use this section to set up a WPS wireless network using Push Button Configuration (PBC). Click this switch to make it turn blue. Click **Apply** to activate WPS method 1 on the Zyxel Device.
WPS	Click this button to add another WPS-enabled wireless device (within wireless range of the Zyxel Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **WPS** button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.

Table 26   Network Setting > Wireless > WPS (continued)

LABEL	DESCRIPTION
Method 2	Use this section to set up a WPS wireless network by entering the PIN of the client into the Zyxel Device. Click this switch and make it turn blue. Click **Apply** to activate WPS method 2 on the Zyxel Device.
Register	Enter the PIN of the device that you are setting up a WPS connection with and click **Register** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the Zyxel Device.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

7.6 WMM Settings

Use this screen to enable WiFi MultiMedia (**WMM**) and **WMM Automatic Power Save** (**APSD**) in wireless networks for multimedia applications. **WMM** enhances data transmission quality, while **APSD** improves power management of wireless clients. This allows delay-sensitive applications, such as voice and videos, to run more smoothly.

Click **Network Setting > Wireless > WMM** to display the following screen.

Figure 59   Network Setting > Wireless > WMM
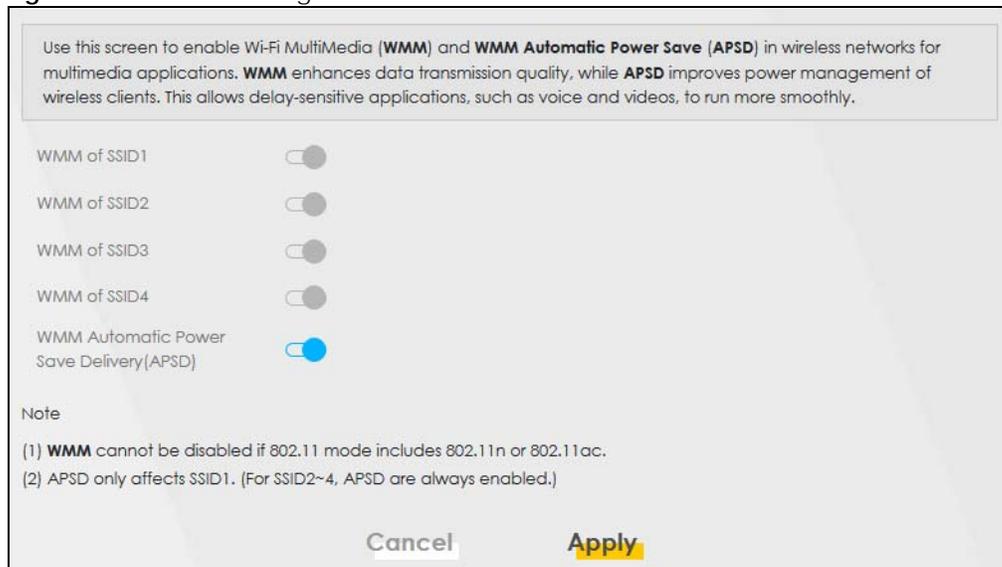
Note: **WMM** cannot be disabled if 802.11 mode includes 802.11n or 802.11ac.

The following table describes the labels in this screen.

Table 27   Network Setting > Wireless > WMM

LABEL	DESCRIPTION
WMM of SSID1~4	Select **On** to have the Zyxel Device automatically give the wireless network (SSIDx) a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (WiFi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. If the **802.11 Mode** in **Network Setting > Wireless > Others** is set to include 802.11n or 802.11ac, WMM cannot be disabled.
WMM Automatic Power Save Delivery (APSD)	Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The Zyxel Device goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the Zyxel Device until the Zyxel Device "wakes up". The Zyxel Device wakes up periodically to check for incoming data. Note: This works only if the wireless device to which the Zyxel Device is connected also supports this feature. APSD only affects SSID1. For SSID2~4, APSD is always enabled.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

7.7 Others Settings

Use this screen to configure advanced wireless settings, such as additional security settings, power saving, and data transmission settings. Click **Network Setting > Wireless > Others**. The screen appears as shown.

See for detailed definitions of the terms listed in this screen.

Figure 60   Network Setting > Wireless > Others

The following table describes the labels in this screen.

Table 28   Network Setting > Wireless > Others

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Output Power	Set the output power of the Zyxel Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: **20%**, **40%**, **60%**, **80%** or **100%**.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 50 ms to 1000 ms. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
802.11 Mode	For 2.4 GHz frequency WiFi devices: • Select **802.11b Only** to allow only IEEE 802.11b compliant WiFi devices to associate with the Zyxel Device. • Select **802.11g Only** to allow only IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. • Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11b/g/n Mixed** to allow IEEE 802.11b, IEEE 802.11g or IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11b/g/n/ax Mixed** to allow IEEE 802.11b, IEEE 802.11g, IEEE 802.11n or IEEE 802.11ax compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. For 5 GHz frequency WiFi devices: • Select **802.11a Only** to allow only IEEE 802.11a compliant WiFi devices to associate with the Zyxel Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. • Select **802.11ac Only** to allow only IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. • Select **802.11a/n Mixed** to allow either IEEE 802.11a or IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11n/ac Mixed** to allow either IEEE 802.11n or IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11a/n/ac Mixed** to allow IEEE 802.11a, IEEE 802.11n or IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11a/n/ac/ax Mixed** to allow IEEE 802.11a, IEEE 802.11n, IEEE 802.11ac or IEEE 802.11ax compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced.

Table 28   Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic).
	Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance.
	Select **Off** to disable 802.11 protection. The transmission rate of your Zyxel Device might be reduced in a mixed-mode network.
	This field displays **Off** and is not configurable when you set **802.11 Mode** to **802.11b Only**.
Preamble	Select a preamble type from the drop-down list box. Choices are **Long** or **Short**. See Section 7.10.7 on page 110 for more information.
	This field is configurable only when you set **802.11 Mode** to **802.11b** or **802.11b/g Mixed**.
Protected Management Frames	This option is only available when using **WPA2-PSK** as the **Security Mode** and **AES** Encryption in **Network Setting > Wireless > General**. Management frame protection (MFP) helps prevent wireless DoS attacks.
	Select **Disable** if you do not want to use MFP.
	Select **Capable** to encrypt management frames of wireless clients that support MFP. Clients that do not support MFP will still be allowed to join the wireless network, but remain unprotected.
	Select **Required** to allow only clients that support MFP to join the wireless network.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

7.8 Channel Status Settings

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

Note: If the current channel is a DFS channel, the warning 'Channel scan process is denied because current channel is a DFS channel (Channel: 52~140). If you want to run channel scan, please select a non-DFS channel and try again.' appears.

Figure 61   Network Setting > Wireless > Channel Status

7.9 MESH

Use this screen to enable or disable AP steering and band steering.

• AP steering allows wireless clients to roam seamlessly between supported devices in your network by using the same SSID and WiFi password. Also, AP steering helps monitor wireless clients and drop their connections to optimize the Zyxel Device bandwidth when the clients are idle or have a low signal. When a wireless client is dropped, it has the opportunity to steer to a supported device with a strong signal.

• Band steering allows 2.4GHz/5GHz dual-band wireless clients to steer from one band to another. For example, if the 2.4GHz channel is congested/lower signal strength, wireless clients that support 5GHz could be moved to the 5GHz channel. The wireless client can also return to the 2.4GHz channel.

The Zyxel Device acts as a controller to manage and coordinate wireless activity in a network, such as:

• AP steering

• Band steering

• Management of SSIDs and password on all APs in a network

    For example, if you change the SSID on a router, all the SSIDs of APs in a network will be changed as well.

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

Figure 62   Network Setting > Wireless > MESH

Use this screen to enable or disable MPro Mesh for wireless devices. MPro Mesh allows you to create a Mesh network using wireless devices designed by different vendors.	
MPro Mesh	⬤
Cancel	**Apply**
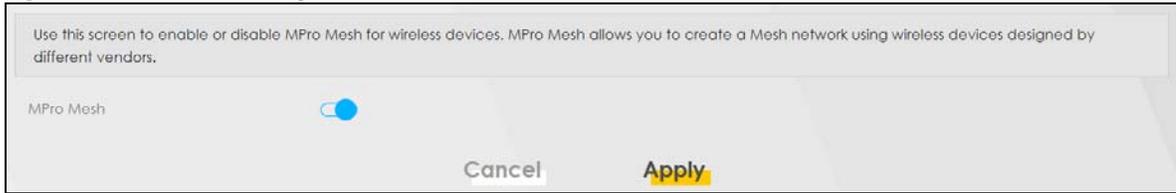
The following table describes the labels in this screen.

Table 29   Network Setting > Wireless > Band Steering

LABEL	DESCRIPTION
MPro Mesh	Click this switch to allow the wireless client to steer to a supported device with a strong signal, or connect to the less congested 2.4GHz/5GHz channel. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

7.10 Technical Reference

This section discusses WiFis in depth.

7.10.1 Wireless Network Overview

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

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

Traditionally, a wireless network operates in one of 2 ways.

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

The following figure provides an example of a wireless network.

Figure 63 Example of a Wireless Network
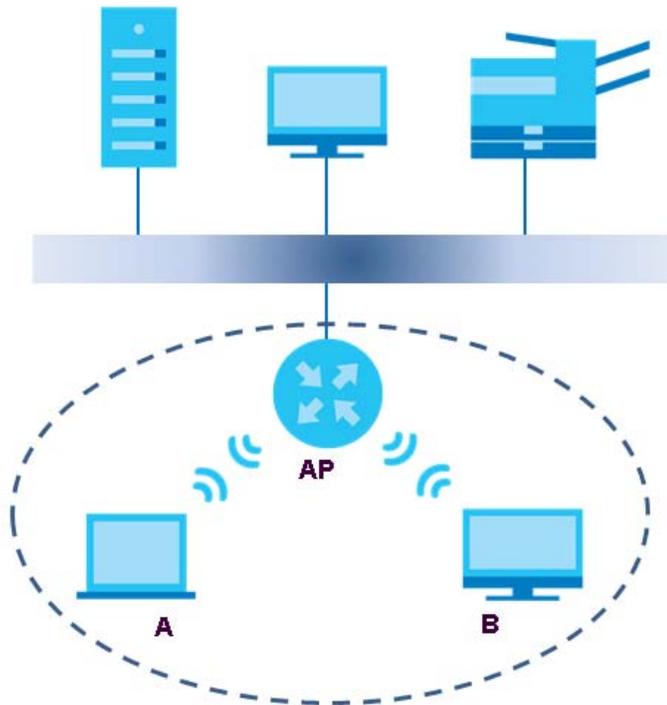
The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your Zyxel Device is the AP.

Every wireless network must follow these basic guidelines.

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

  The SSID is the name of the wireless network. It stands for Service Set IDentifier.

- If two wireless networks overlap, they should use a different channel.

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

- Every device in the same wireless network must use security compatible with the AP.

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

Radio Channels

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

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

7.10.2 Additional Wireless Terms

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

Table 30   Additional Wireless Terms

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

7.10.3 Wireless Security Overview

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

These security standards do 2 things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

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

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

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

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

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

7.10.3.1 SSID

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

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

7.10.3.2 MAC Address Filter

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

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

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

7.10.3.3 User Authentication

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

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

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

---

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

7.10.3.4 Encryption

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

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

7.10.4 Signal Problems

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

Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the 2 radios, muffling the signal.

7.10.5 BSS

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

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

Figure 64   Basic Service Set
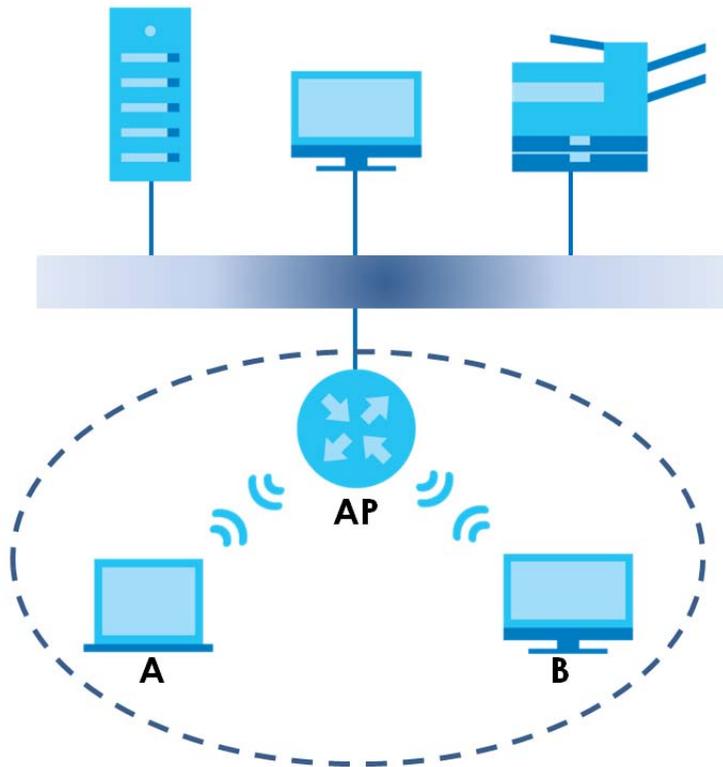
7.10.6 MBSSID

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

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

7.10.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If 2 wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

7.10.7 Preamble Type

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

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

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

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

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

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

7.10.8 WiFi Protected Setup (WPS)

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

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

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

7.10.8.1 Push Button Configuration

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

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

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

1   Ensure that the two devices you want to set up are within wireless range of one another.

2   Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the Zyxel Device, see Section 7.5 on page 98).

3   Press the button on one of the devices (it does not matter which). For the Zyxel Device you must press the WPS button for more than five seconds.

4   Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through a secure connection to the enrollee.

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

7.10.8.2 PIN Configuration

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

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

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

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

1 Ensure WPS is enabled on both devices.

2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.

3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the Zyxel Device, see Section 7.5 on page 98).

4 Enter the client's PIN in the AP's configuration interface.

5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.

6 Start WPS on both devices within 2 minutes.

7 Use the configuration utility to activate WPS, not the push-button on the device itself.

8 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

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

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

Figure 65   Example WPS Process: PIN Method
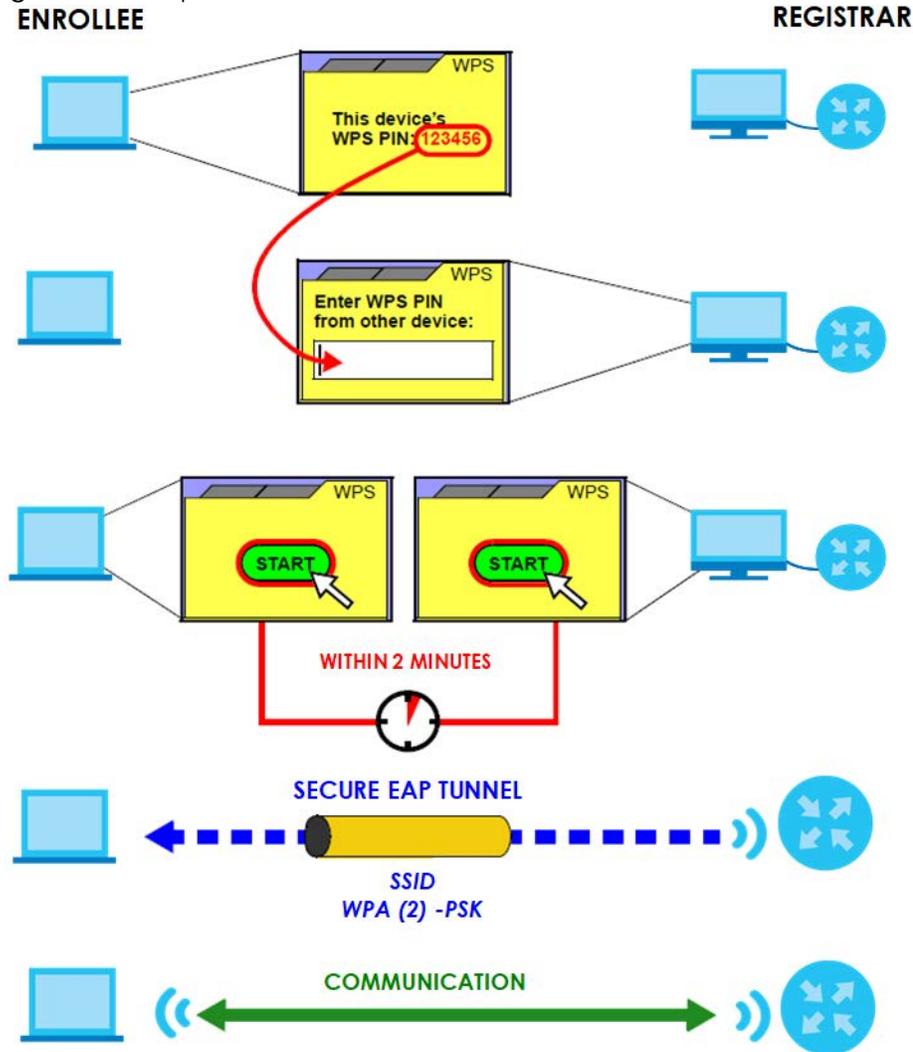
7.10.8.3 How WPS Works

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

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

Figure 66   How WPS Works
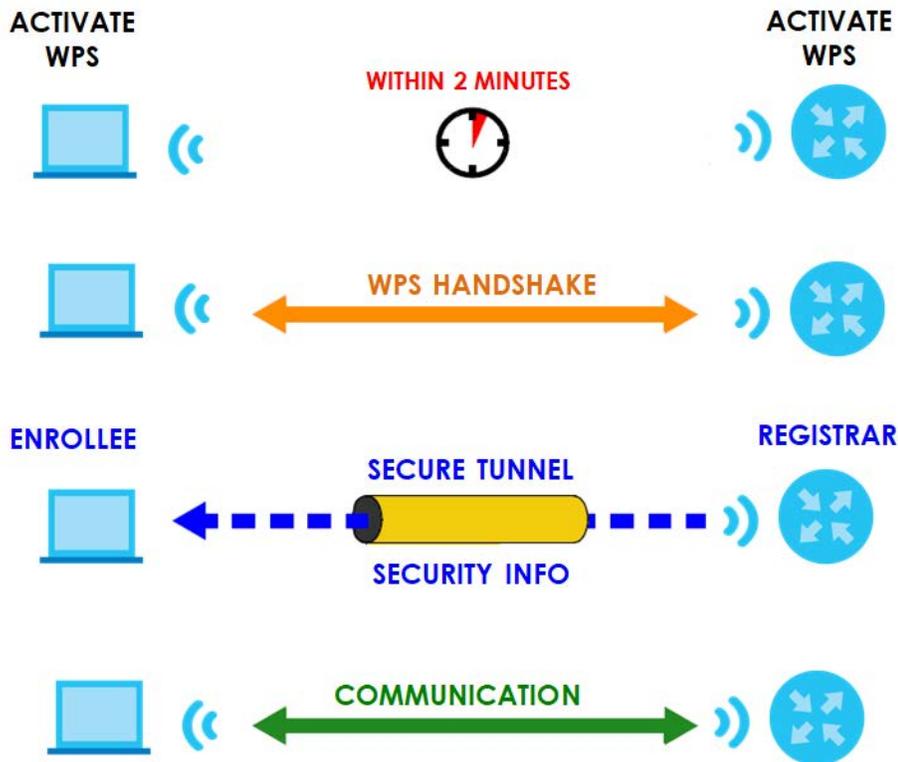
The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

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

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

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

7.10.8.4 Example WPS Network Setup

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

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

Figure 67   WPS: Example Network Step 1
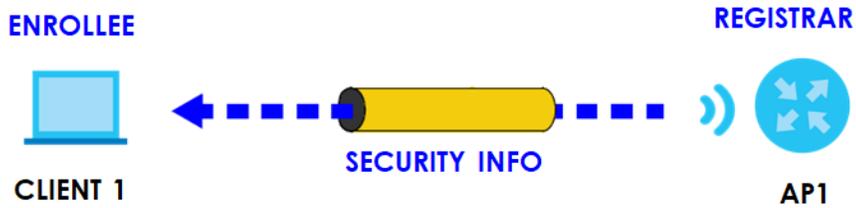
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 68   WPS: Example Network Step 2
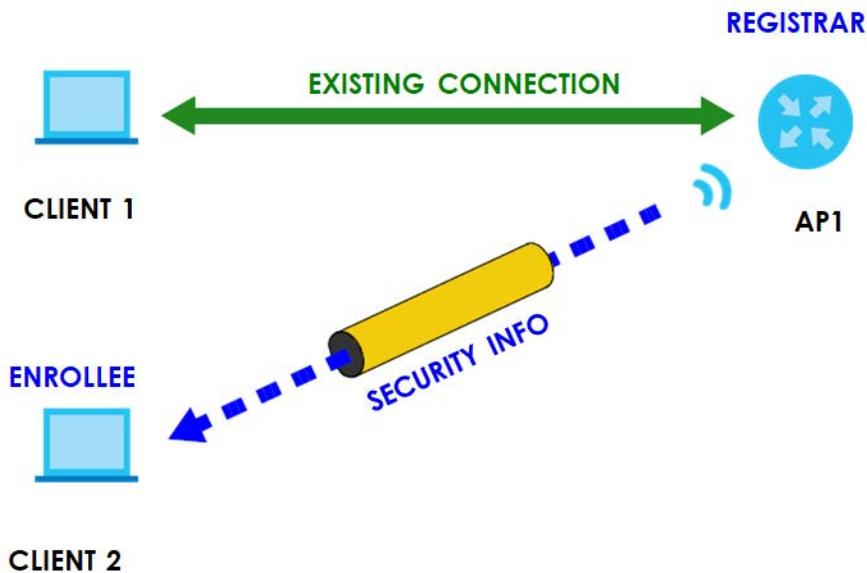
In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 69 WPS: Example Network Step 3
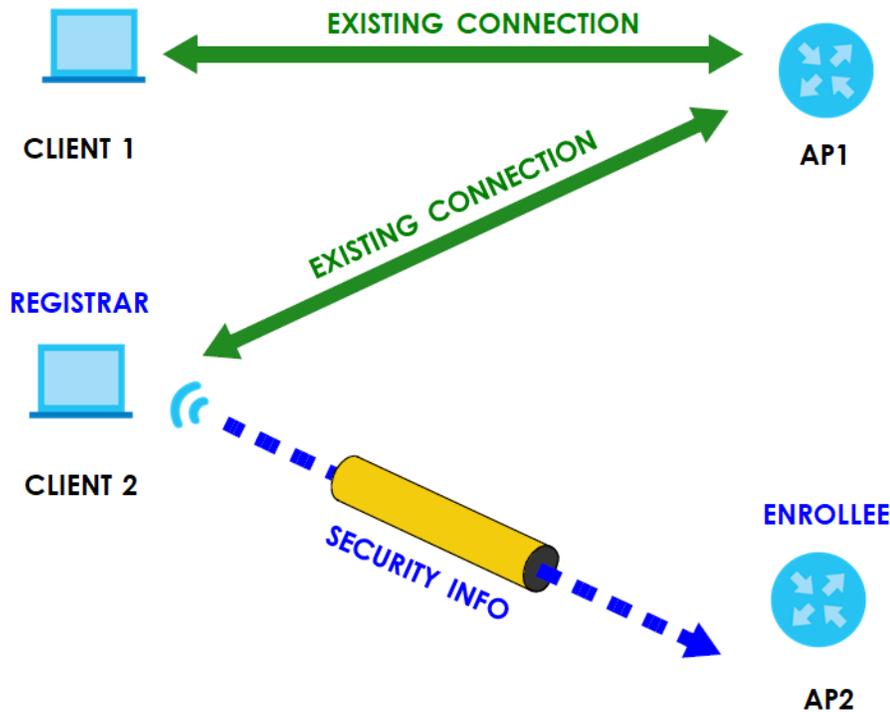
7.10.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).

- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

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

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

CHAPTER 8
Home Networking

8.1 Home Networking Overview

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

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

Figure 70   Home Networking Example
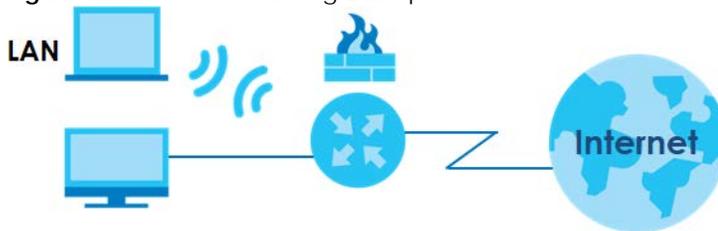
8.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings of your Zyxel Device (Section 8.2 on page 120).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC addresses (Section 8.3 on page 124).
- Use the **UPnP** screen to enable UPnP and UPnP NAT traversal on the Zyxel Device (Section 8.4 on page 126).
- Use the **Additional Subnet** screen to configure IP alias and public static IP (Section 8.5 on page 131).
- Use the **STB Vendor ID** screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the Zyxel Device automatically create static DHCP entries for the STB devices when they request IP addresses (Section 8.6 on page 133).
- Use the **Wake on LAN** screen to remotely turn on a device on the network. (Section 8.7 on page 133).
- Use the **TFTP Server Name** screen to identify a TFTP server for configuration file download using DHCP option 66. (Section 8.8 on page 134).

8.1.2 What You Need To Know

8.1.2.1 About LAN

IP Address

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

Subnet Mask

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

DHCP

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

DNS

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

RADVD (Router Advertisement Daemon)

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

8.1.2.2 About UPnP

Identifying UPnP Devices

UPnP hardware is identified as an icon in the Network Connections folder (Windows 10). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

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

• Dynamic port mapping

• Learning public IP addresses

• Assigning lease times to mappings

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

See the for more information on NAT.

Cautions with UPnP

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

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

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

UPnP and Zyxel

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

See Section 8.4.1 on page 127 for examples of installing and using UPnP.

Finding Out More

See Section 8.9 on page 135 for technical background information on LANs.

8.1.3 Before You Begin

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

8.2 LAN Setup

Use this screen to set the IP address and subnet mask of your Zyxel Device. Configure DHCP settings to have the Zyxel Device or a DHCP server assign IP addresses to devices. Click **Network Setting > Home Networking** to open the **LAN Setup** screen.

Follow these steps to configure your LAN settings.

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

2   Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.

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

Figure 71 Network Setting > Home Networking > LAN Setup

The following table describes the fields in this screen.

