

MAC Filter

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 six 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.

MAC Address Filter ☒ Enable ☐ Disable (Settings are invalid when disable)

MAC Restrict Mode ☒ Allow ☐ Deny

+ Add New Rule

Set	Active	Host Name	MAC Address	Delete
Note 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.				

Cancel Apply

- Click **Add New Rule** to add a new entry. Select **Active**, and then enter the **Host Name** and **MAC Address** of computer B. Click **Apply**.

MAC Address Filter ☒ Enable ☐ Disable (Settings are invalid when disable)

MAC Restrict Mode ☐ Allow ☒ Deny

+ Add New Rule

Set	Active	Host Name	MAC Address	Delete
1	☒	B	00 - 24 - 21 - AB - 1F - 00	

Cancel Apply

5.7 Internet Calls

This section shows you how to:

- [Add a SIP Service Provider](#)
- [Add a SIP Account](#)
- [Configure a Phone](#)
- [Make a VoIP Call](#)

5.7.1 Configure VoIP

To make voice calls over the Internet, you must set up a Session Initiation Protocol (SIP) provider and SIP account on the Zyxel Device. You should have an account with a SIP service provider already set up.

5.7.2 Add a SIP Service Provider

Follow the steps below to add a SIP service provider.

- 1 Make sure your Zyxel Device is connected to the Internet.
- 2 Open the Web Configurator.
- 3 Go to the **VoIP > SIP > SIP Service Provider** screen. Click the **Add New Provider** button to add the SIP Service Provider.

#	SIP Service Provider Name	SIP Proxy Server Address	REGISTER Server Address	SIP Service Domain	Modify
1	Verizon	sip.infostrada.it	sip.infostrada.it	sip.infostrada.it	

- 4 On the **Add New Provider** screen, select **Enable SIP Service Provider**.
- 5 Enter the **SIP Service Provider Name** of up to 64 printable characters except ["], [`], ['], [<], [>], [^], [\$], [|], [&], or [;].
- 6 Enter **SIP Proxy Server Address**, **SIP REGISTRAR Server Address**, and **SIP Service Domain** provided by your SIP service provider. Click **OK** to save your settings.

Add New Provider

SIP Service Provider Selection

Service Provider Selection ADD_NEW

General

SIP Service Provider ☒ Enable SIP Service Provider

SIP Service Provider Name

SIP Local Port (1025~65535)

SIP Proxy Server Address

SIP Proxy Server Port (1025~65535)

SIP REGISTRAR Server Address

SIP REGISTRAR Server Port (1025~65535)

SIP Service Domain



Cancel OK

5.7.3 Add a SIP Account

The SIP account must be associated with the SIP service provider configured above. You may configure several SIP accounts for the same service provider. Follow the steps below to set up your SIP account:

- 1 Make sure your Zyxel Device is connected to the Internet.
- 2 Open the Web Configurator.
- 3 Go to the **VoIP > SIP > SIP Account** screen.
- 4 Click the **Add New Account** button on the **SIP Account** screen to add a SIP account and map it to a phone port.

SIP Account SIP Service Provider

You can make calls over the Internet using VoIP technology. For this, you first need to set up a SIP account with a SIP service provider.

The Zyxel Device uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's VoIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account and map it to a phone port. The SIP account contains information that allows your Zyxel Device to connect to your VoIP service provider.

+ Add New Account

#	Enable	SIP Account	Service Provider	Account Number	Modify
1	Enabled	SIP1	Verizon	Account1	
2	Enabled	SIP2	Verizon	Account2	
3	Disabled	SIP3	Verizon	Account3	

- 5 Under **General**, select **Enable SIP Account**, and then enter the **SIP Account Number**.
- 6 Under **Authentication**, enter **Username** and **Password**. Leave the other settings as default. Click **OK** to save your settings.

SIP Account Entry Edit

SIP Account Selection

SIP Account Selection SIP1

SIP Service Provider Association

SIP Account Associated with Verizon

General

☒ Enable SIP Account

SIP Account Number Account1

Authentication

Username User1

Password *****

URL Type

URL Type SIP

5.7.4 Configure a Phone

You must now configure the phone port to use the SIP account you just configured.

- 1 Go to the **VoIP > Phone > Phone Device** screen.
- 2 Click the **Modify** icon of **PHONE1** to configure PHONE1 on your Zyxel Device. The following screen appears.

Phone Device Region

Use this screen to view detailed information on phones used for Internet phone calls (SIP). You can define which phone(s) will ring when a specific SIP address receives an incoming call, and which SIP address will be used when an outgoing call is made with a specific phone.

Analog Phone

#	Phone ID	Internal Number	Incoming SIP Number	Outgoing SIP Number	Modify
1	PHONE1	**11	Account1	Account1	
2	PHONE2	**12	Account2	Account2	

- 3 Under **SIP1 SIP Account to Make Outgoing Call**, select **SIP1** to have the phone connected to the first phone port use the registered SIP1 account to make outgoing calls.
- 4 Under **SIP Account(s) to Receive Incoming Call**, select **SIP1** to have the phone connected to the first phone port receive phone calls for the SIP1 account. Click **OK** to save your changes.

Phone Device Edit

SIP Account to Make Outgoing Call

SIP Account ☒ SIP1 ☐ SIP2

SIP Number

SIP Account(s) to Receive Incoming Call

SIP Account ☒ SIP1 ☐ SIP2

directoryNumber

Immediate Dial Enable

☒ Immediate Dial Enable

Cancel OK

5.7.5 Make a VoIP Call

Follow these steps to make a phone call using Voice over IP (VoIP).

- 1 Make sure you connect a telephone to phone port 1 on the Zyxel Device.
- 2 Make sure the Zyxel Device is turned on and connected to the Internet.
- 3 Pick up the phone receiver.
- 4 Dial the VoIP phone number you want to call.

5.8 Device Maintenance

This section shows you how to:

- [Upgrade the Firmware](#)
- [Back up the Device Configuration](#)
- [How to Reset the Zyxel Device to the Factory Defaults](#)

You can upgrade the Zyxel Device firmware, back up the configuration and restore the Zyxel Device to its previous or default settings.

5.8.1 Upgrade the Firmware

Upload the latest firmware to the Zyxel Device for feature enhancements.

- 1 To download the latest firmware of your Zyxel Device, go to <https://www.zyxel.com/service-provider> and search for your model. The latest firmware will be available under the **Downloads & resources** tab. The model code for the Zyxel Device in this example is v5.13(ABLZ.1). Note the model code for your Zyxel Device.
- 2 Unzip the file.
- 3 Go to the **Maintenance > Firmware Upgrade** screen.
- 4 Click **Browse/Choose File** and select the file with a ".bin" extension to upload. Click **Upload**.

Firmware Upgrade

This screen lets you upload new firmware to your Zyxel Device.

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.

Restore Partial Default Settings After Firmware Upgrade
Reset All Settings Except Mesh After Firmware Upgrade resets all your configurations, except for Mesh WiFi settings, to the factory defaults after firmware upgrade.

Upgrade Firmware

Reset All Settings After Firmware Upgrade ☐

Reset All Settings Except Mesh After Firmware Upgrade ☐

Current Firmware Version: **V5.18(ACHN.0)b2**

File Path No file chosen

Upgrade WWAN Package

Current WWAN Package Version: **1.24**

File Path No file chosen

- 5 This process may take up to 2 minutes to finish. After 2 minutes, log in again and check your new firmware version in the **Connection Status** screen.

5.8.2 Back up the Device Configuration

Back up a configuration file allows you to return to your previous settings.

- 1 Go to the **Maintenance > Backup/Restore** screen.
- 2 Under **Backup Configuration**, click **Backup**. A configuration file is saved to your computer. In this case, the **Backup/Restore** file is saved.

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.

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.

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

Backup Configuration

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

Backup

Restore Configuration

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

File Path

Back to Factory Default Settings

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

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

Do you want to save **Backup_Restore** (125 KB) from 192.168.1.1?

5.8.3 Restore the Device Configuration

This section shows you how to restore a previously-saved configuration file from your computer to your Zyxel Device.

- 1 Go to the **Maintenance > Backup/Restore** screen.
- 2 Under **Restore Configuration**, click **Browse/Choose File**, and then select the configuration file that you want to upload. Click **Upload**.

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.

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.

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

Backup Configuration

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

Backup

Restore Configuration

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

File Path **Browse...** **Upload**

Back to Factory Default Settings

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

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

Reset

- The Zyxel Device automatically restarts after the configuration file is successfully uploaded. Wait for one minute before logging into the Zyxel Device again. Go to the **Connection Status** page to check the firmware version after the reboot.

5.8.4 How to Reset the Zyxel Device to the Factory Defaults

To reset the Zyxel Device, you can press the **RESET** button on the rear panel for more than 5 seconds. Alternatively, you can use the web configurator to reset the Zyxel Device.

Go to **Maintenance > Backup/Restore** and click the **Reset All Settings** button. The Zyxel Device will reset to factory defaults and the LAN IP address will be set to the default IP address.

Perform Mesh Full Factory Reset

Mesh Full Factory Reset allows you to clear the controller and agents' all user-entered configuration information and return to factory default settings. After resetting, the

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

Reset All Settings**Perform Mesh Partial Factory Reset**

Mesh Partial Factory Reset allows you to keep certain user configurables while bringing the reset of the controller and agents to factory default setting.

- System will keep Wi-Fi settings, include these user settings (Mesh Enable/Disable, Mesh Controller Mode, Mesh Backhaul information, Single SSID Enable/Disable, SSIDs, WPA keys, Encryption modes, 2.4GHz Enable/Disable, 5GHz Enable/Disable, Guest Wi-Fi Enable/Disable, Guest Wi-Fi isolation setting, 802.11 Mode, PMF setting)

Reset All Settings Except Mesh

If you want to reset the Zyxel Device while keeping the Mesh WiFi Settings, click the **Reset All Settings Except Mesh** button. See [Backup/Restore](#) for more details.

5.9 Remote Access from WAN

This section shows you how to:

- [Configure Access to Your Zyxel Device](#)
- [Configure the Trust Domain](#)

You can configure WAN access for a specific trusted computer through HTTPS, SSH to the Zyxel Device. Remote management determines which interface and web services are allowed to access the Zyxel Device.

5.9.1 Configure Access to Your Zyxel Device

Perform the following to configure access to your Zyxel Device:

- 1 Go to the **Maintenance > Remote Management > MGMT Services** screen. Select the WAN interface and services allowed to access the Zyxel Device remotely.

Remote Management

MGMT Services Trust Domain

Use this screen to configure the interfaces through which services can access the Zyxel Device. You can also specify service port numbers computers must use to connect to the Zyxel Device.

Service Control

WAN Interface used for services: ☒ Any_WAN ☐ Multi_WAN
☐ ETHWAN

Service	LAN	WLAN	WAN	Trust Domain	Port
HTTPS	☐ Enable	☐ Enable	☐ Enable	☐ Enable	443
FTP	☐ Enable	☐ Enable	☐ Enable	☐ Enable	21
TELNET	☐ Enable	☐ Enable	☐ Enable	☐ Enable	23
SSH	☐ Enable	☐ Enable	☐ Enable	☐ Enable	22
SNMP	☐ Enable	☐ Enable	☐ Enable	☐ Enable	161
PING	☐ Enable	☐ Enable	☐ Enable	☐ Enable	

Cancel Apply

These are the different ways to access the Zyxel Device remotely.

ACCESS TYPE	LABEL	DESCRIPTION
LAN / WLAN (WiFi)	LAN / WLAN	This allows access of the selected Service from the local LAN.
WAN	WAN	This allows access of the selected Service from the WAN connections.
Trust Domain	Trust Domain	This allows access of the selected Service only from the trusted IPv4 / IPv6 addresses configured under Trust Domain .

- 2 Select how you want to access the Zyxel Device remotely.
- 3 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.

5.9.2 Configure the Trust Domain

Perform the following to configure the Trust Domain on your Zyxel Device:

- 1 Go to the **Maintenance > Remote Management > Trust Domain** screen. Click **+ Add Trust Domain** to go to the **Add Trust Domain** screen to add a trusted host IPv4 / IPv6 address.

The screenshot shows the 'Remote Management' web interface. At the top, there's a header 'Remote Management'. Below it, a breadcrumb trail shows 'MGMT Services' and 'Trust Domain'. A text box explains the purpose: '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.' Below this, there's a table with two columns: 'IP Address' and 'Delete'. A red box highlights a yellow plus icon and the text 'Add Trust Domain' in the top right corner.

- 2 Enter a public IPv4 / IPv6 IP address which is allowed to access the service on the Zyxel Device from the WAN. Then click **OK**.

The screenshot shows the 'Add Trust Domain' dialog box. It has a back arrow in the top left. The title is 'Add Trust Domain'. The text inside says: 'Enter the IP address of the management station permitted to access the local management services. 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.' Below this, there's a form with 'IP Address' and a text input field, followed by a label ' [/prefix length]'. At the bottom, there are 'Cancel' and 'OK' buttons.

PART II

Technical Reference

CHAPTER 6

Connection Status

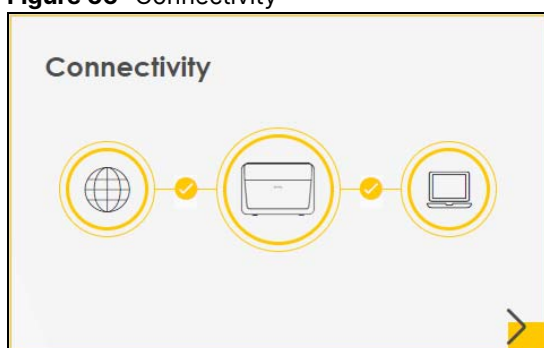
6.1 Connection Status Overview

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

6.1.1 Connectivity

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

Figure 66 Connectivity

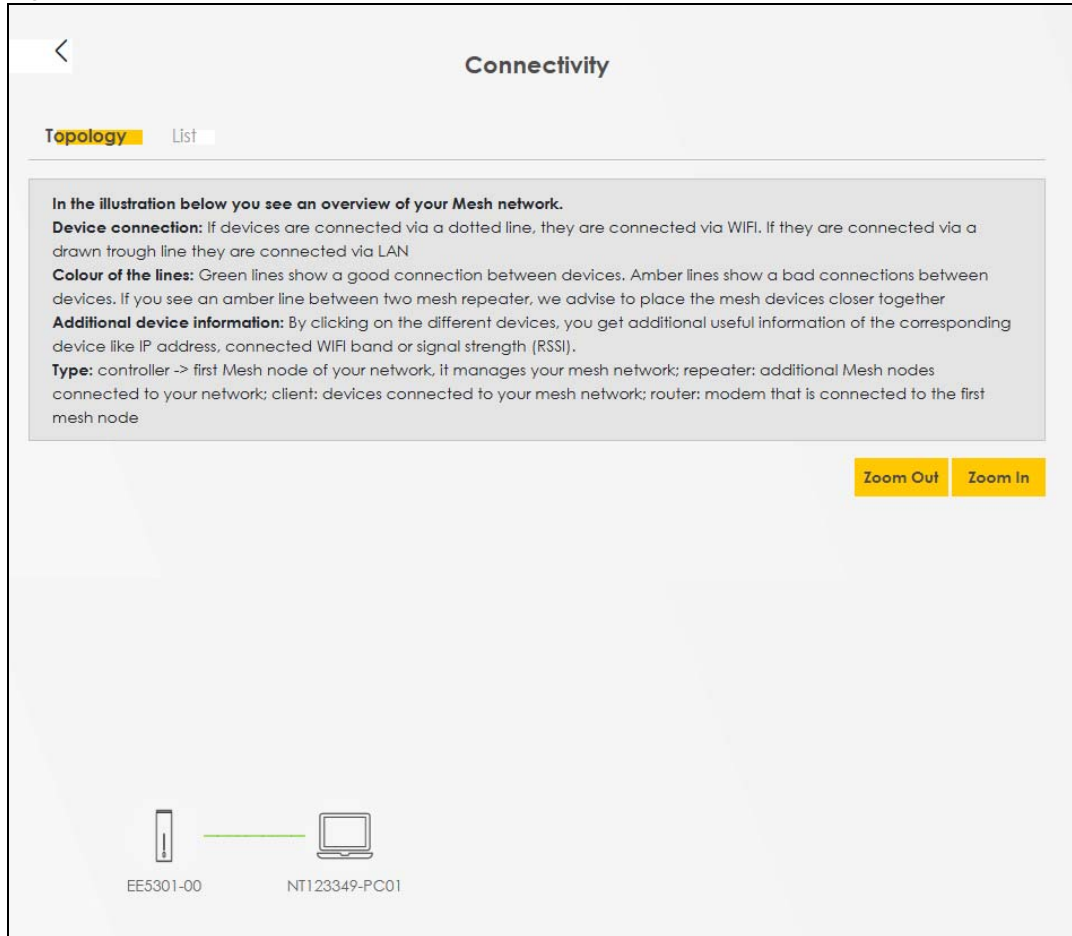


Click the Arrow icon (➡) to view IP addresses and MAC addresses of the wireless and wired devices connected to the Zyxel Device.

You can change the icon and name of a connected device. Place your mouse within the device block, and an Edit icon (✎) will appear. Click the Edit icon, and you will see there are several icon choices for you to select. Enter a name in the **Device Name** field for a connected device. Click to enable (🔵) **Internet Blocking** for a connected WiFi client.

The following screen appears when you enable **MPro Mesh** in the **Network Setting > Wireless > MESH** screen. Check [Overview](#) to see if your Zyxel Device supports Mesh.

Use the **Topology** view screen to display an overview of your Mesh network.

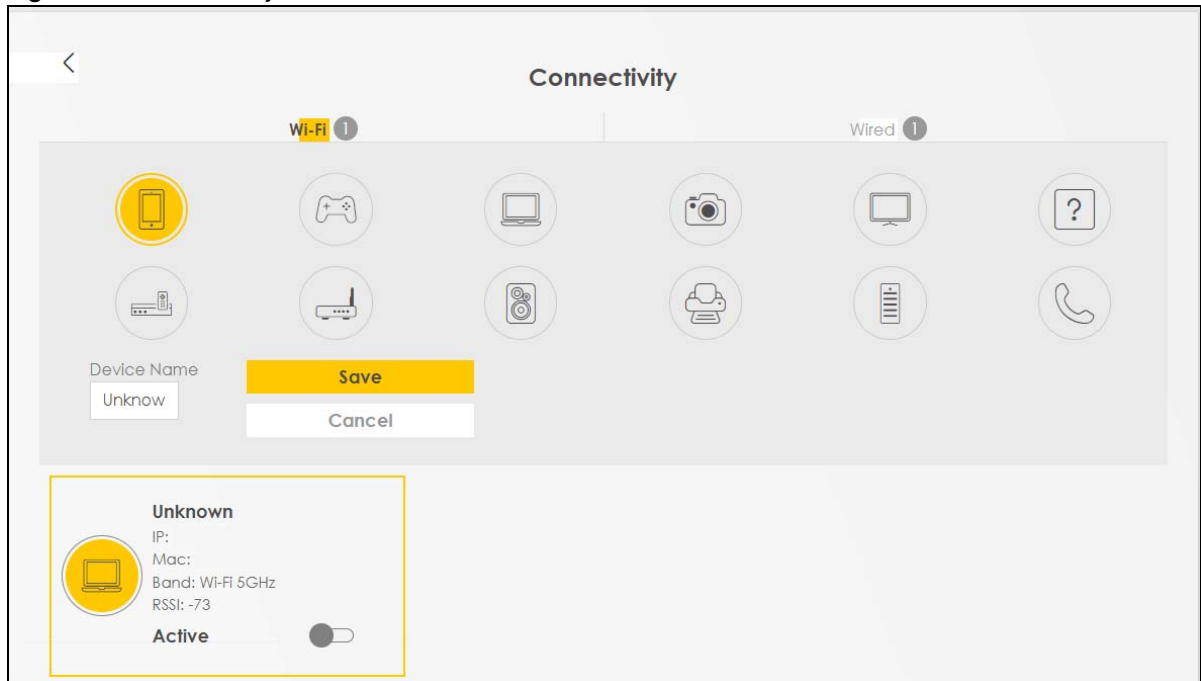
Figure 67 Connectivity: Connected Devices: Topology View

Use the **List** view screen to view IP addresses and MAC addresses of the WiFi 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 68 Connectivity: Connected Devices: List View

6.1.2 Icon and Device Name

Select an icon and/or enter a name in the **Device Name** field for a connected device. Click to enable (🔵) **Internet Blocking** (or **Active**) for a connected WiFi client. Click **Save** to save your changes.

Figure 69 Connectivity: Edit

6.1.3 System Info

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

Figure 70 System Info

Click the Arrow icon () to view more information on the status of your firewall and interfaces (WAN, LAN, and WLAN).

Figure 71 System Info: Detailed Information (Ethernet Gateways)

<

System Info

Host Name

EE5301-00

Model Name

EE5301-00

Serial Number

Firmware Version

V5.63(ACLD.0)b3

System Uptime

0 days 0 hours 58 minutes 23 seconds

Interface Up Time

0 days 0 hours 57 minutes 2 seconds

CPU Usage

0%

Memory Usage

31.7%

Interface Status

LAN1

LAN2

LAN3

WAN

PON

3G/4G(USB)

2.4G WLAN

5G WLAN

-

-

1000M/Full

1000M/Full

-

No Device

688 Mbps

5764 Mbps

WAN Information (Ethernet WAN)

Name

ETHWAN

Encapsulation

IPoE

IP Address

N/A

Renew

IP Subnet Mask

N/A

IPv6 Address

N/A

MAC Address

N/A

IPv4 Gateway

N/A

IPv6 Gateway

N/A

Primary DNS server

N/A

Secondary DNS server

N/A

Connection Uptime

0 days 0 hours 57 minutes 0seconds

LAN Information

IP Address

Subnet Mask

255.255.255.0

IPv6 Address

N/A

IPv6 Link Local Address

DHCP

Server

MAC Address

Security

Firewall

Medium

WLAN Information 2.4GHz

5GHz

MAC Address

Status

On

On

SSID

Zyxel_F6D8

Zyxel_F6D8

Channel

Auto(Current 9)

Auto(Current 60)

Security

WPA3-Personal-Transition

WPA3-Personal-Transition

802.11 Mode

802.11b/g/n/ax/be Mixed

802.11a/n/ac/ax/be Mixed

WPS

On

On

Figure 72 System Info: Detailed Information (PON Gateways)

<
System Info

Host Name PE3101-00

Model Name PE3101-00

Serial Number

GPON Serial Number

Firmware Version V5.67(ACOX.0)a1_0814

System Uptime 0 days 0 hours 33 minutes 27 seconds

CPU Usage 0%

Memory Usage 62.7%

Interface Status

						
LAN1	LAN2	LAN3	LAN4	PON	WLAN	WLAN
1000M/Full	-	-	-	-	344 Mbps	2882 Mbps

WAN Information (No WAN)

LAN Information

IP Address

Subnet Mask

IPv6 Address

N/A

IPv6 Link Local Address

fe80::fe9f:2aff:fe7a:1ae0

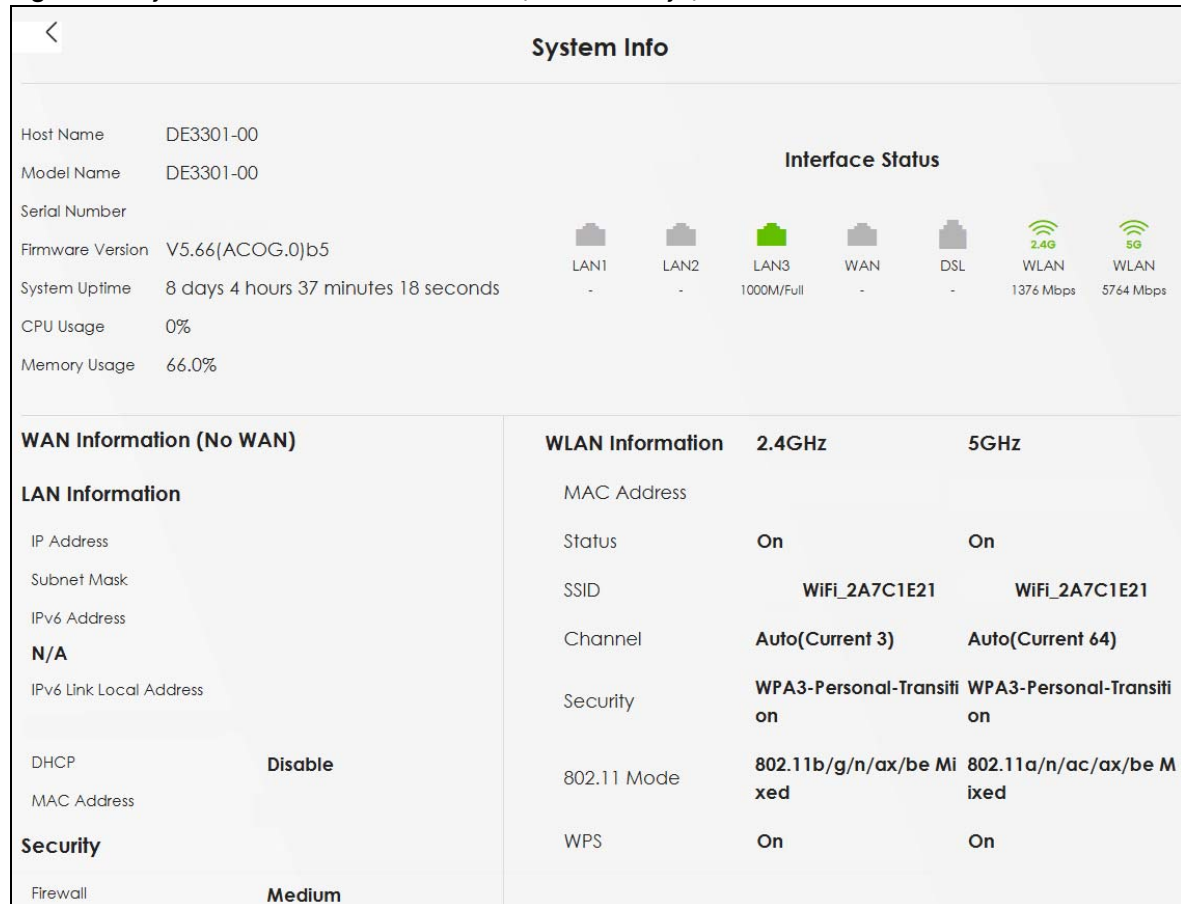
DHCP **Disable**

MAC Address

Security

Firewall **Medium**

WLAN Information	2.4GHz	5GHz
MAC Address		
Status	On	On
SSID	Zyxe1_1AE1	Zyxe1_1AE1
Channel	Auto(Current 1)	Auto(Current 56)
Security	WPA3-Personal-Transiti on	WPA3-Personal-Transiti on
802.11 Mode	802.11b/g/n/ax/be Mi xed	802.11a/n/ac/ax/be M ixed
WPS	On	On

Figure 73 System Info: Detailed Information (DSL Gateways)

Each field is described in the following table.

Table 32 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.
GPON Serial Number	This field displays the unique GPON serial number of the GPON port on the Zyxel Device. Use this serial number to register the Zyxel Device (ONT, Optical Network Terminal) with the OLT (Optical Line Terminal) server.
Firmware Version	This is the current version of the firmware inside the Zyxel Device.
System Uptime	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.
CPU Usage	This displays the current CPU usage percentage.
Memory Usage	This displays the current RAM usage percentage.
Interface Status	
Virtual ports are shown here. You can see the ports in use and their transmission rate.	
WAN Information (These fields display when you have a WAN connection.)	
Name	This field displays the name given to the Internet connection.
Encapsulation	This field displays the current encapsulation method.

Table 32 System Info: Detailed Information (continued)

LABEL	DESCRIPTION
IP Address	This field displays the current IP address of the Zyxel Device in the WAN. Click the Release/Renew button if you want to release/renew your WAN IP address.
IP Subnet Mask	This field displays the current IPv4 subnet mask of the Zyxel Device in the WAN.
IPv6 Address	This field displays the current IPv6 address of the Zyxel Device in the WAN.
MAC Address	This field displays the WAN Ethernet adapter MAC (Media Access Control) address of your Zyxel Device.
IPv4 Gateway	This field displays the IPv4 address of the default gateway. The default gateway is a router or switch on the same segment as your Zyxel Device's interface. The gateway helps forward packets to destinations outside the local network.
IPv6 Gateway	This field displays the IPv6 address of the default gateway. The default gateway is a router or switch on the same segment as your Zyxel Device's interface. The gateway helps forward packets to destinations outside the local network.
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.
Primary DNSv6 server	This field displays the first DNS server IPv6 address assigned by the ISP.
Secondary DNSv6 server	This field displays the second DNS server IPv6 address assigned by the ISP.
LAN Information	
IP Address	This is the current IP 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. A link-local address is a special type of the IP address that is only valid for communication within the local network segment or broadcast domain of the device. Typically, link-local addresses are used for automatic address configuration and neighbor discovery protocols.
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. Disable – The Zyxel Device is not providing any DHCP services to the LAN.
MAC Address	This shows the network adapter MAC (Media Access Control) Address of the LAN interface.
Security	
Firewall	This displays the firewall's current security level (High, Medium, Low, or Disabled).
WLAN Information	
MAC Address	This shows the WiFi adapter MAC (Media Access Control) Address of the WiFi interface.
Status	This displays whether the WLAN is activated.
SSID	This is the descriptive name used to identify the Zyxel Device in a WLAN.
Channel	This is the channel number currently used by the WiFi interface.
Security	This displays the type of security mode the WiFi interface is using in the WLAN.
802.11 Mode	This displays the type of 802.11 mode the WiFi interface is using in the WLAN.
WPS	This displays whether WPS is activated on the WiFi interface.

6.1.4 WiFi Settings

The following compares the main WiFi network and the guest WiFi network.

Table 33 Main/Guest WiFi Networks key Differences

FEATURE	MAIN WI-FI	GUEST WI-FI
Purpose	For primary household or business users.	For visitors.
Network Access	For access to internal devices, such as printers or file servers.	Internet access only; no access to internal devices.

Use this screen to enable or disable the main WiFi network. When the switch turns blue, the function is enabled. 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 WiFi networks. If you want to show or hide your WiFi passwords, click the Eye icon (👁).

Figure 74 WiFi Settings (for 2.4 GHz and 5 GHz models)

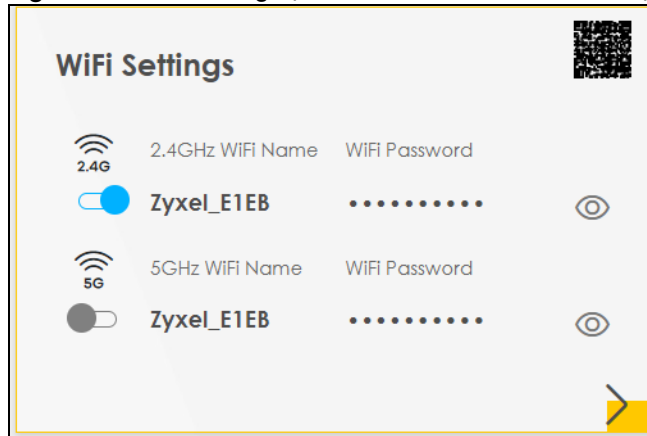
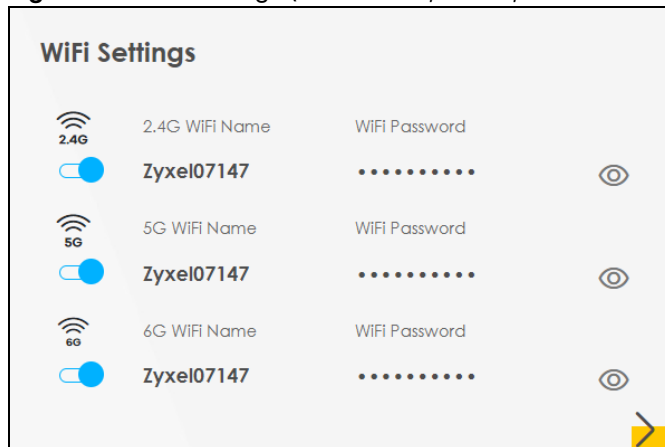


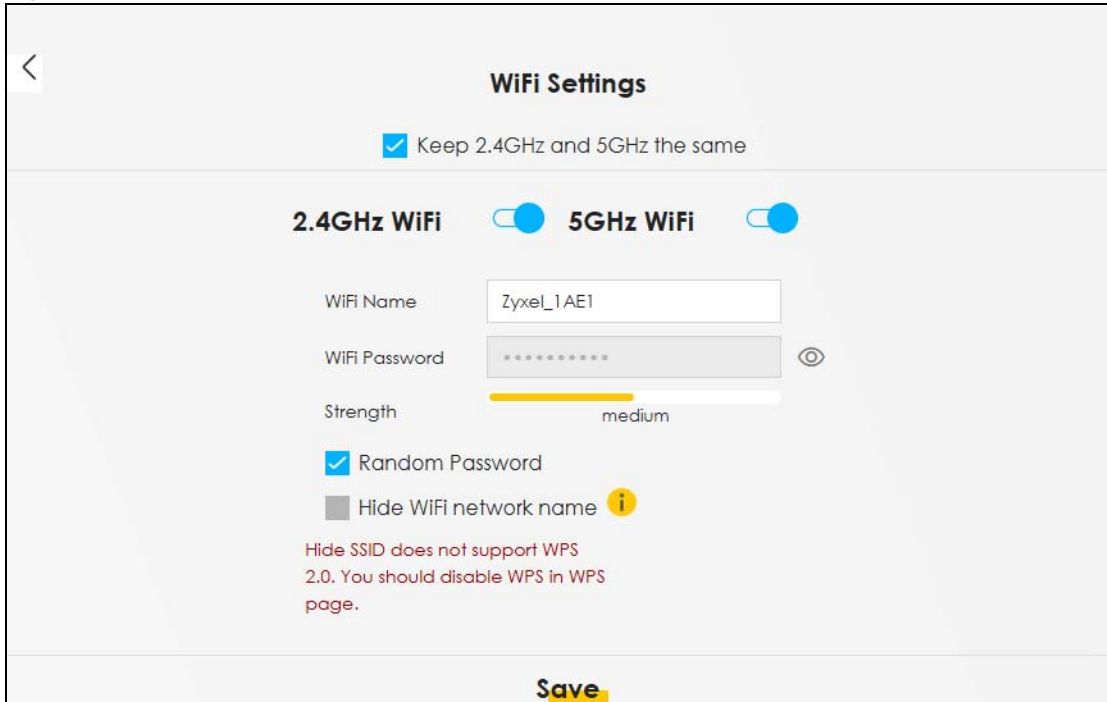
Figure 75 WiFi Settings (for 2.4 GHz, 5 GHz, and 6 GHz models)



Click the Arrow icon (➡) to configure the SSIDs and/or passwords for your main WiFi networks. Click the Eye icon (👁) to display the characters as you enter the WiFi Password.

Scanning the QR code is an alternative way to connect your WiFi client to the WiFi network.

Note: When you enable Mesh in the **Network > Wireless > MESH** screen, **Keep 2.4G, 5G and 6G the same** will be enabled and cannot be disabled.

Figure 76 WiFi Settings: Configuration (for 2.4 GHz and 5 GHz models)

The screenshot shows the 'WiFi Settings' interface. At the top, there is a back arrow and the title 'WiFi Settings'. Below the title, a checkbox labeled 'Keep 2.4GHz and 5GHz the same' is checked. Underneath, there are two toggle switches: '2.4GHz WiFi' and '5GHz WiFi', both of which are turned on. The 'WiFi Name' field contains the text 'ZyxeL1AE1'. The 'WiFi Password' field is masked with dots, and there is an eye icon to its right. Below the password field, a 'Strength' indicator shows a yellow bar and the word 'medium'. There are two checkboxes: 'Random Password' (checked) and 'Hide WiFi network name' (unchecked). A yellow information icon is next to the 'Hide WiFi network name' checkbox. At the bottom, there is a red warning message: 'Hide SSID does not support WPS 2.0. You should disable WPS in WPS page.' and a yellow 'Save' button.

WiFi Settings

☒ Keep 2.4GHz and 5GHz the same

2.4GHz WiFi ☒ 5GHz WiFi ☒

WiFi Name ZyxeL1AE1

WiFi Password 

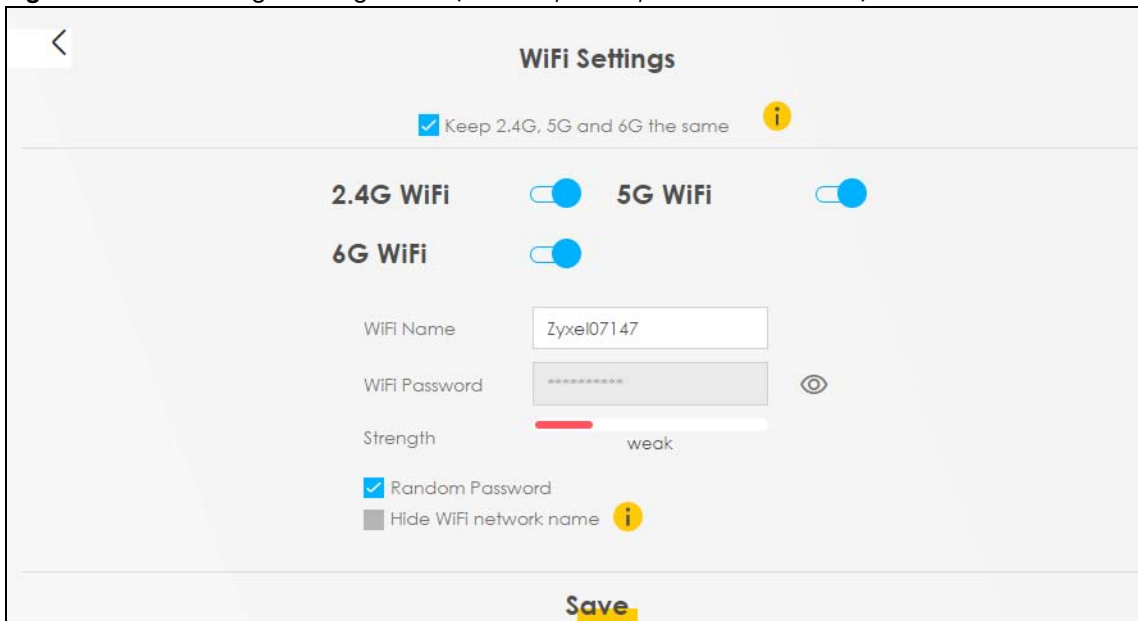
Strength  medium

☒ Random Password

☐ Hide WiFi network name 

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

Save

Figure 77 WiFi Settings: Configuration (2.4 GHz, 5 GHz, and 6 GHz models)

The screenshot shows the 'WiFi Settings' interface for 2.4 GHz, 5 GHz, and 6 GHz models. At the top, there is a back arrow and the title 'WiFi Settings'. Below the title, a checkbox labeled 'Keep 2.4G, 5G and 6G the same' is checked, with a yellow information icon to its right. Underneath, there are three toggle switches: '2.4G WiFi', '5G WiFi', and '6G WiFi', all of which are turned on. The 'WiFi Name' field contains the text 'ZyxeI07147'. The 'WiFi Password' field is masked with dots, and there is an eye icon to its right. Below the password field, a 'Strength' indicator shows a red bar and the word 'weak'. There are two checkboxes: 'Random Password' (checked) and 'Hide WiFi network name' (unchecked). A yellow information icon is next to the 'Hide WiFi network name' checkbox. At the bottom, there is a yellow 'Save' button.

WiFi Settings

☒ Keep 2.4G, 5G and 6G the same 

2.4G WiFi ☒ 5G WiFi ☒ 6G WiFi ☒

WiFi Name ZyxeI07147

WiFi Password 

Strength  weak

☒ Random Password

☐ Hide WiFi network name 

Save

Each field is described in the following table.

Table 34 WiFi Settings: Configuration

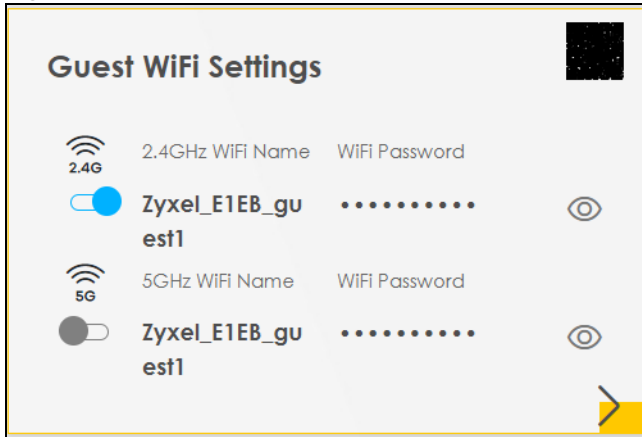
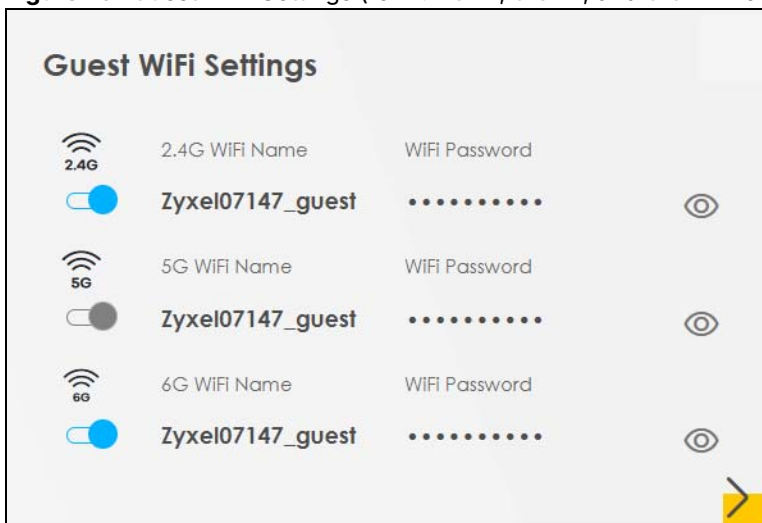
LABEL	DESCRIPTION
Keep 2.4GHz and 5GHz the same / Keep 2.4G, 5G and 6G the same	For models support 2.4 GHz and 5 GHz, select this and the 2.4 GHz and 5 GHz wireless networks will use the same SSID. For models support 2.4 GHz, 5 GHz, and 6 GHz, select this and the 2.4 GHz, 5 GHz and 6 GHz wireless networks will use the same SSID. If you deselect this, the screen will change. You need to assign different SSIDs for the 2.4 GHz and 5 GHz wireless networks. Note: To see if your model supports 6 GHz, please see Overview for more information.
2.4G / 5G / 6G WiFi	Click this switch to enable or disable the 2.4 GHz / 5 GHz / 6 GHz WiFi network. When the switch turns blue , the function is enabled. Note: To see if your model supports 6 GHz, please see Overview for more information.
WiFi Name	The SSID (Service Set Identifier) identifies the service set with which a WiFi device is associated. WiFi devices associating to the access point (AP) must have the same SSID. Enter a descriptive name for the WiFi. You can use up to 32 printable characters, including spaces.
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 enter a pre-shared key from 8 to 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces. Click the Eye icon to show or hide the password for your WiFi network. When the Eye icon is slashed , you will see the password in plain text. Otherwise, it is hidden.
Random Password	Select this to have the Zyxel Device automatically generate a password. The WiFi Password field will not be configurable when you select this option.
Hide WiFi network name	Select this 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.

6.2 Guest WiFi Settings

Use this screen to enable or disable the guest 2.4 GHz / 5 GHz / 6 GHz WiFi 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.

Note: To see if your model supports 6 GHz, please see [Overview](#) for more information.

Note: To see the difference of the main WiFi network and the guest WiFi network, please refer to [Main/Guest WiFi Networks key Differences](#).

Figure 78 Guest WiFi Settings (for 2.4 GHz and 5 GHz models)**Figure 79** Guest WiFi Settings (for 2.4 GHz, 5 GHz, and 6 GHz models)

Click the Arrow icon (➤) to open the following screen. Use this screen to configure the SSIDs and/or passwords for your guest WiFi networks.

To see if your model supports 6 GHz, please see [Overview](#) for more information.

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

To assign different SSIDs to the 2.4 GHz, 5 GHz, and 6 GHz guest wireless networks, clear the **Keep 2.4G, 5G, and 6G the same** checkbox in the **WiFi Settings** screen, and the **Guest WiFi Settings** screen will change.

Figure 80 Guest WiFi Settings: Different SSIDs (for 2.4 GHz and 5 GHz models)

Guest WiFi Settings

2.4GHz WiFi ☐

WiFi Name:

WiFi Password: ☐

Strength: medium

☒ Random Password

☐ Hide WiFi network name ⓘ

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

5GHz WiFi ☐

WiFi Name:

WiFi Password: ☐

Strength: medium

☒ Random Password

☐ Hide WiFi network name ⓘ

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

Save

Figure 81 Guest WiFi Settings: Different SSIDs (for 2.4 GHz, 5 GHz, and 6 GHz models)

Guest WiFi Settings

2.4G WiFi ☐

5G WiFi ☐

6G WiFi ☐

WiFi Name:

WiFi Password: ☐

Strength: weak

☒ Random Password

☐ Hide WiFi network name ⓘ

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

Save

Each field is described in the following table.

Table 35 WiFi Settings: Configuration

LABEL	DESCRIPTION
2.4G / 5G / 6G WiFi	Click this switch to enable or disable the 2.4 GHz / 5 GHz / 6 GHz WiFi networks. When the switch goes to the right , the function is enabled. Otherwise, it is not. Note: To see if your model supports 6 GHz, please see Overview for more information.
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 printable characters, including spaces) for the WiFi.

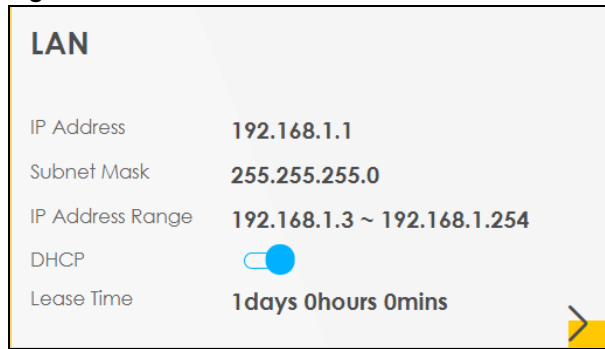
Table 35 WiFi Settings: Configuration (continued)

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 enter a pre-shared key from 8 to 64 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces.
	Click the Eye icon to show or hide the password of your WiFi 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 network name	Select this checkbox 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.

6.2.1 LAN

Use this screen to view the LAN IP address, subnet mask, and DHCP settings of your Zyxel Device. Click the switch button to turn on/off the DHCP server.

Figure 82 LAN



LAN

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

IP Address Range 192.168.1.3 ~ 192.168.1.254

DHCP ☒

Lease Time 1days 0hours 0mins



Click the Arrow icon () to configure the LAN IP settings and DHCP setting for your Zyxel Device.

Figure 83 LAN Setup

LAN

LAN IP Setup

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

IP Addressing Values

Beginning IP Address: 192 . 168 . 1 . 2

Ending IP Address: 192 . 168 . 1 . 254

DHCP Server State

DHCP Server Lease Time: 1 days 0 hours 0 minutes

Save

Each field is described in the following table.

Table 36 LAN Setup

LABEL	DESCRIPTION
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, (factory default).
Subnet Mask	Enter 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 a DHCP-assigned address is valid, before it expires. When a client connects to the Zyxel Device, DHCP automatically assigns the client an IP addresses from the IP address pool. DHCP leases each addresses for a limited period of time, which means that past addresses are "recycled" and made available for future reassignment to other devices.
Days/Hours/Minutes	Enter the lease time of the DHCP server.
Save	Click Save to save your changes.

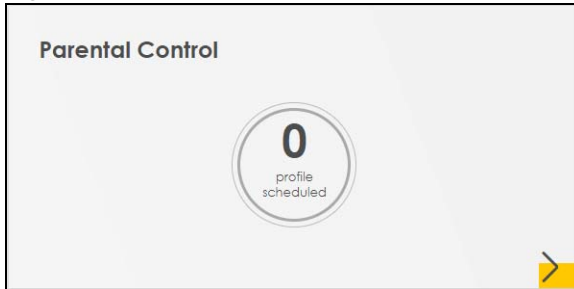
6.3 The Parental Control Screen

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.

Your parental control screens may be different depending on the model you are using. Some Zyxel Devices support scheduling, some support scheduling and URL filtering.

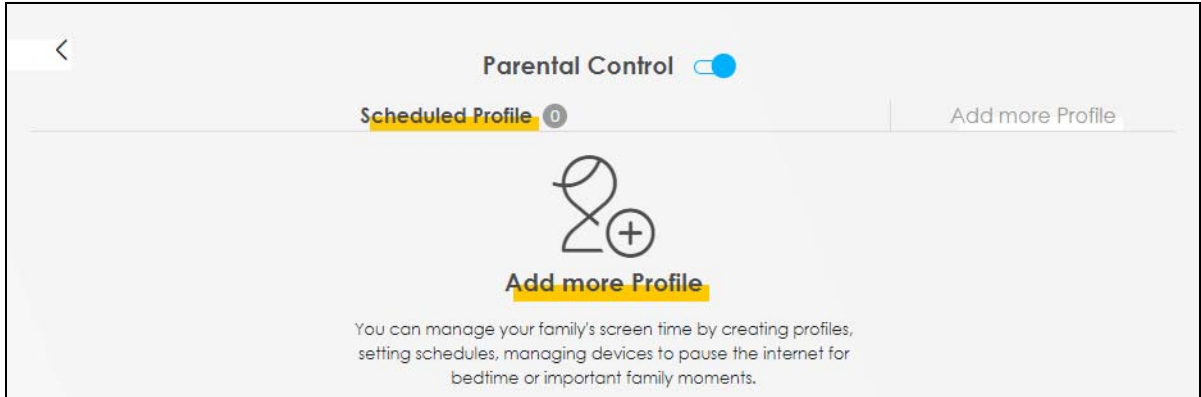
Use this screen to view the number of profiles that were created for parental control.

Figure 84 Parental Control



Click the yellow 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 85 Parental Control: Schedule



Each field is described in the following table.

Table 37 Parental Control: Schedule

LABEL	DESCRIPTION
Parental Control	Click this switch to enable parental control.
Scheduled Profile	This screen shows all the created profiles.
Add More Profile	Click this to create a new profile.

6.3.1 Create a Parental Control Profile

Click **Add more Profile** to create a profile. Use this screen to add a devices in a profile and block Internet access on the profile devices.

Figure 86 Parental Control: Add More Profile

The screenshot shows the 'Parental Control' screen with a progress indicator at the top. Step 1, 'Select Device', is highlighted with a yellow circle and a greater-than sign pointing to Step 2, 'Time limits'. Below the progress indicator, there are four main sections: 'Profile Name' with a text input field containing 'Profile1'; 'Profile Active' with a blue toggle switch; 'Profile Device List' with a text input field containing 'TWPCNT03139-01'; and 'Blocking Schedule' with a text input field. To the right of the 'Profile Device List' field, there is a yellow checkmark icon and the text 'TWPCNT03139-01', 'IP:', and 'Mac:'. At the bottom right, there is a yellow 'Next' button.

Each field is described in the following table.

Table 38 Parental Control: Add More Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile.
Profile Active	Click this switch to enable or disable Internet access. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Profile Device List	This field shows the devices selected on the right for this profile.
Blocking Schedule	This field shows the time during which Internet access is blocked on the profile device(s).
	Select a device(s) on your network for this profile.