Table 31   Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group name for which you want to configure LAN settings. See Chapter 15 on page 194 for how to create a new interface group.
LAN IP Setup	
IP Address	Enter the LAN IPv4 IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
IGMP Snooping	
Active	Select **Enable** to allow the Zyxel Device to passively learn multicast group.
IGMP Mode	Select **Standard Mode** to forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select **Blocking Mode** to block all unknown multicast packets from the WAN.
DHCP Server State	
DHCP	Select **Enable** to have the Zyxel Device act as a DHCP server or DHCP relay agent. Select **Disable** to stop the DHCP server on the Zyxel Device. Select **DHCP Relay** to have the Zyxel Device forward DHCP request to the DHCP server.
DHCP Relay Server Address	This field is only available when you select **DHCP Relay** in the **DHCP** field.
IP Address	Enter the IPv4 IP address of the actual remote DHCP server in this field.
IP Addressing Values	This field is only available when you select **Enable** in the **DHCP** field.
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Click this switch to have the Zyxel Device record DHCP IP addresses with the MAC addresses the IP addresses are assigned to. When the switch goes to the right 🔵, the function is enabled. Otherwise, it is not. The Zyxel Device assigns the same IP address to the same MAC address when the host requests an IP address again through DHCP.
DHCP Server Lease Time	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems. This field is only available when you select **Enable** in the **DHCP** field.
Days/Hours/ Minutes	Enter the lease time of the DHCP server.
DNS Values	This field is only available when you select **Enable** in the **DHCP** field.
DNS	Select the type of service that you are registered for from your DNS service provider (**From ISP**). Select **DNS Proxy** if you have the DNS proxy service. The Zyxel Device redirects clients' DNS queries to a DNS server for resolving domain names. Select **Static** if you have the static DNS service.

Table 31   Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DNS Server 1/2	Enter the first and second DNS (Domain Name System) server IP addresses the Zyxel Device passes to the DHCP clients.
LAN IPv6 Mode Setup	
IPv6 Active	Click this switch to enable or disable the IPv6 mode and configure IPv6 settings on the Zyxel Device. When the switch goes to the right 🔵, the function is enabled. Otherwise, it is not.
Link Local Address Type	
EUI64	Select this to have the Zyxel Device generate an interface ID for the LAN interface's link-local address using the EUI-64 format.
Manual	Select this to manually enter an interface ID for the LAN interface's link-local address.
LAN Global Identifier Type	
EUI64	Select this to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address.
Manual	Select this to manually enter an interface ID for the LAN interface's global IPv6 address.
LAN IPv6 Prefix Setup	
Delegate prefix from WAN	Select this option and specify a WAN interface (connection) through which the Zyxel Device automatically obtains an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 prefix for the Zyxel Device's LAN IPv6 address.
MLD Snooping	Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.
Active	Click this switch to enable or disable MLD Snooping on the Zyxel Device. When the switch goes to the right 🔵, the function is enabled. Otherwise, it is not. This allows the Zyxel Device to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.
MLD Mode	Select **Standard Mode** to forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select **Blocking Mode** to block all unknown multicast packets from the WAN.
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: • **Stateless**: The Zyxel Device uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the Zyxel Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. • **Stateful**: The Zyxel Device uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the Zyxel Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.
LAN IPv6 DNS Assign Setup	Select how the Zyxel Device provide DNS server and domain name information to the clients: • **From Router Advertisement**: The Zyxel Device provides DNS information through router advertisements. • **From DHCPv6 Server**: The Zyxel Device provides DNS information through DHCPv6. • **From RA & DHCPv6 Server**: The Zyxel Device provides DNS information through both router advertisements and DHCPv6.
DHCPv6 Configuration	
DHCPv6 Active	This shows the status of the DHCPv6. **DHCPv6 Server** displays if you configured the Zyxel Device to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients.
IPv6 Router Advertisement State	
RADVD Active	This shows whether RADVD is enabled or not.
IPv6 Address Values (This section is available only when you select **Stateful** in the **LAN IPv6 Address Assign Setup** field.)	

Table 31   Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
IPv6 Start Address	Enter the first of the contiguous addresses in the IPv6 address pool.
IPv6 End Address	Enter the last of the contiguous addresses in the IPv6 address pool.
IPv6 Domain Name	Enter the domain name that is assigned to the DHCPv6 clients.
IPv6 DNS Values	
IPv6 DNS Server 1-3	Select **From ISP** if your ISP dynamically assigns IPv6 DNS server information. Select **User-Defined** if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the Zyxel Device passes to the DHCP clients. Select **None** if you do not want to configure IPv6 DNS servers.
DNS Query Scenario	Select how the Zyxel Device handles clients' DNS information requests. • **IPv4/IPv6 DNS Server**: The Zyxel Device forwards the requests to both the IPv4 and IPv6 DNS servers and sends clients the first DNS information it receives. • **IPv6 DNS Server Only**: The Zyxel Device forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives. • **IPv4 DNS Server Only**: The Zyxel Device forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives. • **IPv6 DNS Server First**: The Zyxel Device forwards the requests to the IPv6 DNS server first and then the IPv4 DNS server. Then it sends clients the first DNS information it receives. • **IPv4 DNS Server First**: The Zyxel Device forwards the requests to the IPv4 DNS server first and then the IPv6 DNS server. Then it sends clients the first DNS information it receives.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

8.3 LAN Static DHCP

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

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

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

Figure 72   Network Setting > Home Networking > Static DHCP
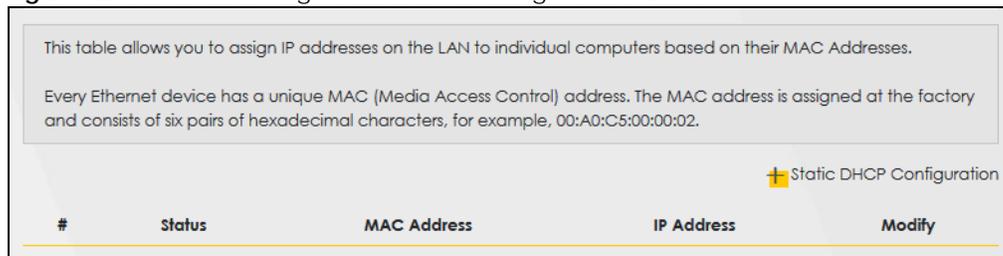
The following table describes the labels in this screen.

Table 32   Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Static DHCP Configuration	Click this to add a new static DHCP entry.
#	This is the index number of the entry.
Status	This field displays whether the client is connected to the Zyxel Device.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation).

A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address. |
| IP Address | This field displays the IP address relative to the # field listed above. |
| Modify | Click the **Edit** icon to have the IP address field editable and change it.

Click the **Delete** icon to delete a static DHCP entry. A window displays asking you to confirm that you want to delete the selected entry. |

If you click **Static DHCP Configuration** in the **Static DHCP** screen or the **Edit** icon next to a static DHCP entry, the following screen displays. Using a static DHCP means a client will always have the same IP address assigned to it by the DHCP server. Assign a fixed IP address to a device by selecting the interface group of this device and its IP address type and selecting the device/computer from a list or manually entering its MAC address and assigned IP address.

Figure 73   Static DHCP: Static DHCP Configuration/Edit

The following table describes the labels in this screen.

Table 33   Static DHCP: Static DHCP Configuration/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the connection between the client and the Zyxel Device. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Group Name	Select the interface group name for which you want to configure static DHCP settings. See Chapter 15 on page 194 for how to create a new interface group.
IP Type	This field displays **IPv4** for the type of the DHCP IP address. At the time of writing, it is not allowed to select other type.

Table 33   Static DHCP: Static DHCP Configuration/Edit (continued)

LABEL	DESCRIPTION
Select Device Info	Select a device or computer from the drop-down list or select **Manual Input** to manually enter a device's MAC address and IP address in the following fields.
MAC Address	If you select **Manual Input**, enter the MAC address of a computer on your LAN.
IP Address	If you select **Manual Input**, enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

8.4 UPnP Settings

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. A device can then leave a network smoothly and automatically when it is no longer in use.

See for more information on UPnP.

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

Note: To use **UPnP NAT-T**, enable **NAT** in the **Network Setting** > **Broadband** > **Edit/Add New WAN Interface** screen.

Figure 74   Network Setting > Home Networking > UPnP

The following table describes the labels in this screen.

Table 34   Network Setting > Home Networking > UPnP

LABEL	DESCRIPTION
UPnP State	
UPnP	Click this switch to enable or disable UPnP. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the Zyxel Device's IP address (although you must still enter the password to access the Web Configurator).
UPnP NAT-T State	
UPnP NAT-T	Click this switch to allow UPnP-enabled applications to automatically configure the Zyxel Device so that they can communicate through the Zyxel Device by using NAT traversal. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application. The table below displays the NAT port forwarding rules added automatically by UPnP NAT-T.
#	This is the index number of the UPnP NAT-T connection.
Description	This is the description of the UPnP NAT-T connection.
Destination IP Address	This is the IP address of the other connected UPnP-enabled device.
External Port	This is the external port number that identifies the service.
Internal Port	This is the internal port number that identifies the service.
Protocol	This is the transport layer protocol used for the service.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

8.4.1 Turning on UPnP in Windows 7 Example

This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the Zyxel Device in **Network Setting** > **Home Networking** > **UPnP**.

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

1   Click the start icon, **Control Panel** and then the **Network and Sharing Center.**
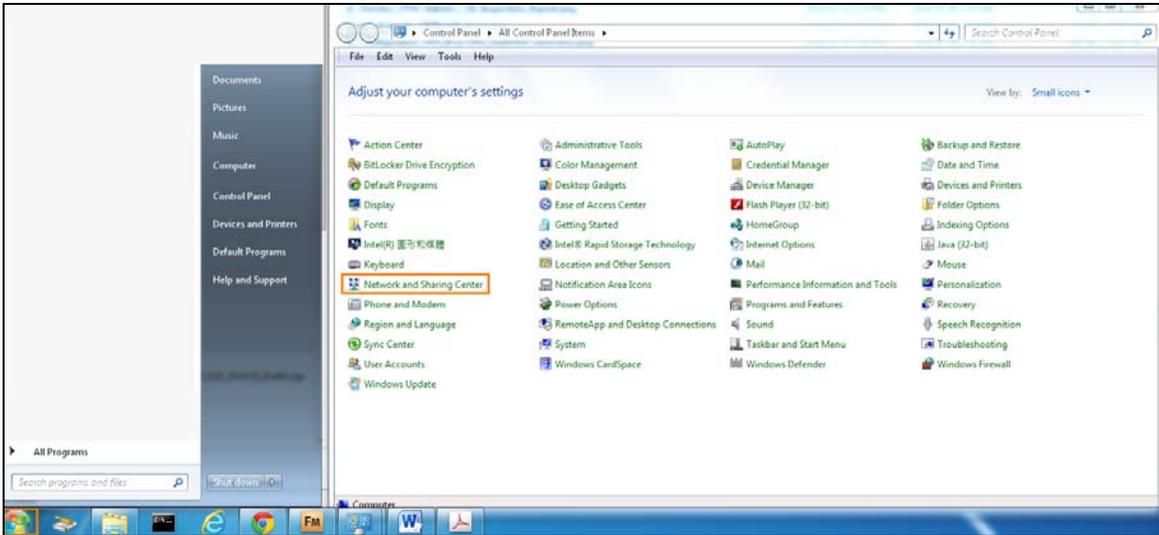
2 Click **Change Advanced Sharing Settings**.
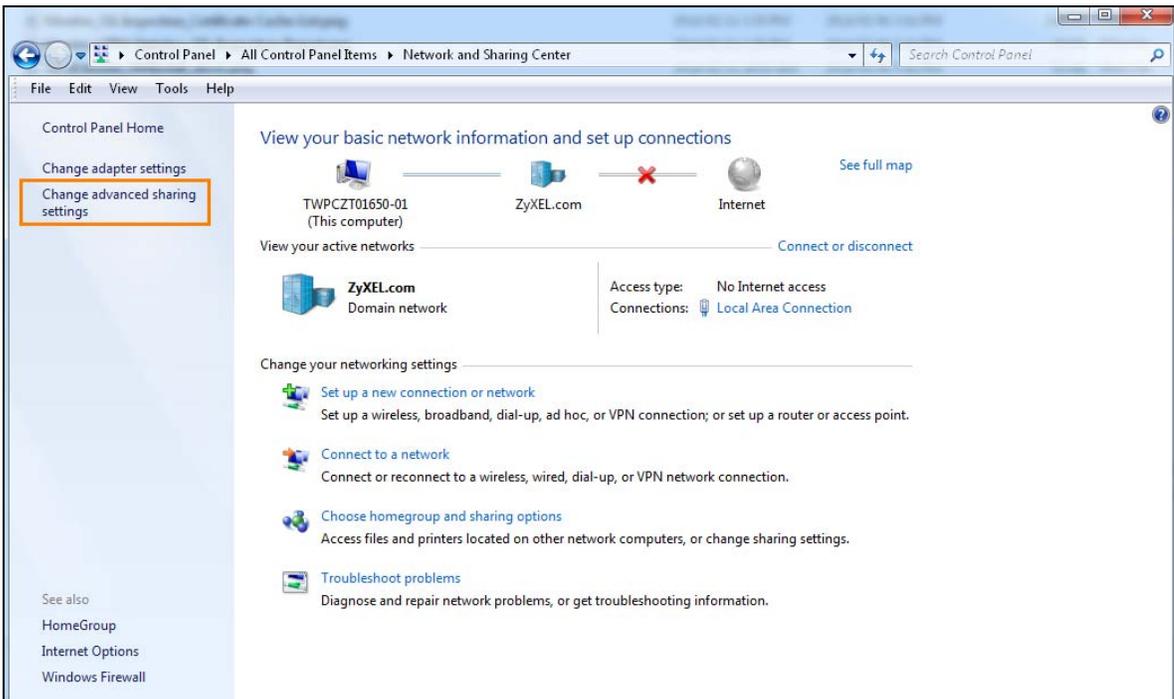
3 Select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.
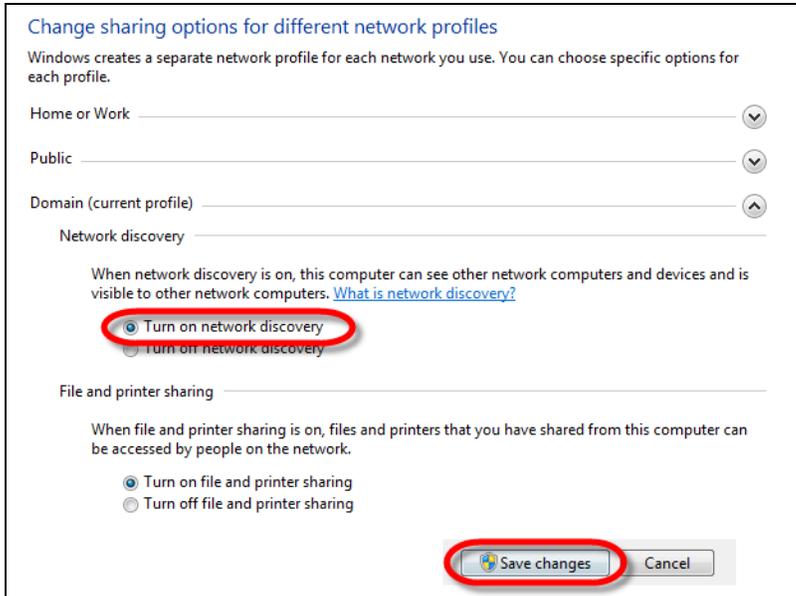
8.4.2 Turning on UPnP in Windows 10 Example

This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the Zyxel Device in **Network Setting > Home Networking > UPnP**.

Make sure the computer is connected to the LAN port of the Zyxel Device. Turn on your computer and the Zyxel Device.

1 Click the start icon, **Settings** and then **Network & Internet**.
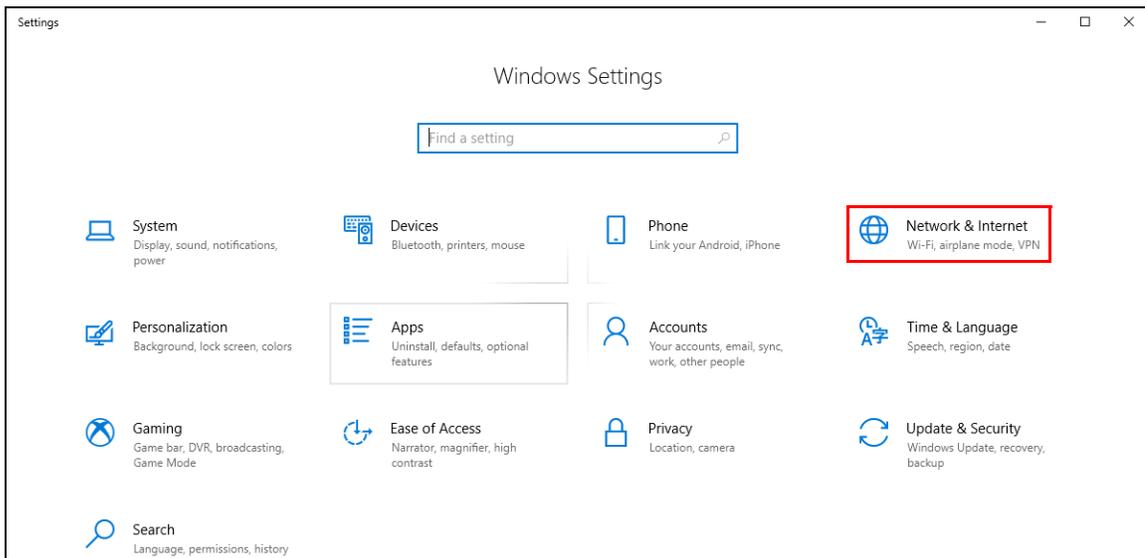
2 Click **Network and Sharing Center**.
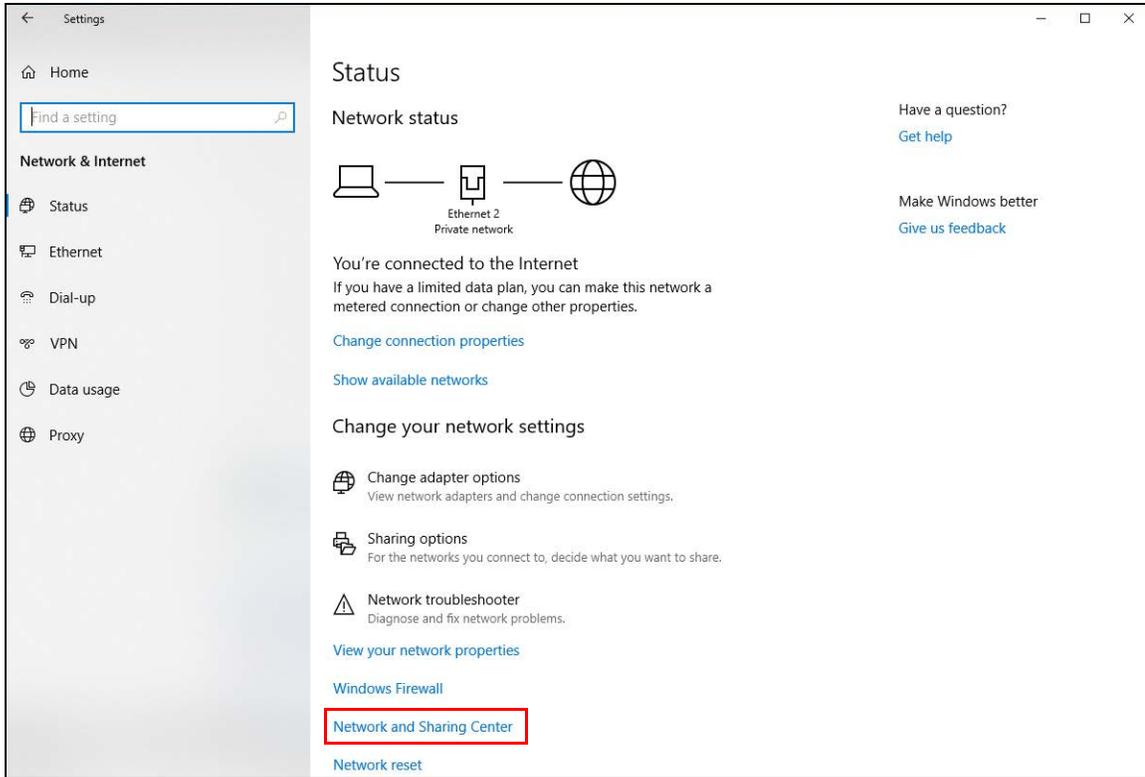
3 Click **Change advanced sharing settings**.
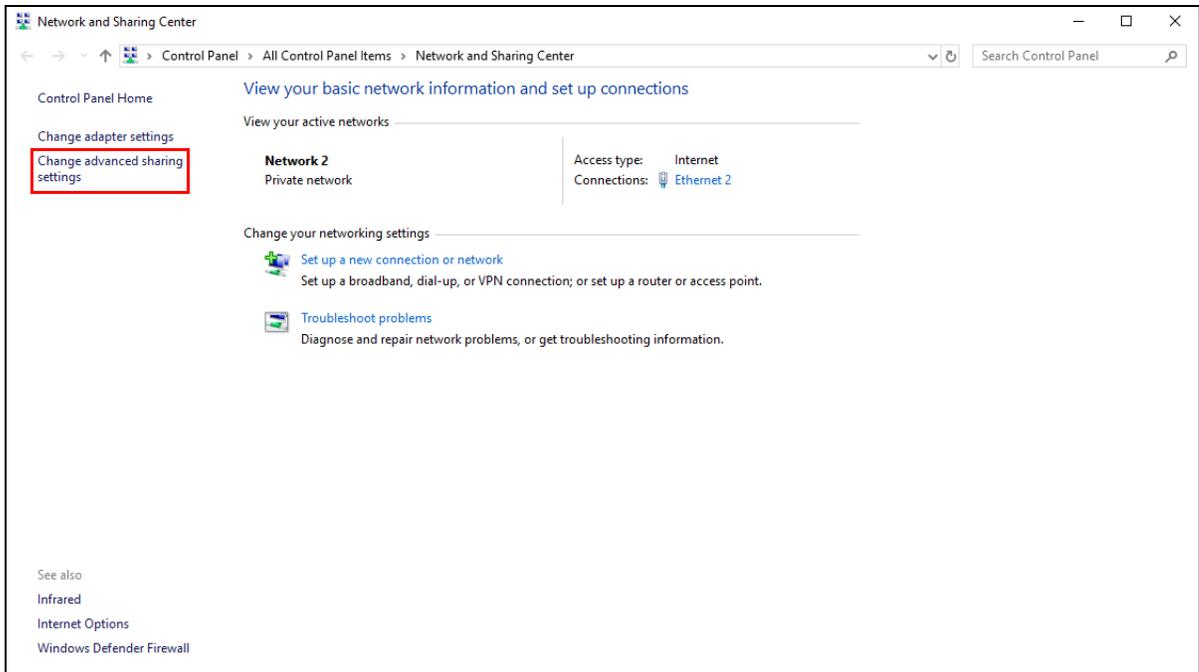
4 Under **Domain**, select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.
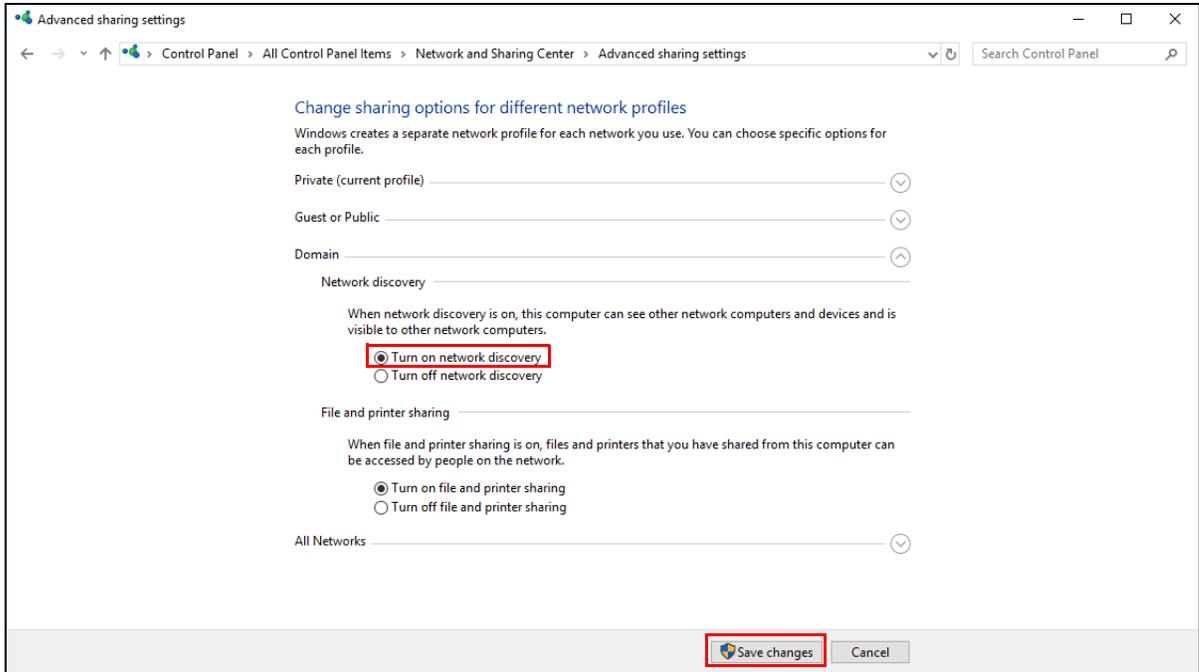
8.5 LAN Additional Subnet

Use this screen to configure IP alias and public static IP.

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

If your ISP provides the **Public LAN** service, the Zyxel Device may use a LAN IP address that can be accessed from the WAN.

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

Figure 75 Network Setting > Home Networking > Additional Subnet

The following table describes the labels in this screen.

Table 35   Network Setting > Home Networking > Additional Subnet

LABEL	DESCRIPTION
IP Alias Setup	
Group Name	Select the interface group name for which you want to configure the IP alias settings. See Chapter 15 on page 194 for how to create a new interface group.
Active	Click this switch to configure a LAN network for the Zyxel Device. When the switch goes to the right , the following fields will be configurable. Otherwise, they are not.
IPv4 Address	Enter the IP address of your Zyxel Device in dotted decimal notation.
Subnet Mask	Your Zyxel Device will automatically calculate the subnet mask based on the IPv4 address that you assign. Unless you are implementing subnetting, use this value computed by the Zyxel Device.
Public LAN	
Active	Click this switch to enable or disable the Public LAN feature. When the switch goes to the right , the function is enabled. Otherwise, it is not. Your ISP must support Public LAN and static IP.
IPv4 Address	Enter the public IP address provided by your ISP.
Subnet Mask	Enter the public IPv4 subnet mask provided by your ISP.