Figure 87 Parental Control: Schedule

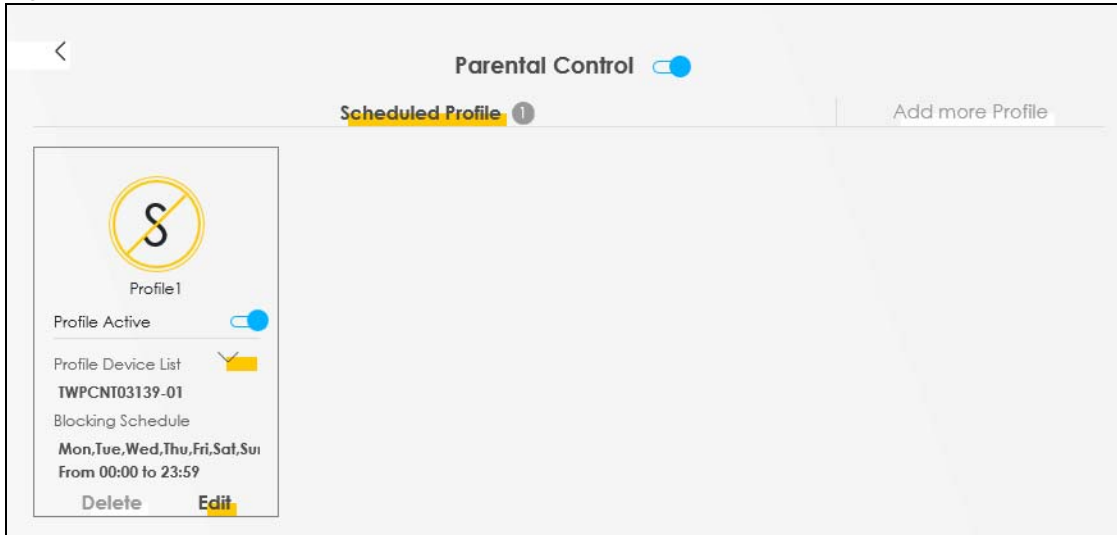
The screenshot shows the 'Parental Control' interface. At the top, there are two numbered steps: '1 Select Device' and '2 Time limits'. The 'Time limits' step is highlighted. Below the steps, the 'Profile Name' is 'yt'. The 'Profile Active' toggle is turned on. The 'Profile Device List' shows 'Unknown'. The 'Blocking Schedule' section indicates that blocking is active from 00:00 to 23:59 on all days of the week (Mon-Sun). The 'Schedule' section allows setting 'Start blocking' (From 00:00) and 'End blocking' (To 23:59) with a '(hh:mm)' format. There is a 'Repeat On' section with buttons for each day of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun). A 'Whole Week' checkbox is checked. At the bottom right, there is an 'Add New Schedule' button. At the bottom center, there are 'Back' and 'Save' buttons.

Each field is described in the following table.

Table 39 Parental Control: Schedule

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile. You can use up to 17 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed.
Profile Active	Click this switch to enable this profile.
Profile Device List	This field shows the devices selected on the right for this profile.
Blocking Schedule	This field shows the time during which Internet access is blocked on the profile devices.
Schedule	
Add New Schedule	Click this to add a new block for scheduling.
Back	Click Back to return to the previous screen.
Save	Click Save to save your changes.

Once a profile is created, it will show in the following screen. Click this  to **Delete** or **Edit** a profile.

Figure 88 Parental Control: Edit/Delete

CHAPTER 7

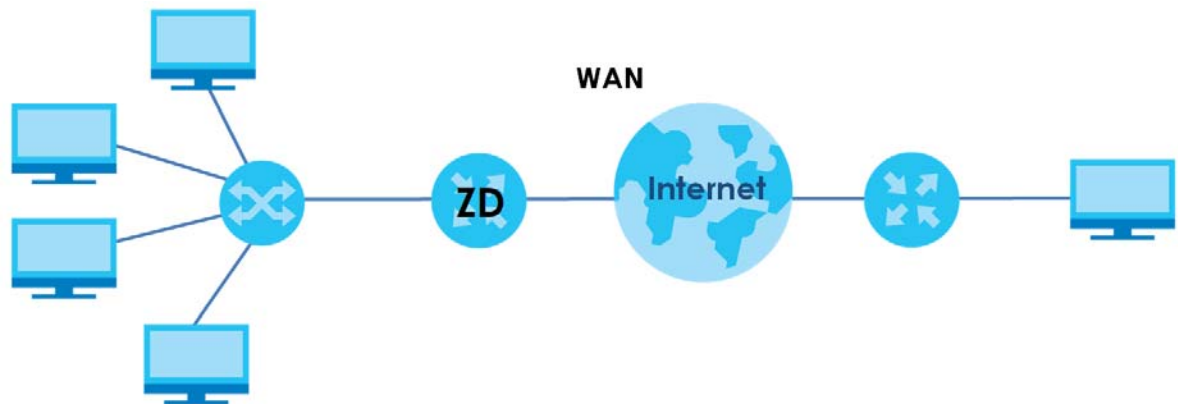
Broadband

7.1 Broadband Overview

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

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

Figure 89 LAN and WAN



7.1.1 What You Can Do in this Chapter

- Use **Broadband** screens to view, remove or add a WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access.
The **Broadband** screens for DSL gateways and Ethernet or AON or PON routers are slightly different. For DSL gateways, see [Broadband Settings for DSL Gateways](#). For Ethernet, AON and PON gateways, see [Broadband Settings for Ethernet, AON and PON Gateways](#). See [Overview](#) to see which gateway type your Zyxel Device belongs to.
- Use the **Cellular Backup** screen to configure cellular WAN connection ([Cellular Backup](#)).
- Use the **Advanced** screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions ([Broadband Advanced Screen for DSL Routers or Gateways](#)). Alternatively, use the **Advanced** screen to configure the Zyxel Device to reduce the power consumption.

Table 40 WAN Setup Overview (Ethernet and PON Gateways)

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 or IPv6 IP address, NAT, DNS server and routing feature
	Bridge	N/A	VLAN
GPON	Routing	PPPoE	PPP user name and password, WAN IPv4 or IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		IPoE	WAN IPv4 or IPv6 IP address, NAT, DNS server and routing feature
	Bridge	N/A	
Note: This table is for the Ethernet and PON gateways. See Overview for more information.			

Table 41 WAN Setup Overview (DSL Gateways)

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

Note: This table is for the DSL gateways. See [Overview](#) for more information.

7.1.2 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 addresses.

ATM

Asynchronous Transfer Mode (ATM) is a WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC).

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

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 3.4×10^{38} IP addresses. The Zyxel Device can use IPv4 or 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

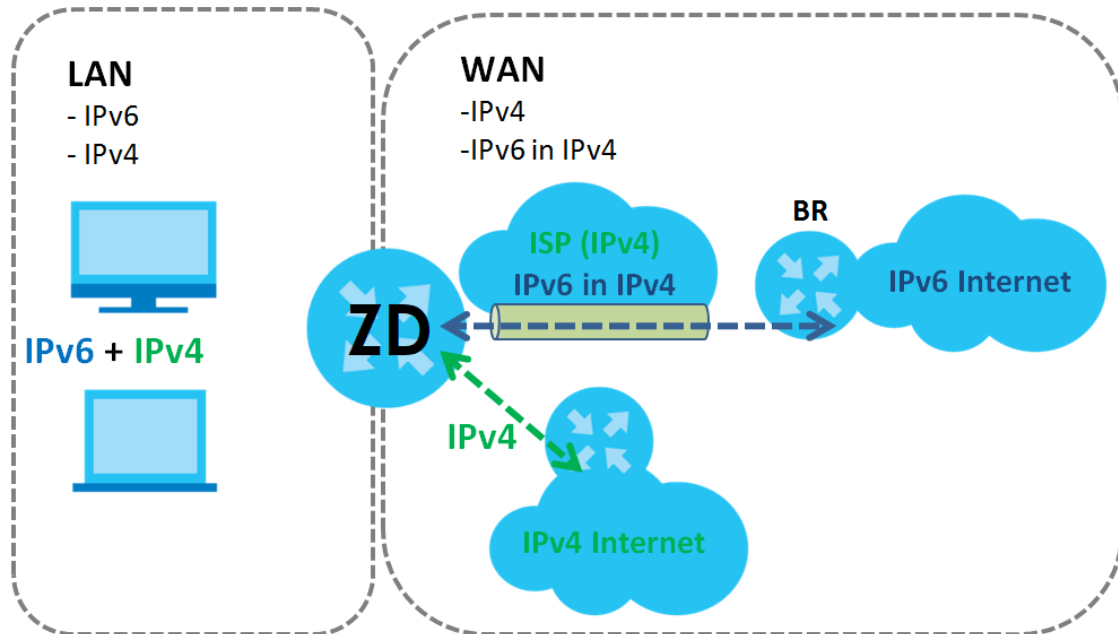
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 – 10, A – F). Each block's 16 bits are then represented by four hexadecimal characters. For example,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

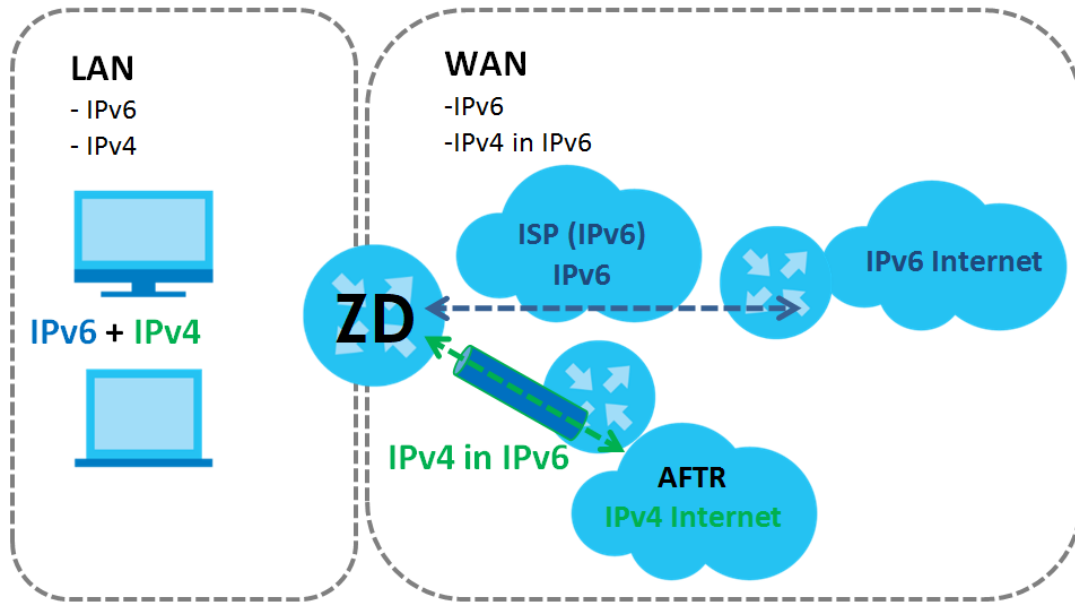
Figure 90 IPv6 Rapid Deployment



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 its configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

Figure 91 Dual Stack Lite**Carrier-Grade NAT (CGNAT)**

CGNAT allows an Internet Service Provider (ISP) to use a single public WAN IP address for multiple customers with different Internet access devices.

7.1.3 Before You Begin

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

7.2 Broadband Settings for DSL Gateways

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 92 Network Setting > Broadband (DSL Gateways)

Broadband

Broadband Advanced

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.

Add New WAN Interface

#	Name	Type	Mode	Encapsulation	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	VDSL	PTM	Routing	IPoE	0	100	Y	Y	Y	N	N	
2	GPON	ETH	Routing	IPoE	0	100	Y	Y	Y	N	N	

The following table describes the labels in this screen.

Table 42 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 types of connections the gateway has.
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.

7.2.1 Add or 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 or 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 or IPv4 mode.

Figure 93 Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode)

<
Edit WAN Interface

General ☒

Name

Type

Mode

Encapsulation

IPv4/IPv6 Mode

VLAN ☒

802.1p

802.1q (0~4094)

MTU

MTU

IP Address

☒ Obtain an IP Address Automatically

☐ Static IP Address

DNS Server

☒ Obtain DNS Info Automatically

☐ Use Following Static DNS Address

Routing Feature

NAT ☒

IGMP Proxy ☒

Apply as Default Gateway ☒

Fullcone NAT ☐

6RD ☐

DHCP Options

Request Options

☐ option 42 ☐ option 43

☐ option 120 ☐ option 121

Sent Options

☐ option 12

☐ option 60

Vendor ID

☐ option 61

IAID

DUID

☐ option 125

Cancel
Apply

The following table describes the labels in this screen.

Table 43 Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode)

LABEL	DESCRIPTION
General	
Click the switch to enable this WAN interface.	
Name	Specify a descriptive name for this connection. You can use up to 15 alphanumeric (0-9, a-z, A-Z) and special characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed. This field is read-only if you are editing the WAN interface.
Type	This field shows the types of available connections. This field is read-only if you are editing the WAN interface.
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. When you select VDSL over PTM or Ethernet , the choices are PPPoE and IPoE . When you select ADSL over ATM , the choices are PPPoE , IPoE , PPPoA and IPoA .
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 and PPPoE or PPPoA in the Encapsulation 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 through 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.
ATM PVC Configuration (This is available only when you select ADSL over ATM in the Type field.)	
VPI [0-255]	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI [32-65535]	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.

Table 43 Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
Encapsulation	Select the method of multiplexing used by your ISP from the drop-down list box. Choices are: • LLC/SNAP-BRIDGING: In LLC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. • VC/MUX: In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the Zyxel Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.
Service Category	Select UBR Without PCR for applications that are non-time sensitive, such as email. Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select Non Realtime VBR (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select Realtime VBR (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
Peak Cell Rate [cells/s]	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustainable Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size [cells]	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
VLAN Click this switch to enable VLAN on this WAN interface. This field is not available if you select ADSL over ATM in the Type field and PPPoA or IPoA in the Encapsulation field.	
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.
MTU (This is not available if you select ADSL over ATM in the Type field and PPPoA or IPoA in the Encapsulation field.)	
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.)	
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 or IPoA.
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.)	
Obtain DNS Info Automatically	Select Obtain DNS Info Automatically if you want the Zyxel Device to use the DNS server addresses assigned by your ISP.
Use Following Static DNS Address	Select Use Following Static DNS Address if you want the Zyxel Device to use the DNS server addresses you configure manually.

Table 43 Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
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 NAT on this connection.
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. 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 this WAN interface of this connection as the system default gateway.
Fullcone NAT	Click this switch to enable full cone NAT on this WAN connection. 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.
6RD The 6RD (IPv6 rapid deployment) fields display when you set the IPv6/IPv4 Mode field to IPv4 Only. See IPv6 Rapid Deployment for more information. Click this switch to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.	
Automatically configured by DHCP	The Automatically configured by DHCP option is configurable only when you set the method of encapsulation to IPoE .
Manually Configured	Select Manually Configured if you have the IPv4 address of the relay server. Otherwise, select Automatically configured by DHCP to have the Zyxel Device detect it automatically through DHCP.
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.
DHCP Options (This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field and IPoE in the Encapsulation field.) Note: The available DHCP options may differ by model.	
Request Options	Select Option 42 to have the Zyxel Device get NTP time server information from DHCP packets sent from the DHCP server. Select Option 43 to have the Zyxel Device get vendor specific information from DHCP packets sent from the DHCP server. Select Option 120 to have the Zyxel Device get static route information from DHCP packets sent from the DHCP server. Select Option 121 to have the Zyxel Device get SIP server information from DHCP packets sent from the DHCP server.

Table 43 Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
Sent Options	
option 12	To identify the Zyxel Device to the DHCP server, select this to automatically add the hostname of the Zyxel Device in the DHCP discovery packets that go to the DHCP server.
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.
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 interfaces. 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 checkbox 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 for more information. Click this switch to enable DS-Lite to let local computers use IPv4 through an ISP's IPv6 network.

Table 43 Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
Automatically configured by DHCP	Select this to have the Zyxel Device detect the relay server automatically through DHCP.
Manually Configured	Select Manually Configured if you have the IPv6 address of the relay server. Otherwise, select Automatically configured by DHCP to have the Zyxel Device detect it automatically through DHCP.
DS-Lite Relay Server IP	Specify the transition router's IPv6 address.
DHCPv6 Option (This is available only when you select IPv6 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
IPv6 Address From DHCPv6 Server	Click the switch to let the Zyxel Device send DHCP requests to the DHCPv6 server to obtain an IPv6 address.
Other Information From DHCPv6 Server	Click the switch to have the Zyxel Device get other information, such as DNS information, from DHCPv6 packets sent from the DHCPv6 server. This will be enabled if IPv6 Address From DHCPv6 Server is enabled.
IPv6 MAP	This is available when you edit an IPv6 WAN interface. Slide the switch to the right to create an IPv6 map domain.
Transport Mode	Select MAP-T (Translation) or MAP-E (Encapsulation) based on the ISP deployment.
Setting Mode	Select DHCP S46 or Manual to configure the following fields.
Note: The following Prefix/Address fields are used for the address mapping rule of MAP-T or MAP-E.	
BR IPv6 Prefix	This is the IPv6 network address/prefix assigned to the BR, including the prefix length.
Rule IPv6 Prefix	This is the IPv6 network prefix, including the prefix length.
Rule IPv4 Prefix	This is the IPv4 network prefix, including the prefix length.
Note: The following PSID fields are used for the port mapping rule of MAP-T or MAP-E.	
PSID Offset	The Port Set Identifier (PSID) offset specifies the excluded port range. The default PSID Offset is 6; port 0~1023 will be reserved for the system to use.
PSID Length	This specifies the number of sharing ratio. When PSID Length is set to 8, the ports will be separated and assigned for 2^8 MAP CEs to use.
PSID	A Port Set ID (PSID) identifies a set of ports assigned to a CE for mapping. PSID should be unique for each CE sharing the IPv4 address.
Cancel	Click Cancel to restore your 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 94 Network Setting > Broadband > Add or Edit New WAN Interface (Bridge Mode)

Edit WAN Interface

General ☒

Name: GPON

Type: Ethernet

Mode: Bridge

VLAN ☒

802.1p: 0

802.1q: 100 (0~4094)

MTU

MTU: 1500

Cancel **Apply**

The following table describes the fields in this screen.

Table 44 Network Setting > Broadband > Add or Edit New WAN Interface (Bridge Mode)

LABEL	DESCRIPTION
General	
Click this switch to enable the WAN interface.	
Name	Enter a service name of the connection. You can use up to 15 alphanumeric (0-9, a-z, A-Z) and special characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed. This field is read-only is you are editing the WAN interface.
Type	Select VDSL over PTM , ADSL over ATM or Ethernet as the WAN interface type. This field is read-only if you are editing the WAN interface.
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 ports.
VLAN	
Click this switch to enable VLAN on this WAN interface.	
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
MTU	
MTU	Enter the MTU (Maximum Transfer Unit) size for traffic through this connection.
Cancel	Click Cancel to exit this screen without saving any changes.
Apply	Click Apply to save your changes.

7.3 Broadband Settings for Ethernet, AON and PON Gateways

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.

Note: The differences of the broadband screens between Ethernet, AON and PON routers or gateways are the type of connections available.

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

Figure 95 Network Setting > Broadband (Ethernet Gateways)

Broadband

Broadband Cellular Backup

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.

+ Add New WAN Interface

#	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	Y	Y	

Figure 96 Network Setting > Broadband (AON and PON Gateways)

Broadband

Broadband Cellular Backup

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.

+ Add New WAN Interface

#	Name	Type	Mode	Encapsulation	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	GPON	PON	Routing	IPoE	N/A	N/A	Y	Y	Y	Y	Y	

The following table describes the labels in this screen.

Table 45 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 displays the type of connections available.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.

Table 45 Network Setting > Broadband (continued)

LABEL	DESCRIPTION
802.1p	This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays N/A when there is no priority level assigned.
802.1q	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays N/A when there is no VLAN ID number assigned.
IGMP Proxy	This shows whether the 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.

7.3.1 Add or 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 or 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 or IPv4 mode.

Figure 97 Network Setting > Broadband > Add or Edit New WAN Interface (Ethernet Gateways: Routing Mode)

<

Add New WAN Interface

General

Name

TypeEthernet

ModeRouting

EncapsulationIPoE

IPv4/IPv6 ModeIPv4 IPv6 DualStack

VLAN

802.1p0

802.1q(0~4094)

MTU

1500

IP Address

Obtain an IP Address Automatically

Static IP Address

DNS Server

Obtain DNS Info Automatically

Use Following Static DNS Address

Routing Feature

NATIGMP Proxy

Apply as Default GatewayFullcone NAT

DHCPv6 Option

Request Options

option 42

option 43

option 120

option 121

Sent Options

option 60

Vendor ID

option 61

IAID

DUID

option 125

IPv6 Address

Obtain an IPv6 Address Automatically

Static IPv6 Address

IPv6 DNS Server

Obtain IPv6 DNS Info Automatically

Use Following Static IPv6 DNS Address

IPv6 Routing Feature

MLD Proxy

Apply as Default Gateway

DHCPv6 Option

IPv6 Address From DHCPv6 Server

Other Information From DHCPv6 Server

Cancel

Apply

Figure 98 Network Setting > Broadband > Add or Edit New WAN Interface (PON Gateways: Routing Mode)

<

Edit WAN Interface

General

NameGPON

TypeGPON

ModeRouting

EncapsulationIPv6

IPv4/IPv6 ModeIPv4 IPv6 DualStack

VLAN

802.1p0

802.1q[0~4094]

MVLAN

MVLAN[1~4094]

MTU

MTU1500

IP Address

Obtain an IP Address Automatically

Static IP Address

DNS Server

Obtain DNS Info Automatically

Use Following Static DNS Address

Routing Feature

NATIGMP Proxy

Apply as Default GatewayFullcone NAT

DHCP Options

Request Options

option 42

option 43

option 120

option 121

Sent Options

option 12

option 60

Vendor ID

option 61

IAID

DUID

option 125

IPv6 Address

Obtain an IPv6 Address Automatically

Static IPv6 Address

IPv6 DNS Server

Obtain IPv6 DNS Info Automatically

Use Following Static IPv6 DNS Address

IPv6 Routing Feature

MLD Proxy

Apply as Default Gateway

DHCPv6 Option

IPv6 Address From DHCPv6 Server

Other Information From DHCPv6 Server

Cancel

Apply

The following table describes the labels in this screen.

Table 46 Network Setting > Broadband > Add or New WAN Interface Edit (Routing Mode)

LABEL	DESCRIPTION
General	Click this switch to enable the WAN interface.
Name	Specify a descriptive name for this connection. You can use up to 15 alphanumeric (0-9, a-z, A-Z) and special characters except ["], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed. This field is read-only is you are editing the WAN interface.
Type	This field shows Ethernet and indicates an Ethernet connection. This field is read-only is you are editing the WAN interface.
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 PPPoE in the Encapsulation 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 only available if you select On Demand in the PPP Connection Trigger field.
PPPoE Passthrough	This field is available when you select PPPoE encapsulation. In addition to the 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 through 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 0 to 4094) for traffic through this connection.
MTU	

Table 46 Network Setting > Broadband > Add or New WAN Interface Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
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.)	
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 Automatically 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.
DHCP 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.)	
Note: The available DHCP options may differ by model.	

Table 46 Network Setting > Broadband > Add or New WAN Interface Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
Request Options	Select Option 42 to have the Zyxel Device get NTP time server information from DHCP packets sent from the DHCP server. Select Option 43 to have the Zyxel Device get vendor specific information from DHCP packets sent from the DHCP server. Select Option 120 to have the Zyxel Device get static route information from DHCP packets sent from the DHCP server. Select Option 121 to have the Zyxel Device get SIP server information from DHCP packets sent from the DHCP server.
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.
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 interfaces. 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 checkbox 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.

Table 46 Network Setting > Broadband > Add or New WAN Interface Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
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 168 for more information. Click this switch to enable DS-Lite to let local computers use IPv4 through an ISP's IPv6 network.
DS-Lite Relay Server IP	Specify the transition router's IPv6 address.
6RD	The 6RD (IPv6 rapid deployment) fields display when you set the IPv6/IPv4 Mode field to IPv4 Only. See IPv6 Rapid Deployment for more information. Click this switch to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.
	Select Manually Configured if you have the IPv4 address of the relay server. Otherwise, select Automatically configured by DHCP to have the Zyxel Device detect it automatically through DHCP. The Automatically configured by DHCP 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.
DHCPv6 Option (This is available only when you select IPv6 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
IPv6 Address From DHCPv6 Server	Click the switch (to the right) to let the Zyxel Device send DHCP requests to the DHCPv6 server to obtain an IPv6 address.
Other Information From DHCPv6 Server	Click the switch (to the right) to have the Zyxel Device get other information, such as DNS information, from DHCPv6 packets sent from the DHCPv6 server. This will be enabled if IPv6 Address From DHCPv6 Server is enabled.
Cancel	Click Cancel to restore your 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 99 Network Setting > Broadband > Add or Edit New WAN Interface (Bridge Mode)

The screenshot shows the 'Edit WAN Interface' configuration screen. The title bar indicates 'Edit WAN Interface'. Below the title, there are two main panels. The left panel is titled 'General' and has a blue toggle switch turned on. It contains three fields: 'Name' with the value 'ETHWAN', 'Type' with the value 'Ethernet', and 'Mode' with a dropdown menu set to 'Bridge'. The right panel is titled 'VLAN' and has a grey toggle switch turned off. It contains three fields: '802.1p' with the value '0', '802.1q' which is empty, and 'MTU' with the value '1500'. At the bottom of the screen are two buttons: 'Cancel' and 'Apply'.

The following table describes the fields in this screen.

Table 47 Network Setting > Broadband > Add or Edit New WAN Interface (Bridge Mode)

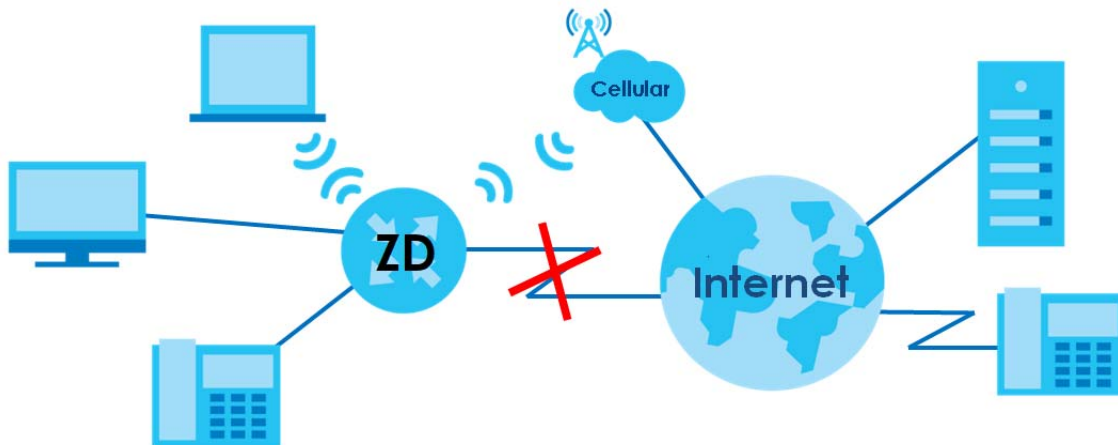
LABEL	DESCRIPTION
General	Click this switch to enable the interface.
Name	Enter a service name of the connection. You can use up to 15 alphanumeric (0-9, a-z, A-Z) and special characters except ["], ['], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed. This field is read-only is you are editing the WAN interface.
Type	This field shows Ethernet and indicates an Ethernet connection. This field is read-only is you are editing the WAN interface.
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 ports.
VLAN	Click this switch to enable VLAN on this WAN interface.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
Cancel	Click Cancel to exit this screen without saving any changes.
Apply	Click Apply to save your changes.

7.4 Cellular Backup

The USB port of the Zyxel Device allows you to attach a cellular dongle to wirelessly connect to a cellular network for Internet access. You can have the Zyxel Device use the cellular WAN connection as a backup to keep you online if the primary WAN connection fails for **Consecutive Fail** times. Consult your cellular service provider to configure the settings in this screen. Disconnect the Fiber port to use the cellular

dongle as your primary WAN connection, as the Zyxel Device automatically uses a wired WAN connection when available.

Figure 100 Internet Access Application: Cellular WAN



Use this screen to configure your cellular settings. Click **Network Setting > Broadband > Cellular Backup**.

The actual data rate you obtain varies depending on the cellular card you use, the signal strength to the service provider's base station, and so on.

Note: Entering a wrong PIN code three times will lock the SIM card in your cellular dongle.

Note: If you select **Drop** in the **Current Cellular Connection** field, the Zyxel Device will drop the cellular WAN connection when the **Time Budget** or **Data Budget** is reached. It may take some time for the cellular WAN connection to be disconnected when the **Time Budget** or **Data Budget** is reached.

Figure 101 Network Setting > Broadband > Cellular Backup

The USB port of the Zyxel Device allows you to attach a cellular dongle to wirelessly connect to a cellular network for Internet access. You can have the Zyxel Device use the cellular WAN connection as a backup to keep you online if the primary WAN connection fails for **Consecutive Fail** times. Consult your cellular service provider to configure the settings in this screen. Disconnect the DSL/Ethernet/Fiber WAN ports to use the cellular dongle as your primary WAN connection, as the Zyxel Device automatically uses a wired WAN connection when available.

General

Cellular Backup ☒

Ping Check ☒

Check Cycle Every (20~180 Sec)

Consecutive Fail (2~5 times)

☐ Ping Default Gateway

☒ Ping Host (Host name or IP address)

Cellular Connection Settings

Card Description N/A

Username (Optional)

Password  (Optional)

Authentication ▼

PIN (Optional) (Only for unlock PIN next time)

(PIN remaining authentication times)

Dial String

APN

Connection ▼

☒ Obtain an IP Address Automatically

☐ Use the Following Static IP Address

☒ Obtain DNS Info Dynamically

☐ Use the Following Static DNS IP Address

Enable e-mail Notification ☐

Note

Entering a wrong PIN code three times will lock the SIM card in your cellular dongle.



Figure 102 Network > Broadband > Cellular Backup (Budget Setup)

Budget Setup

Enable Budget Control ☒

☐ Time Budget hours per month

☐ Data Budget Mbytes per month

☐ Data Budget kPackets per month

Reset all budget counters on day of the month

Reset time and data budget counters

Actions before over budget

☐ Data Budget % of time budget

☐ Data Budget % of data budget (Mbytes)

☐ Data Budget % of data budget (Packets)

Actions when over budget

Current Cellular Connection

Actions

Enable e-mail Notification ☒

☐ Enable Log: Interval minutes

Note

If you select **Drop** in the **Current Cellular Connection** field, the will drop the Zyxel Device cellular WAN connection when the **Time Budget** or **Data Budget** is reached. It may take some time for the cellular WAN connection to be disconnected when the **Time Budget** or **Data Budget** is reached.

Cancel **Apply**

The following table describes the labels in this screen.

Table 48 Network Setting > Broadband > Cellular Backup

LABEL	DESCRIPTION
General	
Cellular Backup	Click this switch to have the Zyxel Device use the cellular connection as your WAN or a backup when the wired WAN connection fails.
Ping Check	Click this switch to ping check the connection status of your WAN. You can configure the frequency of the ping check and number of consecutive failures before triggering cellular backup.
Check Cycle	Enter the frequency of the ping check in this field.

Table 48 Network Setting > Broadband > Cellular Backup (continued)

LABEL	DESCRIPTION
Consecutive Fail	Enter how many consecutive failures are required before cellular backup is triggered.
Ping Default Gateway	Select this to have the Zyxel Device ping the WAN interface's default gateway IP address.
Ping Host	Select this to have the Zyxel Device ping the particular host name or IP address you typed in this field.
Cellular Connection Settings	
Card Description	This field displays the manufacturer and model name of your cellular card if you inserted one in the Zyxel Device. Otherwise, it displays N/A .
Username	Enter the user name (of up to 64 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces) given to you by your service provider.
Password	Enter the password (of up to 64 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces) associated with the user name above.
Authentication	The Zyxel Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Type Handshake Authentication Protocol). In PAP, peers identify themselves with a user name and password. In CHAP, additionally to user name and password the Zyxel Device sends regular challenges to make sure an intruder has not replaced a peer. CHAP is more secure than PAP; however, PAP is available on more platforms. Select an authentication protocol (Auto, CHAP or PAP). Contact your service provider for the correct authentication type.
PIN	A PIN (Personal Identification Number) code is a key to a cellular card. Without the PIN code, you cannot use the cellular card. If your ISP enabled PIN code authentication, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the cellular card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, leave this field blank.
Dial String	Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number. For example, *99# is the dial string to establish a GPRS or cellular connection in Taiwan.
APN	Enter the APN (Access Point Name) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 32 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed.
Connection	Select Nailed UP if you do not want the connection to time out. Select On Demand if you do not want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
Max Idle Timeout	This value specifies the time in minutes that elapses before the Zyxel Device automatically disconnects from the ISP.
Obtain an IP Address Automatically	Select this option if your ISP did not assign you a fixed IP address.
Use the Following Static IP Address	Select this option if the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected Use the following static IP address .
Subnet Mask	Enter the subnet mask of the IP address.
Obtain DNS Info Dynamically	Select this to have the Zyxel Device get the DNS server addresses from the ISP automatically.

Table 48 Network Setting > Broadband > Cellular Backup (continued)

LABEL	DESCRIPTION
Use the Following Static DNS IP Address	Select this to have the Zyxel Device 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.
Enable e-mail Notification	Select this to enable the email notification function. The Zyxel Device will email you a notification when the cellular connection is up.
Mail Account	Select an email address you have configured in Maintenance > E-mail Notification . The Zyxel Device uses the corresponding mail server to send notifications. You must have configured a mail server already in the Maintenance > E-mail Notification screen.
Cellular Backup e-mail Title	Enter a title that you want to be in the subject line of the email notifications that the Zyxel Device sends.
Send Notification to E-mail	Notifications are sent to the email address specified in this field. If this field is left blank, notifications cannot be sent through email.
Click this  to show the advanced cellular backup settings.	
Budget Setup	
Enable Budget Control	Click this switch to set a monthly limit for the user account of the installed cellular card. You can set a limit on the total traffic and/or call time. The Zyxel Device takes the actions you specified when a limit is exceeded during the month.
Time Budget	Select this and specify the amount of time (in hours) that the cellular connection can be used within one month. If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.
Data Budget (Mbytes)	Select this and specify how much downstream and/or upstream data (in Mega bytes) can be transmitted through the cellular connection within one month. Select Download/Upload to set a limit on the total traffic in both directions. Select Download to set a limit on the downstream traffic (from the ISP to the Zyxel Device). Select Upload to set a limit on the upstream traffic (from the Zyxel Device to the ISP). If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.
Data Budget (kPackets)	Select this and specify how much downstream and/or upstream data (in k Packets) can be transmitted through the cellular connection within one month. Select Download/Upload to set a limit on the total traffic in both directions. Select Download to set a limit on the downstream traffic (from the ISP to the Zyxel Device). Select Upload to set a limit on the upstream traffic (from the Zyxel Device to the ISP). If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.
Reset all budget counters on	Select the date on which the Zyxel Device resets the budget every month. Select last if you want the Zyxel Device to reset the budget on the last day of the month. Select specific and enter the number of the date you want the Zyxel Device to reset the budget.
Reset time and data budget counters	Click this button to reset the time and data budgets immediately. The count starts over with the cellular connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart; so if you configured the time and data budget counters to reset on the second day of the month and you use this button on the first, the time and data budget counters will still reset on the second.

Table 48 Network Setting > Broadband > Cellular Backup (continued)

LABEL	DESCRIPTION
Actions before over budget	Specify the actions the Zyxel Device takes before the time or data limit exceeds.
Data Budget % of time budget/data budget (Mbytes)/data budget (kPackets)	Select the checkboxes and enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.
Actions when over budget	Specify the actions the Zyxel Device takes when the time or data limit is exceeded.
Current Cellular Connection	Select Keep to maintain an existing cellular connection or Drop to disconnect it.
Actions	
Enable e-mail Notification	Click this switch to enable the email notification function. The Zyxel Device will email you a notification whenever over budget occurs.
Mail Account	Select an email address you have configured in Maintenance > E-mail Notification . The Zyxel Device uses the corresponding mail server to send notifications. You must have configured a mail server already in the Maintenance > E-mail Notification screen.
Cellular Backup e-mail Title	Enter a title that you want to be in the subject line of the email notifications that the Zyxel Device sends.
Send Notification to E-mail	Notifications are sent to the email address specified in this field. If this field is left blank, notifications cannot be sent through email.
Enable Log: Interval	Select this to and enter the Interval of how many minutes (1 – 9999) you want the Zyxel Device to email you.
Cancel	Click Cancel to discard any changes to the settings.
Apply	Click Apply to save your changes.

7.5 Broadband Advanced Screen for DSL Routers or Gateways

Use the **Advanced** screen to enable or disable ADSL over PTM, Annex M, DSL PhyR, and SRA (Seamless Rate Adaptation) functions. The Zyxel Device supports the PhyR retransmission scheme. PhyR is a retransmission scheme designed to provide protection against noise on the DSL line. It improves voice, video and data transmission resilience by utilizing a retransmission buffer. It also lists ITU-T G.993.2 standard VDSL profiles you can comply with.

ITU-T G.993.2 standard defines a wide range of settings for various parameters, some of which are encompassed in profiles as shown in the next table.

Note: This features is not available on all models. See [Overview](#) for more information.

Note: If the settings in the screen are changed, the Zyxel Device will re-establish the DSL connections.

Table 49 VDSL Profiles

PROFILE	BANDWIDTH (MHZ)	NUMBER OF DOWNSTREAM CARRIERS	CARRIER BANDWIDTH (KHZ)	POWER (DBM)	MAX. DOWNSTREAM THROUGHPUT (MBIT/S)
8a	8.832	2048	4.3125	17.5	50
8b	8.832	2048	4.3125	20.5	50
8c	8.5	1972	4.3125	11.5	50
8d	8.832	2048	4.3125	14.5	50
12a	12	2783	4.3125	14.5	68
12b	12	2783	4.3125	14.5	68
17a	17.664	4096	4.3125	14.5	100
35a	30.000	3479	4.3125	14.5	100
35b	35.328	8192	4.3125	17.0	300

Click **Network Setting > Broadband > Advanced** to display the following screen.

Figure 103 Network Setting > Broadband > Advanced

Broadband

Broadband Cellular Backup **Advanced**

Use the **Advanced** screen to enable or disable ADSL over PTM, Annex M, DSL PhyR, and SRA (Seamless Rate Adaptation) functions. The Zyxel Device supports the PhyR retransmission scheme. PhyR is a retransmission scheme designed to provide protection against noise on the DSL line. It improves voice, video and data transmission resilience by utilizing a retransmission buffer. It also lists ITU-T G.993.2 standard VDSL profiles you can comply with.

DSL Capabilities

PhyR US

☐

PhyR DS

☒

Bitswap

☒

SRA

☒

DSL Modulation

PTM over ADSL

☒

G.dmt

☒

G.lite

☒

T1.413

☒

ADSL2

☒

Annex L

☒

ADSL2+

☒

Annex M

☒

VDSL2

☒

VDSL Profile

8a Enable

☒

8b Enable

☒

8c Enable

☒

8d Enable

☒

12a Enable

☒

12b Enable

☒

17a Enable

☒

30a Enable

☐

35b Enable

☒

US0

☒

Cancel

Apply

The following table describes the labels in this screen.

Table 50 Network Setting > Broadband > Advanced

LABEL	DESCRIPTION
DSL Capabilities	
PhyR US	Enable or disable PhyR US (upstream) for upstream transmission to the WAN. PhyR US should be enabled if data being transmitted upstream is sensitive to noise. However, enabling PhyR US can decrease the US line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled.
PhyR DS	Enable or disable PhyR DS (downstream) for downstream transmission from the WAN. PhyR DS should be enabled if data being transmitted downstream is sensitive to noise. However, enabling PhyR DS can decrease the DS line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled.
PhyR US/DS	Enable or disable PhyR US/DS (upstream or downstream) for both upstream and downstream transmission to the WAN. PhyR US should be enabled if data being transmitted upstream is sensitive to noise. However, enabling PhyR US can decrease the US line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled.
Bitswap	Select Enable to allow the Zyxel Device to adapt to line changes when you are using G.dmt. Bit-swapping is a way of keeping the line more stable by constantly monitoring and redistributing bits between channels.
SRA	Enable or disable Seamless Rate Adaption (SRA). Select Enable to have the Zyxel Device automatically adjust the connection's data rate according to line conditions without interrupting service.
DSL Modulation	
PTM over ADSL	Select Enable to use PTM over ADSL. Since PTM has less overhead than ATM, some ISPs use this for better performance.
G.Dmt	ITU G.992.1 (better known as G.dmt) is an ITU standard for ADSL using discrete multitone modulation. G.dmt full-rate ADSL expands the usable bandwidth of existing copper telephone lines, delivering high-speed data communications at rates up to 8 Mbit/s downstream and 1.3 Mbit/s upstream.
G.lite	ITU G.992.2 (better known as G.lite) is an ITU standard for ADSL using discrete multitone modulation. G.lite does not strictly require the use of DSL filters, but like all variants of ADSL generally functions better with splitters.
T1.413	ANSI T1.413 is a technical standard that defines the requirements for the single asymmetric digital subscriber line (ADSL) for the interface between the telecommunications network and the customer installation in terms of their interaction and electrical characteristics.
ADSL2	It optionally extends the capability of basic ADSL in data rates to 12 Mbit/s downstream and, depending on Annex version, up to 3.5 Mbit/s upstream (with a mandatory capability of ADSL2 transceivers of 8 Mbit/s downstream and 800 kbit/s upstream).
Annex L	Annex L is an optional specification in the ITU-T ADSL2 recommendation G.992.3 titled Specific requirements for a Reach Extended ADSL2 (READSL2) system operating in the frequency band above POTS, therefore it is often referred to as Reach Extended ADSL2 or READSL2. The main difference between this specification and commonly deployed Annex A is the maximum distance that can be used. The power of the lower frequencies used for transmitting data is boosted up to increase the reach of this signal up to 7 kilometers (23,000 ft).
ADSL2+	ADSL2+ extends the capability of basic ADSL by doubling the number of downstream channels. The data rates can be as high as 24 Mbit/s downstream and up to 1.4 Mbit/s upstream depending on the distance from the DSLAM to the customer's premises.
Annex M	Annex M is an optional specification in ITU-T recommendations G.992.3 (ADSL2) and G.992.5 (ADSL2+), also referred to as ADSL2 M and ADSL2+ M. This specification extends the capability of commonly deployed Annex A by more than doubling the number of upstream bits. The data rates can be as high as 12 or 24 Mbit/s downstream and 3 Mbit/s upstream depending on the distance from the DSLAM to the customer's premises.

Table 50 Network Setting > Broadband > Advanced (continued)

LABEL	DESCRIPTION
Annex M/J	Annex M and Annex J are specified in ITU-T recommendations G.992.3 (ADSL2) and G.992.5 (ADSL2+). Annex M and Annex J enhance the capabilities of Annex A and Annex B by increasing the upstream transmission data rate, but slightly reduce the downstream data rates as a trade-off. Annex M supports data rates of up to 12 Mbit/s downstream and 3.5 Mbit/s upstream for ADSL2, and up to 24 Mbit/s downstream and 2.5 Mbit/s upstream for ADSL2+. Annex J supports data rates of up to 12 Mbit/s downstream and 3.5 Mbit/s upstream for ADSL2, and up to 24 Mbit/s downstream and 3.5 Mbit/s upstream for ADSL2+. However, the actual downstream or upstream data rates depend on the distance from the ISP DSLAM to the Zyxel Device and the quality of your telephone line. Click the switch to enable the Zyxel Device to use Annex M for Zyxel Device models that use POTS WAN connection, and use Annex J for Zyxel Device models that use ISDN WAN connection.
VDSL2	VDSL2 (Very High Speed Digital Subscriber Line 2) is the second generation of the VDSL standard (which is currently denoted VDSL1). VDSL2 allows a frequency band of up to 30MHz and transmission rates of up to 100 Mbps in each direction. VDSL2 is defined in G.993.2.
VDSL Profile	VDSL2 profiles differ in the width of the frequency band used to transmit the broadband signal. Profiles that use a wider frequency band can deliver higher maximum speeds.
8a, 8b, 8c, 8d, 12a, 12b, 17a, 30a, 35b US0	The G.993.2 VDSL standard defines a wide range of profiles that can be used in different VDSL deployment settings, such as in a central office, a street cabinet or a building. The Zyxel Device must comply with at least one profile specified in G.993.2. but compliance with more than one profile is allowed.
Cancel	Click Cancel to return to the previous configuration.
Apply	Click Apply to save your changes back to the Zyxel Device.

7.6 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 ATM (PPPoA)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The Zyxel Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

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, WiFi, 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.

RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

Multiplexing

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

VC-based Multiplexing

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

LLC-based Multiplexing

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

Traffic Shaping

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

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum

speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

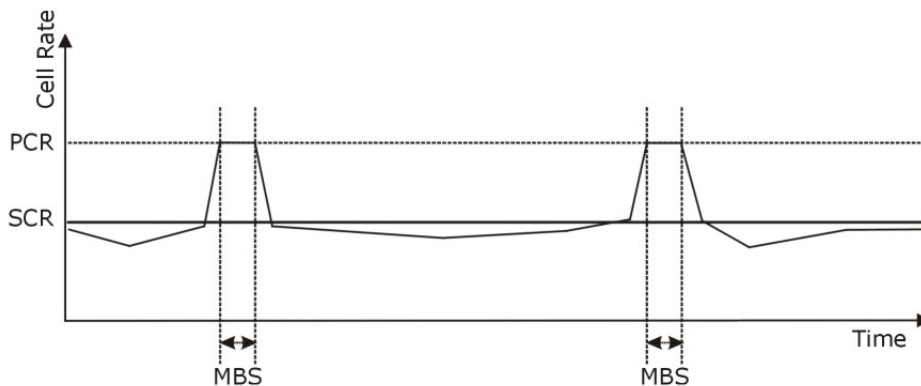
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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

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

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

Figure 104 Example of Traffic Shaping



ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (does not tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR

and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR does not guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

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 groups; 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.

CHAPTER 8

Wireless

8.1 Wireless Overview

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

8.1.1 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 WiFi connection.

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the WiFi security mode ([Wireless General Settings](#)).
- Use the **Guest/More AP** screen to set up multiple WiFi networks on your Zyxel Device ([Guest/More AP Screen](#)).
- [Guest/More AP Screen](#) Use the **MAC Authentication** screen to allow or deny WiFi clients based on their MAC addresses from connecting to the Zyxel Device ([MAC Authentication](#)).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) ([WPS](#)).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in WiFi networks for multimedia applications ([WMM](#)).
- Use the **Others** screen to configure WiFi advanced features, such as the RTS/CTS Threshold ([Others](#)).
- Use the **Channel Status** screen to scan the number of accessing points and view the results ([Channel Status](#)).
- Use the **MESH** screen to enable or disable Mesh on your Zyxel Device ([MESH](#)).

8.1.2 What You Need to Know

WiFi Standard / IEEE 802.11

IEEE 802.11 is a set of standards developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless local area networks (WLANs). These standards define how devices like laptops, smartphones, and routers communicate wirelessly using radio waves.

WiFi 6 / IEEE 802.11ax

WiFi 6 is backwards compatible with IEEE 802.11a/b/g/n/ac and is most suitable in areas with a high concentration of users. WiFi 6 devices support Target Wakeup Time (TWT) allowing them to automatically power down when they are inactive.

WiFi 6E (IEEE802.11ax – Extended Standard)

WiFi 6E is an extended standard of WiFi 6 (IEEE 802.11ax). WiFi 6E inherits all the WiFi 6 features and brings with an additional 6 GHz band. The 6 GHz band allows you to avoid possible congested traffic in the lower 2.4 GHz and 5 GHz bands. WiFi clients must support WiFi 6E to connect to the device using the 6 GHz band.

Note: Check your client device's product specification to see if your client device supports the 6 GHz band (WiFi 6E). If not, you should still use the 2.4/5 GHz bands for connection.

WiFi 7 (IEEE802.11be)

WiFi 7 (802.11be) is backwards compatible with WiFi 6 and WiFi 6E. WiFi 7 is a WiFi standard that supports 2.4 GHz, 5 GHz and 6 GHz frequency bands with the following improvements over WiFi 6 and WiFi 6E.

Table 51 WiFi 6, WiFi 6E and WiFi 7 Comparison

FEATURES		WiFi 6	WiFi 6E	WiFi 7
Theoretical Maximum Speed (Up-to)		9.6 Gbps		46 Gbps
Supported Frequency Bands		2.4 GHz/5 GHz	2.4 GHz/5 GHz/6 GHz	2.4 GHz/5 GHz/6 GHz
Supported Channel Bandwidth		20/40/80/160 MHz	20/40/80/160 MHz	20/40/80/160/320 MHz
Total Spectrum (Up-to)	2.4 GHz	80 MHz		80 MHz
	5 GHz	500 MHz		500 MHz
	6 GHz	Not supported.	1200 MHz	1200 MHz
Other Features (OFDMA/BSS Coloring/TWT/Two-Way MU-MIMO/Beamforming/1024-QAM)		The same (WiFi 6E inherits all the features from WiFi 6).		WiFi 7 inherits all the features from WiFi 6 and WiFi 6E, with the addition of multi-link operation and preamble puncturing.

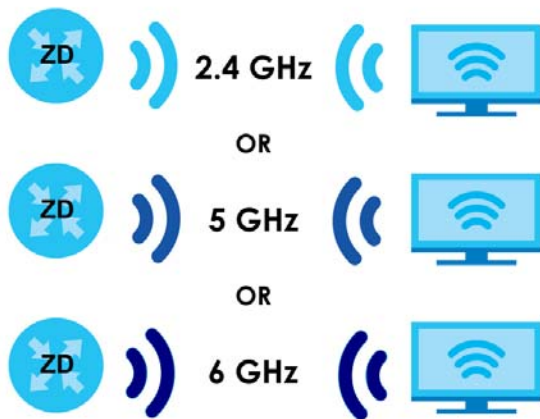
Faster Data Transmission

WiFi 7 allows faster data transmission using:

- 4096 QAM (Quadrature Amplitude Modulation) – enhances the amount of data transmitted over the available bandwidth.
- 320 MHz Channel Bandwidth – enlarges the supported channel bandwidth to 320 MHz, allowing higher data throughput.
- Multiple Resource Units (RUs) – allows an AP to allocate multiple RUs to a WiFi client.

Multi-Link Operation (MLO)

WiFi 7 MLO allows a WiFi client to connect to the Zyxel Device using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi 7 ideal for streaming 4K/8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games. Devices without MLO can only transmit data on one band at a time.

Figure 105 Without Multi-Link Operation

The Zyxel Device can support multiple frequency bands (2.4 GHz, 5 GHz and 6 GHz), but a WiFi client can only connect to the Zyxel Device using one of these frequency bands. The other frequency bands are unused. The client's data transmission speed depends on the frequency band they are connected to.

To use MLO, both the Zyxel Device and the WiFi client have to support MLO.

Figure 106 Multi-Link Operation Example

Finding Out More

See [Technical Reference](#) for advanced technical information on WiFi networks.

8.2 Wireless General Settings

Use this screen to enable the WiFi, enter the SSID and select the WiFi security mode. We recommend that you select **More Secure** to enable **WPA3-SAE** data encryption.

Note: If you are configuring the Zyxel Device from a computer connected by WiFi and you change the Zyxel Device's SSID, channel or security settings, you will lose your WiFi connection when you press **Apply**. You must change the WiFi settings of your computer to match the new settings on the Zyxel Device.