Table 35   Network Setting > Home Networking > Additional Subnet (continued)

LABEL	DESCRIPTION
Offer Public IP by DHCP	Click this switch to enable or disable the Zyxel Device to provide public IP addresses by DHCP server. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Enable ARP Proxy	Click this switch to enable or disable the ARP (Address Resolution Protocol) proxy. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

8.6 STB Vendor ID

Use this screen to configure the Vendor IDs of connected Set Top Boxes (STBs) so the Zyxel Device can automatically create static DHCP entries for them when they request IP addresses.

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

Figure 76   Network Setting > Home Networking > STB Vendor ID
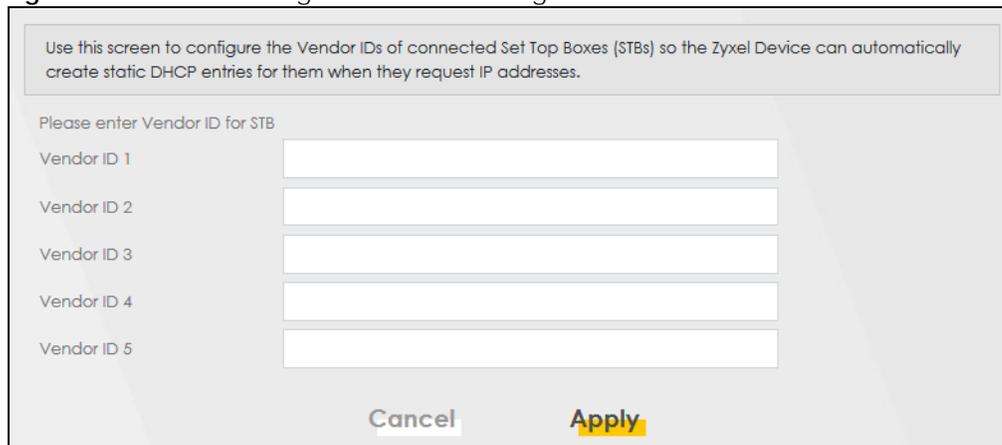
The following table describes the labels in this screen.

Table 36   Network Setting > Home Networking > STB Vendor ID

LABEL	DESCRIPTION
Vendor ID 1~5	These are STB's Vendor Class Identifiers (DHCP option 60). A Vendor Class Identifier is usually used to inform the DHCP server a DHCP client's vendor and functionality.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

8.7 Wake on LAN

Wake on LAN (WoL) allows you to remotely turn on a device on the network, such as a computer, storage device or media server. To use this feature the remote hardware (for example the network adapter on a computer) must support Wake on LAN using the 'Magic Packet' method.

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

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

Figure 77   Network Setting > Home Networking > Wake on LAN

The following table describes the labels in this screen.

Table 37   Network Setting > Home Networking > Wake on LAN

LABEL	DESCRIPTION
Wake by Address	Select **Manual** and enter the IP address or MAC address of the device to turn it on remotely. The drop-down list also lists the IP addresses that can be found in the Zyxel Device's ARP table. If you select an IP address, the MAC address of the device with the selected IP address then displays in the **MAC Address** field.
IP Address	Enter the IPv4 IP address of the device to turn it on. This field is not available if you select an IP address in the **Wake by Address** field.
MAC Address	Enter the MAC address of the device to turn it on. A MAC address consists of six hexadecimal character pairs.
Wake up	Click this to send a WoL magic packet to wake up the specified device.

8.8 TFTP Server Name

Use the **TFTP Server Name** screen to identify a TFTP server for configuration file download using DHCP option 66. RFC 2132 defines the option 66 open standard. DHCP option 66 supports the IP address or the host name of a single TFTP server.

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

Figure 78   Network Setting > Home Networking > TFTP Server Name

The following table describes the labels in this screen.

Table 38   Network Setting > Home Networking > TFTP Server Name

LABEL	DESCRIPTION
TFTP Server Name	Enter the IP address or the host name of a single TFTP server.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

8.9 Technical Reference

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

8.9.1 LANs, WANs and the Zyxel Device

The actual physical connection determines whether the Zyxel Device ports are LAN or WAN ports. There are 2 separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 79   LAN and WAN IP Addresses
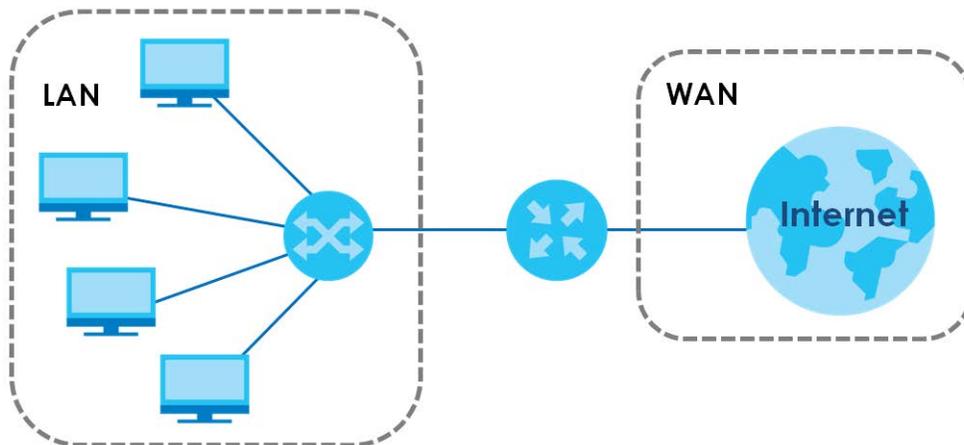
8.9.2 DHCP Setup

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

IP Pool Setup

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

8.9.3 DNS Server Addresses

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

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

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.

- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The Zyxel Device supports the IPCP DNS server extensions through the DNS proxy feature.

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

8.9.4 LAN TCP/IP

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

IP Address and Subnet Mask

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

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

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

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

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

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your 2 branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

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

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

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

CHAPTER 9
Routing

9.1 Overview

The Zyxel Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Zyxel Device 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 Zyxel Device's LAN interface. The Zyxel Device routes most traffic from **A** to the Internet through the Zyxel Device'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 80   Example of Routing Topology
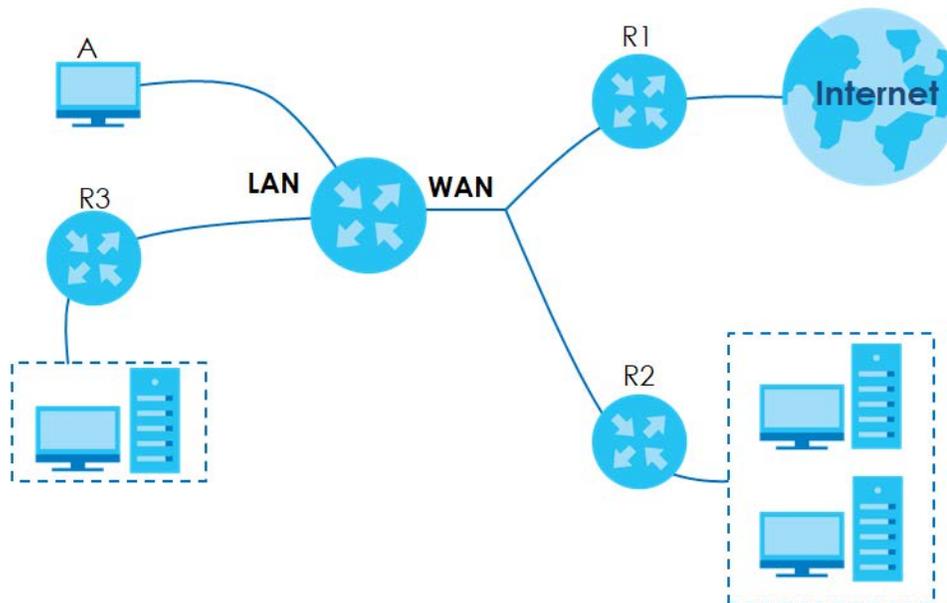
9.2 Static Route Settings

Use this screen to view and configure the static route rules on the Zyxel Device. A static route is used to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets, especially when there are more than two Internet connections available in your home or office network. Click **Network Setting** > **Routing** > **Static Route** to open the following screen.

Figure 81   Network Setting > Routing > Static Route

Use this screen to view and configure the static route rules on the Zyxel Device. A static route is used to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets, especially when there are more than two Internet connections available in your home or office network.

＋Add New Static Route

#	Status	Name	Destination IP	Subnet Mask/Prefix Length	Gateway	Interface	Modify
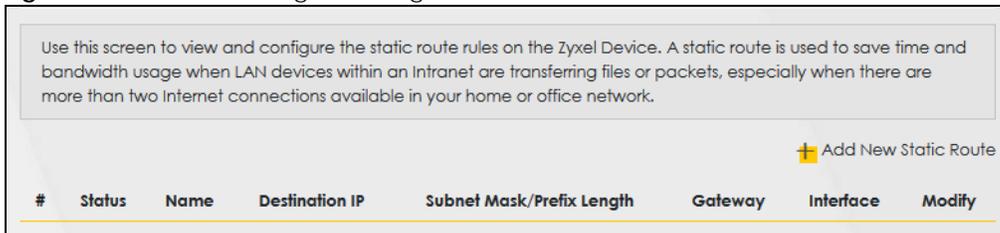
The following table describes the labels in this screen.

Table 39   Network Setting > Routing > Static Route

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

9.2.1 Add/Edit Static Route

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

Note: The **Gateway IP Address** must be within the range of the selected interface in **Use Interface**.

Figure 82 Network Setting > Routing > Static Route: Add/Edit

The following table describes the labels in this screen.

Table 40   Network Setting > Routing > Static Route: Add/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable or disable this static route. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Route Name	Enter a descriptive name for the static route.
IP Type	Select whether your IP type is **IPv4** or **IPv6**.
Destination IP Address	Enter the IPv4 or IPv6 network address of the final destination.
Subnet Mask	If you are using IPv4 and need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. Enter the IP subnet mask here.
Use Gateway IP Address	The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. Click this switch to enable or disable the gateway IP address. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Gateway IP Address	Enter the IP address of the gateway.
Use Interface	Select the WAN interface you want to use for this static route.
Cancel	Click **Cancel** to exit this screen without saving any changes.
Apply	Click **Apply** to save your changes.

9.3 DNS Route

Use this screen to view and configure DNS routes on the Zyxel Device. A DNS route entry defines a policy for the Zyxel Device to forward a particular DNS query to a specific WAN interface.

Note: A maximum of 20 DNS routes can be added.

Click **Network Setting > Routing > DNS Route** to open the following screen.

Figure 83   Network Setting > Routing > DNS Route
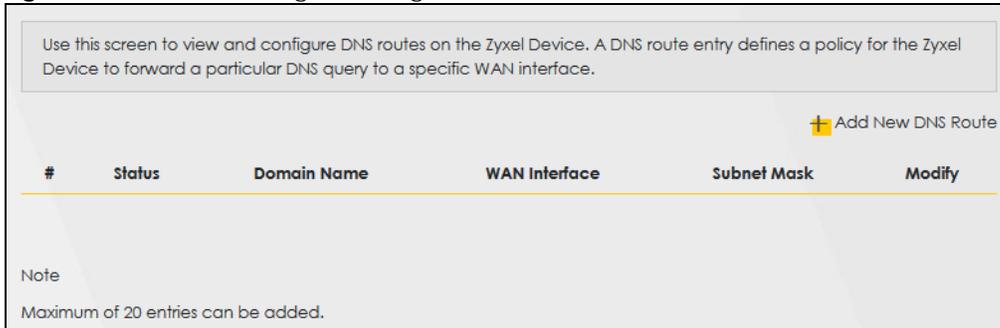
The following table describes the labels in this screen.

Table 41   Network Setting > Routing > DNS Route

LABEL	DESCRIPTION
Add New DNS Route	Click this to add a new DNS route.
#	This is the index number of a DNS route.
Status	This field displays whether the DNS route is active or not. A yellow bulb signifies that this DNS route is active. A gray bulb signifies that this DNS route is not active.
Domain Name	This is the host name or domain name of the DNS route entry.
WAN Interface	This is the WAN connection through which the Zyxel Device forwards DNS requests for this domain name.
Subnet Mask	This is the subnet mask of the DNS route entry.
Modify	Click the **Edit** icon to modify the DNS route.
	Click the **Delete** icon to delete the DNS route.

9.3.1 Add DNS Route

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

Figure 84   DNS Route Add

The following table describes the labels in this screen.

Table 42   DNS Route Add

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the DNS route. When the switch goes to the right ⬤ , the function is enabled. Otherwise, it is not.
Domain Name	Enter the domain name of the DNS route entry.
Subnet Mask	Enter the subnet mask of the DNS route entry.
WAN Interface	Select the WAN connection through which the Zyxel Device forwards DNS requests for this domain name. **ETHWAN** means the wireless cellular interface.
Cancel	Click this to exit this screen without saving any changes.
OK	Click this to save your changes.

9.4 Policy Route

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

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

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

Figure 85 Network Setting > Routing > Policy Route
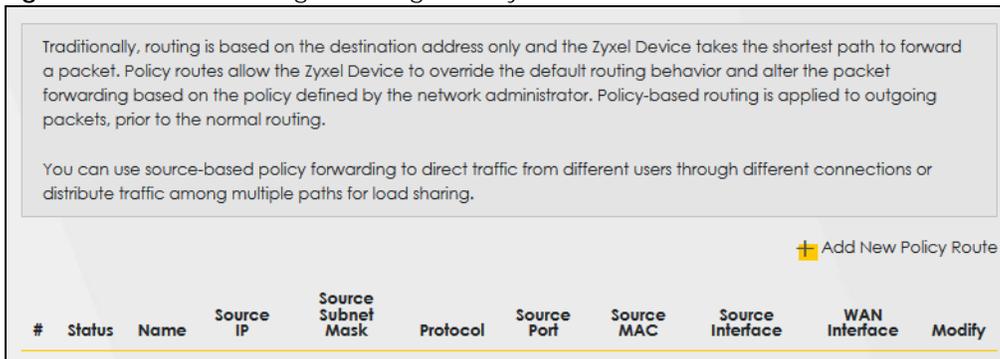
The following table describes the labels in this screen.

Table 43   Network Setting > Routing > Policy Route

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

9.4.1 Add/Edit Policy Route

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

Figure 86   Policy Route: Add/Edit

The following table describes the labels in this screen.

Table 44   Policy Route: Add/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the policy route. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Route Name	Enter a descriptive name of up to 8 printable English keyboard characters, not including spaces.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (**TCP** or **UDP**).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Source Interface (ex: br0 or LAN1~LAN4)	Type the name of the interface from which the matched traffic is sent.
WAN Interface	This field shows **ETHWAN** as the WAN interface through which the traffic is sent.

Table 44   Policy Route: Add/Edit (continued)

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

9.5 RIP Settings

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

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

Figure 87   Network Setting > Routing > RIP

The following table describes the labels in this screen.

Table 45   Network Setting > Routing > RIP

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

CHAPTER 10
Quality of Service (QoS)

10.1 QoS Overview

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

Configure QoS on the Zyxel Device 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 Zyxel Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video. There are eight priority levels, with 1 having the highest priority.

This chapter contains information about configuring QoS and editing classifiers.

10.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth (Section 10.3 on page 148).
- The **Queue Setup** screen lets you configure QoS queue assignment (Section 10.4 on page 150).
- The **Classification Setup** screen lets you add, edit or delete QoS classifiers (Section 10.5 on page 152).
- The **Shaper Setup** screen limits outgoing traffic transmission rate on the selected interface (Section 10.6 on page 157).

- The **Policer Setup** screen lets you control incoming traffic transmission rate and bursts (Section 10.7 on page 158).

- The **Monitor** screen lets you view statistics of QoS on WAN/LAN interface and the status of queues (Section 10.8 on page 161).

10.2 What You Need to Know

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

QoS versus CoS

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

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

Tagging and Marking

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

Traffic Shaping

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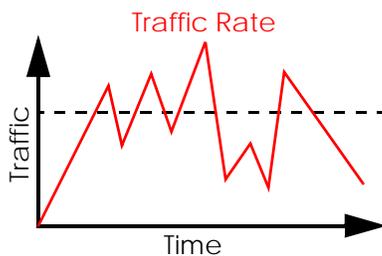
(Before Traffic Shaping)   (After Traffic Shaping)
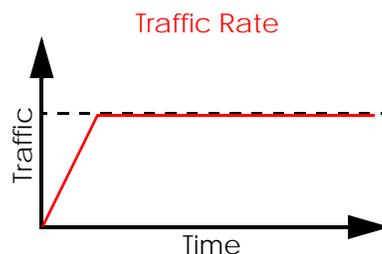
Traffic Policing

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)
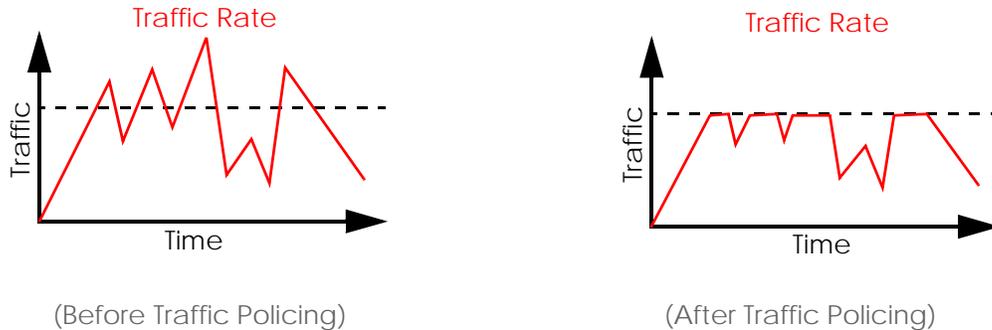
The Zyxel Device supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Maker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See Section 10.8 on page 161 for more information on each metering algorithm.

10.3 Quality of Service General Settings

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

Use this screen to enable or disable QoS and set the upstream bandwidth or assign traffic priority. See Section 10.1 on page 146 for more information.

When one of the following situations happens, the current WAN linkup rate will be used instead:

1 **WAN Managed Upstream Bandwidth** is set to 0

2 **WAN Managed Upstream Bandwidth** is empty

3 **WAN Managed Upstream Bandwidth** is higher than the current WAN interface linkup rate

Note: Manually defined QoS is ignored when **Upstream Traffic Priority** is selected.

Note: **Upstream Traffic Priority** automatically assigns a traffic priority level based on the selected criteria.

Note: To have your QoS settings configured in other **QoS** screens take effect, select **None** in the **Upstream Traffic Priority Assigned by** field.

Figure 88 Network > QoS > General

The following table describes the labels in this screen.

Table 46   Network Setting > QoS > General

LABEL	DESCRIPTION
QoS	Click this switch to enable or disable QoS to improve your network performance. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
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 Zyxel Device 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 Zyxel Device to not use some of the interfaces' available bandwidth. If you leave this field blank, the Zyxel Device 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 wireless LAN) 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 Zyxel Device to not use some of the interfaces' available bandwidth. If you leave this field blank, the Zyxel Device automatically sets this to the LAN interfaces' maximum supported connection speed.

Table 46   Network Setting > QoS > General (continued)

LABEL	DESCRIPTION
Upstream traffic priority Assigned by	Select how the Zyxel Device assigns priorities to various upstream traffic flows. • **None:** Disables auto priority mapping and has the Zyxel Device put packets into the queues according to your classification rules. Traffic which does not match any of the classification rules is mapped into the default queue with the lowest priority. • **Ethernet Priority:** Automatically assign priority based on the IEEE 802.1p priority level. • **IP Precedence:** Automatically assign priority based on the first three bits of the TOS field in the IP header. • **Packet Length:** Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, Internet gaming, or other real-time packets are usually small while larger packets are usually best effort data packets like file transfers.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

10.4 Queue Setup

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

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

Note: Apart from the default entry that cannot be edited, you can add up to 6 extra entries.

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

Note: The corresponding classifier(s) will be removed automatically if a queue is deleted.

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

Note: Priority level 1 is the highest priority for QoS.

Figure 89   Network Setting > QoS > Queue Setup

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

Add New Queue

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

Note

(1) Apart from the default entry that cannot be edited, you can add up to 6 extra entries.

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

(3) Rate limit 0 means there's no rate limit on a queue.

(4) The corresponding classifier(s) will be removed automatically if a queue is deleted.

The following table describes the labels in this screen.

Table 47   Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add New Queue	Click this button to create a new queue entry.
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the Zyxel Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue. The lower the number, the higher the priority level.
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 Zyxel Device should handle packets when it receives too many (network congestion).
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue. Rate limit 0 means there's no rate limit on this queue.
Modify	Click the **Edit** icon to edit the queue. Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

10.4.1 Adding a QoS Queue

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

Figure 90   Queue Setup: Add

The following table describes the labels in this screen.

Table 48   Queue Setup: Add

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the queue. When the switch turns blue ⬤, the function is enabled. Otherwise, it is not.
Name	Enter the descriptive name of this queue.
Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 7) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the Zyxel Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Buffer Management	This field displays **Drop Tail (DT)**. **Drop Tail (DT)** is a simple queue management algorithm that allows the Zyxel Device buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it).
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue. If you enter 0 here, this means there's no rate limit on this queue.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

10.5 QoS Classification Setup

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

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

Figure 91 Network Setting > QoS > Classification Setup

The following table describes the labels in this screen.

Table 49   Network Setting > QoS > Classification Setup

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

10.5.1 Add/Edit QoS Class

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

Figure 92 Classification Setup: Add/Edit

The following table describes the labels in this screen.

Table 50   Classification Setup: Add/Edit

LABEL	DESCRIPTION
Step1: Class Configuration	
Active	Click this switch to enable or disable the classifier. When the switch turns blue ◯●, the function is enabled. Otherwise, it is not.
Class Name	Enter a descriptive name of up to 15 printable English keyboard characters, not including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**. Select **Last** to put this rule in the back of the classifier list.
Step2: Criteria Configuration	
Basic	
From Interface	If you want to classify the traffic by an ingress interface, select an interface from the **From Interface** drop-down list box.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select **802.1Q**, you can configure an 802.1p priority level.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Mask	Enter the source subnet mask.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Mask	Enter the source subnet mask.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	

Table 50   Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Service	This field is available only when you select **IP** in the **Ether Type** field. This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields.
IP Protocol	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select the protocol (service type) from **TCP**, **UDP**, **ICMP** or **IGMP**. If you select **User defined**, enter the protocol (service type) number.
DHCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select a DHCP option. If you select **Vendor Class ID (DHCP Option 60)**, enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware. If you select **Client ID (DHCP Option 61)**, enter the Identity Association IDentifier (IAD Option 61) of the matched traffic, such as the MAC address of the device. If you select **User Class ID (DHCP Option 77)**, enter a string that identifies the user's category or application type in the matched DHCP packets. If you select **Vendor Specific Info (DHCP Option 125)**, enter the vendor specific information of the matched traffic, such as the product class, model name, and serial number of the device.
IP Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.
DSCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
802.1P	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and select a priority level (between 0 and 7) from the drop-down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and specify a VLAN ID number.
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Step3: Packet Modification	
DSCP Mark	This field is available only when you select **IP** in the **Ether Type** field. If you select **Remark**, enter a DSCP value with which the Zyxel Device replaces the DSCP field in the packets. If you select **Unchange**, the Zyxel Device keep the DSCP field in the packets.
VLAN ID	If you select **Remark**, enter a VLAN ID number with which the Zyxel Device replaces the VLAN ID of the frames. If you select **Remove**, the Zyxel Device deletes the VLAN ID of the frames before forwarding them out. If you select **Add**, the Zyxel Device treat all matched traffic untagged and add a second VLAN ID. If you select **Unchange**, the Zyxel Device keep the VLAN ID in the packets.

Table 50   Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
802.1P Mark	Select a priority level with which the Zyxel Device replaces the IEEE 802.1p priority field in the packets.
	If you select **Unchange**, the Zyxel Device keep the 802.1p priority field in the packets.
Step4: Class Routing	
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the Zyxel Device forward traffic of this class according to the default routing table.
Step5: Outgoing Queue Selection	
To Queue Index	Select a queue that applies to this class.
	You should have configured a queue in the **Queue Setup** screen already.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

10.6 QoS Shaper Setup

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

Figure 93   Network Setting > QoS > Shaper Setup
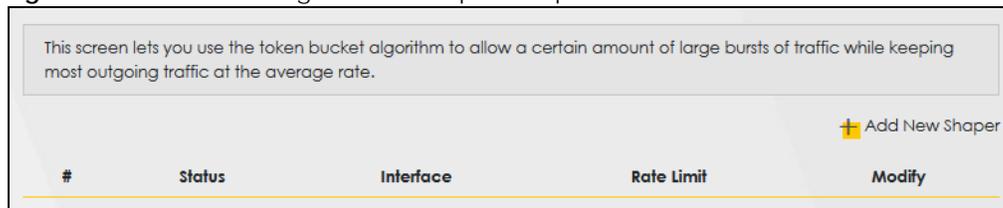
The following table describes the labels in this screen.

Table 51   Network Setting > QoS > Shaper Setup

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

10.6.1 Add/Edit a QoS Shaper

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

Figure 94 Shaper Setup: Add/Edit

The following table describes the labels in this screen.

Table 52 Shaper Setup: Add/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the shaper. When the switch turns blue 🔵, the function is enabled. Otherwise, it is not.
Interface	Select a Zyxel Device interface through which traffic in this shaper applies.
Rate Limit	Enter the average rate limit of traffic bursts for this shaper.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

10.7 QoS Policer Setup

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

Figure 95 Network Setting > QoS > Policer Setup

The following table describes the labels in this screen.

Table 53   Network Setting > QoS > Policer Setup

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

10.7.1 Add/Edit a QoS Policer

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

Figure 96   Policer Setup: Add/Edit

The following table describes the labels in this screen.

Table 54   Policer Setup: Add/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the policer. When the switch turns blue 〇●, the function is enabled. Otherwise, it is not.
Name	Enter the descriptive name of this policer.
Meter Type	This shows the traffic metering algorithm used in this policer. The **Simple Token Bucket** algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size. The **Single Rate Three Color Marker** (srTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR), the Committed Burst Size (CBS) and the Excess Burst Size (EBS). The **Two Rate Three Color Marker** (trTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR) and the Peak Information Rate (PIR).
Committed Rate	Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic.