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

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

Note: For the Zyxel Device that supports 2.4 GHz and 5 GHz, **Keep the same settings for 2.4 GHz and 5 GHz, 6 GHz wireless networks** is enabled and cannot be disabled when you enable **Mesh** in the **Network > Wireless > MESH** screen. To see if your model supports 6 GHz, please see [Overview](#) for more information.

For the Zyxel Device that supports 2.4 GHz, 5 GHz, and 6 GHz, **Keep the same settings for 2.4 GHz, 5 GHz, and 6 GHz wireless networks** is enabled and cannot be disabled when you enable **Mesh** in the **Network > Wireless > MESH** screen. To see if your model supports 6 GHz, please see [Overview](#) for more information.

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

Figure 107 Network Setting > Wireless > General (for 2.4 GHz and 5 GHz models)

Wireless

General Guest/More AP MAC Authentication WPS WMM Others Channel Status MESH

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. We recommend that you select **More Secure** to enable **WPA3-SAE/WPA2-PSK** data encryption.

Wireless

Wireless ☐ Keep the same settings for 2.4GHz and 5GHz wireless networks ⓘ

Keep 2.4GHz and 5GHz the same cannot be turned off when MESH or MLO is active.

Note

To enable MLO, please enable **Keep the same setting for 2.4G and 5G WiFi networks**

MLO ☐

Wireless Network Setup

Band 2.4GHz

Wireless ☒

Channel Auto Current: 3 / 40 MHz

Bandwidth 20/40MHz

Control Sideband Upper

Wireless Network Settings

Wireless Network Name enel-WiFi_2A7C1E21

Max Clients 64

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

☒ Multicast Forwarding

Max. Upstream Bandwidth Kbps

Max. Downstream Bandwidth Kbps

Note

(1) If you are configuring the Zyxel Device from a computer connected by WIFI and you change the Zyxel Device's SSID, channel or security settings, you will lose your WIFI connection when you press **Apply**. You must change the WIFI settings of your computer to match the new settings on the Zyxel Device.

(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 FC:9F:2A:7C:1E:21

Security Level

No Security More Secure (Recommended)

⬇

Security Mode WPA3-SAE/WPA2-PSK

Protected Management Frames Capable

☐ Generate password automatically

The password and SSID must contain at least 8 alphanumeric characters and only the following special characters are allowed (<>| ^_~)

Password ***** ⓘ

Strength strong

Encryption AES

Timer 3600 sec

Cancel Apply

Figure 108 Network Setting > Wireless > General (for 2.4 GHz, 5 GHz, and 6 GHz models)

Wireless

General
Guest/More AP
MAC Authentication
WPS
WMM
Others
Channel Status

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. We recommend that you select **More Secure** to enable **WPA3-SAE/WPA2-PSK** data encryption.

Wireless

Wireless ☐ Keep the same settings for 2.4GHz, 5GHz and 6GHz wireless networks ⓘ
 Keep 2.4GHz, 5GHz and 6GHz the same cannot be turned off when MESH or MLO is active

Note
 To enable MLO, please enable **Keep the same setting for 2.4G, 5G and 6G WiFi networks** and make sure to select **802.11_ax/be Mixed** for **802.11 Mode** in **Wireless > Others: Band:2.4GHz/5GHz/6GHz**

MLO ☒

Wireless Network Setup

Band 2.4GHz ▼

Wireless ☒

Channel Auto ▼ Current: / MHz

Bandwidth 20/40MHz ▼

Control Sideband Lower

Wireless Network Settings

Wireless Network Name Zyxel_8181

Max Clients 64

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

☒ Multicast Forwarding

Max. Upstream Bandwidth Kbps

Max. Downstream Bandwidth Kbps

Note
 (1) If you are configuring the Zyxel Device from a computer connected by WIFI and you change the Zyxel Device's SSID, channel or security settings, you will lose your WIFI connection when you press **Apply**. You must change the WIFI settings of your computer to match the new settings on the Zyxel Device.
 (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 00:00:00:00:00:00

Security Level

**More Secure
(Recommended)**

Security Mode WPA3-SAE/WPA2-PSK

Protected Management Frames Capable

☒ Generate password automatically

The password must be at least 8 characters long, including 1 uppercase letter, 1 lowercase letter, 1 number and 1 special character.

Password ***** ⓘ

Strength medium

Cancel
Apply

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

Table 52 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless	
Wireless	For the Zyxel Device that supports 2.4 GHz and 5 GHz, select Keep the same settings for 2.4GHz and 5GHz wireless networks, and the 2.4 GHz and 5 GHz WiFi networks will use the same SSID and wireless security settings. For the Zyxel Device that supports 2.4 GHz, 5 GHz, and 6 GHz, select Keep the same settings for 2.4GHz, 5GHz and 6GHz wireless networks, and the 2.4 GHz, 5 GHz and 6 GHz WiFi networks will use the same SSID and wireless security settings. Note: To see if your model supports 6 GHz, please see Overview for more information. Note: "One SSID" means the 2.4 GHz, 5 GHz, and 6 GHz Wi-Fi bands use the same network name (SSID) and some security settings. If your Zyxel Devices supports only 2.4 GHz and 5 GHz, "One SSID" means the 2.4 GHz and 5 GHz Wi-Fi bands use the same network name (SSID) and some security settings. This allows Wi-Fi clients to seamlessly connect to either band depending on signal strength and Wi-Fi client specifications. If One SSID is disabled, the SSID and some security settings remain the same across all bands. You should assign different network names (SSIDs) to each band if you want to distinguish between the bands. However, band steering may not work properly unless a WiFi client connects to all supported bands already.
MLO	Select MLO to allow a WiFi 7 client to connect to the AP using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi 7 ideal for streaming 4K / 8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games. Note: To enable MLO, select Keep the same settings for 2.4GHz, 5GHz and 6GHz wireless networks. Note: To use MLO, both the AP and the WiFi client have to support MLO. Note: To see if your model supports 6 GHz, please see Overview for more information.
Wireless/WiFi Network Setup	
Band	This shows the WiFi band which this radio profile is using. 2.4GHz is the frequency used by IEEE 802.11b/g/n/ax WiFi clients, 5GHz is used by IEEE 802.11a/n/ac/ax WiFi clients. Note: To see if your model supports 6 GHz, please see Overview for more information.
Wireless/WiFi	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.

Table 52 Network Setting > Wireless > General (continued)

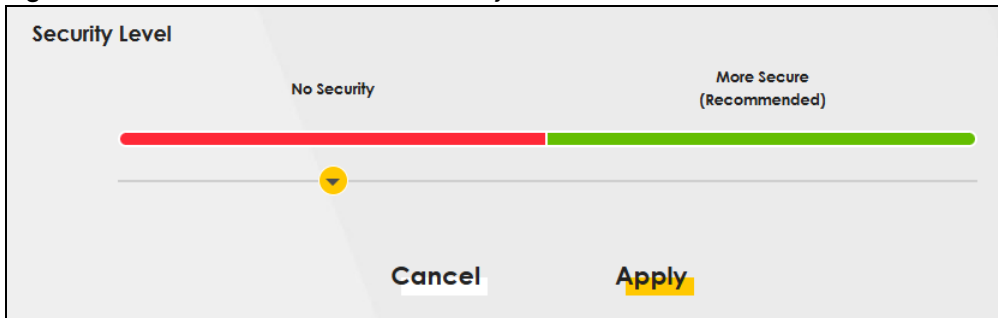
LABEL	DESCRIPTION
Bandwidth	A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The WiFi clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the WiFi 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 WiFi clients do not support channel bonding. Not all Zyxel Devices support all channels. The Zyxel Device will choose the best bandwidth available automatically depending on the radio you chose and network conditions.
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/WiFi Network Settings	
Wireless/WiFi 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 for this WiFi network. You can use up to 32 printable characters, including spaces.
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. This checkbox is grayed out if the WPS function is enabled in the Network Setting > Wireless > WPS screen.
Multicast Forwarding	Select this checkbox 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).
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 WiFi network. The WiFi clients want to associate to this network must have same WiFi security settings as the Zyxel Device. When you 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 your previously saved settings.
Apply	Click Apply to save your changes.

8.2.1 No Security

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

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

Figure 109 Wireless > General: No Security



The following table describes the labels in this screen.

Table 53 Wireless > General: No Security

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

8.2.2 More Secure (Recommended)

The WPA-PSK (WiFi Protected Access-Pre-Shared Key) security mode provides both improved data encryption and user authentication over WEP. Using a pre-shared key, 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 more robust version of the WPA encryption standard. It offers better security, although the use of PSK makes it less robust than it could be.

The WPA3-SAE (Simultaneous Authentication of Equals handshake) security mode protects against dictionary attacks (password guessing attempts). It improves security by requiring a new encryption key every time a WPA3 connection is made. A handshake is the communication between the Zyxel Device and a connecting client at the beginning of a WiFi session.

Click **Network Setting > Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA3-SAE** from the **Security Mode** list if your WiFi client supports it. If you are not sure, select **WPA3-SAE/WPA2-PSK** or **WPA2-PSK**.

Figure 110 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK

Security Level

No Security More Secure (Recommended)

Security Mode: WPA3-SAE/WPA2-PSK

Protected Management Frames: Capable

☒ Generate password automatically

The password must be at least 8 characters long, including 1 uppercase letter, 1 lowercase letter, 1 number and 1 special character.

Password: [masked] 👁

Strength: [medium]

Encryption: AES

Timer: 3600 sec

Cancel **Apply**

The following table describes the labels in this screen.

Table 54 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select More Secure to enable data encryption.
Security Mode	Select a security mode from the drop-down list box.
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 present WiFi DoS (Denial of Service) attacks. Select Disable if you do not want to use MFP. Select Capable to encrypt management frames of WiFi clients that support MFP. Clients that do not support MFP will still be allowed to join the WiFi network, but remain unprotected. Select Required to allow only clients that support MFP to join the WiFi network. When Mesh is enabled, the settings of Protected Management Frames of 5G will follow 2.4G.
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.

Table 54 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK (continued)

LABEL	DESCRIPTION
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. The password must be at least 8 characters long, including one uppercase letter, one lowercase letter, one number, and one special character. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. Note: More than 63 hexadecimal characters are not accepted for WPS. 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.
Strength	This displays the current password strength – weak , medium , strong .
Click this  to show more fields in this section. Click this  to hide them.	
Encryption	AES is the default data encryption type, which uses a 128-bit key. Select the encryption type (AES or TKIP+AES) for data encryption. Select AES if your WiFi clients can all use AES. Select TKIP+AES to allow the WiFi clients to use either TKIP or AES. Note: Not all models support TKIP+AES encryption.
Timer	This is the rate at which the RADIUS server sends a new group key out to all clients.

8.3 Guest/More AP Screen

Use this screen to configure a guest WiFi network that allows access to the Internet through the Zyxel Device. You can use one access point to provide several BSSs simultaneously. You can then assign varying security types to different SSIDs. WiFi clients can use different SSIDs to associate with the same access point.

Click **Network Setting > Wireless > Guest/More AP**.

The following table introduces the supported WiFi networks.

Table 55 Supported WiFi Networks

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

The following screen displays.

Figure 111 Network Setting > Wireless > Guest/More AP

Band		2.4GHz ▼			
#	Status	SSID	Security	Guest WLAN	Modify
1		ZyxeL_CFC1_guest1	WPA2-Personal	External Guest	
2		ZyxeL_CFC1_guest2	WPA2-Personal	External Guest	
3		ZyxeL_CFC1_guest3	WPA2-Personal	External Guest	

The following table describes the labels in this screen.

Table 56 Network Setting > Wireless > Guest/More AP

LABEL	DESCRIPTION
Band	For the Zyxel Device that supports 2.4 GHz and 5 GHz, select a 2.4GHz or 5GHz frequency band to display the SSID profile of the selected band. For the Zyxel Device that supports 2.4 GHz, 5 GHz, and 6 GHz, select a 2.4GHz , 5GHz , or 6GHz frequency band to display the SSID profile of the selected band.
#	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.
Security	This field indicates the security mode of the SSID profile.
Guest WLAN	This displays if the guest WLAN function has been enabled for this WLAN. A Home Guest can access the Internet, LAN wired devices connected to the Zyxel Device, and other Home Guest WiFi clients. An External Guest can just access the Internet through the Zyxel Device. N/A displays if guest WLAN is disabled.
Modify	Click the Edit icon of an SSID profile to configure the SSID profile.

8.3.1 The Edit More AP Screen

Use this screen to create Guest and additional WiFi 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 WiFi performance.

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

Figure 112 Network Setting > Wireless > Guest/More AP > Edit

More AP Edit

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

Wireless Network Setup

Wireless

Wireless Network Settings

Wireless Network Name

Zyxel_CFC1_guest1

☐

Hide SSID

☒

Guest WLAN

Access Scenario

External Guest

Max. Upstream Bandwidth

Kbps

Max. Downstream Bandwidth

Kbps

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.

BSSID

00:00:00:00:00:00

SSID Subnet

Security Level

No Security

More Secure
(Recommended)

Security Mode

WPA3-SAE/WPA2-PSK

Protected Management Frames

Capable

☒

Generate password automatically

The password must be at least 8 characters long, including 1 uppercase letter, 1 lowercase letter, 1 number and 1 special character.

Password

Strength

medium

Encryption

AES

Timer

3600

sec

Cancel

OK

The following table describes the fields in this screen.

Table 57 Network Setting > Wireless > Guest/More AP > Edit

LABEL	DESCRIPTION
WiFi/Wireless Network Setup	
WiFi/Wireless	Click this switch to enable or disable the WiFi in this field. When the switch turns blue  , the function is enabled; otherwise, it is not.
WiFi/Wireless Network Settings	
WiFi/Wireless Network Name	The SSID (Service Set Identifier) 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 for the WiFi. You can use up to 32 printable characters, including spaces.
Hide SSID	Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Guest WLAN	Select this to create Guest WLANs for home and external clients. Select the WLAN type in the Access Scenario field.
Access Scenario	Select Home Guest or External Guest to provide different levels of access to the Zyxel Device and the other WiFi clients. A Home Guest can access the Internet, LAN wired devices connected to the Zyxel Device, and other Home Guest WiFi clients. An External Guest can just access the Internet through the Zyxel Device.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the WiFi 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 WiFi clients. This option cannot be used if Keep 2.4G and 5G wireless network name the same is enabled in Network > 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 WiFi 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	
Security Mode	Select More Secure (Recommended) to add security on this WiFi network. The WiFi clients which want to associate to this network must have the same WiFi 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 No Security for more details about this field.

Table 57 Network Setting > Wireless > Guest/More AP > Edit (continued)

LABEL	DESCRIPTION
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 WiFi DoS (Denial of Service) attacks. Select Disable if you do not want to use MFP. Select Capable to encrypt management frames of WiFi clients that support MFP. Clients that do not support MFP will still be allowed to join the WiFi network, but remain unprotected. Select Required to allow only clients that support MFP to join the WiFi network. When Mesh is enabled, the settings of Protected Management Frames of 5G will follow 2.4G.
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. 1. If you did not select Generate password automatically, you can manually enter a pre-shared key at least 8 characters long, including one uppercase letter, one lowercase letter, one number, and one special character. Click the Eye icon to show or hide the password of your WiFi network. When the Eye icon is slashed , you will see the password in plain text. Otherwise, it is hidden.
Strength	This displays the current password strength – weak, medium, strong .
Click this  to show more fields in this section. Click again to hide them.	
Encryption	Select the encryption type (AES or TKIP+AES) for data encryption. Select AES if your WiFi clients can all use AES. Select TKIP+AES to allow the WiFi clients to use either TKIP or AES. Not all models support the TKIP+AES option.
Timer	The Timer is the rate at which the RADIUS server sends a new group key out to all clients.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

8.4 MAC Authentication

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

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

Note: This screen is not available when Mesh is enabled in the **Network Setting > Wireless > MESH** screen.

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 113 Network Setting> Wireless > MAC Authentication

Use this screen to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the Zyxel Device (**Deny**) based on the MAC address of each device. 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.

General

Band

2.4GHz

SSID

Zyxel_E1EB

MAC Restrict Mode

☒ Disable ☐ Deny ☐ Allow

MAC address List

Add new MAC address

#	MAC Address	Modify
---	-------------	--------

Cancel

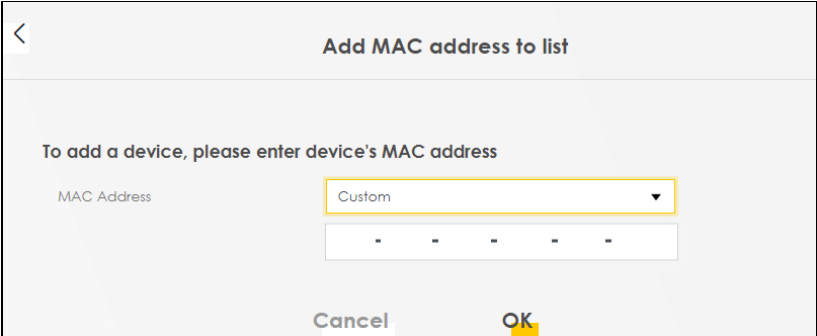
Apply

The following table describes the labels in this screen.

Table 58 Network Setting > Wireless > MAC Authentication

LABEL	DESCRIPTION
General	
Band	For Zyxel Device supports 2.4 GHz and 5 GHz, select a 2.4GHz or 5GHz frequency band to display associated WiFi devices in the selected band, identified by MAC address. For Zyxel Device supports 2.4 GHz, 5 GHz, and 6 GHz, select a 2.4GHz , 5GHz , or 6GHz frequency band to display associated WiFi devices in the selected band, identified by MAC address.
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the MAC Address table. Select Disable to turn off MAC filtering. Select Deny to block access to the 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	

Table 58 Network Setting > Wireless > MAC Authentication (continued)

LABEL	DESCRIPTION
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. Select an existing WiFi client from the list to add as a new entry. Select Custom if you want to manually enter the Host Name and MAC Address. Enter the MAC addresses of the 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. 
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the 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 exit this screen without saving.
Apply	Click Apply to save your changes.

8.5 WPS

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

WiFi Protected Setup (WPS) allows you to quickly set up a WiFi network with strong security, without having to configure security settings manually. Select one of the WPS methods and follow the instructions to establish a WPS connection. Your WiFi devices must support WPS to use this feature. We recommend using Push Button Configuration (**PBC**) if your WiFi device supports it.

Note: The Zyxel Device applies the security settings of the main SSID (**SSID1**) profile to the WPS wireless connection (see [More Secure \(Recommended\)](#)). Some models support more than one SSID profile, check the supported number on the **Network Setting > Wireless > General** screen.

Note: The WPS switch is unavailable if the WiFi is disabled.
If WPS is enabled, UPnP will automatically be turned on.

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

Figure 114 Network Setting > Wireless > WPS

WiFi Protected Setup (WPS) allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Select one of the WPS methods and follow the instructions to establish a WPS connection. Your device must support WPS to use this feature. We recommend using Push Button Configuration (**PBC**) if your device supports it.

General

Band

2.4GHz

WPS

Add a new device with WPS Method

Method 1 PBC

Step1.Click WPS button

WPS

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

Method 2 PIN

Step1.Enter the PIN of your new wireless client device and then click Register

Register

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

Method 3

Enter AP's PIN Number in wireless Client

Current state Configured

1. Please release configuration if you want to configure the wireless settings

Release Configuration

2. Enter current PIN number on your wireless client

Generate New PIN

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 to the WPS wireless connection.

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

Cancel

Apply

The following table describes the labels in this screen.

Table 59 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
General	
Band	For Zyxel Device that supports 2.4 GHz and 5 GHz, select a 2.4GHz or 5GHz frequency band to enable WPS for all WiFi networks in the selected band. For Zyxel Device that supports 2.4 GHz, 5 GHz, and 6 GHz, select a 2.4GHz , 5GHz , or 6GHz frequency band to enable WPS for all WiFi networks in the selected band. If you use the WPS button on the Zyxel Device ports panel, WPS is automatically enabled on both 2.4 GHz and 5 GHz bands. See Ports Panel for more information about the WPS button.
WPS	Slide this to the right to enable and have the Zyxel Device activate WPS. Otherwise, it is disabled.
Add a new device with WPS Method	
Method 1 PBC	Use this section to set up a WPS 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.

DE/EE/PE Series User's Guide

220

Table 59 Network Setting > Wireless > WPS (continued)

LABEL	DESCRIPTION
WPS	Click this button to add another WPS-enabled device (within range of the Zyxel Device) to your network. This button may either be a physical button on the outside of a WiFi device, or a menu button similar to the WPS button on this screen. Note: You must press the other device's WPS button within 2 minutes of pressing this button.
Method 2 PIN	Use this section to set up a WPS network by entering the PIN of the client into the Zyxel Device. Click this switch to make it turn blue. Click Apply to activate WPS method 2 on the Zyxel Device.
Register	Enter the PIN of the WiFi device that you are setting up a WPS connection with and click Register to authenticate and add the device to your network. You can find the PIN either on the outside of the WiFi device, or by checking the WiFi device's settings. Note: You must also activate WPS on that WiFi device within 2 minutes to have it present its PIN to the Zyxel Device.
Method 3	Use this section to set up a WPS network by entering the PIN of the Zyxel Device into the client. Click this switch to make it turn blue. Click Apply to activate WPS method 3 on the Zyxel Device.
Release Configuration	The default WPS status is configured . Click this button to remove all configured and security settings for WPS connections on the Zyxel Device.
Generate New PIN	If this method has been enabled, the PIN (Personal Identification Number) of the Zyxel Device is shown here. Enter this PIN in the configuration utility of the WiFi device you want to connect to using WPS. The PIN is not necessary when you use the WPS push-button method. Click the Generate New PIN button to have the Zyxel Device create a new PIN.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

8.6 WMM

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

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

Figure 115 Network Setting > Wireless > WMM

Use this screen to enable Wi-Fi 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 video, to run more smoothly.

Band: 2.4GHz

WMM of SSID1: ☐

WMM of SSID2: ☐

WMM of SSID3: ☐

WMM of SSID4: ☐

WMM Automatic Power Save Delivery (APSD): ☒

Note
(1) WMM cannot be disabled if 802.11 mode includes 802.11n or 802.11ac.

Cancel Apply

Note: **WMM** cannot be disabled if 802.11 mode includes 802.11n or 802.11ac.

Note: APSD only affects SSID1. For SSID2 to SSID4, APSD is always enabled.

Note: This screen is not available when Mesh is enabled in the **Network Setting > Wireless > MESH** screen.

The following table describes the labels in this screen.

Table 60 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
Band	For Zyxel Device supports 2.4 GHz and 5 GHz, select a 2.4GHz or 5GHz frequency band to enable or disable the WMM of SSID of the selected band. For Zyxel Device supports 2.4 GHz, 5 GHz, and 6 GHz, select a 2.4GHz , 5GHz , or 6GHz frequency band to enable or disable the WMM of SSID of the selected band.
WMM of SSID	Select On to have the Zyxel Device automatically give the network (SSIDx) a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (MultiMedia Quality of Service) gives high priority to video, which makes them run more smoothly. SSID1 is the General WiFi SSID; SSID2 to SSID4 are the Guest WiFi SSIDs. 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 device to which the Zyxel Device is connected also supports this feature.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

8.7 Others

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

Note: This screen is not available when Mesh is enabled in the **Network Setting > Wireless > MESH** screen.

See [Additional WiFi Terms](#) for detailed definitions of the terms listed here.

Figure 116 Network Setting > Wireless > Others

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

Band	2.4GHz	
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	

Cancel Apply

The following table describes the labels in this screen.

Table 61 Network Setting > Wireless > Others

LABEL	DESCRIPTION
Band	For Zyxel Device supports 2.4 GHz and 5 GHz, select a 2.4GHz or 5GHz frequency band to display the following wireless settings for the selected band. For Zyxel Device supports 2.4 GHz, 5 GHz, or 6 GHz, select a 2.4GHz, 5GHz, or 6GHz frequency band to display the following wireless settings for the selected band.
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.

Table 61 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
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. - Select 802.11b/g/n/ax/be Mixed to allow IEEE 802.11b, IEEE 802.11g, IEEE 802.11n IEEE 802.11ax or 802.11be compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. If the WiFi device isn't compatible with 802.11be, the Zyxel Device will communicate with the WiFi device using 802.11ax, and so on. For 5 GHz / 6 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. - Select 802.11a/n/ac/ax/be Mixed to allow IEEE 802.11a, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax or IEEE 802.11be compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. If the WiFi device isn't compatible with 802.11be, the Zyxel Device will communicate with the WiFi device using 802.11ax, and so on. Note: To see if your model supports 6 GHz, please see Overview for more information.
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.

Table 61 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
Preamble	Select a preamble type from the drop-down list box. Choices are Long or Short . See Preamble Type for more information. This field is configurable only when you set 802.11 Mode to 802.11b .
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

8.8 Channel Status

Use this screen to scan for WiFi channel noise and view the results. Click **Scan** to start, and then view the results in the **Channel Scan Result** section. The value on each channel number indicates the number of Access Points (AP) using that channel. The Auto-channel-selection algorithm does not always directly follow the AP count; other factors about the channels are also considered. Click **Network Setting > Wireless > Channel Status**. The screen appears as shown.

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 to 140). If you want to run channel scan, please select a non-DFS channel and try again.' appears.

Note: The AP count may not be a real-time value.

Figure 117 Network Setting > Wireless > Channel Status

The following table describes the labels in this screen.

Table 62 Network Setting > Wireless > Channel Status

LABEL	DESCRIPTION
Channel Monitor	
Wireless Network Setup	
Band	For Zyxel Device supports 2.4 GHz and 5 GHz, select a 2.4 GHz or 5 GHz frequency band on which you want to conduct a channel scan. For Zyxel Device supports 2.4 GHz, 5 GHz, and 6 GHz, select a 2.4 GHz, 5 GHz or 6 GHz frequency band on which you want to conduct a channel scan.

Table 62 Network Setting > Wireless > Channel Status (continued)

LABEL	DESCRIPTION
Scan wireless LAN Channels	Click the Scan button to scan WiFi channels.
Channel Scan Result	This displays the results of the channel scan. The blue bar displays the number of access points (AP count) in the WiFi channel. The orange bar displays the WiFi channel that the Zyxel Device is now using.

8.9 MESH

The Zyxel Device supports Mesh to manage your WiFi network. Mesh is the Zyxel implantation of WiFi-Alliance Easy Mesh. It supports AP steering, band steering, auto-configuration and other advances for your WiFi network.

The Zyxel Device can function as a controller to automatically configure WiFi settings on extenders in the network as well as optimize bandwidth usage.

The Zyxel Device optimizes bandwidth usage by directing WiFi clients to an extender (AP steering) or a 2.4 GHz or 5 GHz band (band steering) that is less busy.

See [Ways to Manage the Zyxel Device](#) for the complete tutorials with the MPro Mesh app or Zyxel One app.

- Setting up your Mesh network with the Zyxel Device and an Mesh extender,
- setting up your general/guest WiFi,
- basic configurations.

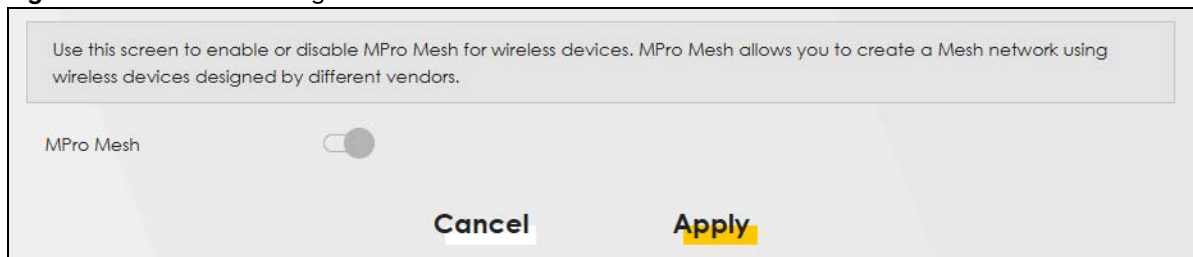
8.9.1 MPro Mesh

Use this screen to enable or disable the Mesh on the Zyxel Device.

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

Note: When MPro Mesh is enabled, the SSID and WiFi password of the main 2.4 GHz WiFi network will be copied to the main 5 GHz WiFi network.

Figure 118 Network Setting > Wireless > MESH



The following table describes the labels in this screen.

Table 63 Network Setting > Wireless > MESH

LABEL	DESCRIPTION
MPro Mesh	Click the button (to the right) to enable the Mesh feature on the Zyxel Device and set up your Mesh network.

8.10 Technical Reference

This section discusses WiFi in depth.

8.10.1 WiFi Network Overview

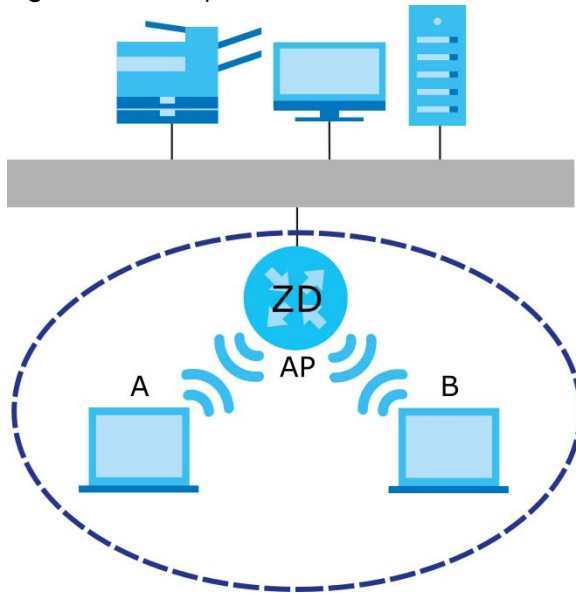
WiFi networks consist of WiFi clients, access points and bridges.

- A WiFi 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 WiFi clients and let them access the network.
- A bridge is a radio that relays communications between access points and WiFi clients, extending a network's range.

Normally, a WiFi network operates in an "infrastructure" type of network. An "infrastructure" type of network has one or more access points and one or more WiFi clients. The WiFi clients connect to the access points.

The following figure provides an example of a WiFi network.

Figure 119 Example of a WiFi Network



The WiFi network is the part in the blue circle. In this WiFi 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 WiFi network must follow these basic guidelines.

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

The SSID is the name of the WiFi network. It stands for Service Set Identifier.

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

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

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

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

8.10.2 Additional WiFi Terms

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

Table 64 Additional Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a network which covers a large area, 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 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 devices never have to get permission to send information to the Zyxel Device.
Preamble	A preamble affects the timing in your network. There are two preamble modes: long and short. If a WiFi 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 device is allowed to use the 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.

8.10.3 WiFi Security Overview

By their nature, radio communications are simple to intercept. For WiFi data networks, this means that anyone within range of a WiFi 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 WiFi data network, or understand the data carried on it.

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

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them

properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess – for example, a twenty-letter long string of apparently random numbers and letters – but it is not very secure if you use a short key which is very easy to guess – for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it is not just people who have sensitive information on their network who should use security. Everybody who uses any WiFi 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 WiFi security you can set up in the WiFi network.

8.10.3.1 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 WiFi devices to get the SSID. In addition, unauthorized WiFi devices can still see the information that is sent in the WiFi network.

8.10.3.2 MAC Address Filter

Every device that can use a WiFi network has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each WiFi device in the WiFi network, see the WiFi 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 WiFi network. If a WiFi device is allowed to use the WiFi network, it still has to have the correct information (SSID, channel, and security). If a WiFi device is not allowed to use the WiFi 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 WiFi network. Furthermore, there are ways for unauthorized WiFi devices to get the MAC address of an authorized WiFi device. Then, they can use that MAC address to use the WiFi network.

8.10.3.3 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See [Encryption](#) for information about this.)

-
1. Some devices, such as scanners, can detect networks but cannot use 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.

Table 65 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
	WPA-PSK	WPA2
	WPA2	
Strongest	WPA3-SAE	WPA3 (server certificate validation)

For example, if the WiFi network has a RADIUS server, you can choose **WPA**, **WPA2**, or **WPA3**. If users do not log in to the WiFi network, you can choose no encryption, **WPA2-PSK**, or **WPA3-SAE**.

Note: It is recommended that WiFi networks use **WPA3-SAE**, **WPA2-PSK**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized WiFi devices to figure out the original information pretty quickly.

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

8.10.4 Signal Problems

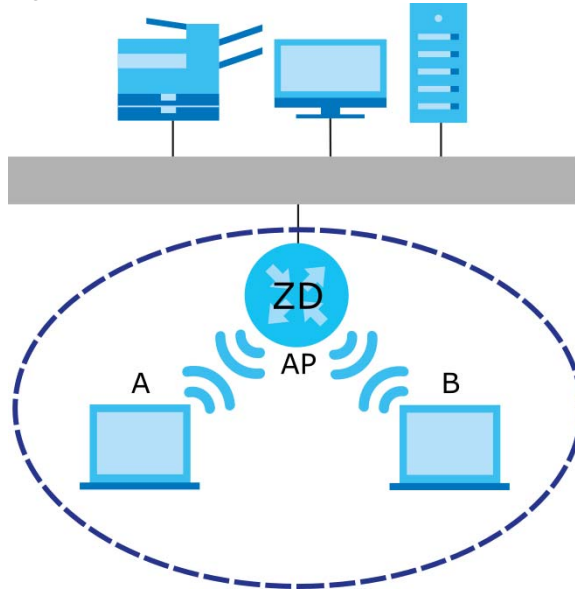
Because WiFi networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

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

8.10.5 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations 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 120 Basic Service Set

8.10.6 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.

8.10.6.1 Notes on Multiple BSSs

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

8.10.7 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 WiFi adapters support long preamble, but not all support short preamble.

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

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

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

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

8.10.8 WiFi Protected Setup (WPS)

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

WPS allows you to quickly set up a WiFi 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 2 minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

8.10.8.1 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 WiFi 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).
- 3 Press the button on one of the devices (it does not matter which). For the Zyxel Device you must press the **WiFi** button for more than 5 seconds.
- 4 Within 2 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.

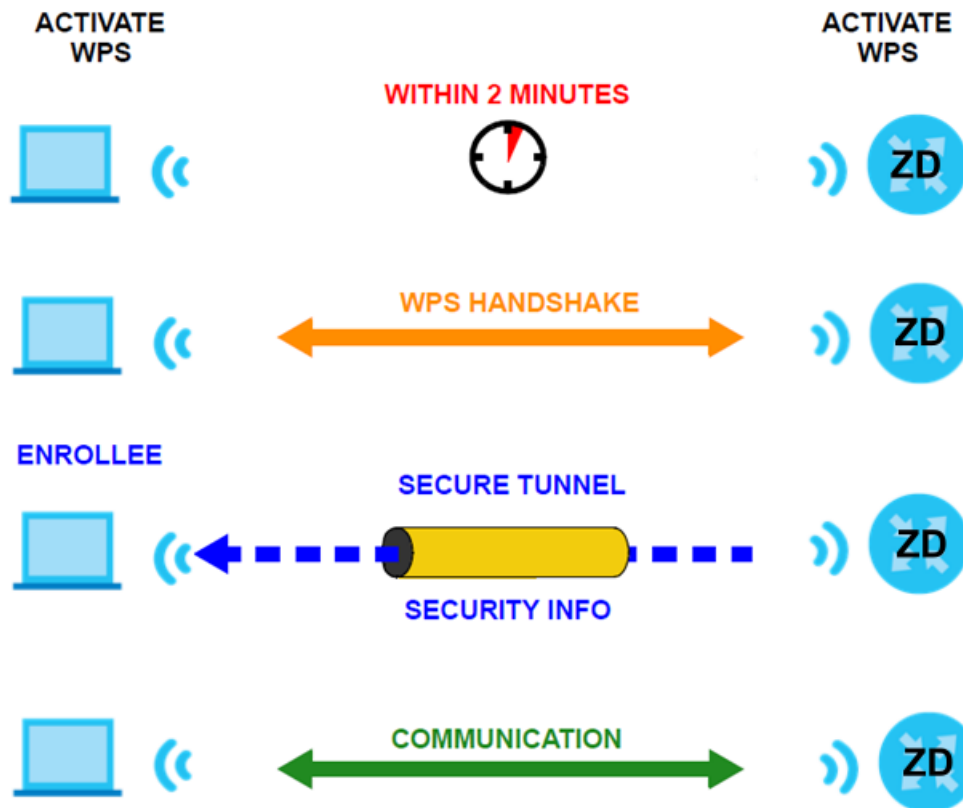
If you need to make sure that WPS worked, check the list of associated WiFi clients in the AP's configuration utility. If you see the WiFi client in the list, WPS was successful.

8.10.8.2 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings). The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the 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 121 How WPS Works



The roles of registrar and enrollee last only as long as the WPS setup process is active (2 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 WiFi client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled WiFi clients.

By default, a WPS device is 'un-configured'. 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 un-configured, 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 WiFi 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.

8.10.8.3 Example WPS Network Setup

This section shows how security settings are distributed in a sample WPS setup.

The following figure shows a sample network. In step 1, both **AP1** and **Client 1** are un-configured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is

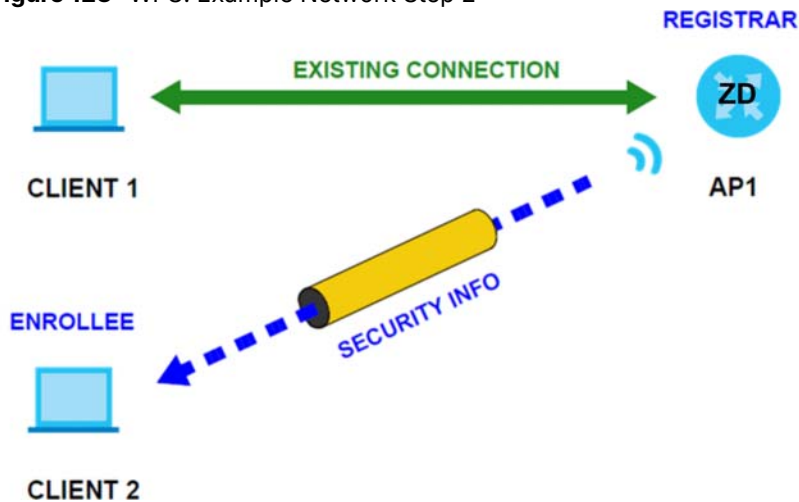
the enrollee. The registrar randomly generates the security information to set up the network, since it is un-configured and has no existing information.

Figure 122 WPS: Example Network Step 1

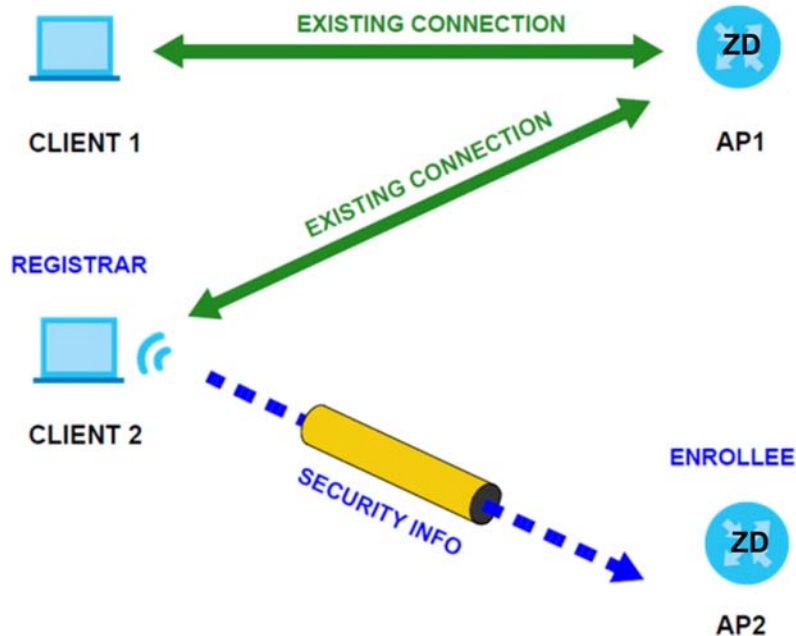


In step 2, you add another WiFi client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar,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

Figure 123 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 124 WPS: Example Network Step 3

8.10.8.4 Limitations of WPS

WPS has some limitations of which you should be aware.

- 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 was 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 only works simultaneously between two devices, 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 WiFi 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 9

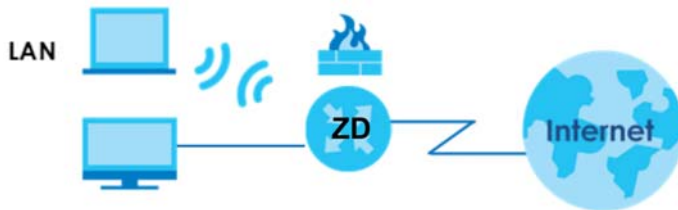
Home Networking

9.1 Home Networking Overview

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

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

Figure 125 Home Networking Example



9.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings ([LAN Setup](#)).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC addresses ([Static DHCP](#)).
- Use the **UPnP** screen to enable UPnP ([UPnP](#)).
- Use the **Additional Subnet** screen to configure IP alias and public static IP ([the LAN Additional Subnet section](#)).
- 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 ([STB Vendor ID](#)).
- Use the **APAS** screen to allow incoming traffic from any port to access any service on a LAN device ([Section 9.9 on page 251](#)).

9.1.2 What You Need To Know

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

9.1.2.1 About LAN

IP Address

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. This is known as an Internet Protocol address.

Subnet Mask

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.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server. This Zyxel Device has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DNS

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.

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.

9.1.2.2 About UPnP

How do I know if I am using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows 7). 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.

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).

See [Turn on UPnP in Windows 10 Example](#) for examples on installing and using UPnP.

9.1.3 Before You Begin

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

9.2 LAN Setup

A LAN IP address is the IP address of a networking device in the LAN. You can use the Zyxel Device's LAN IP address to access its Web Configurator from the LAN. The DHCP server settings define the rules on assigning IP addresses to LAN clients on your network.

Use this screen to set the Local Area Network 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 Select the **Interface Group** you want to set up the LAN. To configure an interface group, go to **Network Setting > Interface Grouping**. See [Interface Grouping](#) for more details about interface group.
- 2 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.
- 3 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.
- 4 Click **Apply** to save your settings.

Figure 126 Network Setting > Home Networking > LAN Setup

Use this screen to set the Local Area Network 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.

Interface Group

Group Name

LAN IP Setup

IP Address

Subnet Mask

DHCP Server State

DHCP ☒ Enable ☐ Disable ☐ DHCP Relay

IP Addressing Values

Beginning IP Address

Ending IP Address

Auto reserve IP for the same host ☐

DHCP Server Lease Time

days hours minutes

DNS Values

DNS ☒ DNS Proxy ☐ Static ☐ From ISP

Figure 127 Network Setting > Home Networking > LAN Setup (Continued)

The screenshot displays the 'LAN Setup' configuration page, which is part of the 'Home Networking' section under 'Network Setting'. The page is organized into several sections, each with a title and specific configuration options.

- LAN IPv6 Mode Setup**: Features a toggle switch for 'IPv6 Active', which is currently turned on (blue).
- Link Local Address Type**: Includes two radio button options: 'EUI64' (selected) and 'Manual'.
- LAN Global Identifier Type**: Includes two radio button options: 'EUI64' (selected) and 'Manual'.
- LAN IPv6 Prefix Setup**: Includes a radio button for 'Delegate prefix from WAN' (selected) and a dropdown menu set to 'Default'. There is also an unselected 'Static' radio button option.
- LAN IPv6 Address Assign Setup**: Includes a dropdown menu set to 'Stateless'.
- LAN IPv6 DNS Assign Setup**: Includes a dropdown menu set to 'From RA & DHCPv6 Server'.
- DHCPv6 Configuration**: Includes a 'DHCPv6 Active' toggle (on) and a 'DHCPv6 Server' dropdown menu.
- IPv6 Router Advertisement State**: Includes a 'RADVD Active' toggle (on) and an 'Enable' checkbox.
- IPv6 DNS Values**: Includes three rows for 'IPv6 DNS Server 1', 'IPv6 DNS Server 2', and 'IPv6 DNS Server 3'. Each row has a 'Proxy' dropdown menu and an adjacent empty text input field.
- DNS Query Scenario**: Includes a dropdown menu set to 'IPv4/IPv6 DNS Server'.

At the bottom of the page, there are two buttons: 'Cancel' and 'Apply'.

The following table describes the fields in this screen.

Table 66 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group that you want to configure for the LAN settings. You must enable DHCP.
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your in dotted decimal notation, for example, (factory default).
Subnet Mask	Enter 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.
DHCP Server State	
DHCP	Select Enable to have your Zyxel Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients. If you select Disable, you need to manually configure the IP addresses of the computers and other devices on your LAN. If you select DHCP Relay, the Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.
IP Addressing Values	
The IP Addressing Values fields appear only 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	Enable this if you want to reserve the IP address for the same host.
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	DHCP server leases an address to a new client device for a period of time, called the DHCP lease time. When the lease expires, the DHCP server might assign the IP address to a different client device.
DNS Values	
This field appears only when you select Enable in the DHCP field.	
DNS	The Zyxel Device supports DNS proxy by default. The Zyxel Device sends out its own LAN IP address to the DHCP clients as the first DNS server address. DHCP clients use this first DNS server to send domain-name queries to the Zyxel Device. The Zyxel Device sends a response directly if it has a record of the domain-name to IP address mapping. If it does not, the Zyxel Device queries an outside DNS server and relays the response to the DHCP client. Select DNS Proxy to have the DHCP clients use the Zyxel Device's own LAN IP address. The Zyxel Device works as a DNS relay. Select Static if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select From ISP if your ISP dynamically assigns DNS server information (and the Zyxel Device's WAN IP address).

Table 66 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION						
LAN IPv6 Mode Setup							
IPv6 Active	Use this to enable or disable IPv6 on the Zyxel Device. When IPv6 is used, the following fields need to be set.						
Link Local Address Type	A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv6. 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. Select EUI64 to allow the Zyxel Device to generate an interface ID for the LAN interface's link-local address using the EUI-64 format. Otherwise, enter an interface ID for the LAN interface's link-local address if you select Manual . Link-local Unicast Address Format <table><tr><td>1111 1110 10</td><td>0</td><td>Interface ID</td></tr><tr><td>10 bits</td><td>54 bits</td><td>64 bits</td></tr></table>	1111 1110 10	0	Interface ID	10 bits	54 bits	64 bits
1111 1110 10	0	Interface ID					
10 bits	54 bits	64 bits					
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	Select EUI64 to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address. Select Manual to manually enter an interface ID for the LAN interface's global IPv6 address.						
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	Select Delegate prefix from WAN to automatically obtain an IPv6 network prefix from the service provider or an uplink router. Select Static to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.						
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.						
Static	Select this option to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.						
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: Stateless: The Zyxel Device uses IPv6 stateless auto-configuration. 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 auto-configuration. 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 RA & DHCPv6 Server: The Zyxel Device provides DNS information through both router advertisements and DHCPv6. From DHCPv6 Server: The Zyxel Device provides DNS information through DHCPv6. From Router Advertisement: The Zyxel Device provides DNS information through router advertisements.						
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							

Table 66 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
RADVD Active	This shows whether RADVD is enabled or not.
IPv6 DNS Values	
IPv6 DNS Server 1 – 3	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. User Defined – Select this if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the Zyxel Device passes to the DHCP clients. From ISP – Select this if your ISP dynamically assigns IPv6 DNS server information. Proxy – Select this if the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay. Otherwise, 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.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

9.3 Static DHCP

When any of the LAN clients in your network want an assigned fixed IP address, add a static lease for each LAN client. Knowing the LAN client's MAC addresses is necessary. 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.

9.3.1 Before You Begin

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

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 128 Network Setting > Home Networking > Static DHCP

When any of the LAN clients in your network want an assigned fixed IP address, add a static lease for each LAN client. Knowing the LAN client's MAC addresses is necessary. Assign IP addresses on the LAN to specific individual computers based on their MAC addresses.

+ Static DHCP Configuration

#	Status	MAC Address	IP Address	Modify
---	--------	-------------	------------	--------

The following table describes the labels in this screen.

Table 67 Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Static DHCP Configuration	Click this to configure a 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 configure the connection. Click the Delete icon to remove the connection.

If you click **Static DHCP Configuration** in the **Static DHCP** screen, the following screen displays. Using a static DHCP means a LAN client will always have the same IP address assigned to it by the DHCP server. Assign a fixed IP address to a client device by selecting the interface group of this client 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 129 Network Setting > Home Networking > Static DHCP: Static DHCP Configuration

Static DHCP Configuration

Active ☒

Group Name Default

IP Type IPv4

Select Device Info Manual Input

MAC Address - - - - -

IP Address - . - . - .

Cancel **OK**

The following table describes the labels in this screen.

Table 68 Network Setting > Home Networking > Static DHCP: Configuration

LABEL	DESCRIPTION
Active	Select Enable to activate static DHCP in your
Group Name	Select the interface group for which you want to configure the static DHCP settings.
IP Type	The IP Type is normally IPv4 (non-configurable).
Select Device Info	Select between Manual Input which allows you to enter the next two fields (MAC Address and IP Address); or select an existing
MAC Address	Enter the MAC address of a computer on your LAN if you select Manual Input in the previous field.
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify if you select Manual Input in the previous field.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

9.4 UPnP

Universal Plug and Play (UPnP) is an open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between networking devices or software applications which have UPnP enabled. A UPnP device can dynamically join a network, obtain an IP address, advertise its services, and learn about other devices on the network. A device can also leave a network automatically when it is no longer in use.

See [Turn on UPnP in Windows 10 Example](#) for more information on UPnP.

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

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.

Figure 130 Network Setting > Home Networking > UPnP

Universal Plug and Play (UPnP) is an open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between networking devices or software applications which have UPnP enabled. A UPnP device can dynamically join a network, obtain an IP address, advertise its services, and learn about other devices on the network. A device can also leave a network automatically when it is no longer in use.

UPnP State

UPnP ☒

UPnP NAT-T State

UPnP NAT-T ☒

Note

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

#	Description	Destination IP Address	External Port	Internal Port	Protocol
Cancel Apply					

The following table describes the labels in this screen.

Table 69 Network Settings > Home Networking > UPnP

LABEL	DESCRIPTION
UPnP State	
UPnP	Select Enable to activate UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the Zyxel Device's IP address (although you must still enter the password to access the Web Configurator).
UPnP NAT-T State	
UPnP NAT-T	Select Enable to activate UPnP with NAT enabled. 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.
#	This field displays the index number of the entry.
Description	This field displays the description of the UPnP NAT-T connection.
Destination IP Address	This field displays the IP address of the other connected UPnP-enabled device.
External Port	This field displays the external port number that identifies the service.
Internal Port	This field displays the internal port number that identifies the service.
Protocol	This field displays the protocol of the NAT mapping rule. Choices are TCP or UDP .
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

9.5 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 through 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 131 Network Setting > Home Networking > 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.

IP Alias Setup

Group Name:

Active: ☐

IPv4 Address:

Subnet Mask:

Public LAN

Active: ☐

IPv4 Address:

Subnet Mask:

Offer Public IP by DHCP: ☐

Enable ARP Proxy: ☐

The following table describes the labels in this screen.

Table 70 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.
Active	Click this switch to enable a logical LAN for the Zyxel Device. When this is enabled, the following fields will be configurable.
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. Your ISP must support Public LAN and static IP.
IPv4 Address	Enter the public IP address provided by your ISP.
Subnet Mask	Enter the public IPv4 subnet mask provided by your ISP.
Offer Public IP by DHCP	Click this switch to enable the Zyxel Device to provide public IP addresses by DHCP server. Otherwise, click to disable.