Table 54   Policer Setup: Add/Edit

LABEL	DESCRIPTION
Committed Burst Size	Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured. This is the maximum size of the (first) token bucket in a traffic metering algorithm.
Excess Burst Size	Specify the additional amount of bytes that are admitted at the committed rate besides the committed burst size. This is the maximum size of the second token bucket in the srTCM. This field is only available when you select **Single Rate Three Color** in the **Meter Type** field.
Peak Rate	Specify the maximum rate at which packets are admitted to the network. The peak rate should be greater than or equal to the committed rate. This is to specify how many bytes of tokens are added to the second bucket every second in the trTCM. This field is only available when you select **Two Rate Three Color** in the **Meter Type** field.
Peak Burst Size	Specify the maximum amount of bytes that are admitted at the committed rate. This is the maximum size of the second token bucket in the trTCM. This field is only available when you select **Two Rate Three Color** in the **Meter Type** field.
Conforming Action	Specify what the Zyxel Device does for packets within the committed rate and burst size (green-marked packets). • **Pass:** Send the packets without modification. • **DSCP Mark:** Change the DSCP mark value of the packets. Enter the DSCP mark value to use.
Partial Conforming Action	Specify the action that the Zyxel Device takes on yellow-marked packets. Select **Pass** to forward the packets. Select **Drop** to discard the packets. Select **DSCP Mark** to assign a specified DSCP number (between 0 and 63) to the packets and forward them. The packets are dropped if there is congestion on the network. This field is only available when you select **Single/Two Rate Three Color** in the **Meter Type** field.
Non-Conforming Action	Specify what the Zyxel Device does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets). • **Drop:** Discard the packets. • **DSCP Mark:** Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network.
Available Class	Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier.
Selected Class	Highlight a QoS classifier in the **Available Class** box and use the **>** button to move it to the **Selected Class** box. To remove a QoS classifier from the **Selected Class** box, select it and use the **<** button.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

10.8 QoS Monitor

To view the Zyxel Device's QoS packet statistics, click **Network Setting** > **QoS** > **Monitor**. The screen appears as shown.

Figure 97 Network Setting > QoS > Monitor

The following table describes the labels in this screen.

Table 55   Network Setting > QoS > Monitor

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the Zyxel Device to update this screen. Select **None** to stop refreshing statistics.
Interface Monitor	
#	This is the index number of the entry.
Name	This shows the name of the interface on the Zyxel Device.
Pass Rate (bps)	This shows how many packets forwarded to this interface are transmitted successfully.
Drop Rate (bps)	This shows how many packets forwarded to this interface are dropped.
Queue Monitor	
#	This is the index number of the entry.
Name	This shows the name of the queue.
Pass Rate (bps)	This shows how many packets assigned to this queue are transmitted successfully.
Drop Rate (bps)	This shows how many packets assigned to this queue are dropped.

10.9 Technical Reference

The following section contains additional technical information about the Zyxel Device 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 8 separate traffic types. The following table

describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 56   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)
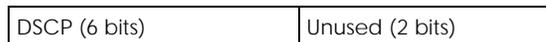
The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the 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 Zyxel Device, the Zyxel Device 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 Zyxel Device. On the Zyxel Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 57   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 Zyxel Device stops transmitting until enough tokens are generated.
- If not enough tokens are available, the Zyxel Device 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 Zyxel Device 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 Zyxel Device 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 Zyxel Device checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

CHAPTER 11
Network Address Translation (NAT)

11.1 NAT Overview

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

11.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network (Section 11.2 on page 168).
- Use the **Port Triggering** screen to add and configure the Zyxel Device's trigger port settings (Section 11.3 on page 172).
- Use the **DMZ** screen to configure a default server (Section 11.4 on page 175).
- Use the **ALG** screen to enable and disable the ALGs in the Zyxel Device (Section 11.5 on page 176).
- Use the **Address Mapping** screen to configure the Zyxel Device's address mapping settings (Section 11.6 on page 177).
- Use the **Sessions** screen to configure the Zyxel Device's maximum number of NAT sessions (Section 11.6 on page 177).

11.1.2 What You Need To Know

Inside/Outside

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

Global/Local

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

NAT

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

back to the inside local address before forwarding it to the original inside host.

Port Forwarding

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

Finding Out More

See Section 11.8 on page 180 for advanced technical information on NAT.

11.2 Port Forwarding

Use **Port Forwarding** to forward incoming service requests from the Internet to the server(s) on your local network. Port forwarding is commonly used when you want to host online gaming, P2P file sharing, or other servers on your network.

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

The most often used port numbers and services are shown in Appendix C on page 295. Please refer to RFC 1700 for further information about port numbers.

Note: TCP port 7547 is reserved for system use.

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

Configuring Servers Behind Port Forwarding (Example)

Let us 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 98 Multiple Servers Behind NAT Example
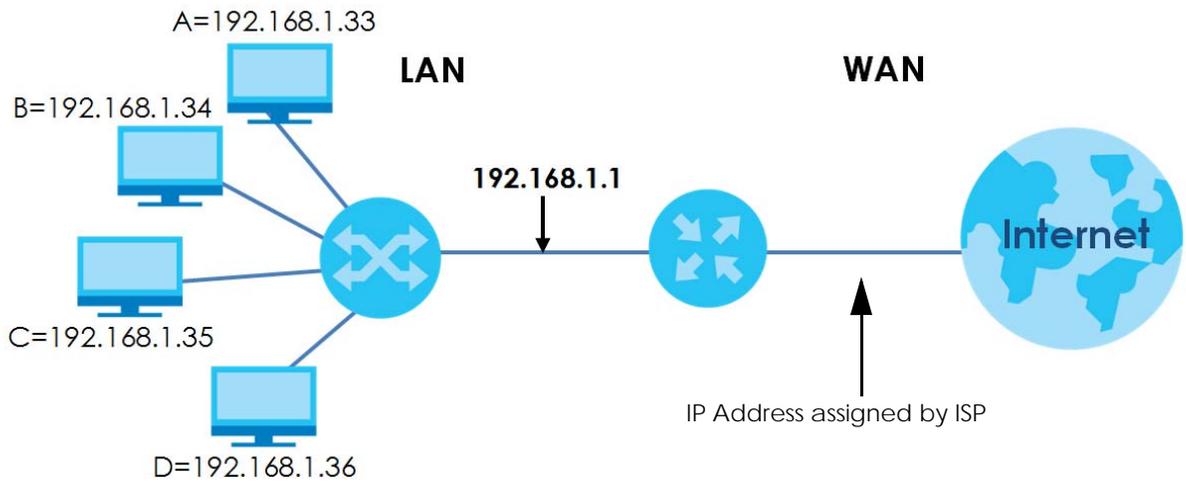
Click **Network Setting > NAT > Port Forwarding** to open the following screen.

Figure 99 Network Setting > NAT > Port Forwarding

The following table describes the fields in this screen.

Table 58 Network Setting > NAT > Port Forwarding

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

Table 58   Network Setting > NAT > Port Forwarding (continued)

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

11.2.1 Add/Edit Port Forwarding

Click **Add New Rule** in the **Port Forwarding** screen or click the **Edit** icon next to an existing rule to open the following screen. Specify either a port or a range of ports, a server IP address, and a protocol to configure a port forwarding rule.

Note: To configure port forwarding, you need to have the same configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.

Note: To configure port translation, you need to have different configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.

Here is an example to configure port translation. Configure **Start Port** to 100, **End Port** to 120, **Translation Start Port** to 200, and **Translation End Port** to 220.

Figure 100   Port Forwarding: Add/Edit

The following table describes the labels in this screen.

Table 59   Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the rule. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
Obtain WAN IP Automatically	Select the **Enable** check box to have the Zyxel Device automatically detect and use an available WAN interface for port forwarding.
WAN IP	Enter your WAN IP address in this field if you did not select **Obtain WAN IP Automatically**.
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled. Note: This field is not available if you enable **Obtain WAN IP Automatically**.

Table 59   Port Forwarding: Add/Edit (continued)

LABEL	DESCRIPTION
Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port** field.
End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port** field above.
Translation Start Port	This shows the port number to which you want the Zyxel Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Configure Originating IP	Select **Enable** to enter the source IP address of WAN interface.
Originating IP	Enter the source IP address of WAN interface.
Protocol	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

11.3 Port Triggering

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 addresses this problem. Trigger port forwarding allows computers on the LAN to dynamically take turns using the service. The Zyxel Device 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 Zyxel Device's WAN port receives a response with a specific port number and protocol ("open" port), the Zyxel Device 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.

Note: TCP port 7547 is reserved for system use.

Note: The maximum number of trigger ports for a single rule or all rules is 999.

Note: The maximum number of open ports for a single rule or all rules is 999.

Note: The sum of trigger ports in all rules must be less than 1000 and every open port range must be less than 1000. When the protocol is TCP/UDP, the ports are counted twice.

For example:

Figure 101 Trigger Port Forwarding Process: Example
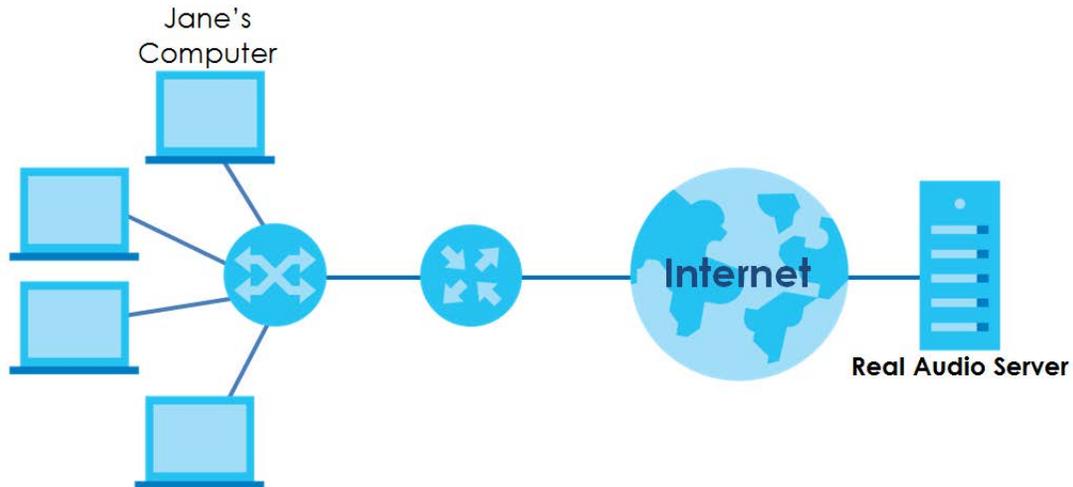
1   Jane requests a file from the Real Audio server (port 7070).

2   Port 7070 is a "trigger" port and causes the Zyxel Device to record Jane's computer IP address. The Zyxel Device associates Jane's computer IP address with the "open" port range of 6970-7170.

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

4   The Zyxel Device 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 Zyxel Device times out in three minutes with UDP (User Datagram Protocol) or 2 hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

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

Figure 102 Network Setting > NAT > Port Triggering

Trigger port forwarding allows computers on the LAN to dynamically take turns using the service. The Zyxel Device 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 Zyxel Device's WAN port receives a response with a specific port number and protocol ("open" port), the Zyxel Device 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.

+ Add New Rule

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

Note

(1) The maximum number of trigger ports for a single rule or all rules is 999.

(2) The maximum number of open ports for a single rule or all rules is 999.

(3) TCP port 7547 is reserved for system use.

The following table describes the labels in this screen.

Table 60   Network Setting > NAT > Port Triggering

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

11.3.1 Add/Edit Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add new rule** in the **Port Triggering** screen or click a rule's **Edit** icon to open the following screen. Use this screen to configure a port or range of ports and protocols for sending out requests and for receiving responses.

Figure 103   Port Triggering: Add/Edit

The following table describes the labels in this screen.

Table 61   Port Triggering: Configuration Add/Edit

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

11.4 DMZ Settings

A client in the Demilitarized Zone (DMZ) is no longer behind the Zyxel Device and therefore can run any Internet applications such as video conferencing and Internet gaming without restrictions. This, however, may pose a security threat to the Zyxel Device.

Note: Use an IPv4 address for the DMZ server.

Note: Enter the IP address of the default server in the **Default Server Address** field, and click **Apply** to active the DMZ host. Otherwise, clear the IP address in the **Default Server Address** field, and click **Apply** to deactivate the DMZ host.

Figure 104 Network Setting > NAT > DMZ

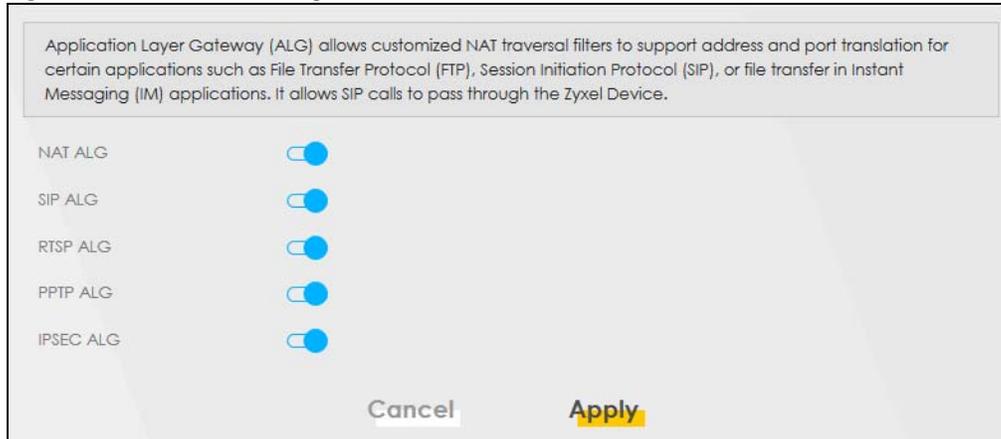The following table describes the fields in this screen.

Table 62 Network Setting > NAT > DMZ

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

11.5 ALG Settings

Application Layer Gateway (ALG) allows customized NAT traversal filters to support address and port translation for certain applications such as File Transfer Protocol (FTP), Session Initiation Protocol (SIP), or file transfer in Instant Messaging (IM) applications. It allows SIP calls to pass through the Zyxel Device. When the Zyxel Device registers with the SIP register server, the SIP ALG translates the Zyxel Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your Zyxel Device is behind a SIP ALG.

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

Figure 105   Network Setting > NAT > ALG

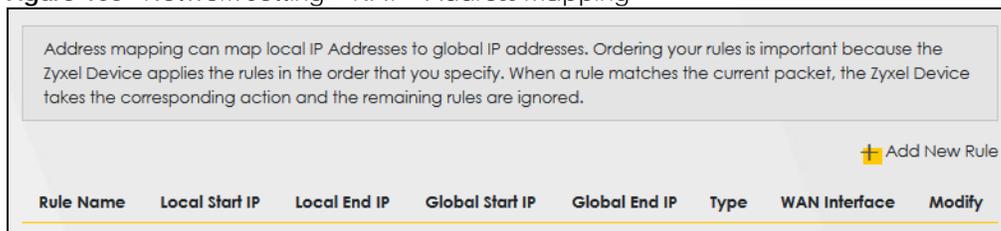The following table describes the fields in this screen.

Table 63   Network Setting > NAT > ALG

LABEL	DESCRIPTION
NAT ALG	Enable this to make sure applications such as FTP and file transfer in IM applications work correctly with port-forwarding and address-mapping rules.
SIP ALG	Enable this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
RTSP ALG	Enable this to have the Zyxel Device detect RTSP traffic and help build RTSP sessions through its NAT. The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
PPTP ALG	Enable this to turn on the PPTP ALG on the Zyxel Device to detect PPTP traffic and help build PPTP sessions through the Zyxel Device's NAT.
IPSEC ALG	Enable this to turn on the IPsec ALG on the Zyxel Device to detect IPsec traffic and help build IPsec sessions through the Zyxel Device's NAT.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

11.6 Address Mapping

Address mapping can map local IP Addresses to global IP addresses. Ordering your rules is important because the Zyxel Device applies the rules in the order that you specify. When a rule matches the current packet, the Zyxel Device takes the corresponding action and the remaining rules are ignored.

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

Figure 106   Network Setting > NAT > Address Mapping

The following table describes the fields in this screen.

Table 64   Network Setting > NAT > Address Mapping

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

11.6.1 Add/Edit Address Mapping Rule

To add or edit an address mapping rule, click **Add new rule** or the rule's edit icon in the **Address Mapping** screen to display the screen shown next. Specify the NAT mapping type, the local and global IP address(es), and a WAN interface in this screen.

Figure 107 Address Mapping: Add/Edit

The following table describes the fields in this screen.

Table 65   Address Mapping: Add/Edit

LABEL	DESCRIPTION
Rule Name	Type up to 20 alphanumeric characters for the name of this rule.
Type	Choose the IP/port mapping type from one of the following. **One-to-One**: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for example, PAT, port address translation), the Zyxel Device's Single User Account feature that previous routers supported only. **Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses.
Local Start IP	Enter the starting Inside Local IP Address (ILA).
Local End IP	Enter the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for **One-to-One** mapping types.
Global Start IP	Enter the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the **Many-to-One** mapping type.
Global End IP	Enter the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types.
WAN Interface	Select a WAN interface to which the address mapping rule applies.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

11.7 NAT Sessions

Use this screen to limit the number of concurrent NAT sessions a client can use, to ensure that no single client uses up too many available NAT sessions. Some applications, such as P2P file sharing, demand a greater number of NAT sessions in order to get a better uploading and downloading rate. Click **Network**

Setting > NAT > Sessions to display the following screen.

Note: Enter a number of concurrent NAT sessions in the **MAX NAT Session Per Host** field, and click **Apply** to limit the number of concurrent NAT sessions a client can use. Otherwise, clear the number in the **MAX NAT Session Per Host** field. Click **Apply** and there's no limit for concurrent NAT sessions a client can use.

Figure 108 Network Setting > NAT > Sessions

The following table describes the fields in this screen.

Table 66   Network Setting > NAT > Sessions

LABEL	DESCRIPTION
MAX NAT Session Per Host (0 ~ 20480)	Use this field to set a limit to the number of concurrent NAT sessions each client host can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer-to-peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Cancel	Click this to restore the default or previously saved settings.
Apply	Click this to save your changes on this screen.

11.8 Technical Reference

This part contains more information regarding NAT.

11.8.1 NAT Definitions

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

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

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the

same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 67   NAT Definitions

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

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

11.8.2 What NAT Does

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

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

11.8.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The Zyxel Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.
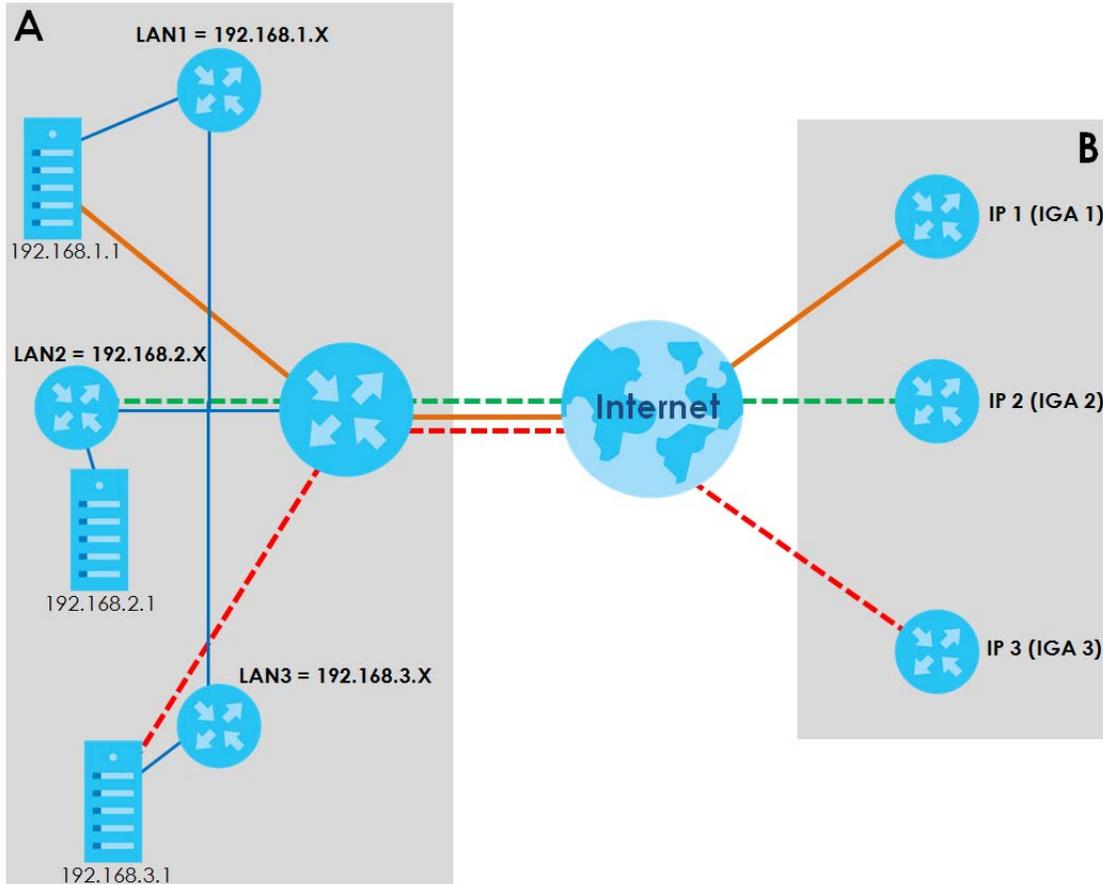
Figure 109 How NAT Works
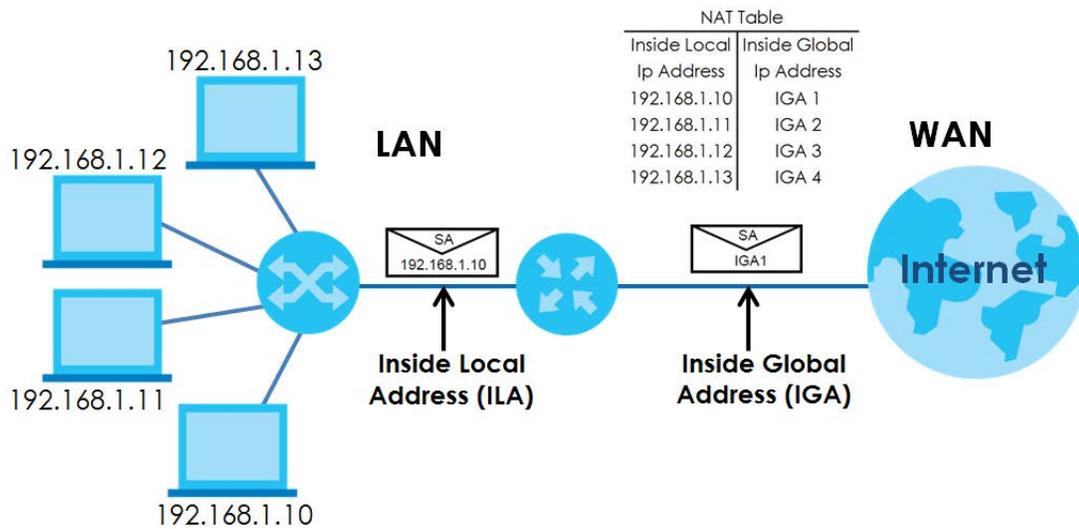
11.8.4 NAT Application

The following figure illustrates a possible NAT application, where 3 inside LANs (logical LANs using IP alias) behind the Zyxel Device can communicate with 3 distinct WAN networks.

Figure 110 NAT Application With IP Alias

Port Forwarding: Services and Port Numbers

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

Table 68   Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Port Forwarding Example

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

Figure 111   Multiple Servers Behind NAT Example
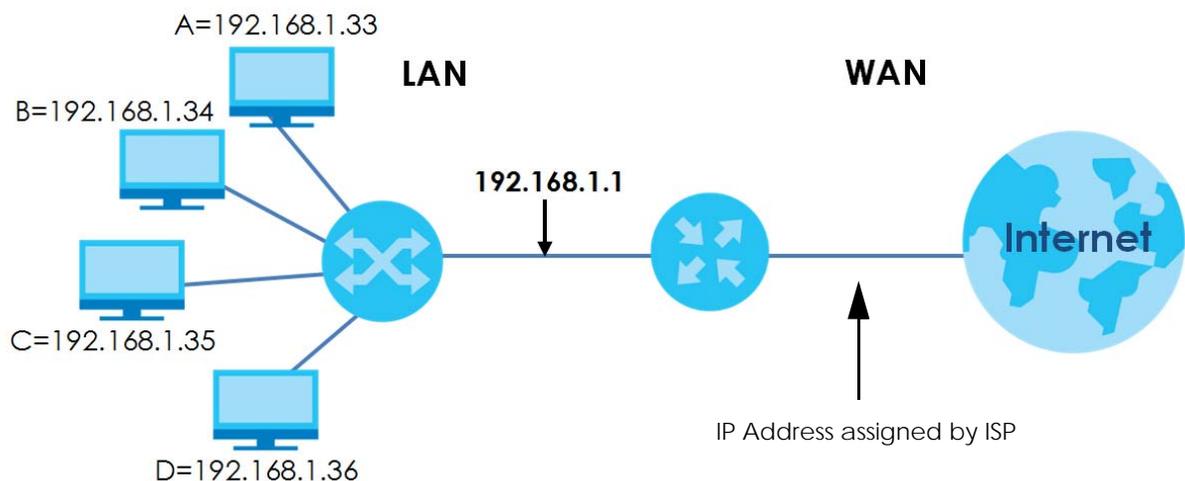
CHAPTER 12
Dynamic DNS Setup

12.1 DNS Overview

DNS

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

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

Dynamic DNS

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

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

12.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes ().
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Zyxel Device ().

12.1.2 What You Need To Know

DYNDNS Wildcard

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

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

12.2 DNS Entry

DNS (Domain Name System) is used for mapping a domain name to its corresponding IP address and vice versa. Use this screen to view and configure DNS routes on the Zyxel Device. Click **Network Setting > DNS** to open the **DNS Entry** screen.

Note: The host name should consist of the host's local name and the domain name. For example, Mycomputer.home is a host name where Mycomputer is the host's local name, and .home is the domain name.