Table 70 Network Setting > Home Networking > Additional Subnet (continued)

LABEL	DESCRIPTION
Enable ARP Proxy	Click this switch to enable the Address Resolution Protocol (ARP) proxy. Otherwise, click to disable.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

9.6 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 132 Network Setting > Home Networking > STB Vendor ID

The following table describes the labels in this screen.

Table 71 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 your previously saved settings.
Apply	Click Apply to save your changes.

9.7 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 LAN device.

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

Figure 133 Network Setting > Home Networking > 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.

Wake by Address:

IP Address:

MAC Address:

Wake Up

The following table describes the labels in this screen.

Table 72 Network Setting > Home Networking > Wake on LAN

LABEL	DESCRIPTION
Wake by Address	Select Manual and enter the IP address or MAC address of the LAN 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 LAN device with the selected IP address then displays in the MAC Address field.
IP Address	Enter the IPv4 IP address of the LAN 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 LAN 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 LAN device.

9.8 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 134 Network Setting > Home Networking > 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 hostname of a single TFTP server.

TFTP Server Name:

Cancel **Apply**

The following table describes the labels in this screen.

Table 73 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 your previously saved settings.
Apply	Click Apply to save your changes.

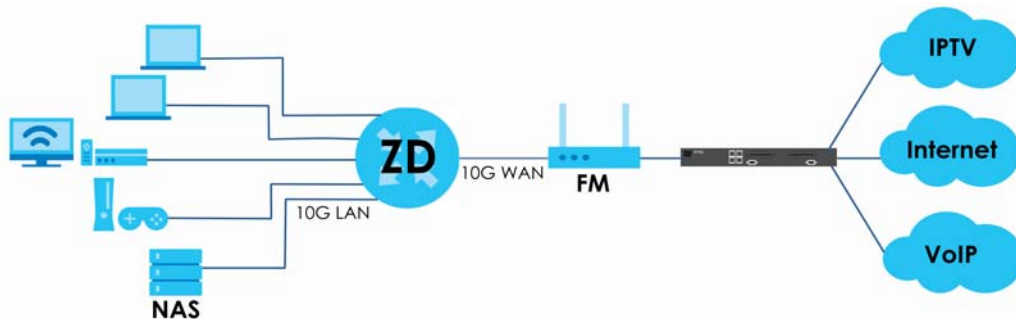
9.9 Any Port Any Service (APAS)

Any Port Any Service (APAS) allows a LAN device to use any available port to access any available service from a remote WAN device. Typically, a LAN device, such as a Set Top Box (STB), would have to use a specific port to access video streams from a video server. With APAS, the video streams only need to be received through the specified Bridge WAN interface for the LAN device specified in the APAS rule. You can connect the LAN device to any LAN port. Other LAN devices can access the Internet using the default gateway.

Unlike **Port Forwarding**, which forwards traffic based on port numbers, you do not need to know the port number for the video traffic from the IPTV server. You just select the LAN device host name or enter its MAC address and select a Bridge WAN interface.

Use the wildcard '*' for a range of MAC addresses for multiple LAN devices. For example, enter 00:13:49:*:* for all LAN devices from a vendor with the MAC OUI 00:13:49. (range). Any device with that MAC OUI aa:bb:cc connected to any LAN port on the Zyxel Device can access services or can be accessed for services through the specified Bridge WAN interface. For example, the LAN device could be an STB receiving video streams from a video server, or it could be a server, allowing access to it through the specified Bridge WAN interface.

Note: You must configure a Bridge WAN interface in advance.



As APAS allows incoming traffic from any port to access any service on a configured LAN device, it may be difficult to distinguish between appropriate and malicious traffic going to the LAN device. Make sure to properly configure firewall rules to protect the LAN device, and monitor network traffic for suspicious activity.

Click **Network Setting > Home Networking > APAS** to open this screen.

Network Setting > Home Networking > APAS

The following table describes the labels in this screen.

Table 74 Network Setting > Home Networking > APAS

LABEL	DESCRIPTION
Enable	Click Enable to activate APAS.
Add new MAC Rule	Click this button to add a new MAC rule. You can create up to eight MAC rules.
#	This is the index number.
Name	This is the name of the rule.
MAC Rule	This is the LAN host MAC address that is applied to the rule.
WAN Interface	This is the bridge WAN interface for incoming traffic.
Cancel	Click Cancel to restore your previously saved changes.
OK	Click OK to save your changes.

9.9.1 Add APAS

Use this screen to create a new MAC rule. Click **Network Setting > Home Networking > APAS > Add New MAC Rule** to open the following screen.

Figure 135 Network Setting > Home Networking > APAS > Add New MAC Rule

The screenshot shows a configuration screen titled "Any Port Any Service Configuration". It contains the following elements:

- Enable:** A toggle switch that is currently turned off.
- Name:** A text input field for naming the rule.
- Select Device Info:** A dropdown menu with "Manual Input" selected.
- MAC Rule:** A text input field for specifying the MAC rule.
- Bridge WAN name:** A dropdown menu for selecting a Bridge WAN interface.
- Buttons:** "Cancel" and "OK" buttons at the bottom right.

The following table describes the labels in this screen.

Table 75 Network Setting > Home Networking > APAS > Add New MAC Rule

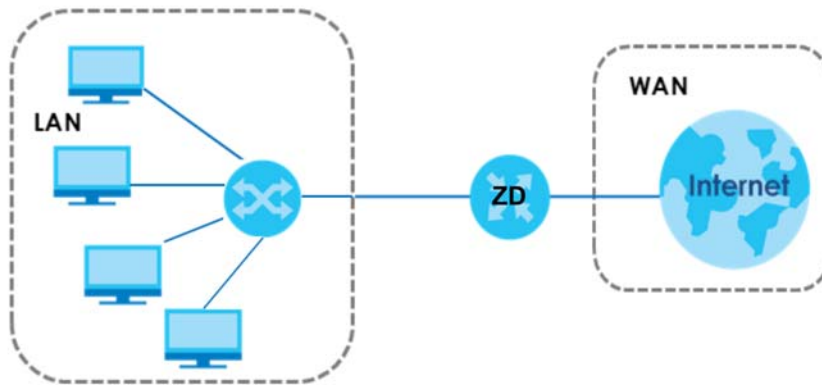
LABEL	DESCRIPTION
Enable	Click this to enable APAS on the Zyxel Device.
Name	Enter a name of up to 64 characters for the APAS rule to this host(s). Allowed characters for Name include the following within quotes: " !#%()*+,-./0123456789:;=?@ABCDEFGHIJKLMNPQRSTUVWXYZ[_abcdefghijklmnopqrstuvwxyz~"
Select Device Info	Select a connected LAN host or select Manual Input to enter the MAC address of a client that is not yet connected and does not display in Connection Status > Connectivity .
MAC Rule	If you selected Manual Input for Select Device Info , then enter the LAN host MAC address here. You can use the wildcard '*' for a MAC address range. For example, enter 00:13:49:*:*:* for all LAN devices from a vendor with the MAC OUI 00:13:49.
Bridge WAN Name	Select a Bridge WAN interface for incoming traffic to apply the rule. You must have created at least one Bridge WAN interface in Network Setting > Broadband screen.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

9.10 Technical Reference

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

LANs, WANs and the Zyxel Device

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

Figure 136 LAN and WAN IP Addresses

9.10.1 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.

9.10.2 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.

9.10.3 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's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your 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 two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

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

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

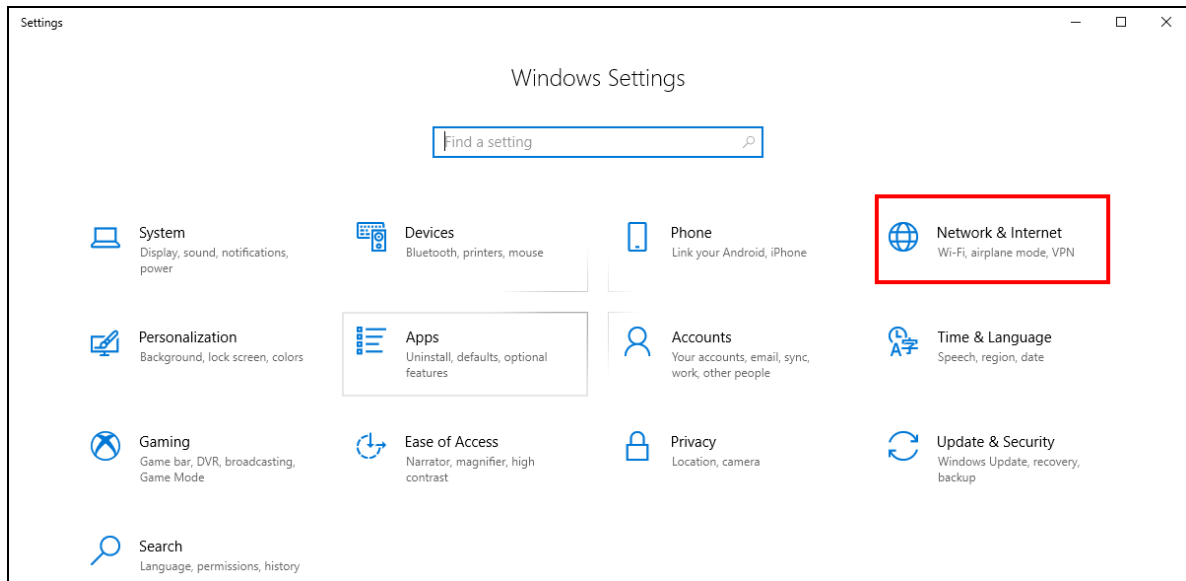
Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space".

9.11 Turn on UPnP in Windows 10 Example

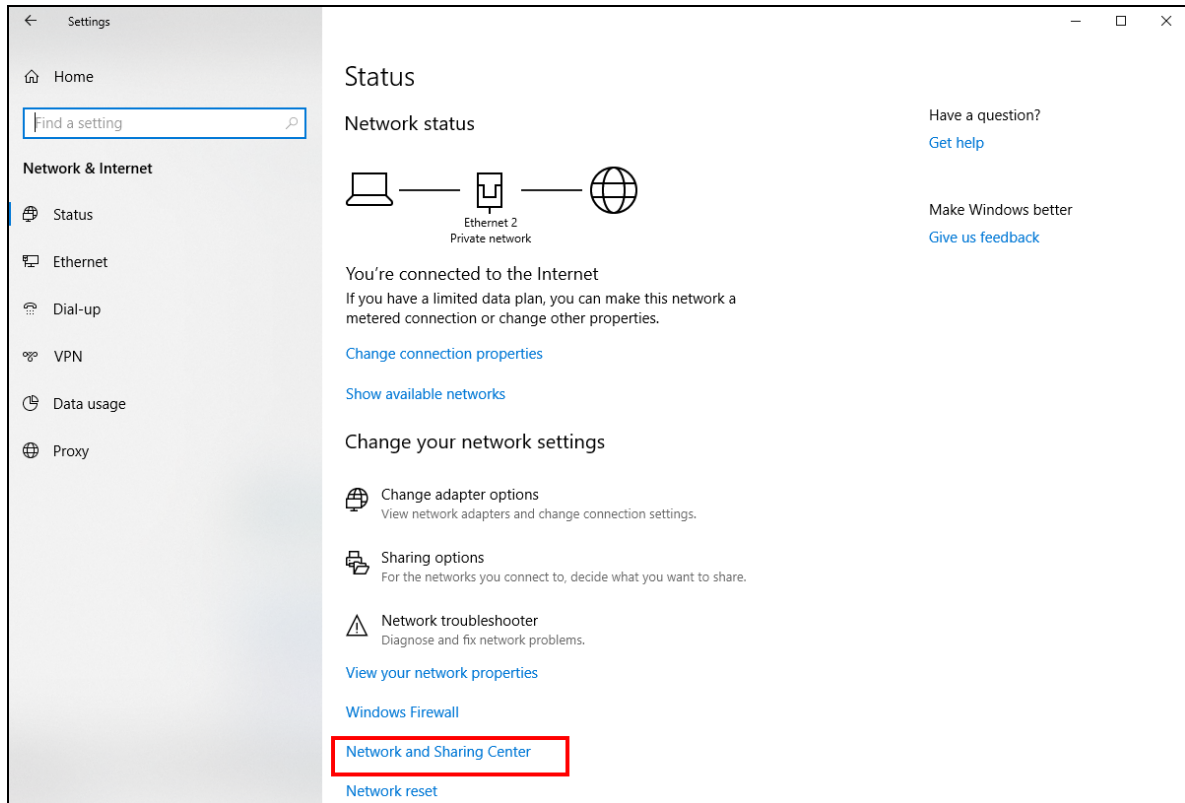
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the Zyxel Device by clicking **Network Setting** > **Home Networking** > **UPnP**.

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

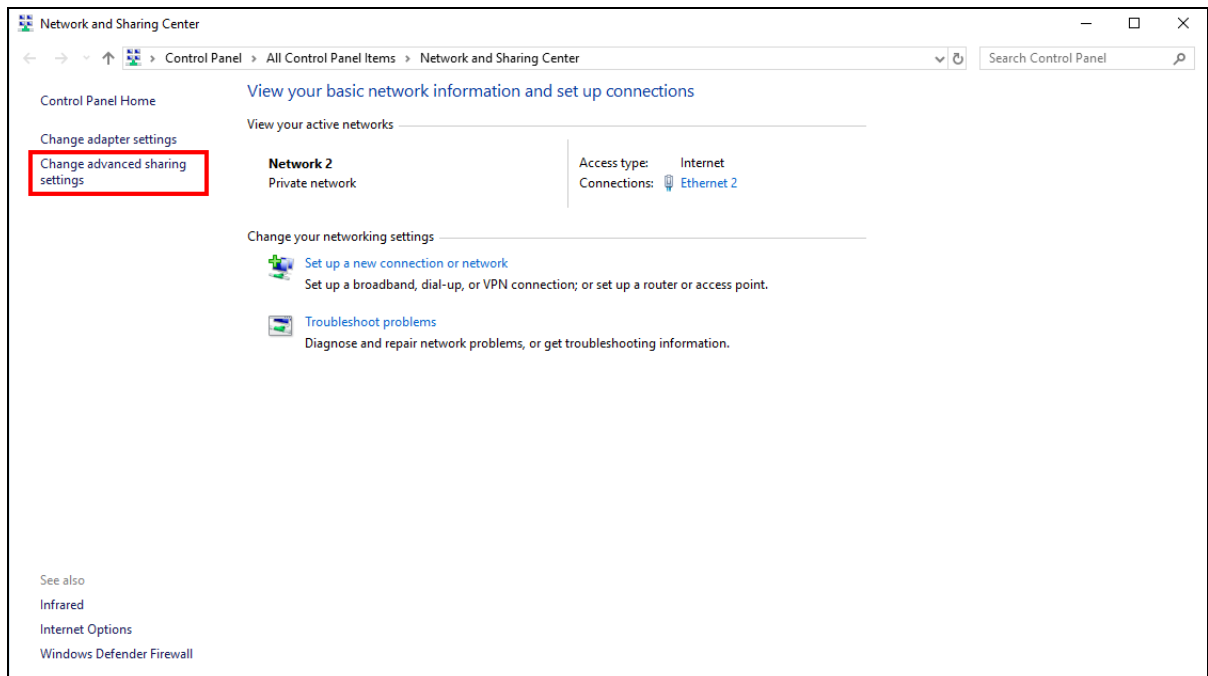
- 1 Click the start icon, **Settings** and then **Network & Internet**.



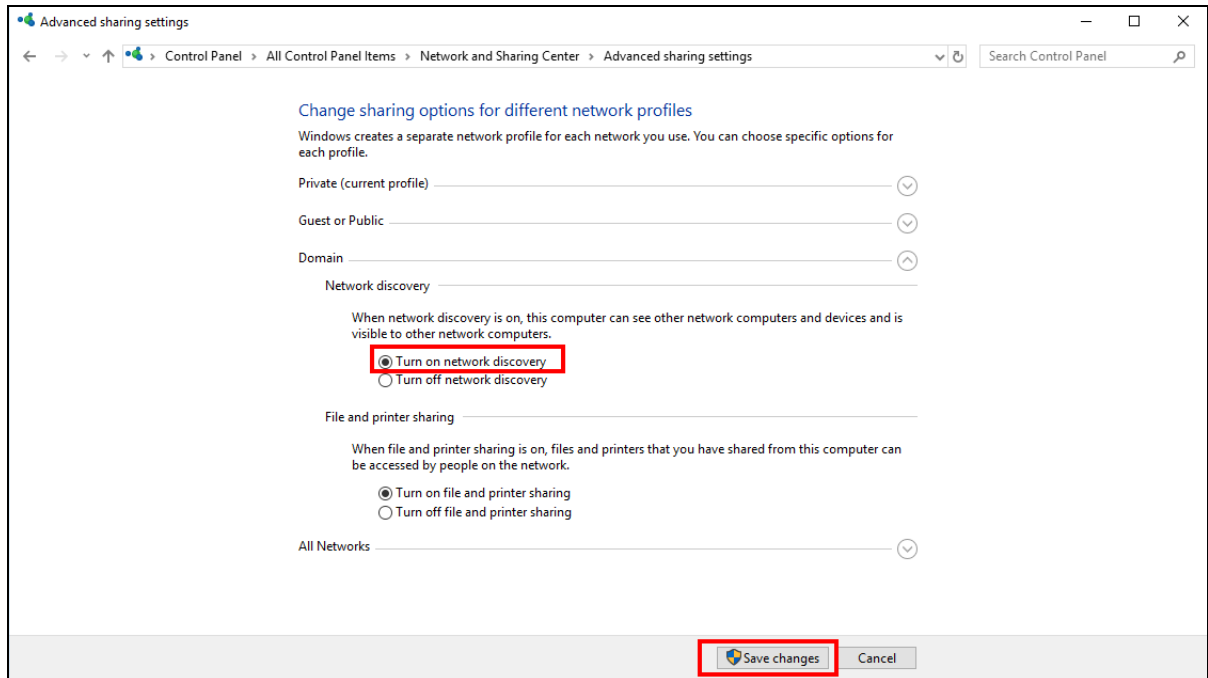
- 2 Click **Network and Sharing Center**.



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.

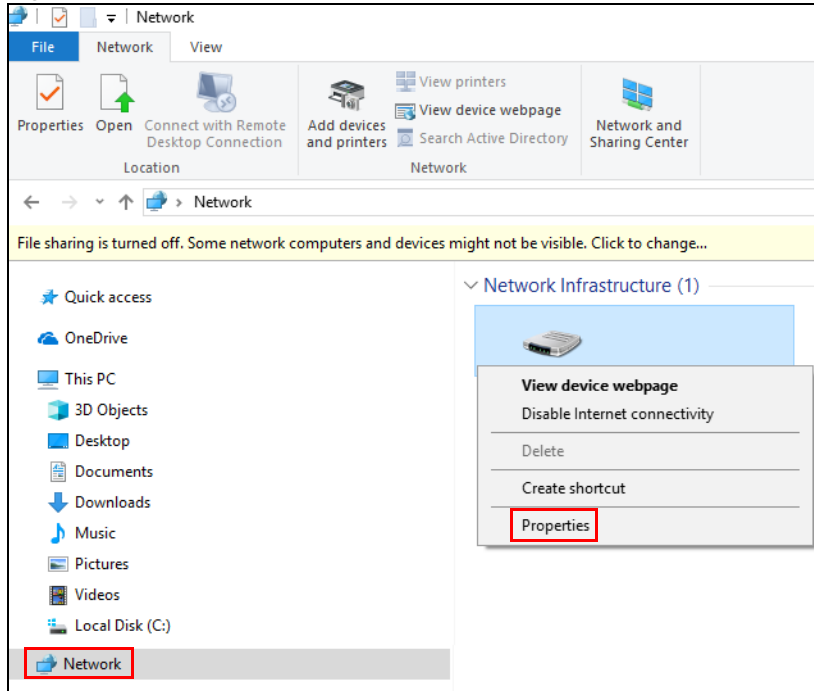


9.11.1 Auto-discover Your UPnP-enabled Network Device

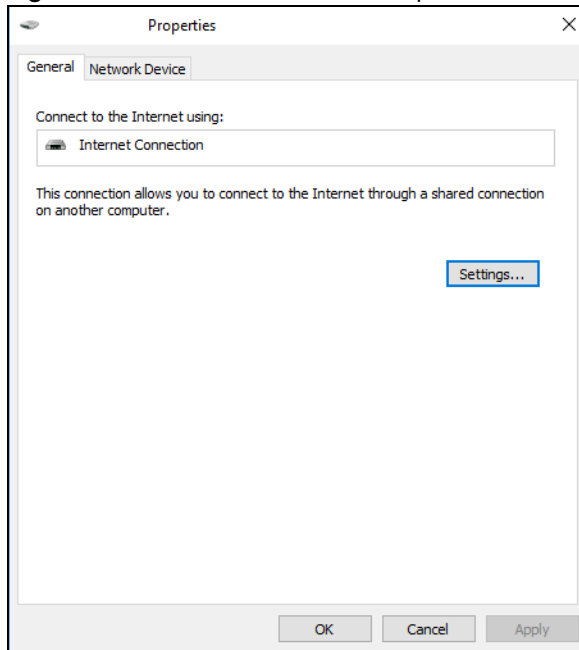
Before you follow these steps, make sure you already have UPnP activated on the Zyxel Device and in your computer.

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

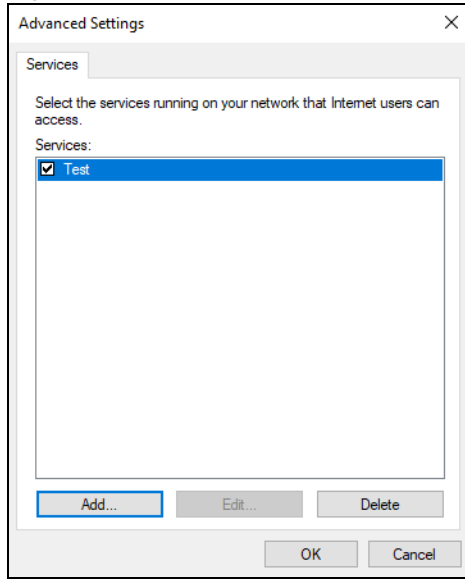
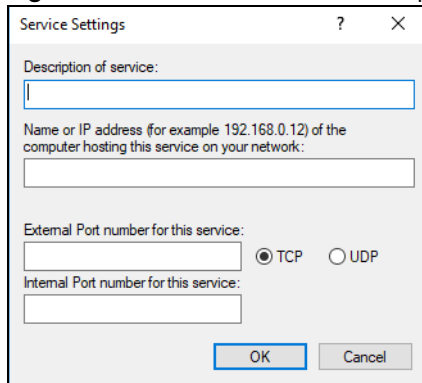
- 1 Open **File Explorer** and click **Network**.
- 2 Right-click the Zyxel Device icon and select **Properties**.

Figure 137 Network Connections

- 3 In the **Internet Connection Properties** window, click **Settings** to see port mappings.

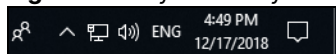
Figure 138 Internet Connection Properties

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

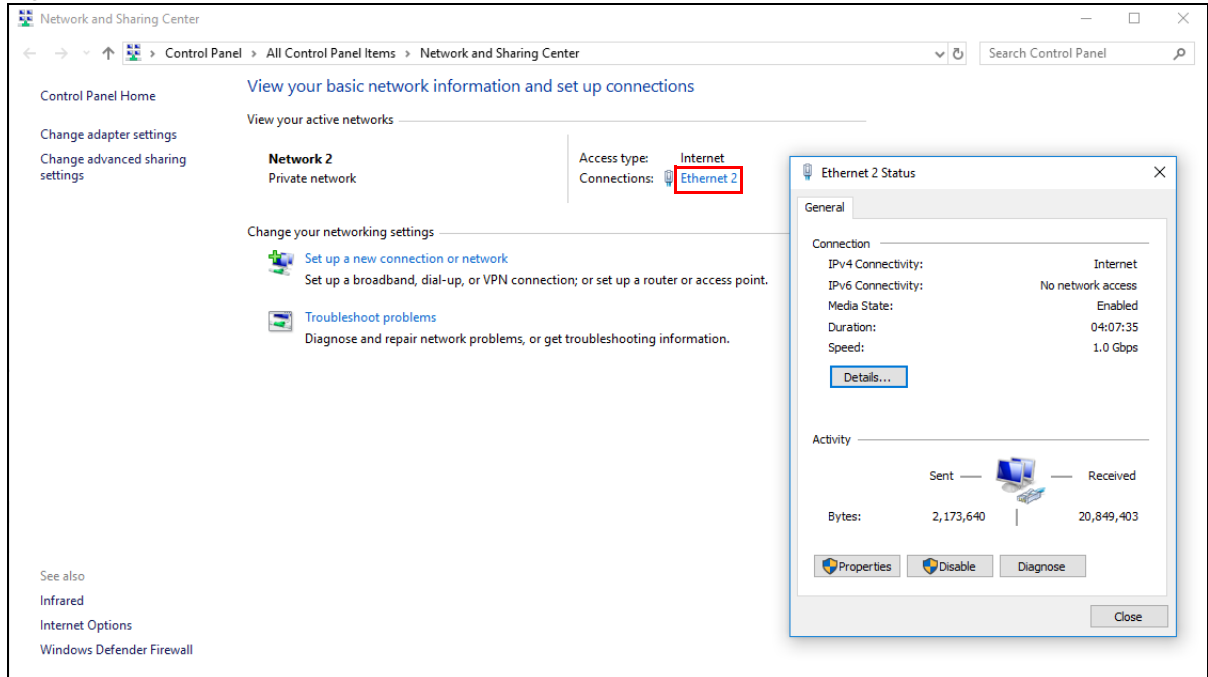
Figure 139 Internet Connection Properties: Advanced Settings**Figure 140** Internet Connection Properties: Advanced Settings: Add

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

- 5 Click **OK**. Check the network icon on the system tray to see your Internet connection status.

Figure 141 System Tray Icon

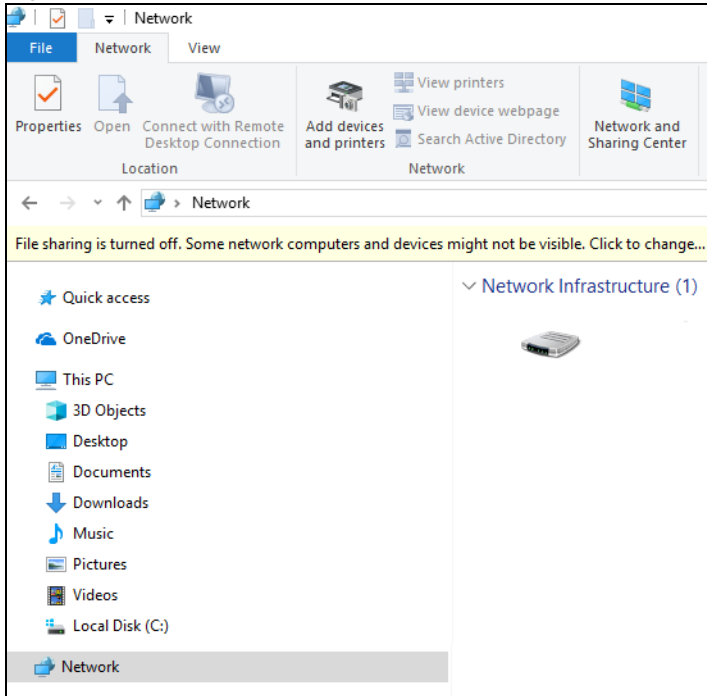
- 6 To see more details about your current Internet connection status, right click the network icon in the system tray and click **Open Network & Internet settings**. Click **Network and Sharing Center** and click the **Connections**.

Figure 142 Internet Connection Status

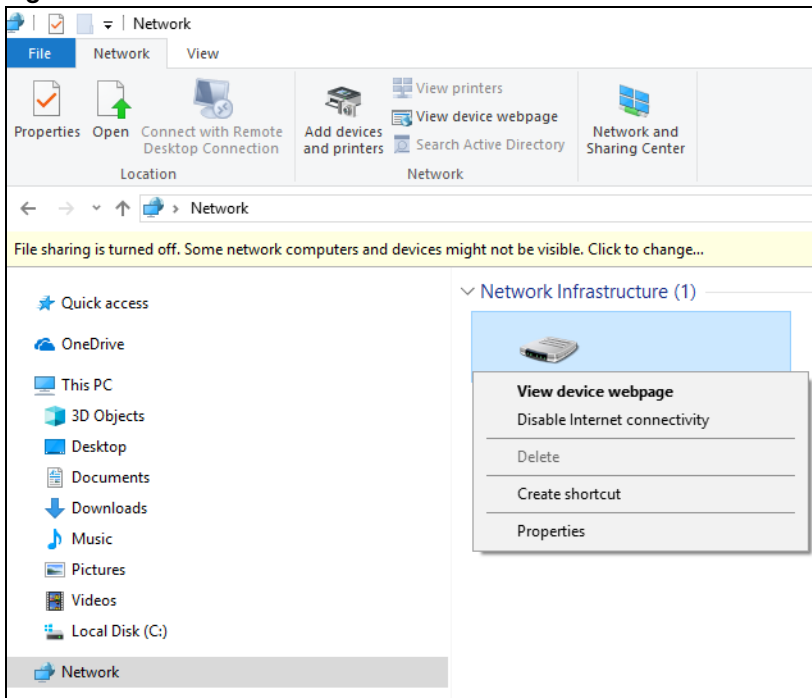
9.12 Web Configurator Access with UPnP in Windows 10

Follow the steps below to access the Web Configurator.

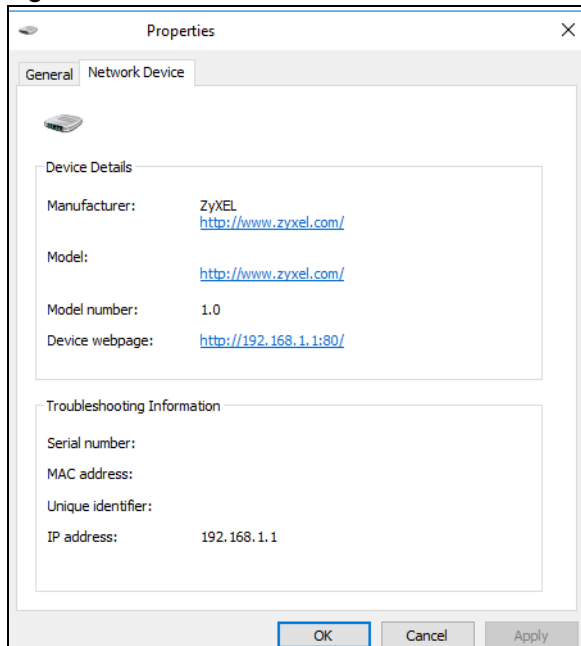
- 1 Open **File Explorer**.
- 2 Click **Network**.

Figure 143 Network Connections

- 3 An icon with the description for each UPNP-enabled device displays under **Network Infrastructure**.
- 4 Right-click the icon for your Zyxel Device and select **View device webpage**. The Web Configurator login screen displays.

Figure 144 Network Connections: Network Infrastructure

- 5 Right-click the icon for your Zyxel Device and select **Properties**. Click the **Network Device** tab. A window displays information about the Zyxel Device.

Figure 145 Network Connections: Network Infrastructure: Properties: Example

CHAPTER 10

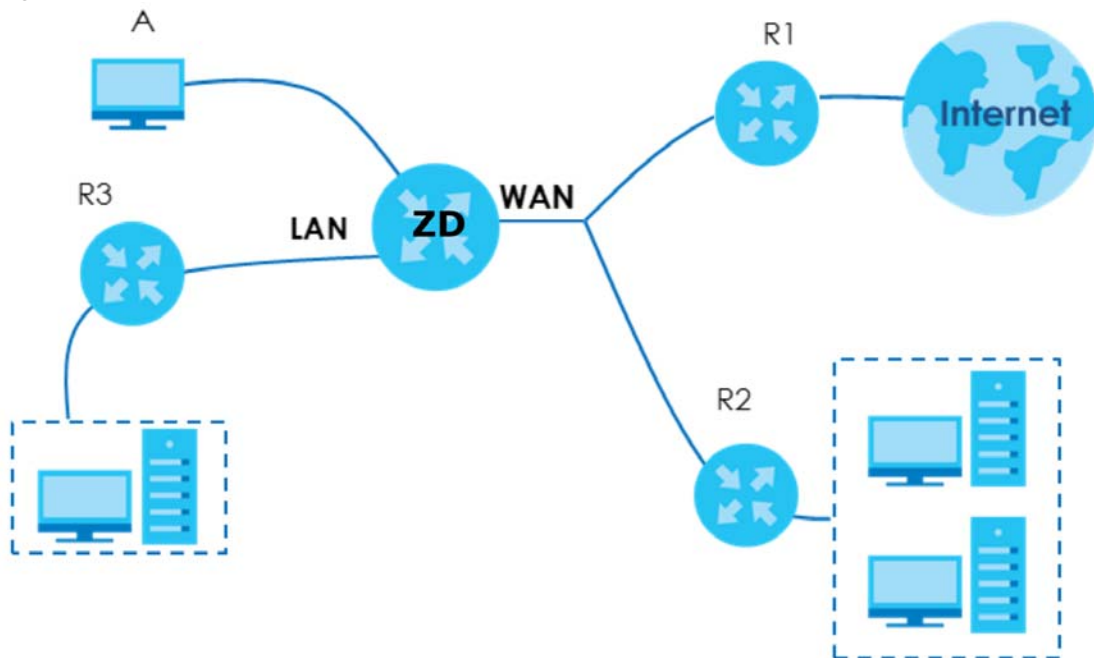
Routing

10.1 Routing 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 146 Example of Static Routing Topology



10.2 Configure Static Route

Use this screen to view and configure 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 in your home or office network. Click **Network Setting** > **Routing** to open the **Static Route** screen.

Figure 147 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 76 Network Setting > Routing > Static Route

LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the Zyxel Device.
#	This is the number of an individual static route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Name	This is the name of the static 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 through which the traffic is routed.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the Zyxel Device. Click the Delete icon to remove a static route from the Zyxel Device.

10.2.1 Add or Edit Static Route

Use this screen to add or edit a static route. Click **Add New Static Route** in the **Static Route** screen, the following screen appears. Configure the required information for a static route.

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

Figure 148 Network Setting > Routing > Static Route > Add New Static Route

Add New Static Route

Active ☒

Route Name

IP Type IPv4 ▼

Destination IP Address

Subnet Mask

Use Gateway IP Address ☒

Gateway IP Address

Use Interface Default ▼

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

Cancel **OK**

The following table describes the labels in this screen.

Table 77 Network Setting > Routing > Static Route > Add New Static Route

LABEL	DESCRIPTION
Active	Click this switch to activate static route. Otherwise, click to disable.
Route Name	Enter a name for your static route. You can use up to 15 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed.
IP Type	Select between IPv4 or IPv6 . Compared to IPv4 , 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).
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
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. Note: This field appears only when you select IPv4 in the IP Type field.
Prefix Length	If you are using IPv6, enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address. Note: This field appears only when you select IPv6 in the IP Type field.
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.

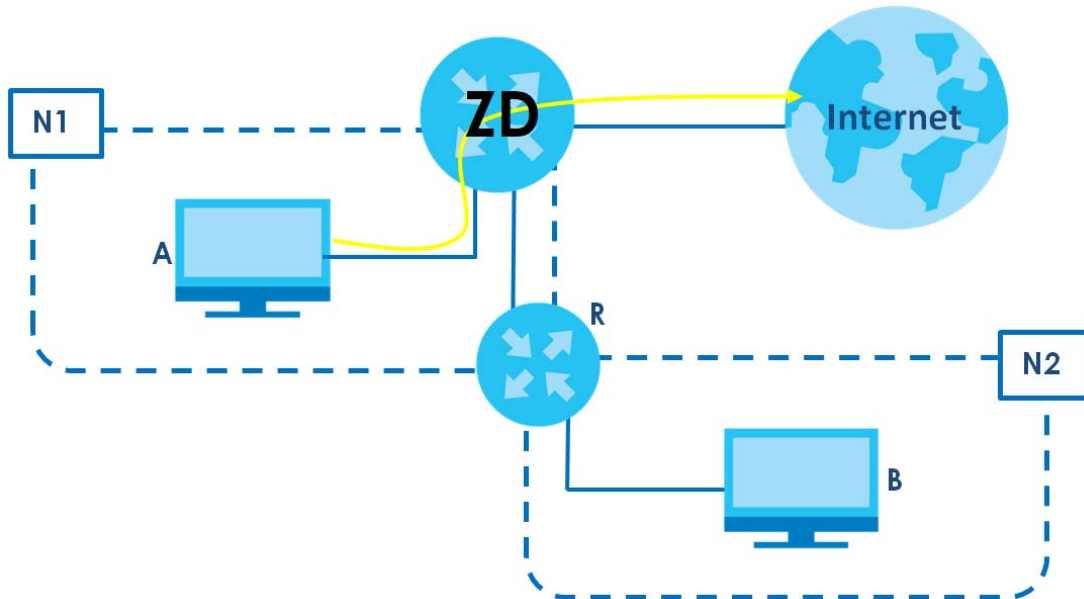
Table 77 Network Setting > Routing > Static Route > Add New Static Route (continued)

LABEL	DESCRIPTION
Gateway IP Address	Enter the IP address of the gateway.
User Interface	Select the WAN interface you want to use for this static route.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

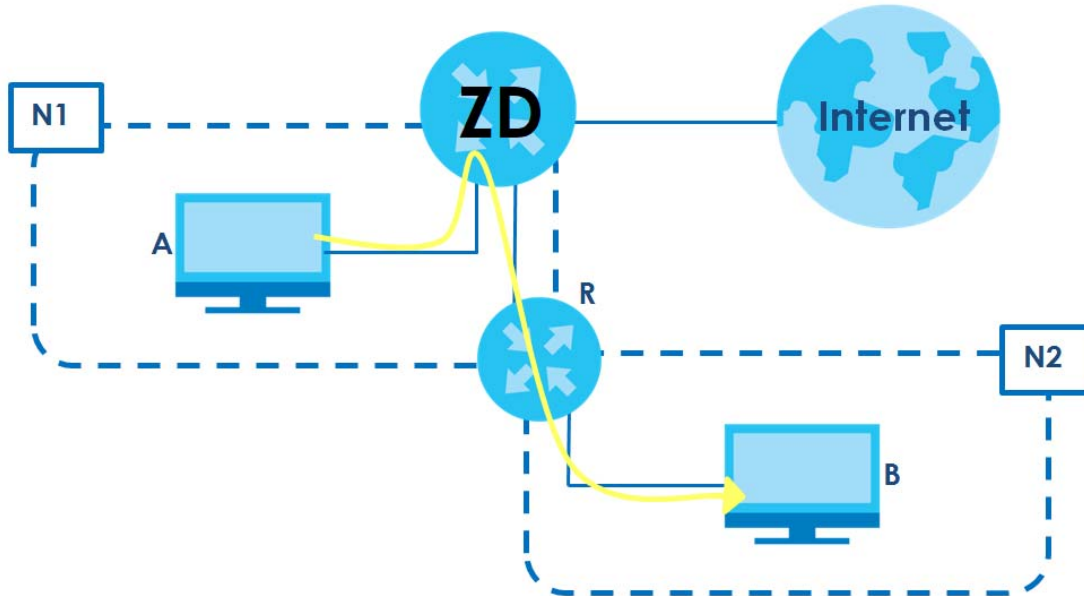
10.2.1.1 An Example of Adding a Static Route

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**.



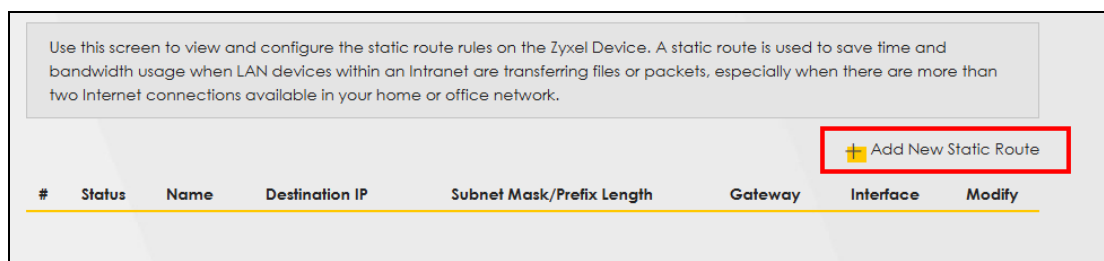
This tutorial uses the following example IP settings:

Table 78 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The Zyxel Device's WAN	172.16.1.1
The Zyxel Device's LAN	
IP Type	IPv4
Use Interface	Default
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.
- 2 Click **Network Setting > Routing**.
- 3 Click **Add new Static Route** in the **Static Route** screen.



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

- 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**.
- Set **IP Type** to **IPv4**.
- Enter the **Destination IP Address** **192.168.10.1** and **IP Subnet Mask** **255.255.255.0** for the destination, **N2**.
- Click the **Use Gateway IP Address** button to enable this function. When the switch goes to the right, the function is enabled. Enter **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.
- Select **Default** as the **Use Interface**.
- 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.

Add New Static Route

Configure the required information for a static route.

Active ☒

Route Name

IP Type

Destination IP Address

Subnet Mask

Use Gateway IP Address ☒

Gateway IP Address

Use Interface

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

Cancel **OK**

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

Figure 149 Network Setting > Routing > 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.

+ Add New DNS Route

#	Status	Domain Name	WAN Interface	Subnet Mask	Modify
Note Maximum of 20 entries can be added.					

The following table describes the labels in this screen.

Table 79 Network Setting > Routing > DNS Route

LABEL	DESCRIPTION
Add New DNS Route	Click this to create a new entry.
#	This is the number of an individual DNS route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Domain Name	This is the domain name to which the DNS route applies.
WAN Interface	This is the WAN interface through which the matched DNS request is routed.
Subnet Mask	This parameter specifies the IP network subnet mask.
Modify	Click the Edit icon to configure a DNS route on the Zyxel Device. Click the Delete icon to remove a DNS route from the Zyxel Device.

10.3.1 Add or Edit DNS Route

You can manually add the Zyxel Device's DNS route entry. Click **Add New DNS Route** in the **DNS Route** screen, use this screen to configure the required information for a DNS route.

Figure 150 Network Setting > Routing > DNS Route > Add New DNS Route

< Add New DNS Route

Active ☒

Domain Name

Subnet Mask

WAN Interface

Cancel OK

The following table describes the labels in this screen.

Table 80 Network Setting > Routing > DNS Route > Add New DNS Route

LABEL	DESCRIPTION
Active	Enable DNS route in your Zyxel Device.
Domain Name	Enter the domain name you want to resolve. You can use up to 64 alphanumeric (0-9, a-z, A-Z) characters with hyphens [-] and periods [.]. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com. The Zyxel Device forwards DNS queries for any domain name ending in example.com to the WAN interface specified in this route.
Subnet Mask	Enter the subnet mask of the network for which to use the DNS route in dotted decimal notation, for example 255.255.255.255.
WAN Interface	Select a WAN interface through which the matched DNS query is sent. You must have the WAN interfaces already configured in the Broadband screen.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

10.4 Policy Route

By default, the Zyxel Device routes packets based on the shortest path to the destination address. Policy routes allow you to override the default behavior and route packets based on other criteria, such as the source address. For example, you can use policy-based routing to direct traffic from specific users through specific connections or distribute traffic across multiple paths for load sharing. Policy-based routing is applied to outgoing packets before the default routing rules are applied.

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 151 Network Setting > Routing > Policy Route

By default, the Zyxel Device routes packets based on the shortest path to the destination address. Policy routes allow you to override the default behavior and route packets based on other criteria, such as the source address. For example, you can use policy-based routing to direct traffic from specific users through specific connections or distribute traffic across multiple paths for load sharing. Policy-based routing is applied to outgoing packets before the default routing rules are applied.  Add New Policy Route										
#	Status	Name	Source IP	Source Subnet Mask	Protocol	Source Port	Source MAC	Source Interface	WAN Interface	Modify

The following table describes the labels in this screen.

Table 81 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.

Table 81 Network Setting > Routing > Policy Route (continued)

LABEL	DESCRIPTION
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.

10.4.1 Add or 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 152 Network Setting > Routing > Policy Route: Add or Edit

The screenshot shows the 'Add New Policy Route' configuration window. It includes a back arrow in the top left corner. The title 'Add New Policy Route' is centered at the top. The configuration fields are as follows:

- Active:** A toggle switch that is currently turned on (blue).
- Route Name:** A text input field.
- Source IP Address:** A text input field with four dots as placeholders.
- Source Subnet Mask:** A text input field with four dots as placeholders.
- Protocol:** A dropdown menu with 'None' selected.
- Source Port:** A text input field with '0' entered.
- Source MAC:** A text input field with five dashes as placeholders.
- Source Interface(ex: br0 or LAN1~LAN4):** A text input field.
- WAN Interface:** A dropdown menu with 'WWAN' selected.

At the bottom of the window, there are two buttons: 'Cancel' and 'OK'.

The following table describes the labels in this screen.

Table 82 Network Setting > Routing > Policy Route: Add or Edit

LABEL	DESCRIPTION
Active	Click this switch to activate this policy route. Otherwise, click to disable.
Route Name	Enter a descriptive name of this policy route. You can use up to 15 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (TCP , UDP , or None).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Source Interface (example: br0 or LAN1 – LAN4)	Enter the name of the interface from which the matched traffic is sent.
WAN Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interfaces already configured in the Broadband screens.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

10.5 RIP Overview

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows the Zyxel Device to exchange routing information with other routers. To activate RIP for the WAN interface, select the supported RIP version and operation.

10.5.1 RIP

Click **Network Setting > Routing > RIP** to open the **RIP** screen. Select the desired RIP version and operation by clicking the checkbox. To stop RIP on the WAN interface, clear the checkbox. Click the **Apply** button to start or stop RIP and save the configuration.

Figure 153 Network Setting > Routing > RIP

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

#	Interface	Version	Operation	Enable	Disable Default Gateway
1	VDSL	RIPv2 ▼	Active ▼	☐	☐
2	GPON	RIPv2 ▼	Active ▼	☐	☐

Cancel
Apply

The following table describes the labels in this screen.

Table 83 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). RIPv1 is universally supported but RIPv2 carries more information. RIPv1 is probably adequate for most networks, unless you have an unusual network topology. When set to Both , the Zyxel Device will broadcast its routing table periodically and incorporate the RIP information that it
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 checkbox to activate the settings.
Disable Default Gateway	Select the checkbox to set the Zyxel Device to not send the route information to the default gateway.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes back to the Zyxel Device.

CHAPTER 11

Quality of Service (QoS)

11.1 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.

11.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth ([Quality of Service General Settings](#)).
- The **Queue Setup** screen lets you configure QoS queue assignment ([Queue Setup](#)).
- The **Classification Setup** screen lets you add, edit or delete QoS classifiers ([QoS Classification Setup](#)).
- The **Shaper Setup** screen limits outgoing traffic transmission rate on the selected interface ([QoS Shaper Setup](#)).

11.2 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.

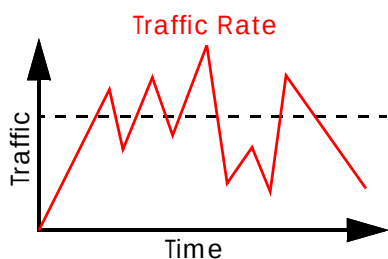
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of 3 bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

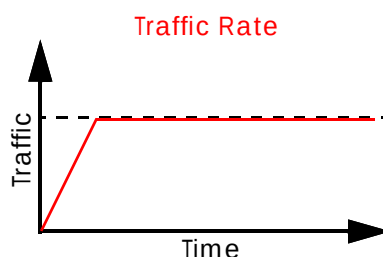
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or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



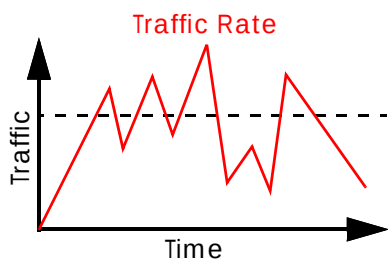
(Before Traffic Shaping)



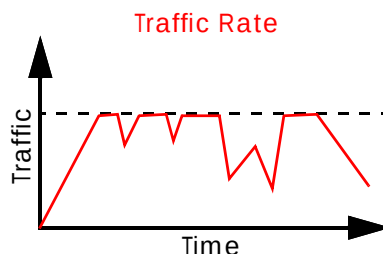
(After Traffic Shaping)

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 Marker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See [Queue Setup](#) for more information on each metering algorithm.

Strictly Priority

Strictly Priority (SP) services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.

Weighted Round Robin Schedule (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

11.3 Quality of Service General Settings

Use this screen to enable or disable QoS and set the upstream bandwidth or assign traffic priority. See [QoS Overview](#) 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.

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

Figure 154 Network Setting > QoS > General

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 (kbps)

Upstream Traffic Priority Assigned by

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 Assigned by** field.

[Cancel](#) [Apply](#)

The following table describes the labels in this screen.

Table 84 Network Setting > QoS > General

LABEL	DESCRIPTION
QoS	Click this switch to enable QoS to improve your network performance.
WAN Managed Upstream Bandwidth	Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS. The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. You can also set this number lower than the interfaces' actual transmission speed. This will cause the 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.
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 your previously saved settings.
Apply	Click Apply to save your changes.

11.4 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 or LAN interfaces. Traffic with higher priority gets through faster than those with lower priority. Low-priority traffic is dropped first when the network is congested.

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

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

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

Figure 155 Network Setting > QoS > Queue Setup

QoS

General **Queue Setup** Classification Setup Shaper Setup Policer 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.

Queue Setting: SP

#	Status	Name	Interface	Discipline	Priority	Weight	Buffer Management	Rate Limit
1		Highest	WAN	SP	1	8	DT	N/A
2		High	WAN	SP	2	5	DT	N/A
3		Medium	WAN	SP	3	3	DT	N/A
4		Low	WAN	SP	4	1	DT	N/A

Cancel Apply

Note
Priority level 1 is the highest priority for QoS.

The following table describes the labels in this screen.

Table 85 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Queue Setting	Select between SP (Strict Priority), SP+WRR , or WRR (Weighted Round Robin). SP scheduling singles out the highest priority queue and ensures all queued traffic in this queue is transmitted before servicing the lower priority queues. WRR scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue Weight field. Queues with larger weights get more service than queues with smaller weights. If you choose SP+WRR , the first and second queue will be SP , and the third and fourth queue will be WRR .
#	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.

Table 85 Network Setting > QoS > Queue Setup (continued)

LABEL	DESCRIPTION
Discipline	This shows the discipline of the queue. The discipline is changed according to the option chosen in Queue Setting. If you choose SP, the discipline will be SP. If you choose SP+WRR, the discipline of the first and second queue will be SP, and the third and fourth queue will be WRR. If you choose WRR, the discipline will be WRR. Strict Priority scheduling services the remaining queues using WRR. WRR scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue Weight field). Queues with larger weights get more service than queues with smaller weights. Note: Queue weights can only be changed when Weighted Round Robin is selected.
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.
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.

11.4.1 Add a QoS Queue

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

Figure 156 Network Setting > QoS > Queue Setup > Add New Queue/Edit

Add New Queue

Active ☐

Name

Interface

Priority

Weight

Buffer Management

Rate Limit (kbps)

Cancel OK

The following table describes the labels in this screen.

Table 86 Network Setting > QoS > Queue Setup > Add New Queue/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable the queue.
Name	Enter a descriptive name for this queue. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed.
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 8) 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.
OK	Click OK to save your changes.

11.5 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 157 Network Setting > QoS > Classification Setup

QoS

General Queue Setup **Classification Setup** Shaper Setup Policer 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.

Add New Classification

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

The following table describes the labels in this screen.

Table 87 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.

11.5.1 Add or 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.