Figure 112   Network Setting > DNS > DNS Entry
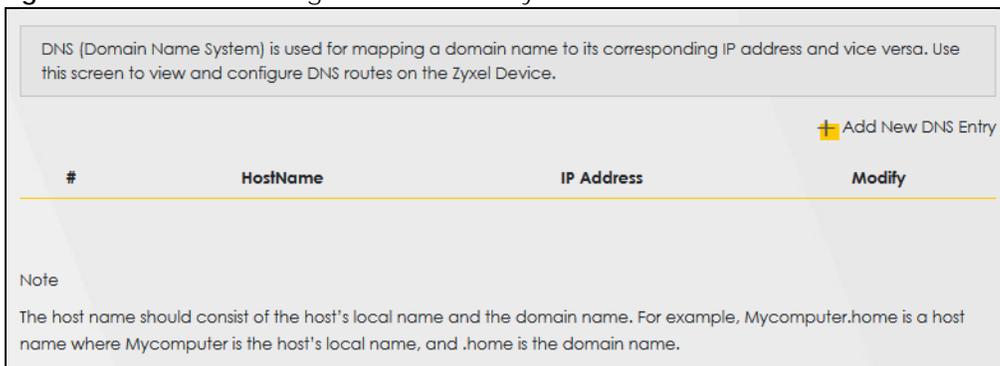
The following table describes the fields in this screen.

Table 69   Network Setting > DNS > DNS Entry

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

12.2.1 Add/Edit DNS Entry

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

Figure 113   DNS Entry: Add/Edit

The following table describes the labels in this screen.

Table 70   DNS Entry: Add/Edit

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

12.3 Dynamic DNS

Dynamic DNS can update your current dynamic IP address mapping to a hostname. Use this screen to configure a DDNS service provider on your Zyxel Device. Click **Network Setting > DNS > Dynamic DNS**. The screen appears as shown.

Figure 114 Network Setting > DNS > Dynamic DNS

The following table describes the fields in this screen.

Table 71 Network Setting > DNS > > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select **Enable** to use dynamic DNS.
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Host Name	Type the domain name assigned to your Zyxel Device by your Dynamic DNS provider. You can specify up to 2 host names in the field separated by a comma (",").
Username	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable Off Line Option (Only applies to custom DNS)	Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Dynamic DNS Status	
User Authentication Result	This shows **Success** if the account is correctly set up with the Dynamic DNS provider account.
Last Updated Time	This shows the last time the IP address the Dynamic DNS provider has associated with the hostname was updated.
Current Dynamic IP	This shows the IP address your Dynamic DNS provider has currently associated with the hostname.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

IGMP/MLD

13.1 IGMP/MLD Overview

Multicast delivers IP packets to a group of hosts on the network defined by multicast groups. Membership to these multicast groups are established using IGMP/MLD.

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

13.1.1 What You Need To Know

Multicast and IGMP

See Multicast on page 86 for more information.

Multicast Listener Discovery (MLD)

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.
- MLD allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.
- MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.
- MLD filtering controls which multicast groups a port can join.
- An MLD Report message is equivalent to an IGMP Report message, and a MLD Done message is equivalent to an IGMP Leave message.

IGMP Fast Leave

When a host leaves a multicast group (224.1.1.1), it sends an IGMP leave message to inform all routers (224.0.0.2) in the multicast group. When a router receives the leave message, it sends a specific query message to all multicast group (224.1.1.1) members to check if any other hosts are still in the group. Then the router deletes the host's information.
With the IGMP fast leave feature enabled, the router removes the host's information from the group member list once it receives a leave message from a host and the fast leave timer expires.

13.2 IGMP/MLD Settings

Use this screen to configure multicast groups that the Zyxel Device manages through IGMP/MLD settings. To open this screen, click **Network Setting** > **IGMP/MLD**.

Figure 115 Network Setting > IGMP/MLD

The following table describes the labels in this screen.

Table 72   Network Setting > IGMP/MLD

LABEL	DESCRIPTION
IGMP/MLD Configuration	
Default Version	Enter the version of IGMP (1~3) and MLD (1~2) that you want the Zyxel Device to use on the WAN.
Query Interval	Enter the number of seconds the Zyxel Device sends a query message to hosts to get the group membership information.
Query Response Interval	Enter the maximum number of seconds the Zyxel Device can wait for receiving a General Query message. Multicast routers use general queries to learn which multicast groups have members.
Last Member Query Interval	Enter the maximum number of seconds the Zyxel Device can wait for receiving a response to a Group-Specific Query message. Multicast routers use group-specific queries to learn whether any member remains in a specific multicast group.
Robustness Value	Enter the number of times (1~7) the Zyxel Device can resend a packet if packet loss occurs due to network congestion.

Table 72   Network Setting > IGMP/MLD (continued)

| LABEL	DESCRIPTION
Maximum Multicast Groups	Enter a number to limit the number of multicast groups an interface on the Zyxel Device is allowed to join. Once a multicast member is registered in the specified number of multicast groups, any new IGMP or MLD join report frames are dropped by the interface.
Maximum Multicast Data Sources(for IGMPv3)	Enter a number to limit the number of multicast data sources (1-24) a multicast group is allowed to have. Note: The setting only works for IGMPv3 and MLDv2.
Maximum Multicast Groups Members	Enter a number to limit the number of multicast members a multicast group can have.
Fast Leave Enable	Select this option to set the Zyxel Device to remove a port from the multicast tree immediately (without sending an MLD membership query message) once it receives an MLD leave message. This is helpful if a user wants to quickly change a TV channel (multicast group change) especially for IPTV applications.
LAN to LAN (Intra LAN) Multicast Enable	Select this to enable LAN to LAN IGMP snooping capability.
Membership Join Immediate (IPTV)	Select this to have the Zyxel Device add a host to a multicast group immediately once the Zyxel Device receives an IGMP join message.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

CHAPTER 14
VLAN Group

14.1 Overview

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

Ports in the same VLAN group share the same frame broadcast domain thus increase network performance through reduced broadcast traffic. Shared resources such as a server can be used by all ports in the same VLAN as the server. Ports can belong to other VLAN groups too. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges. The VLAN ID associates a frame with a specific VLAN and provides the information that switches the need to process the frame across the network.

In the following example, VLAN IDs (VIDs) 100 and 200 are added to identify Video-on-Demand and IPTV traffic respectively coming from the VoD and IPTV multicast servers. The Zyxel Device can also tag outgoing requests to the servers with these VLAN IDs.

Figure 116   VLAN Group Example
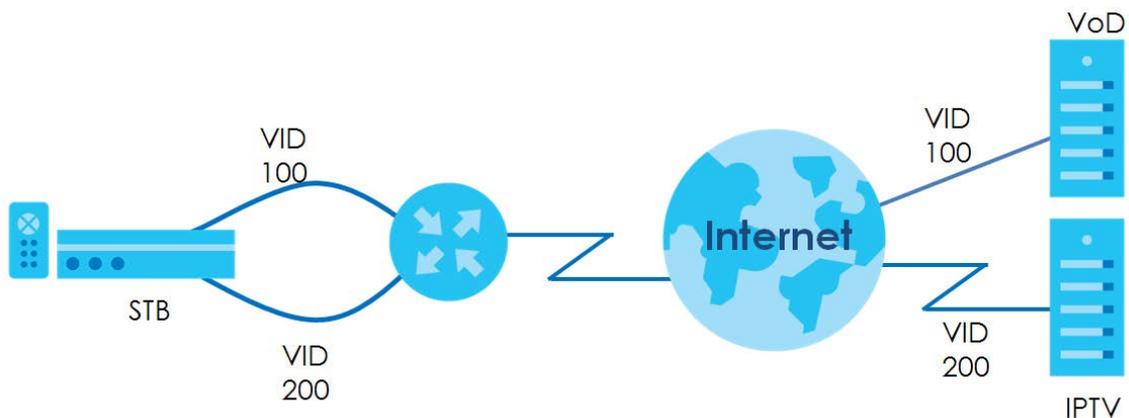
14.1.1 What You Can Do in this Chapter

Use these screens to manage VLAN groups on the Zyxel Device.

14.2 VLAN Group Settings

This screen shows the VLAN groups created on the Zyxel Device. Click **Network Setting > VLAN Group** to open the following screen.

Figure 117 Network Setting > VLAN Group

The following table describes the fields in this screen.

Table 73   Network Setting > VLAN Group

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

14.2.1 Add/Edit a VLAN Group

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

Figure 118 Add/Edit VLAN Group

The following table describes the fields in this screen.

Table 74   Add/Edit VLAN Group

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

CHAPTER 15
Interface Grouping

15.1 Interface Grouping Overview

By default, all LAN and WAN interfaces on the Zyxel Device are in the same group and can communicate with each other. Create interface groups to have the Zyxel Device assign IP addresses in different domains to different groups. Each group acts as an independent network on the Zyxel Device. Devices in different groups cannot communicate with each other directly.

15.1.1 What You Can Do in this Chapter

The **Interface Grouping** screen lets you create multiple networks on the Zyxel Device ().
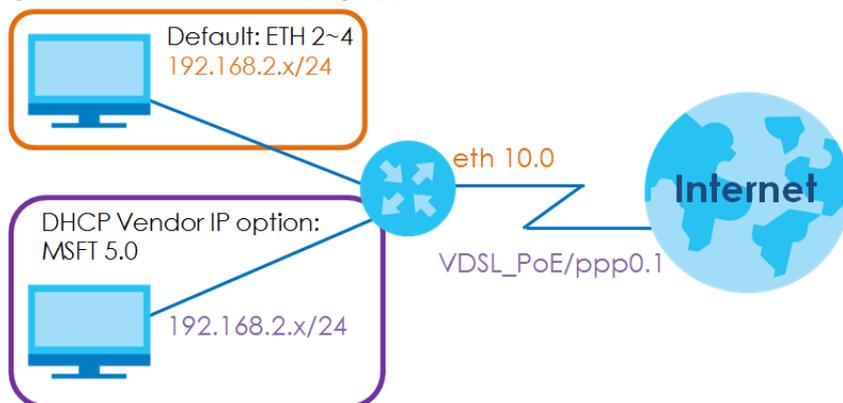
15.2 Interface Grouping Setup

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

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

In the following example, the client that sends packets with the DHCP Vendor ID option set to MSFT 5.0 (meaning it is a Windows 2000 DHCP client) is assigned the IP address 192.168.2.2 and uses the WAN VDSL_PoE/ppp0.1 interface.
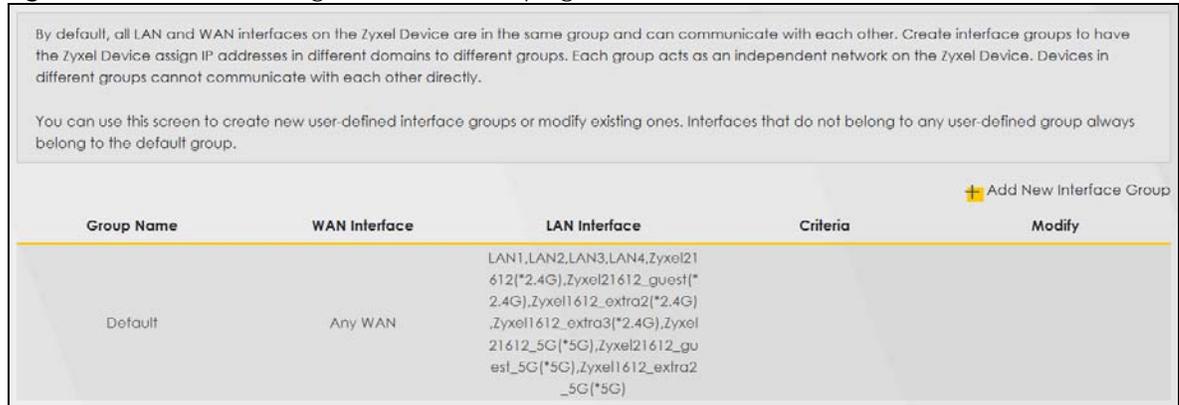
Figure 119 Interface Grouping Application

You can use this screen to create new user-defined interface groups or modify existing ones. Interfaces that do not belong to any user-defined group always belong to the default group.

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

Figure 120 Network Setting > Interface Grouping

By default, all LAN and WAN interfaces on the Zyxel Device are in the same group and can communicate with each other. Create interface groups to have the Zyxel Device assign IP addresses in different domains to different groups. Each group acts as an independent network on the Zyxel Device. Devices in different groups cannot communicate with each other directly.

You can use this screen to create new user-defined interface groups or modify existing ones. Interfaces that do not belong to any user-defined group always belong to the default group.

＋Add New Interface Group

Group Name	WAN Interface	LAN Interface	Criteria	Modify
Default	Any WAN	LAN1,LAN2,LAN3,LAN4,Zyxel21612(*2.4G),Zyxel21612_guest(*2.4G),Zyxel1612_extra2(*2.4G),Zyxel1612_extra3(*2.4G),Zyxel21612_5G(*5G),Zyxel21612_guest_5G(*5G),Zyxel1612_extra2_5G(*5G)		

The following table describes the fields in this screen.

Table 75   Network Setting > Interface Grouping

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

15.2.1 Interface Group Configuration

Click the **Add New Interface Group** button in the **Interface Grouping** screen to open the following screen. Use this screen to create a new interface group. If you want to automatically add LAN clients to a new group, use filtering criteria.

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

Note: After configuring a vendor ID, reboot the client device attached to the Zyxel Device to obtain an appropriate IP address.

Note: You can have up to 15 filter criteria.

Figure 121 Interface Group Configuration

The following table describes the fields in this screen.

Table 76 Interface Group Configuration

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (–) and underscores (_). Spaces are not allowed.
WAN Interfaces used in the grouping	Select the WAN interface this group uses. The group can have up to one ETH interface. Select **None** to not add a WAN interface to this group.
Selected LAN Interfaces Available LAN Interfaces	Select one or more LAN interfaces (Ethernet LAN, HPNA or wireless LAN) in the **Available LAN Interfaces** list and use the left arrow to move them to the **Selected LAN Interfaces** list to add the interfaces to this group. To remove a LAN or wireless LAN interface from the **Selected LAN Interfaces**, use the right-facing arrow.
Automatically Add Clients With the following DHCP Vendor IDs	Click **Add** to identify LAN hosts to add to the interface group by criteria such as the type of the hardware or firmware. See Section 15.2.2 on page 197 for more information.
#	This shows the index number of the rule.

Table 76   Interface Group Configuration (continued)

LABEL	DESCRIPTION
Filter Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.
WildCard Support	This shows if wildcard on DHCP option 60 is enabled.
Modify	Click the **Edit** icon to change the group setting. Click the **Delete** icon to delete this group from the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

15.2.2 Interface Grouping Criteria

Click the **Add** button in the **Interface Grouping Configuration** screen to open the following screen. Use this screen to automatically add clients to an interface group based on specified criteria. You can choose to define a group based on a MAC address, a vendor ID (DHCP option 60), an Identity Association Identifier (DHCP option 61), vendor specific information (DHCP option 125), or a VLAN group.

Figure 122   Interface Grouping Criteria

The following table describes the fields in this screen.

Table 77   Interface Grouping Criteria

| LABEL	DESCRIPTION
Source MAC Address	Enter the source MAC address of the packet.
DHCP Option 60	Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
Enable wildcard	Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60.
DHCP Option 61	Select this and enter the device identity of the matched traffic.
	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.
Enterprise Number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first 3 bytes of the MAC address.
Serial Number	Enter the serial number of the device.
Product Class	Enter the product class of the device.
VLAN Group	Select this and the VLAN group of the matched traffic from the drop-down list box. A VLAN group can be configured in **Network Setting > VLAN Group**.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

16.1 Firewall Overview

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

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

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

Figure 123 Default Firewall Action
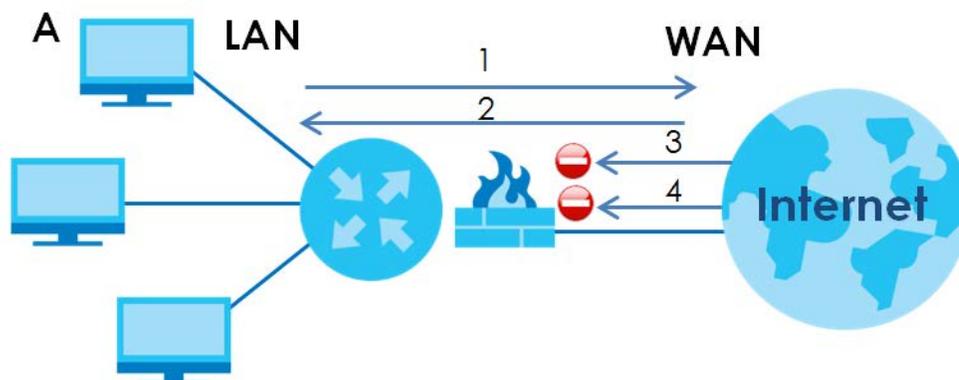
16.1.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the Zyxel Device (Section 16.2 on page 200).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 16.3 on page 201).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules (Section 16.4 on page 203).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (.Section 16.5 on page 206).

16.1.2 What You Need to Know

SYN Attack

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

DoS

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

DDoS

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

LAND Attack

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

Ping of Death

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

SPI

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

16.2 Firewall Settings

Use this screen to set the security level of the firewall on the Zyxel Device. Firewall rules are grouped based on the direction of travel of packets to which they apply. A higher firewall level means more restrictions on the Internet activities you can perform.

Note: LAN to WAN is your access to all Internet services. WAN to LAN is the access of other computers on the Internet to devices behind the Zyxel Device.

Note: When the security level is set to **High**, Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and/or IPv6 ICMPv6 (Ping) traffic from the LAN are still allowed.

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

Figure 124 Security > Firewall > General
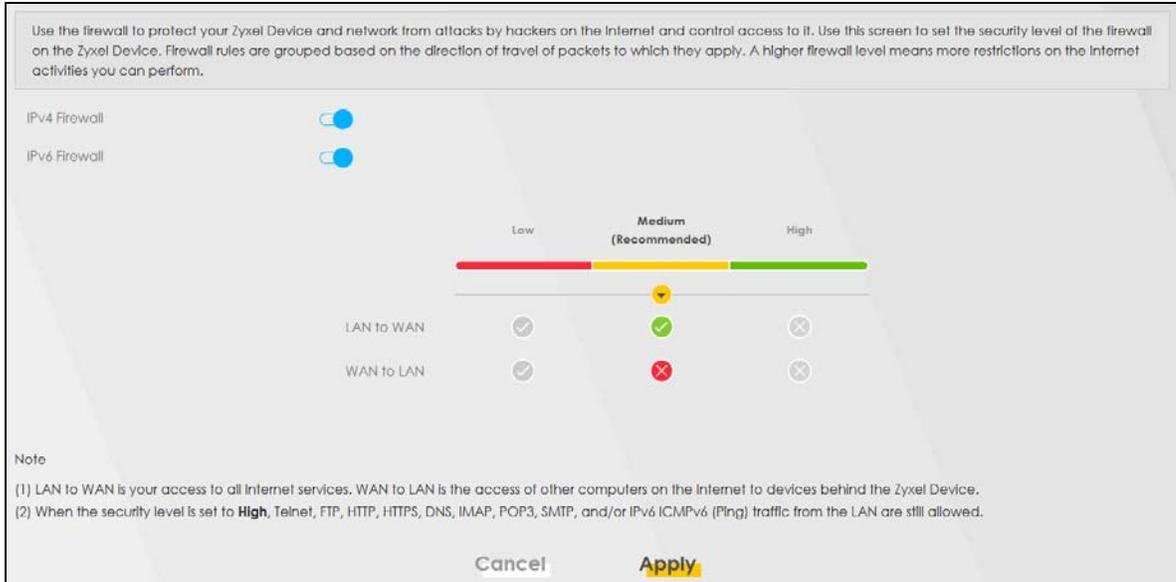
The following table describes the labels in this screen.

Table 78 Security > Firewall > General

LABEL	DESCRIPTION
IPv4 Firewall	Use the switch to turn on or off the firewall feature on the Zyxel Device for IPv4 traffic. When the switch goes to the right ⟨⬤, the function is enabled. Otherwise, it is disabled.
IPv6 Firewall	Use the switch to turn on or off the firewall feature on the Zyxel Device for IPv6 traffic. When the switch goes to the right ⟨⬤, the function is enabled. Otherwise, it is disabled.
Low	Select **Low** to allow traffic from LAN to WAN or from WAN to LAN.
Medium	Select **Medium** to allow traffic from LAN to WAN but deny traffic from WAN to LAN.
High	Select **High** to deny both directions of travel of packets (LAN to WAN and WAN to LAN).
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

16.3 Protocol Settings

You can configure customized services and port numbers in the **Protocol** screen. Each set of protocol rules listed in the table are reusable objects to be used in conjunction with ACL rules in the Access Control screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See *Appendix C on page 295* for some examples.

Note: Removing a protocol rule will also remove associated ACL rules.

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

Figure 125 Security > Firewall > Protocol
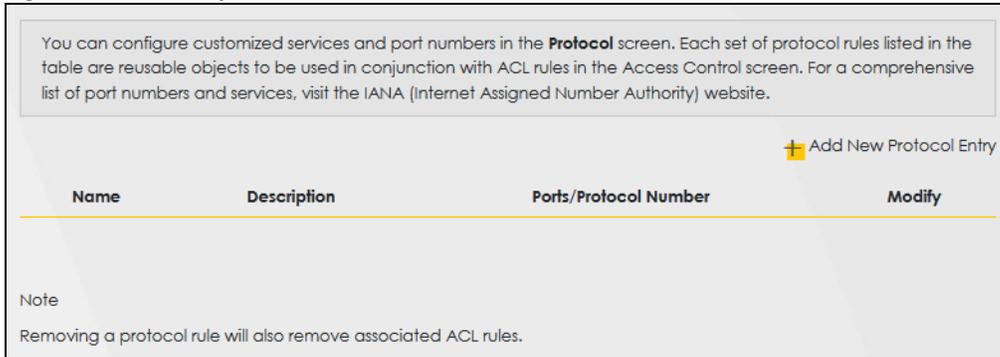
The following table describes the labels in this screen.

Table 79   Security > Firewall > Protocol

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

16.3.1 Add New/Edit Protocol Entry

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

Figure 126   Protocol Entry: Add New/Edit

The following table describes the labels in this screen.

Table 80   Security > Firewall > Protocol: Add/Edit

LABEL	DESCRIPTION
Service Name	Enter a unique name (up to 32 printable English keyboard characters, including spaces) for your customized port.
Description	Enter a description for your customized port.
Protocol	Choose the IP protocol (**TCP**, **UDP**, **ICMP**, **ICMPv6**, or **Other**) that defines your customized port from the drop-down list box. Select **Other** to be able to enter a protocol number.
Protocol Number	This field is displayed if you select **Other** as the protocol. Enter the protocol number of your customized port.
Source Port	This field is displayed if you select either the **TCP** or **UDP** protocol. You may set it to **Any**, **Single**, or **Range** and enter the Port Number or range of Port Numbers for your source port.
Destination Port	This field is displayed if you select either the **TCP** or **UDP** protocol. You may set it to **Any**, **Single**, or **Range** and enter the Port Number or range of Port Numbers for your destination port.
ICMPv6type	This field is displayed if you select the **ICMPv6** protocol. From the drop-down menu, select which type value you would like to use.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

16.4 Access Control

Click **Security > Firewall > Access Control** to display the following screen. An Access Control List (ACL) rule is a manually-defined rule that can accept, reject, or drop incoming or outgoing packets from your network. This screen displays a list of the configured incoming or outgoing filtering rules.

Figure 127   Security > Firewall > Access Control

The following table describes the labels in this screen.

Table 81   Security > Firewall > Access Control

LABEL	DESCRIPTION
Add New ACL Rule	Click this to add a filter rule for incoming or outgoing IP traffic.
#	This is the index number of the entry.
Status	The yellow bulb signifies that the Access Control List rule is active.
Name	This displays the name of the rule.
Src IP	This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to **Any**.
Dst IP	This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to **Any**.

Table 81   Security > Firewall > Access Control (continued)

LABEL	DESCRIPTION
Service	This displays the transport layer protocol that defines the service and the direction of traffic to which this rule applies.
Action	This field displays whether the rule silently discards packets (**DROP**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**REJECT**) or allows the passage of packets (**ACCEPT**).
Modify	Click the **Edit** icon to edit the rule. Click the **Delete** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action. Click the **Move To** icon to change the order of the rule. Enter the number in the # field.

16.4.1 Add/Edit an ACL Rule

Click **Add new ACL rule** or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays. Use this screen to accept, reject, or drop packets based on specified parameters, such as source and destination IP address, IP Type, service, and direction. You can also specify a limit as to how many packets this rule applies to at a certain period of time or specify a schedule for this rule.

Figure 128 Access Control: Add/Edit

The following table describes the labels in this screen.

Table 82 Access Control: Add/Edit

LABEL	DESCRIPTION
Active	Slide this switch to activate the Access Control List rule.
Filter Name	Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes. You must enter the filter name to add an ACL rule. This field is read-only if you are editing the ACL rule.
Order	Select the order of the ACL rule.
Select Source IP Address	Select the source device to which the ACL rule applies. If you select **Specific IP Address**, enter the source IP address in the field below.
Source IP Address	Enter the source IP address.

Table 82   Access Control: Add/Edit (continued)

LABEL	DESCRIPTION
Select Destination Device	Select the destination device to which the ACL rule applies. If you select **Specific IP Address**, enter the destiniation IP address in the field below.
Destination IP Address	Enter the destination IP address.
MAC Address	Enter the MAC address of the destination device.
IP Type	Select whether your IP type is **IPv4** or **IPv6**.
Select Service	Select the transport layer protocol that defines your customized port from the drop-down list box. The specific protocol rule sets you add in the **Security > Firewall > Protocol > Add** screen display in this list. If you want to configure a customized protocol, select **Specific Service**.
Protocol	This field is displayed only when you select **Specific Service** in **Select Service**. Choose the IP port (**TCP/UDP**, **TCP**, **UDP**, **ICMP**, or **ICMPv6**) that defines your customized port from the drop-down list box.
Custom Source Port	This field is displayed only when you select **Specific Service** in **Select Service** and have either **TCP** or **UDP** in the **Protocol** field. Enter a single port number or the range of port numbers of the source.
Custom Destination Port	This field is displayed only when you select **Specific Service** in **Select Service** and have either **TCP** or **UDP** in the **Protocol** field. Enter a single port number or the range of port numbers of the destination.
TCP flag	This field is displayed only when you select **Specific Service** in **Select Service** and have **TCP** in the **Protocol** field. Select one of the following TCP flags: **SYN** (Synchronize), **ACK** (Acknowledge), **URG** (Urgent), **PSH** (Push), **RST** (Reset), or **FIN** (Finished).
Type	This field is displayed only when you select **Specific Service** in **Select Service** and **ICMPv6** in the protocol field. From the drop-down list box, select which ICMPv6 type you would like to use.
Policy	Use the drop-down list box to select whether to discard (**DROP**), deny and send an ICMP destination-unreachable message to the sender of (**REJECT**) or allow the passage of (**ACCEPT**) packets that match this rule.
Direction	Use the drop-down list box to select the direction of traffic to which this rule applies.
Enable Rate Limit	Slide this switch to set a limit on the upstream/downstream transmission rate for the specified protocol. Specify how many packets per minute or second the transmission rate is.
Scheduler Rules	Select a schedule rule for this ACL rule form the drop-down list box. You can configure a new schedule rule by click **Add New Rule**. This will bring you to the **Security > Scheduler Rules** screen.
Cancel	Click **Cancel** to restore the default or previously saved settings.
OK	Click **OK** to save your changes.

16.5 DoS Settings

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

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

Figure 129 Security > Firewall > DoS

The following table describes the labels in this screen.

Table 83 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Select **Enable** to enable protection against DoS attacks.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

MAC Filter

17.1 MAC Filter Overview

You can configure the Zyxel Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of 6 pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the LAN client to configure this screen.

17.2 MAC Filter Settings

Enable **MAC Address Filter** and add the host name and MAC address of a LAN client to the table if you wish to allow or deny them access to your network. Click **Security** > **MAC Filter**. The screen appears as shown.

Figure 130   Security > MAC Filter

You can choose to enable or disable the filters per entry; make sure that the check box under **Active** is selected if you want to use a filter, as shown in the example below.

Figure 131 Enabling individual MAC Filters

The following table describes the labels in this screen.

Table 84   Security > MAC Filter

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

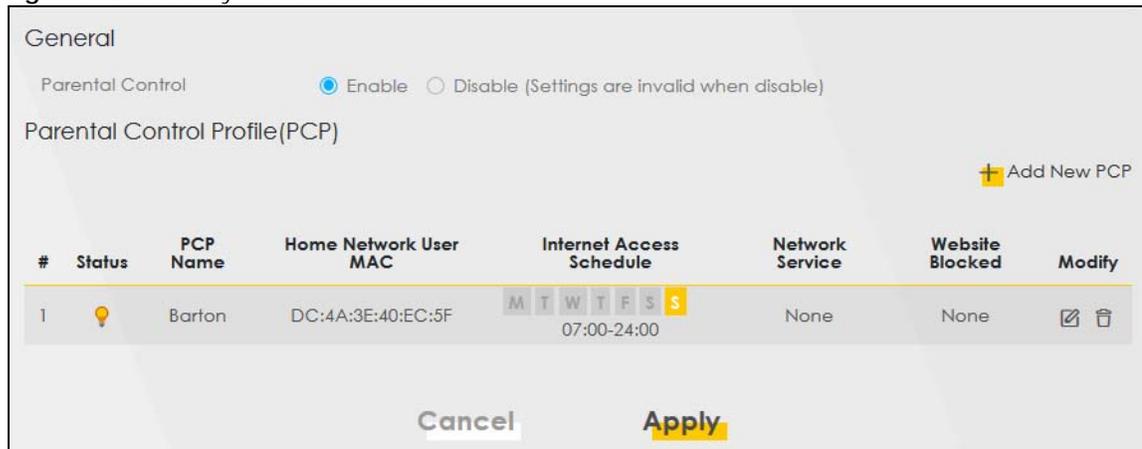# Parental Control

18.1 Parental Control Overview

Parental control allows you to limit the time a user can access the Internet and prevent users from viewing inappropriate content or participating in specified online activities.

18.2 Parental Control Settings

Use this screen to enable parental control and view parental control rules and schedules. You can limit the time a user can access the Internet and prevent users from viewing inappropriate content or participating in specified online activities. These rules are defined in a Parental Control Profile (PCP).

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

Figure 132 Security > Parental Control

The following table describes the fields in this screen.

Table 85   Security > Parental Control

LABEL	DESCRIPTION
General	
Parental Control	Select **Enable** to activate parental control on the Zyxel Device.
Parental Control Profile (PCP)	
Add new PCP	Click this if you want to configure a new Parental Control Profile (PCP).
#	This shows the index number of the rule.
Status	This indicates whether the rule is active or not.
	A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.

Table 85   Security > Parental Control (continued)

LABEL	DESCRIPTION
PCP Name	This shows the name of the rule.
Home Network User MAC	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the day(s) and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, **None** will be shown.
Website Block	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.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

18.2.1 Add/Edit a Parental Control Profile

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

Figure 133 Security > Parental Control > Add/Edit PCP (General, Rule List & Internet Access Schedule)
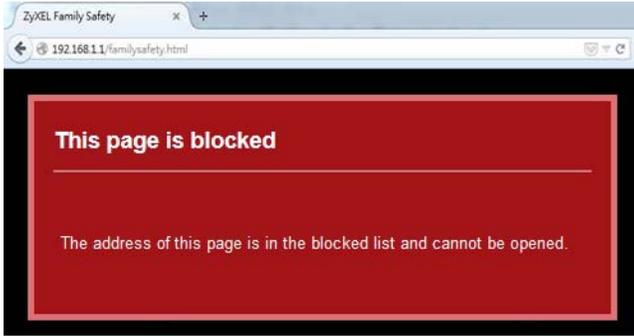
Figure 134 Security > Parental Control > Add/Edit PCP (Network Service & Site/URL Keyword)

The following table describes the fields in this screen.

Table 86 Security > Parental Control >Add/Edit PCP

LABEL	DESCRIPTION
General	
Active	Select **Enable** or **Disable** to activate or deactivate the parental control rule.
Parental Control Profile Name	Enter a descriptive name for the rule.
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select **Custom**, enter the LAN user's MAC address. If you select **All**, the rule applies to all LAN users.
Rule List	In **Home Network User**, select **Custom**, enter the LAN user's MAC address, then click the **Add** icon to enter a computer MAC address for this PCP. Up to five are allowed. Click the **Delete** icon to remove one.
Internet Access Schedule	
Day	Select check boxes for the days that you want the Zyxel Device to perform parental control.
Time	Drag the time bar to define the time that the LAN user is allowed access (**Authorized access**) or denied access (**No access**).
Add New Service	Click this to add a new time bar. Up to 3 are allowed.
Network Service	
Network Service Setting	If you select **Block**, the Zyxel Device prohibits the users from viewing the web sites with the URLs listed below.
	If you select **Allow**, the Zyxel Device blocks access to all URLs except ones listed below.
Add New Service	Click this to show a screen in which you can add a new service rule. You can configure the **Service Name**, **Protocol**, and **Port** of the new rule, as shown in Figure 136.
#	This shows the index number of the rule.

Table 86   Security > Parental Control >Add/Edit PCP (continued)

LABEL	DESCRIPTION
Service Name	This shows the name of the rule.
Protocol:Port	This shows the protocol and the port of the rule.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Site/URL Keyword	
Block or Allow the Web Site	If you select **Block the Web URLs**, the Zyxel Device prohibits the users from viewing the Web sites with the URLs listed below. If you select **Allow the Web URLs**, the Zyxel Device blocks access to all URLs except ones listed below.
Add	Click **Add** to show a screen to enter the URL of web site or URL keyword to which the Zyxel Device blocks or allows access.
#	This shows the index number of the rule.
Website	This shows the URL of web site or URL keyword to which the Zyxel Device blocks or allows access.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Redirect blocked site to Zyxel Family Safety page	Select this to redirect users who access any blocked websites listed above to the Zyxel Family Safety page as shown next. **Figure 135** Zyxel Family Safety Page Example
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

Add New Service

Use this screen to add a new service rule.

Figure 136 Security > Parental Control > Add/Edit PCP > Add New Service

The following table describes the fields in this screen.

Table 87 Security > Parental Control > Add/Edit PCP > Add New Service

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

Add Site/URL Keyword

Click **Add** in the **Site/URL Keyword** section of the **Edit/Add new PCP** screen to open the following screen.

Note: Do not include "HTTP" or "HTTPS" in the keyword. HTTPS connections cannot be blocked by Parental Control.

Figure 137 Security > Parental Control > Add/Edit PCP > Add Keyword

The following table describes the fields in this screen.

Table 88   Security > Parental Control > Add/Edit PCP > Add Keyword

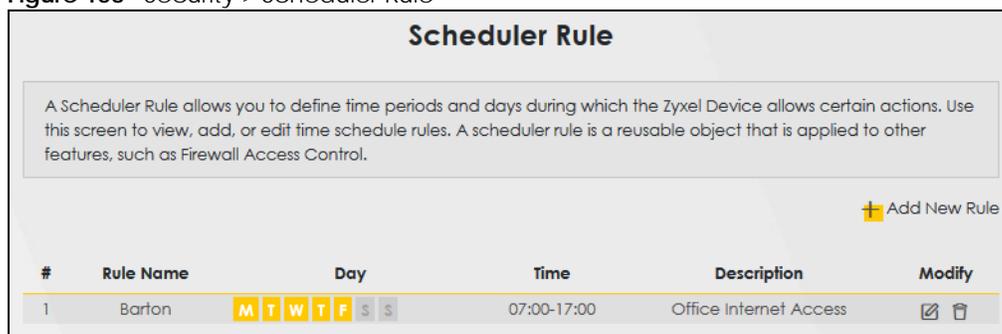| LABEL	DESCRIPTION
Site/URL Keyword	Enter a keyword and click **OK** to have the Zyxel Device block access to the website URLs that contain the keyword.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

Scheduler Rule

19.1 Scheduler Rule Overview

A Scheduler Rule allows you to define time periods and days during which the Zyxel Device allows certain actions.

19.2 Scheduler Rule Settings

Use this screen to view, add, or edit time schedule rules. A scheduler rule is a reusable object that is applied to other features, such as Firewall Access Control.

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

Figure 138 Security > Scheduler Rule

The following table describes the fields in this screen.

Table 89   Security > Scheduler Rule

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

19.2.1 Add/Edit a Schedule Rule

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

Figure 139 Scheduler Rule: Add/Edit

The following table describes the fields in this screen.

Table 90 Scheduler Rule: Add/Edit

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

CHAPTER 20
Certificates

20.1 Certificates Overview

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

20.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the Zyxel Device's CA-signed certificates (Section 20.4 on page 223).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the Zyxel Device (Section 20.4 on page 223).

20.2 What You Need to Know

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

Certification Authority

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

20.3 Local Certificates

Click **Security** > **Certificates** to open the **Local Certificates** screen. Use this screen to view the Zyxel Device's summary list of certificates, generate certification requests, and import the signed certificates.

Figure 140 Security > Certificates > Local Certificates

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

Use this screen to view the Zyxel Device's summary list of certificates, generate certification requests, and import the signed certificates.

Replace PrivateKey/Certificate file in PEM format

☑ Private Key is protected by password

Browse... No file selected.

	Import Certificate		Create Certificate Request

| Current File | Subject | Issuer | Valid From | Valid To | Modify |

The following table describes the labels in this screen.

Table 91   Security > Certificates > Local Certificates

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

20.3.1 Create Certificate Request

Click **Security** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the Zyxel Device generate a certification request. To create a certificate signing request, you need to enter a common name, organization name, state/province name, and the two-letter country code for the certificate.

Figure 141 Create Certificate Request

The following table describes the labels in this screen.

Table 92 Create Certificate Request

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

20.3.2 View Certificate Request

Click the **View** icon in the **Local Certificates** screen to open the following screen. Use this screen to view in-depth information about the certificate request. The **Certificate** is used to verify the authenticity of the certification authority. The **Private Key** serves as your digital signature for authentication and must be safely stored.

Figure 142 Certificate Request: View

The following table describes the fields in this screen.

Table 93 Certificate Request: View

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

Table 93   Certificate Request: View (continued)

LABEL	DESCRIPTION
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution.
Private Key	This field displays the private key of this certificate.
Signing Request	This field displays the CSR (Certificate Signing Request) information of this certificate. The CSR will be provided to a certificate authority, and it includes information about the public key, organization name, domain name, location, and country of this certificate.
Back	Click **Back** to return to the previous screen.

20.4 Trusted CA

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

Note: You can have a maximum of 10 trusted certificates.

Figure 143   Security > Certificates > Trusted CA

The following table describes the fields in this screen.

Table 94   Security > Certificates > Trusted CA

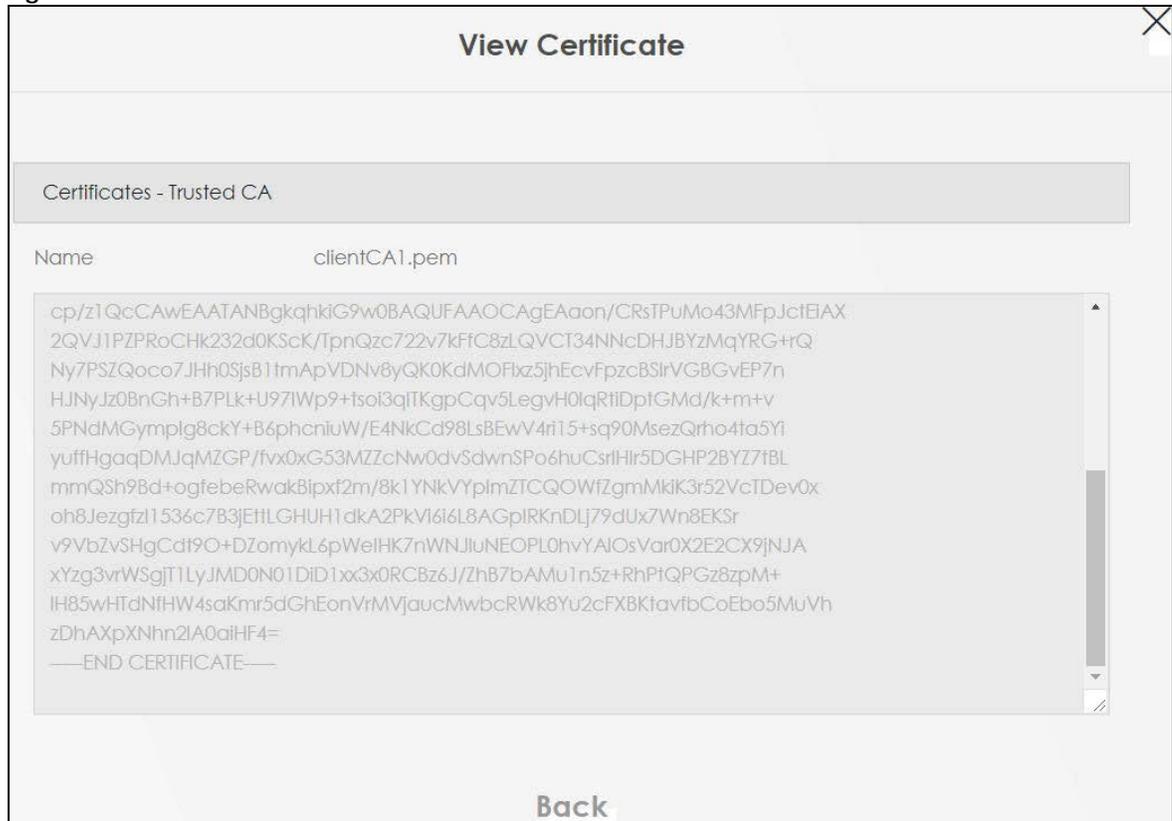| LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the Zyxel Device.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.

Table 94   Security > Certificates > Trusted CA (continued)

LABEL	DESCRIPTION
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request).
	Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

20.4.1 View Trusted CA Certificate

Click the **View** icon in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate. The certificate text box is read-only and can be distributed to others.

Figure 144   Trusted CA: View

The following table describes the fields in this screen.

Table 95   Trusted CA: View

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

20.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The Zyxel Device trusts any valid certificate signed by any of the imported trusted CA certificates. Certificates should be in one of the following formats: Binary X.509, PEM (base-64) encoded, Binary PKCS#7, or PEM (base-64) encoded PKCS#7.

Figure 145   Trusted CA: Import Certificate

The following table describes the fields in this screen.

Table 96   Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate File Path	Click **Browse** or **Choose File** and select the certificate you want to upload.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

CHAPTER 21
Log

21.1 Log Overview

These screens allow you to determine the categories of events that the Zyxel Device logs and then display these logs or have the Zyxel Device send them to an administrator (through e-mail) or to a syslog server.

21.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs (Section 21.2 on page 227).
- Use the **Security Log** screen to see the security-related logs for the categories that you select (Section 21.3 on page 228).

21.1.2 What You Need To Know

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

Alerts and Logs

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

Syslog Overview

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

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

Table 97   Syslog Severity Levels

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

Table 97   Syslog Severity Levels (continued)

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

21.2 System Log

Use the **System Log** screen to see the system logs. You can filter the entries by selecting a severity level and/or category. Click **System Monitor > Log** > **System Log** to open the **System Log** screen.

Figure 146   System Monitor > Log > System Log

The following table describes the fields in this screen.

Table 98   System Monitor > Log > System Log

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

21.3 Security Log

Use the **Security Log** screen to see the security-related logs for the categories that you select. You can filter the entries by selecting a severity level and/or category. Click **System Monitor > Log > Security Log** to open the following screen.

Figure 147 System Monitor > Log > Security Log

The following table describes the fields in this screen.

Table 99 System Monitor > Log > Security Log

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

Traffic Status

22.1 Traffic Status Overview

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

22.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 22.2 on page 229).
- Use the **LAN** screen to view the LAN traffic statistics (Section 22.3 on page 230).
- Use the **NAT** screen to view the NAT status of the Zyxel Device's client(s) (Section 22.4 on page 231).

22.2 WAN Status

Click **System Monitor** > **Traffic Status** to open the **WAN** screen. The figures in this screen show the total number of bytes received and sent through the Zyxel Device's WAN interface. Packet statistics for each WAN interface are listed in the tables below.

Figure 148 System Monitor > Traffic Status > WAN
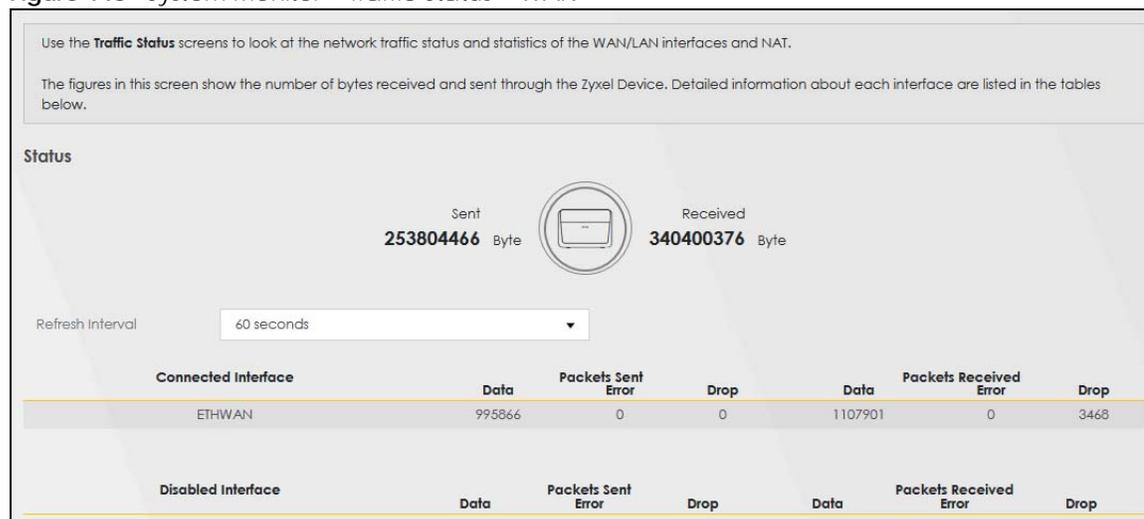
The following table describes the fields in this screen.

Table 100   System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.
Disabled Interface	This shows the name of the WAN interface that is currently disabled.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

22.3 LAN Status

Click **System Monitor > Traffic Status > LAN** to open the following screen. This screen allows you to view packet statistics for each LAN or WLAN interface on the Zyxel Device.

Figure 149   System Monitor > Traffic Status > LAN

The following table describes the fields in this screen.

Table 101   System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Interface	This shows the LAN or wireless LAN interface on the Zyxel Device.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN or wireless LAN interfaces on the Zyxel Device.
Sent (Packets)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packets)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

22.4 NAT Status

Click **System Monitor > Traffic Status > NAT** to open the following screen. This screen lists the devices that have received an IP address from the Zyxel Device's LAN or WLAN interfaces and have ever established a session with the Zyxel Device.

Figure 150   System Monitor > Traffic Status > NAT

The following table describes the fields in this screen.

Table 102   System Monitor > Traffic Status > NAT

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

CHAPTER 23
ARP Table

23.1 ARP Table Overview

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

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

23.1.1 How ARP Works

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

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

23.2 ARP Table Settings

Use the ARP table to view the IPv4-to-MAC address mapping(s) for each device connected to the Zyxel Device. The neighbor table shows the IPv6-to-MAC address mapping(s) of each neighbor. To open this screen, click **System Monitor** > **ARP Table**.

Figure 151   System Monitor > ARP Table

The following table describes the labels in this screen.

Table 103   System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the index number of the ARP or neighbor table entry.
IPv4/IPv6 Address	This is the learned IPv4 or IPv6 IP address of a device connected to a port on the Zyxel Device.
MAC Address	This is the MAC address of the device with the listed IP address.
Device	This is the name of the Zyxel Device's interface to which the device is connected.

CHAPTER 24
Routing Table

24.1 Routing Table Overview

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

24.2 Routing Table Settings

The table below shows IPv4 and IPv6 routing information. The IPv4 subnet mask is '255.255.255.255' for a host destination and '0.0.0.0' for the default route. The gateway address is written as '*' (IPv4)/'::' (IPv6) if none is set.

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

Figure 152 System Monitor > Routing Table

Routing Table

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

The table below shows IPv4 and IPv6 routing information. The IPv4 subnet mask is '255.255.255.255' for a host destination and '0.0.0.0' for the default route. The gateway address is written as '*'(IPv4)/'::'(IPv6) if none is set.

Destination: This indicates the destination IPv4 address or IPv6 address and prefix of this route.
Gateway: This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask: This indicates the destination subnet mask of the IPv4 route.
Flag: This indicates the route status.
U-Up: The route is up.
!-Reject: The route is blocked and will force a route lookup to fail.
G-Gateway: The route uses a gateway to forward traffic.
H-Host: The target of the route is a host.
R-Reinstate: The route is reinstated for dynamic routing.
D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect.
M-Modified (redirect): The route is modified from a routing daemon or redirect.
Metric: The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".
Interface: This indicates the name of the interface through which the route is forwarded.

IPv4 Routing Table

Destination	Gateway	Subnet Mask	Flag	Metric	Interface
0.0.0.0	172.21.43.254	0.0.0.0	UG	0	eth4.2
172.21.40.0	0.0.0.0	255.255.252.0	U	0	eth4.2
192.168.1.0	0.0.0.0	255.255.255.0	U	0	br0

IPv6 Routing Table

Destination	Gateway	Flag	Metric	Interface
fe80::/64	::	U	256	eth1.0
fe80::/64	::	U	256	br0
::1/128	::	U	0	lo
fe80::/128	::	U	0	lo
fe80::/128	::	U	0	lo
fe80::10:18ff:fe01:1/128	::	U	0	lo
fe80::10:18ff:fe01:1/128	::	U	0	lo
ff00::/8	::	U	256	eth1.0
ff00::/8	::	U	256	br0

The following table describes the labels in this screen.

Table 104   System Monitor > Routing Table

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

Table 104   System Monitor > Routing Table (continued)

LABEL	DESCRIPTION
Flag	This indicates the route status. **U-Up:** The route is up. **!-Reject:** The route is blocked and will force a route lookup to fail. **G-Gateway:** The route uses a gateway to forward traffic. **H-Host:** The target of the route is a host. **R-Reinstate:** The route is reinstated for dynamic routing. **D-Dynamic (redirect):** The route is dynamically installed by a routing daemon or redirect. **M-Modified (redirect):** The route is modified from a routing daemon or redirect.
Metric	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".
Interface	This indicates the name of the interface through which the route is forwarded. **brx** indicates a LAN interface where x can be 0~3 to represent LAN1 to LAN4 respectively. **ethx** indicates an Ethernet WAN interface using IPoE or in bridge mode. **ppp0** indicates a WAN interface using PPPoE. **wlx** indicates a wireless interface where x can be 0~1. For some models, **wl1** indicates 5 GHz wireless interface, and **wl0** indicates 2.4 GHz wireless interface. For the other models, **wl1** indicates 5 GHz wireless interface, and **wl0** indicates 2.4 GHz wireless interface.

CHAPTER 25
Multicast Status

25.1 Multicast Status Overview

Use the **Multicast Status** screens to view IPv4 or IPv6 multicast group information.

25.2 IGMP Status

Use this screen to look at the current list of IPv4 multicast groups the Zyxel Device manages through 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. You can configure IGMP settings in **Network Setting > IGMP/MLD**.

Figure 153   System Monitor > Multicast Status > IGMP Status

Use this screen to look at the current list of IPv4 multicast groups the Zyxel Device manages through IGMP. You can configure IGMP settings in Network Setting > IGMP/MLD

Refresh

| Interface | Multicast Group | Filter Mode | Source List | Member |
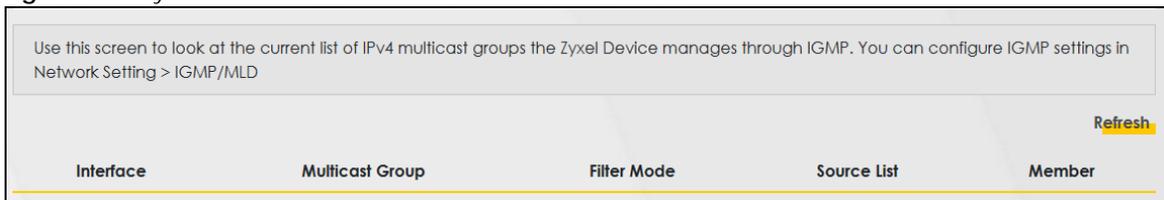
The following table describes the labels in this screen.

Table 105   System Monitor > Multicast Status > IGMP Status

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

25.3 MLD Status

Use this screen to look at the current list of IPv6 multicast groups the Zyxel Device manages through MLD. Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3. You can configure MLD settings in **Network Setting > IGMP/MLD**. To open this screen, click **System Monitor > Multicast Status > MLD Status**.

Figure 154 System Monitor > Multicast Status > MLD Status

Use this screen to look at the current list of IPv6 multicast groups the Zyxel Device manages through MLD. You can configure MLD settings in Network Setting > IGMP/MLD

Refresh

| Interface | Multicast Group | Filter Mode | Source List | Member |
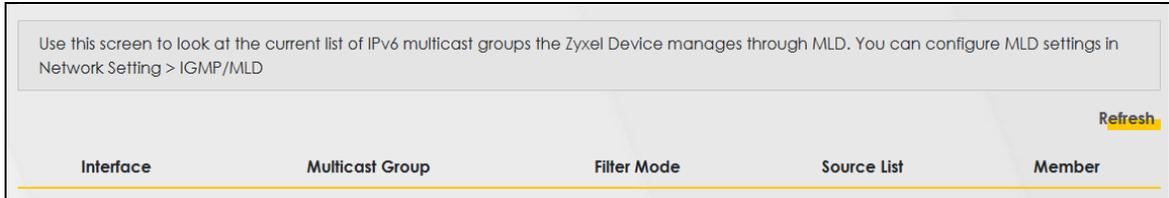
The following table describes the labels in this screen.

Table 106   System Monitor > Multicast Status > MLD Status

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

CHAPTER 26
WLAN Station Status

26.1 WLAN Station Status Overview

Click **System Monitor** > **WLAN Station Status** to open the following screen. Use this screen to view information and status of the wireless stations (wireless clients) that are currently associated with the Zyxel Device. Being associated means that a wireless client (for example, your computer with a wireless network card installed) has connected successfully to an AP (or wireless router) using the same SSID, channel, and WiFi security settings.

Figure 155 System Monitor > WLAN Station Status

The following table describes the labels in this screen.

Table 107   System Monitor > WLAN Station Status

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Rate (Mbps)	This field displays the transmission rate of WiFi traffic between an associated wireless station and the Zyxel Device.
RSSI (dBm)	The RSSI (Received Signal Strength Indicator) field shows the WiFi signal strength of the station's wireless connection. The normal range is –30dBm to –79dBm. If the value drops below -80dBm, try moving the associated wireless station closer to the Zyxel Device to get better signal strength.

Table 107   System Monitor > WLAN Station Status (continued)

LABEL	DESCRIPTION
SNR	The Signal-to-Noise Ratio (SNR) is the ratio between the received signal power and the received noise power. The normal range is 15 to 40. If the value drops below 15, try moving the associated wireless station closer to the Zyxel Device to get better quality WiFi.
Level	This field displays a number which represents the strength of the WiFi signal between an associated wireless station and the Zyxel Device. The Zyxel Device uses the RSSI and SNR values to determine the strength of the WiFi signal. **5** means the Zyxel Device is receiving an excellent WiFi signal. **4** means the Zyxel Device is receiving a very good WiFi signal. **3** means the Zyxel Device is receiving a weak WiFi signal. **2** means the Zyxel Device is receiving a very weak WiFi signal. **1** means the Zyxel Device is not receiving a WiFi signal.

CHAPTER 27
System

27.1 System Overview

In the **System** screen, you can name your Zyxel Device (Host) and give it an associated domain name. Domain is the name given to a network. It will be required to reach a network from an external point (like the Internet). Knowing the domain name will allow you to reach a particular network, and knowing the host name will allow you to reach a particular device. For this reason, accessing a device from another device within a network may work with just the host name (without the use of the domain name).

27.2 System Settings

Click **Maintenance > System** to open the following screen. Assign a unique name to the Zyxel Device so it can be easily recognized on your network. You can use up to 30 characters, including spaces.

Figure 156   Maintenance > System

The following table describes the labels in this screen.

Table 108   Maintenance > System

LABEL	DESCRIPTION
Host Name	Type a host name for your Zyxel Device. Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes.
Domain Name	Type a Domain name for your Zyxel Device.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 28
User Account

28.1 User Account Overview

In the **User Account** screen, you can view the settings of the 'admin' and other user accounts that you use to log into the Zyxel Device to manage it.

28.2 User Account Settings

Click **Maintenance > User Account** to open the following screen. Use this screen to create or manage user accounts and their privileges on the Zyxel Device.

Figure 157   Maintenance > User Account

The following table describes the labels in this screen.

Table 109   Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account.
#	This is the index number of the user account.
Active	This field indicates whether the user account is active or not. Clear the check box to disable the user account. Select the check box to enable it.
User Name	This field displays the name of the account used to log into the Zyxel Device Web Configurator.

Table 109   Maintenance > User Account (continued)

LABEL	DESCRIPTION
Retry Times	This field displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	This field displays the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	This field displays the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	This field displays whether this user has **Administrator** or **User** privileges.
Modify	Click the **Edit** icon to configure the entry. Click the **Delete** icon to remove the entry.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

28.2.1 User Account Add/Edit

Click **Add New Account** or the **Edit** icon of an existing account in the **Maintenance > User Account** to open the following screen.

Figure 158   Maintenance > User Account > Add/Edit

The following table describes the labels in this screen.

Table 110   Maintenance > User Account > Add/Edit

LABEL	DESCRIPTION
Active	Select **Enable** or **Disable** to activate or deactivate the user account.
User Name	Enter a new name for the account. The **User Name** must contain 1 to 15 characters, including 0 to 9, a to z, and !@#%*()-_+=~,.{}[]\. Spaces are not allowed.

Table 110   Maintenance > User Account > Add/Edit (continued)

LABEL	DESCRIPTION
Password	Type your new system password. The **Password** must contain 6 to 64 characters, including 0 to 9 and a to z. Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Zyxel Device.
Verify New Password	Type the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	Enter the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number if consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	Specify whether this user will have **Administrator** or **User** privileges. **Administrator** and **User** privileges are mostly the same, but the following menu items will only display when you log in as an **Administrator**. • Quick Start **Wizard** • **Network Setting** • **Security** settings • **Maintenance** > **System** • **Maintenance** > **SNMP**
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

CHAPTER 29
Remote Management

29.1 Remote Management Overview

Use remote management to control what services you can use through which interface(s) in order to manage the Zyxel Device.

29.1.1 What You Can Do in this Chapter

- Use the **MGMT Services** screen to allow various approaches to access the Zyxel Device remotely from a WAN and/or LAN connection (Section 29.2 on page 245).
- Use the **Trust Domain** screen to enable users to permit access from local management services by entering specific IP addresses (Section 29.3 on page 247).

Note: The Zyxel Device is managed using the Web Configurator.

29.2 MGMT Services

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

Figure 159 Maintenance > Remote Management > MGMT Services

The following table describes the fields in this screen.

Table 111   Maintenance > Remote Management > MGMT Services

LABEL	DESCRIPTION
WAN Interface used for services	Select **Any_WAN** to have the Zyxel Device automatically activate the remote management service when any WAN connection is up.
	Select **Multi_WAN** and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up.
Service	This is the service you may use to access the Zyxel Device.
	• **HTTP** provides a non secured way.
	• **HTTPS** is the secured version of HTTP, it makes sure that your data cannot be read during transmission.
	• **FTP** is the most common way of communication between 2 devices.
	• **TELNET** provides a way to control your Zyxel Device remotely.
	• **SSH** prevents leakage of data during remote management. Additionally, it can encrypt all transmitted data.
	• **SNMP** is a management system that monitors devices connected to the Internet.
	• **PING** is a diagnostic tool that can check if your Zyxel Device is connected to the Internet.
LAN/WLAN	Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from the LAN/WLAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from the trusted hosts configured in the **Maintenance > Remote MGMT > Trust Domain** screen.
	If you only want certain WAN connections to have access to the Zyxel Device using the corresponding services, then clear **WAN**, select **Trust Domain** and configure the allowed IP address(es) in the **Trust Domain** screen.

Table 111   Maintenance > Remote Management > MGMT Services (continued)

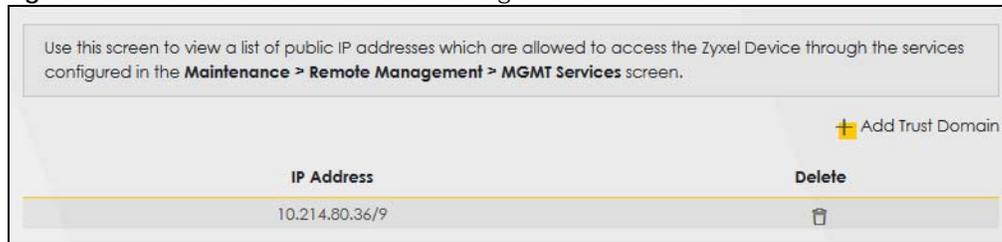| LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

29.3 Trust Domain

Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance > Remote Management > MGMT Services** screen.

Click **Maintenance > Remote Management > Trust Domain** to open the following screen.

Note: If specific services from the trusted hosts are allowed access but the trust domain list is empty, all public IP addresses can access the Zyxel Device from the WAN using the specified services.

Figure 160   Maintenance > Remote Management > Trust Domain

Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance > Remote Management > MGMT Services** screen.

           ➕ Add Trust Domain

IP Address	Delete
10.214.80.36/9	🗑

The following table describes the fields in this screen.

Table 112   Maintenance > Remote Management > Trust Domain

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

29.3.1 Add Trust Domain

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

Figure 161   Maintenance > Remote Management > Trust Domain > Add Trust Domain

The following table describes the fields in this screen.

Table 113   Maintenance > Remote Management > Trust Domain > Add Trust Domain

LABEL	DESCRIPTION
IP Address	Enter a public IP address which is allowed to access the service on the Zyxel Device from the WAN. You can enter an IPv4 or IPv6 address and subnet mask or prefix length.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes back to the Zyxel Device.

CHAPTER 30
SNMP

30.1 SNMP Overview

This screen allows you to configure the SNMP settings on the Zyxel Device.

The Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Zyxel Device supports SNMP agent functionality, which allows a manager station to manage and monitor the Zyxel Device through the network. The next figure illustrates an SNMP management operation.

Figure 162 SNMP Management Model
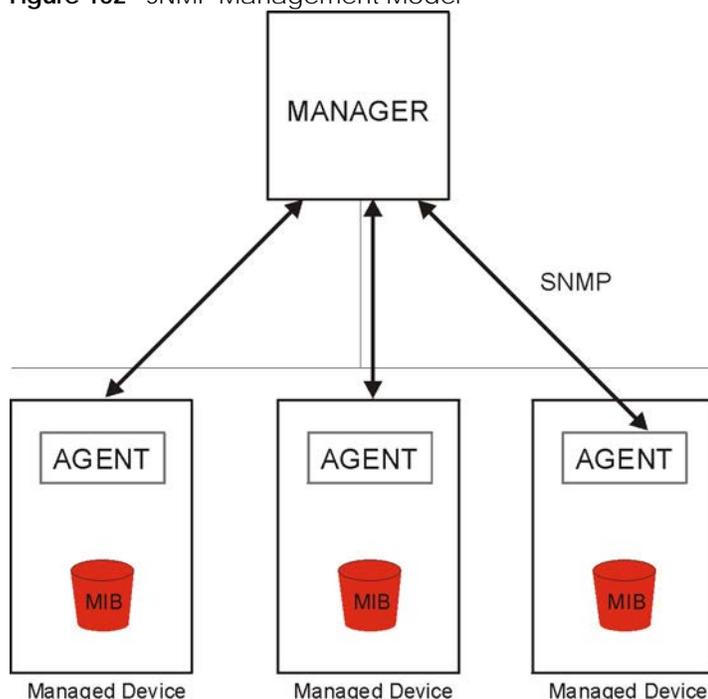
An SNMP managed network consists of two main types of components: agents and a manager.

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

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

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

• Get - Allows the manager to retrieve an object variable from the agent.

• GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.

• Set - Allows the manager to set values for object variables within an agent.

Trap - Used by the agent to inform the manager of some events.

30.2 SNMP Settings

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

Configure how the Zyxel Device reports to the Network Management System (NMS) via SNMP using the screen below.

Figure 163   Maintenance > SNMP

The following table describes the fields in this screen.

Table 114   Maintenance > SNMP

LABEL	DESCRIPTION
SNMP Agent	Enable this switch to let the Zyxel Device act as an SNMP agent, which allows a manager station to manage and monitor the Zyxel Device through the network, Click this switch to enable/disable it. When the switch goes to the right ⬤, the function is enabled.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station.
Set Community	Enter the **Set Community**, which is the password for the incoming Set requests from the management station.
Trap Community	Enter the **Trap Community**, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
System Name	Enter the SNMP system name.
System Location	Enter the SNMP system location.
System Contact	Enter the SNMP system contact.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

31.1 Time Settings Overview

This chapter shows you how to configure the Zyxel Device's system date and time.

31.2 Time

For effective scheduling and logging, the Zyxel Device's system time must be accurate. Use this screen to configure the Zyxel Device's time based on your local time zone. You can enter a time server address, select the time zone where the Zyxel Device is physically located, and configure Daylight Savings settings if needed.

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

Figure 164   Maintenance > Time

Time

Use this screen to configure the Zyxel Device's time based on your local time zone. You can enter a time server address, select the time zone where the Zyxel Device is physically located, and configure Daylight Savings settings if needed.

Current Date/Time

Current Time	02:34:45
Current Date	1970-01-01

Time and Date Setup

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

Time Zone

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

Daylight Savings

Active

Start Rule

Day	1	in
	Last Sunday	in
Month	March	
Hour	2	0

End Rule

Day	1	in
	Last Sunday	in
Month	October	
Hour	3	0

Cancel   Apply

The following table describes the fields in this screen.

Table 115   Maintenance > Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your Zyxel Device.
	Each time you reload this page, the Zyxel Device synchronizes the time with the time server.
Current Date	This field displays the date of your Zyxel Device.
	Each time you reload this page, the Zyxel Device synchronizes the date with the time server.
Time and Date Setup	
Time Protocol	This displays SNTP (RFC-1769) as the time protocol used.
First ~ Fifth Time Server Address	Select an NTP time server from the drop-down list box.
	Otherwise, select **Other** and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server.
	Select **None** if you do not want to configure the time server.
	Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Active	Click this switch to enable or disable Daylight Saving Time. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Start Rule	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Hour** field uses the 24 hour format. Here are a couple of examples:
	Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to **Second**, **Sunday**, the month to **March** and the time to **2** in the **Hour** field.
	Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday** and the month to **March**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Rule	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Hour** field uses the 24 hour format. Here are a couple of examples:
	Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would set the day to **First**, **Sunday**, the month to **November** and the time to **2** in the **Hour** field.
	Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday**, and the month to **October**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 115   Maintenance > Time (continued)

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

E-mail Notification

32.1 E-mail Notification Overview

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

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

32.2 E-mail Notification Settings

Click **Maintenance** > **E-mail Notification** to open the **E-mail Notification** screen. Use this screen to view, remove and add e-mail account information on the Zyxel Device. This account can be set to receive e-mail notifications for logs.

Note: The default port number of the mail server is 25.

Figure 165 Maintenance > E-mail Notification
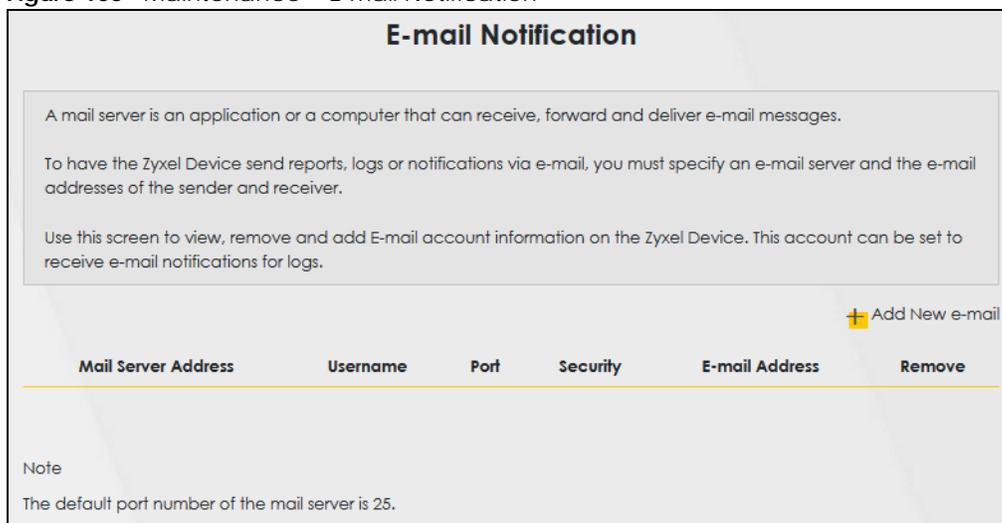
The following table describes the labels in this screen.

Table 116   Maintenance > E-mail Notification

LABEL	DESCRIPTION
Add New e-mail	Click this button to create a new entry.
Mail Server Address	This field displays the server name or the IP address of the mail server.
Username	This field displays the user name of the sender's mail account.

Table 116   Maintenance > E-mail Notification (continued)

LABEL	DESCRIPTION
Port	This field displays the port number of the mail server.
Security	This field displays the protocol used for encryption.
E-mail Address	This field displays the e-mail address that you want to be in the from/sender line of the e-mail that the Zyxel Device sends.
Remove	Click this to delete the entry.

32.2.1 E-mail Notification Edit

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

Figure 166   E-mail Notification > Add

The following table describes the labels in this screen.

Table 117   E-mail Notification > Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the **Account e-mail Address** field.
	If this field is left blank, reports, logs or notifications will not be sent via e-mail.
Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication User name	Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the **Account e-mail Address** field.
Authentication Password	Enter the password associated with the user name above.
Account e-mail Address	Enter the e-mail address that you want to be in the from/sender line of the e-mail notification that the Zyxel Device sends.
	If you activate SSL/TLS authentication, the e-mail address must be able to be authenticated by the mail server as well.

Table 117   E-mail Notification > Add (continued)

LABEL	DESCRIPTION
Connection Security	Select **SSL** to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the Zyxel Device. Select **STARTTLS** to upgrade a plain text connection to a secure connection using SSL/TLS.
Cancel	Click this button to exit this screen without saving any changes.
OK	Click this button to save your changes and return to the previous screen.

CHAPTER 33
Log Setting

33.1 Logs Setting Overview

You can configure where the Zyxel Device sends logs and which type of logs the Zyxel Device records in the **Logs Setting** screen.

33.2 Log Settings

To change your Zyxel Device's log settings, click **Maintenance** > **Log Setting**. The screen appears as shown.

If you have a LAN client on your network or a remote server that is running a syslog utility, you can also save its log files by enabling **Syslog Logging**, selecting **Remote** or **Local File and Remote** in the **Mode** field, and entering the IP address of the LAN client in the **Syslog Server** field. **Remote** allows you to store logs on a syslog server, while **Local File** allows you to store them on the Zyxel Device. **Local File and Remote** means your logs are stored both on the Zyxel Device and on a syslog server.

Figure 167   Maintenance > Log Setting

The following table describes the fields in this screen.

Table 118   Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Setting	
Syslog Logging	The Zyxel Device sends a log to an external syslog server. Click this switch to enable or disable syslog logging. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Mode	Select the syslog destination from the drop-down list box.
	If you select **Remote**, the log(s) will be sent to a remote syslog server. If you select **Local File**, the log(s) will be saved in a local file. If you want to send the log(s) to a remote syslog server and save it in a local file, select **Local File and Remote**.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.

Table 118   Maintenance > Log Setting (continued)

LABEL	DESCRIPTION
E-mail Log Settings	
E-mail Log Settings	Click this switch to have the Zyxel Device send logs and alarm messages to the configured e-mail addresses. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Mail Account	Select a mail account from which you want to send logs. You can configure mail accounts in the **Maintenance > E-mail Notification** screen.
System Log Mail Subject	Type a title that you want to be in the subject line of the system log e-mail message that the Zyxel Device sends.
Security Log Mail Subject	Type a title that you want to be in the subject line of the security log e-mail message that the Zyxel Device sends.
Send Log to	The Zyxel Device sends logs to the e-mail address specified in this field. If this field is left blank, the Zyxel Device does not send logs via e-mail.
Send Alarm to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the e-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via e-mail.
Alarm Interval	Specify how often the alarm should be updated.
Active Log	
System Log	Select the categories of system logs that you want to record.
Security Log	Select the categories of security logs that you want to record.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

33.2.1 Example E-mail Log

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

• You may edit the subject title.

• The date format here is Day-Month-Year.

• The date format here is Month-Day-Year. The time format is Hour-Minute-Second.

• 'End of Log' message shows that a complete log has been sent.

Figure 168   E-mail Log Example

```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2019 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
   1|Apr  7 00 |From:192.168.1.1    To:192.168.1.255  |default policy  |forward
    | 09:54:03 |UDP     src port:00520 dest port:00520 |<1,00>          |
   2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255  |default policy  |forward
    | 09:54:17 |UDP     src port:00520 dest port:00520 |<1,00>          |
   3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10     |match           |forward
    | 09:54:19 |UDP     src port:03516 dest port:00053 |<1,01>          |
……………………………..{snip}……………………………………..
……………………………..{snip}……………………………………..
126|Apr  7 00 |From:192.168.1.1    To:192.168.1.255  |match           |forward
    | 10:05:00 |UDP     src port:00520 dest port:00520 |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255  |match           |forward
    | 10:05:17 |UDP     src port:00520 dest port:00520 |<1,02>          |
128|Apr  7 00 |From:192.168.1.1    To:192.168.1.255  |match           |forward
    | 10:05:30 |UDP     src port:00520 dest port:00520 |<1,02>          |

End of Firewall Log
```

Firmware Upgrade

34.1 Firmware Upgrade Overview

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

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

34.2 Firmware Upgrade Settings

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

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

Figure 169 Maintenance > Firmware Upgrade

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

Table 119   Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Select the check box to have the Zyxel Device automatically reset itself after the new firmware is uploaded.

Table 119   Maintenance > Firmware Upgrade

| LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type the location of the file you want to upload in this field or click **Browse** or **Choose File** to find it.
Browse/ Choose File	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.

Figure 170   Firmware Uploading
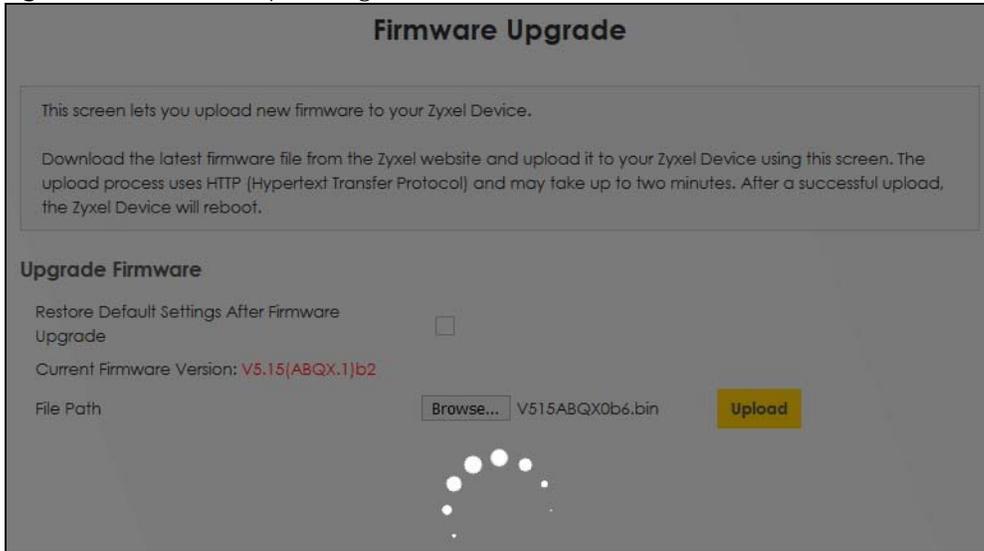
After two minutes, log in again and check your new firmware version in the **Status** screen.

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

Figure 171   Error Message
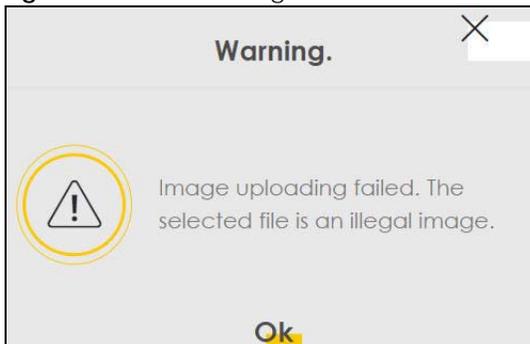
Note that the Zyxel Device automatically restarts during the upload, causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Network Temporarily Disconnected

CHAPTER 35
Backup/Restore

35.1 Backup/Restore Overview

This chapter describes the Zyxel Device's **Maintenance** > **Backup/Restore** screens. Use these screens to perform maintenance on your Zyxel Device's settings.

35.1.1 What You Can Do in this Chapter

- Use the **Backup/Restore** screen to backup/restore/reset device settings ().

35.2 Backup/Restore Settings

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

Figure 172   Maintenance > Backup/Restore

Backup Configuration

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

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

Restore Configuration

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

Table 120   Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.

Table 120   Restore Configuration

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

Do NOT turn off the Zyxel Device while configuration file upload is in progress.

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

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

Figure 173   Network Temporarily Disconnected
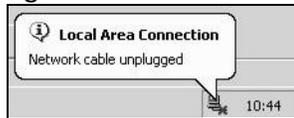
If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

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

Figure 174   Configuration Upload Error
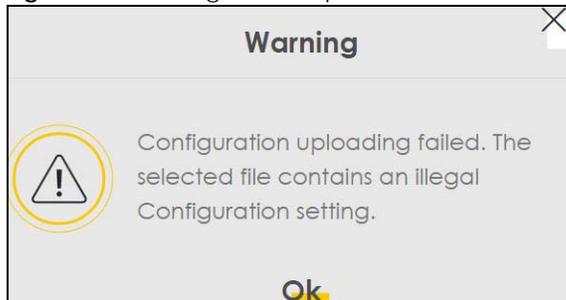
Reset to Factory Defaults

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

Figure 175   Reset Warning Message
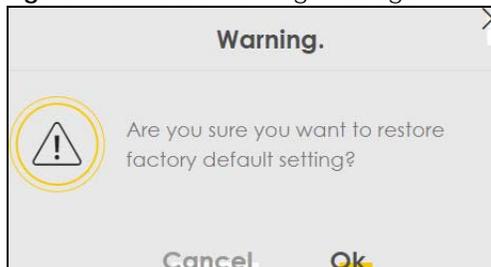
Figure 176   Reset In Process Message
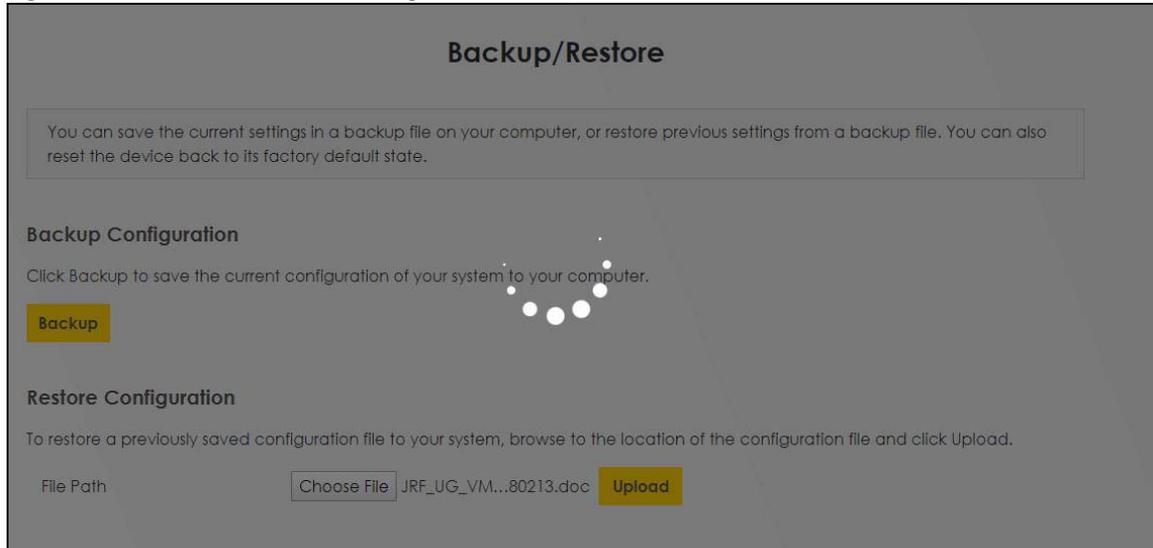
You can also press the **RESET** button on the rear panel to reset the factory defaults of your Zyxel Device. Refer to Section 1.5.4 on page 23 for more information on the **RESET** button.

35.3 Reboot

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

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

Figure 177   Maintenance > Reboot
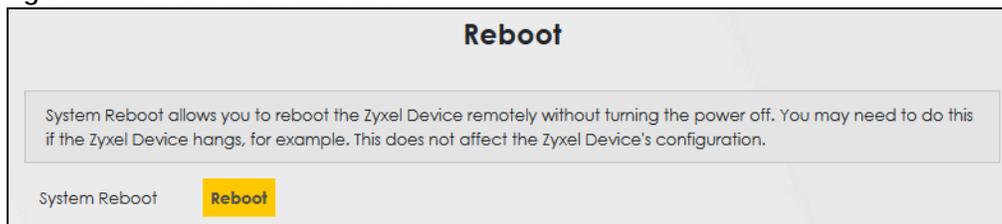
CHAPTER 36
Diagnostic

36.1 Diagnostic Overview

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

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

36.1.1 What You Can Do in this Chapter

- The **Ping & TraceRoute & NsLookup** screen lets you ping an IP address or trace the route packets or take to a host (Section 36.3 on page 271).
- The **802.1ag** screen lets you perform CFM actions (Section 36.4 on page 272).
- The **802.3ah** screen lets you configure link OAM port parameters(Section 36.5 on page 273).

36.2 What You Need to Know

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

How CFM Works

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

CFM provides two tests to discover connectivity faults.

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

36.3 Ping & TraceRoute & NsLookup

Use this screen use ping, traceroute, or nslookup for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking on one of the buttons to start a test, the results will be shown in the Ping/Traceroute Test area. Use nslookup to find the IP address for a host name and vice versa. Click **Maintenance > Diagnostic > Ping&TraceRoute&NsLookup** to open the screen shown next.

Figure 178   Maintenance > Diagnostic > Ping&TraceRoute&NsLookup

The following table describes the fields in this screen.

Table 121   Maintenance > Diagnostic > Ping & TraceRoute & NsLookup

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

EX3510-B1 User's Guide

271

36.4 802.1ag (CFM)

Click **Maintenance > Diagnostic** > **802.1ag** to open the following screen. Use this screen to configure and perform Connectivity Fault Management (CFM) actions as defined by the IEEE 802.1ag standard. CFM protocols include Continuity Check Protocol (CCP), Link Trace (LT), and Loopback (LB).

Figure 179   Maintenance > Diagnostic > 802.1ag

The following table describes the fields in this screen.

Table 122   Maintenance > Diagnostic > 802.1ag

LABEL	DESCRIPTION
802.1ag Connectivity Fault Management	
IEEE 802.1ag CFM	Click this switch to enable or disable the IEEE 802.1ag CFM specification, which allows network administrators to identify and manage connection faults. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Y.1731	Click this switch to enable or disable Y.1731, which monitors Ethernet performance. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Interface	Select the interface on which you want to enable the IEEE 802.1ag CFM.

Table 122   Maintenance > Diagnostic > 802.1ag (continued)

LABEL	DESCRIPTION
Maintenance Domain (MD) Level	Select a level (0-7) under which you want to create an MA.
MD Name	Enter a descriptive name for the MD (Maintenance Domain). This field only appears if the **Y.1731** field is disabled.
MA ID	Enter a descriptive name to identify the Maintenance Association. This field only appears if the **Y.1731** field is disabled.
MEG ID	Enter a descriptive name to identify the Maintenance Entity Group. This field only appears if the **Y.1731** field is enabled.
802.1Q VLAN ID	Type a VLAN ID (1~4094) for this MA.
Local MEP ID	Enter the local Maintenance Endpoint Identifier (1~8191).
CCM	Select **Enable** to continue sending MEP information by CCM (Connectivity Check Messages). When CCMs are received the Zyxel Device will always process it, whether **CCM** is enabled or not.
Remote MEP ID	Enter the remote Maintenance Endpoint Identifier (1–8191).
Test the connection to another Maintenance End Point (MEP)	
Destination MAC Address	Enter the target device's MAC address to which the Zyxel Device performs a CFM loopback and linktrace test.
Test Result	
Loopback Message (LBM)	This shows **Pass** if a Loop Back Messages (LBMs) responses are received. If LBMs do not get a response it shows **Fail**.
Linktrace Message (LTM)	This shows the MAC address of MEPs that respond to the LTMs.
Apply	Click this button to save your changes.
Send Loopback	Click this button to have the selected MEP send the LBM (Loop Back Message) to a specified remote end point.
Send Linktrace	Click this button to have the selected MEP send the LTMs (Link Trace Messages) to a specified remote end point.

36.5 802.3ah (OAM)

Click **Maintenance > Diagnostic** > **803.ah** to open the following screen. Link layer Ethernet OAM (Operations, Administration and Maintenance) as described in IEEE 802.3ah is a link monitoring protocol. It utilizes OAM Protocol Data Units (OAM PDU's) to transmit link status information between directly connected Ethernet devices. Both devices must support IEEE 802.3ah.

Figure 180 Maintenance > Diagnostic > 802.3ah

The following table describes the labels in this screen.

Table 123   Maintenance > Diagnostics > 802.3ah

LABEL	DESCRIPTION
IEEE 802.3ah Ethernet OAM	Click this switch to enable or disable the Ethernet OAM on the specified interface. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Interface	Select the interface on which you want to enable the IEEE 802.3ah.
OAM ID	Enter a positive integer to identify this node.
Auto Event	Click this switch to detect link status and send a notification when an error (such as errors in symbol, frames, or seconds) is detected. Otherwise, disable this and you will not be notified. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Features	Select **Variable Retrieval** so the Zyxel Device can respond to requests for information, such as requests for Ethernet counters and statistics, about link events. Select **Link Events** so the Zyxel Device can interpret link events, such as link fault and dying asp. Link events are set in event notification PDUs (Protocol Data Units), and indicate when the number of errors in a certain given interval (time, number of frames, number of symbols, or number of error frame seconds) exceeds a specified threshold. Organizations may create organization-specific link event TLVs as well. Select **Remote Loopback** so the Zyxel Device can accept loopback control PDUs to convert Zyxel Device into loopback mode. Select **Active Mode** so the Zyxel Device initiates OAM discovery, send information PDUs; and may send event notification PDUs, variable request/response PDUs, or loopback control PDUs.
Apply	Click this button to save your changes.

PART III

Troubleshooting and Appendices

Appendices contain general information. Some information may not apply to your Zyxel Device.

CHAPTER 37
Troubleshooting

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

- Power, Hardware Connections, and LEDs
- Zyxel Device Access and Login
- Internet Access
- Wireless Internet Access
- UPnP
- IP Address Setup

37.1 Power, Hardware Connections, and LEDs

The Zyxel Device does not turn on. None of the LEDs turn on.

1   Make sure the Zyxel Device is turned on.

2   Make sure you are using the power adapter included with the Zyxel Device.

3   Make sure the power adapter is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.

4   Turn the Zyxel Device off and on.

5   If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1   Make sure you understand the normal behavior of the LED. See Table 2 on page 20.

2   Check the hardware connections.

3   Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4   Turn the Zyxel Device off and on.

5   If the problem continues, contact the vendor.

37.2 Zyxel Device Access and Login

I forgot the IP address for the Zyxel Device.

1   The default LAN IP address is 192.168.1.1.

2   If you changed the IP address and have forgotten it, you might get the IP address of the Zyxel Device 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 Zyxel Device (it depends on the network), so enter this IP address in your Internet browser.

3   If this does not work, you have to reset the device to its factory defaults. See Section 1.5.4 on page 23.

I forgot the password.

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

2   If those do not work, you have to reset the device to its factory defaults. See Section 1.5.4 on page 23.

I cannot see or access the **Login** screen in the Web Configurator.

1   Make sure you are using the correct IP address.
   • The default IP address is 192.168.1.1.
   • If you changed the IP address (Section 8.2 on page 120), use the new IP address.
   • If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Zyxel Device.
   • Make sure your computer has an IP address in the same subnet as the Zyxel Device. Your computer should have an IP address from 192.168.1.2 to 192.168.1.254. See Section 37.6 on page 281.

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

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

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

5 Reset the device to its factory defaults, and try to access the Zyxel Device with the default IP address. See Section 1.5.4 on page 23.

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

Advanced Suggestions

• Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.

• Try to access the Zyxel Device using another service, such as Telnet. If you can access the Zyxel Device, check the remote management settings and firewall rules to find out why the Zyxel Device does not respond to HTTP.

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

1 Make sure you have entered the password correctly. See the cover page for the default login names and associated passwords. The field is case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the Web Configurator while someone is using Telnet to access the Zyxel Device. Log out of the Zyxel Device in the other session, or ask the person who is logged in to log out.

3 Turn the Zyxel Device off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 37.1 on page 276.

I cannot Telnet to the Zyxel Device.

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

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

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

37.3 Internet Access

I cannot access the Internet.

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

2   Make sure you entered your ISP account information correctly in the **Network Setting > Broadband** screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.

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

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

5   If the problem continues, contact your ISP.

I cannot connect to the Internet using an Ethernet connection.

1   Make sure you have the Ethernet WAN port connected to a MODEM or Router.

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

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

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

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

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

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

3   Turn the Zyxel Device off and on.

4   If the problem continues, contact your vendor.

37.4 Wireless Internet Access

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

The following factors may cause interference:

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

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

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

What is a Server Set ID (SSID)?

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

37.5 UPnP

When using UPnP and the Zyxel Device reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

1 Disconnect the Ethernet cable from the Zyxel Device's LAN port or from your computer.

2 Re-connect the Ethernet cable.

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

Restart your computer.

37.6 IP Address Setup

I need to set the computer's IP address to be in the same subnet as the Zyxel Device.

---

1   In Windows 10, open the **Control Panel**.

2   Click **Network and Internet** (this field may be missing in your version) > **Network and Sharing Center**.
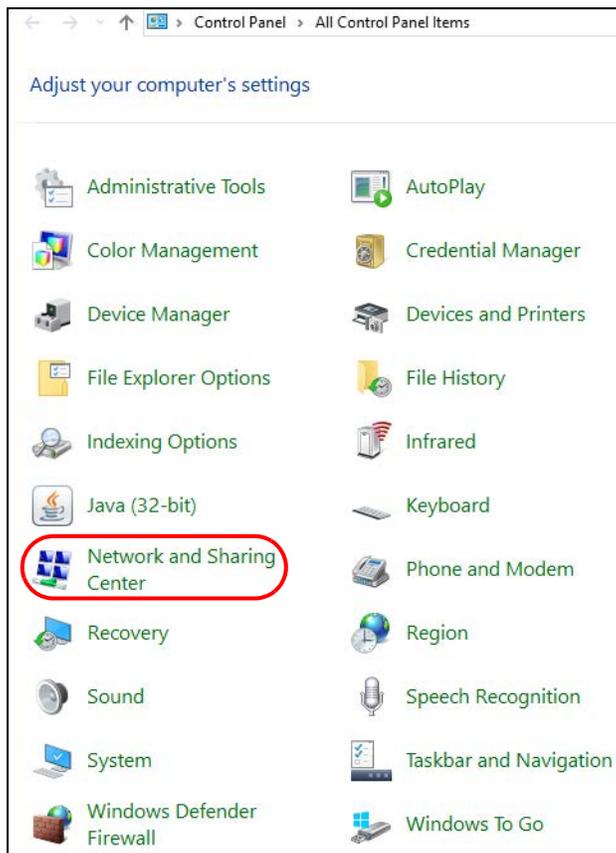
3   Click **Change adapter settings**.
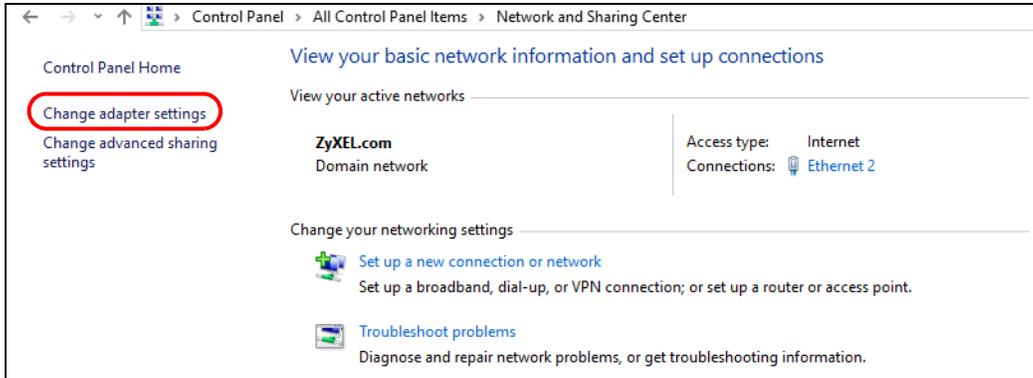
4 Right-click the **Ethernet** icon, and then select **Properties**.
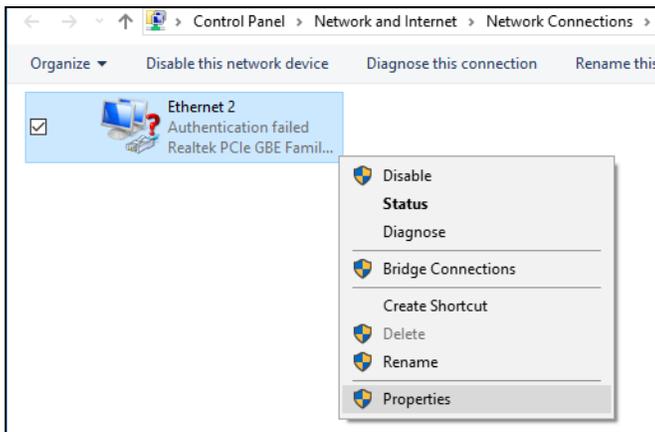
5 Click **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.
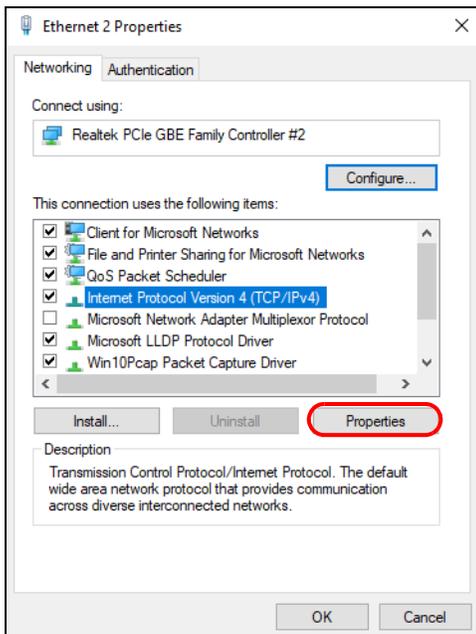
6 Select **Use the following IP address** and enter an **IP address** from **192.168.1.2** to **192.168.1.254**. The **Subnet mask** will be entered automatically.
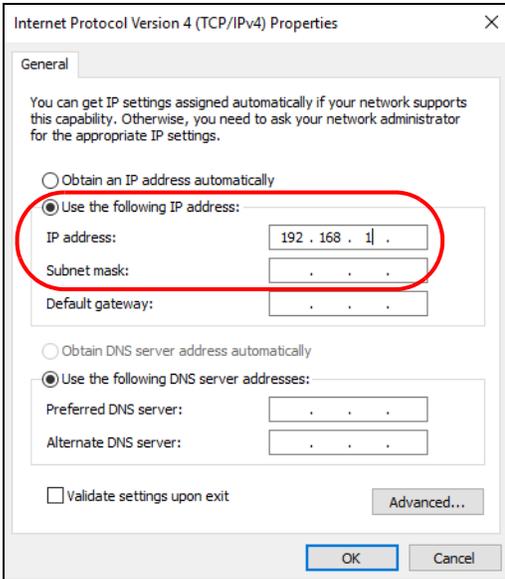
7 Click **OK** when you are done and close all windows.

APPENDIX A
Customer Support

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

For Zyxel Communications offices, see *https://service-provider.zyxel.com/global/en/contact-us* for the latest information.

For Zyxel Networks offices, see *https://www.zyxel.com/index.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
- *https://www.zyxel.com*

Asia

China

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

India

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

Kazakhstan

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

Korea

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

Malaysia

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

Pakistan

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

Philippines

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

Singapore

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

Taiwan

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

Thailand

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

Vietnam

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

Europe

Belarus

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

Bulgaria

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

Czech Republic

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

Denmark

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

Finland

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

France

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

Germany

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

Hungary

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

Italy

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

Netherlands

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

Norway

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

Poland

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

Romania

- Zyxel Romania

- *https://www.zyxel.com/ro/ro*

Russia

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

Slovakia

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

Spain

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

Sweden

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

Switzerland

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

Turkey

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

UK

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

Ukraine

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

South America

Argentina

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

Brazil

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

Colombia

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

Ecuador

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

South America

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

Middle East

Israel

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

North America

USA

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

APPENDIX B
IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses.

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

Prefix and Prefix Length

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

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

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

Link-local Address

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

Table 124   Link-local Unicast Address Format

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

Global Address

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

Unspecified Address

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

Loopback Address

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

Multicast Address

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

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

Table 125   Predefined Multicast Address

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

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

Table 126   Reserved Multicast Address

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

Table 126   Reserved Multicast Address (continued)

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

Subnet Masking

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

Interface ID

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

EUI-64

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

MAC	00	: 13	: 49	: 12	: 34	: 56

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

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.
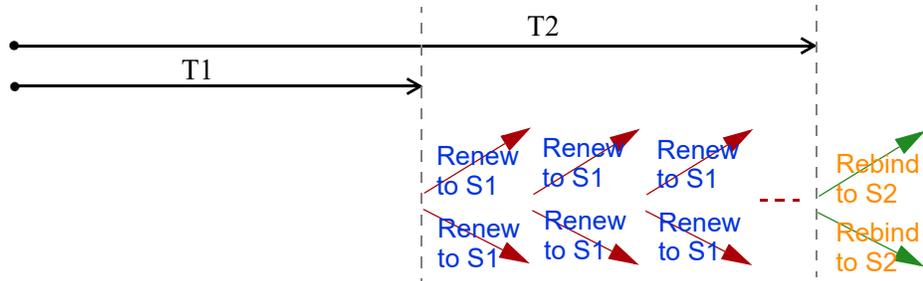
DHCP Relay Agent

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

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

Prefix Delegation

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

ICMPv6

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

Neighbor Discovery Protocol (NDP)

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

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.

- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Zyxel Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Zyxel Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Zyxel Device also sends out a neighbor solicitation message. When the Zyxel Device receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Zyxel Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Zyxel Device creates an entry in the default router list cache if the router can be used as a default router.

When the Zyxel Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Zyxel Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is unlink, the address is considered as the next hop. Otherwise, the Zyxel Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Zyxel Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Zyxel Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

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

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example – Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.
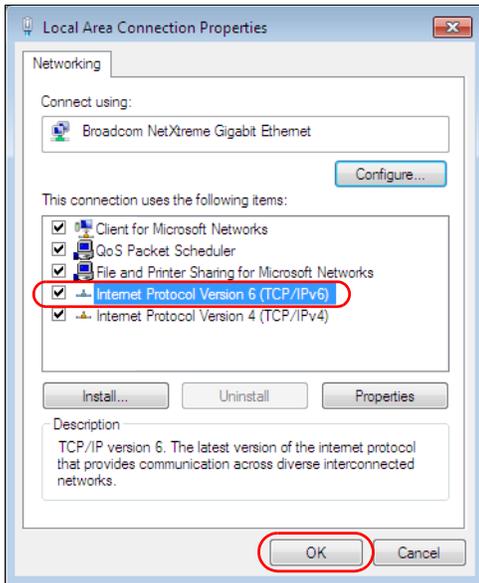
4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

APPENDIX C
Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 127   Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP	7648	A popular videoconferencing solution from White Pines Software.
	TCP/UDP	24032	
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP	20	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
	TCP	21	
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP	137	The Network Basic Input/Output System is used for communication between computers in a LAN.
	TCP/UDP	138	
	TCP/UDP	139	
	TCP/UDP	445	
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.

Table 127   Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.

Table 127   Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

APPENDIX D
Legal Information

Copyright

Copyright © 2022 by Zyxel and/or its affiliates.

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 and/or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any devices, 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 devices 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 device within the USA.

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 device 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 device with RF function within the USA.

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 46 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment.
- For 2.4G WLAN, only channels 1 – 11 are operational. Selection of other channels is NOT possible.

CANADA

The following information applies if you use the device within Canada.

Innovation, Science and Economic Development Canada ICES Statement

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

Innovation, Science and Economic Development Canada RSS-GEN & RSS-247 Statement

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(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.
- L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique 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; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- For 2.4G WLAN, only channels 1 – 11 are operational. Selection of other channels is NOT possible.

If the device 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.

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 de 5 150 à 5 250 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;

Industry Canada radiation exposure statement

This device complies with ISED radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 27 cm between the radiator and your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 27 cm de distance entre la source de rayonnement et votre corps.

EUROPEAN UNION

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

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for wireless devices relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this device 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 5 GHz 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 5 GHz wireless LANs.
- If this device for operation in the band 5150 – 5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20 cm between the radio equipment and your body.

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/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 timto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.
	National Restrictions
	• In Denmark, the band 5150 – 5350 MHz is also allowed for outdoor usage. • I Danmark må frekvensbåndet 5150 – 5350 også anvendes udendørs.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.

Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. **National Restrictions** • This device meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN device is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details. • Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. **National Restrictions** • The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details. • 2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atiauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.

Notes:
• Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
• The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not use this device 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. 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 device 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 device, please contact your local city office, your household waste disposal service or the store where you purchased the device.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  – For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

  – For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Important Safety Instructions

- Caution! The RJ-45 jacks are not used for telephone line connection.
- Caution! Do not use this device near water, for example a wet basement or near a swimming pool.
- Caution! Avoid using this device (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Caution! Always disconnect all telephone lines from the wall outlet before servicing or disassembling this device.
- Attention: Les prises RJ-45 ne sont pas utilisés pour la connexion de la ligne téléphonique.
- Attention: Ne pas utiliser ce produit près de l'eau, par exemple un sous-sol humide ou près d'une piscine.
- Attention: Évitez d'utiliser ce produit (autre qu'un type sans fil) pendant un orage. Il peut y avoir un risque de choc électrique de la foudre.
- Attention: Toujours débrancher toutes les lignes téléphoniques de la prise murale avant de réparer ou de démonter ce produit.

Environment Statement

ErP (Energy-related Products)

Zyxel devices 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 the chapter about wireless settings for more detail.)

European Union – Disposal and Recycling Information

The symbol below means that according to local regulations your device and/or its battery shall be disposed of separately from domestic waste. If this device is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your device 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。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。

- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  – 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  – 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this device 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 device's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this device 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 device. During the warranty period, and upon proof of purchase, should the device have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective devices or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the device or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent device of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the device has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online at www.zyxel.com to receive email notices of firmware upgrades and related information.

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses, please go to: https://service-provider.zyxel.com/global/en/gpl-oss-software-notice.

Index

U

unicast **86**

Universal Plug and Play, see UPnP

upgrading firmware **263**

UPnP **126**
    cautions **119**
    NAT traversal **119**
    turn on in Windows 10 Example **129**
    turn on in Windows 7 Example **127**

USB LED **21**

USB port **22**

V

Vendor ID **133**

Virtual Local Area Network, see VLAN

VLAN **86**
    introduction **86**
    number of possible VIDs
    priority frame
    static **86**

VLAN ID **86**

VLAN tag **86**

W

Wake on LAN **133**

wall mounting information **23**

wall mounting steps **23**

WAN
    status **64**
    Wide Area Network, see WAN **74**

WAN IP address **75**

WAN LED **21**

warranty **304**
    note **304**

web browser pop-up **26**

web browser pop-up window **26**

web browser version recommended **26**

Web Configurator
    layout **28**
    login **26**

overview **26**
password **26**

WEP Encryption **93**

WiFi **105**
    authentication **107**, **108**
    BSS **109**
        example **110**
    channel **106**
    encryption **109**
    example **105**
    fragmentation threshold **102**, **107**
    limitations **109**
    MAC address filter **97**, **108**
    MBSSID **110**
    preamble **103**, **107**
    RADIUS server **108**
    RTS/CTS threshold **102**, **107**
    security **107**
    SSID **108**
        activation **94**
    status **65**
    WPS **111**, **113**
        example **114**
        limitations **116**
        PIN **112**
        push button **111**

WiFi overview **88**, **266**

WiFi Protected Setup (WPS) **18**

WiFi setting
    configuration **66**

WiFi6 introduction **89**

wireless basics **88**

wireless group
    multiple setup **46**

wireless network
    secure setup **39**

wireless network tutorial **41**

Wizard icon **33**

Wizard setup
    Internet **34**

WLAN Station Status screen **239**

WPS **111**, **113**
    activate **23**
    example **114**
    limitations **116**
    PIN **112**
        example **113**
    push button **111**