

8.6 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.

Note: This screen appears when the WE Device is in Router or Access Point (AP) mode.

Figure 91 Network Setting > Home Networking > Additional Subnet

Home Networking

LAN Setup Static DHCP UPnP **Additional Subnet** STB Vendor ID

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: lan

Active: ☒

IPv4 Address: . . .

Subnet Mask: . . .

Public LAN

Active: ☒

IPv4 Address: . . .

Subnet Mask: 255 . 255 . 255 0

Offer Public IP by DHCP: ☒

Enable ARP Proxy: ☒

Cancel Apply

The following table describes the labels in this screen.

Table 44 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 WE Device. When this is enabled, the following fields will be configurable.
IPv4 Address	Enter the IP address of your WE Device in dotted decimal notation.
Subnet Mask	Your WE 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 WE 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 WE Device to provide public IP addresses by DHCP server. Otherwise, click to disable.
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.

8.7 STB Vendor ID

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

Note: This screen appears when the WE Device is in Router or Access Point (AP) mode.

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

Figure 92 Network Setting > Home Networking > STB Vendor ID

The following table describes the labels in this screen.

Table 45 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.

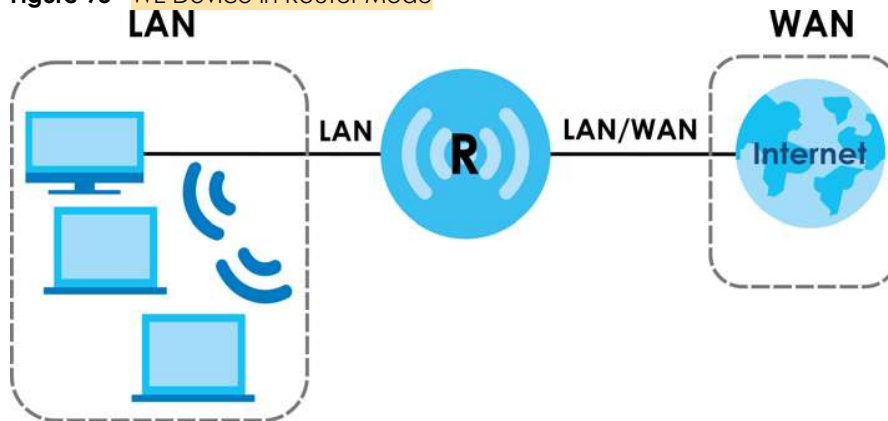
8.8 Technical Reference

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

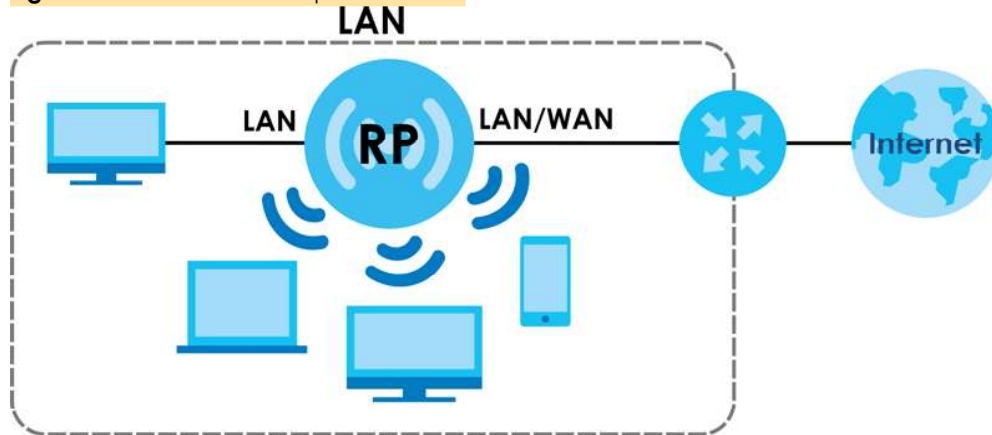
LANs, WANs and the WE Device

The WE Device has two Ethernet ports: one LAN and one LAN/WAN.

For the WE Device in Router mode (**R**), the LAN/WAN port functions as a WAN port for Internet access. You can use the LAN port to connect to client devices, such as a PC.

Figure 93 WE Device in Router Mode

For the WE Device in Repeater mode (RP), both the LAN/WAN and LAN ports function as LAN ports. You can use one to connect to a client device and the other to a router or extender as the Ethernet uplink.

Figure 94 WE Device in Repeater Mode

8.8.1 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 WE Device as a DHCP server or disable it. When configured as a server, the WE 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 WE Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

8.8.2 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 WE Device supports the IPCP DNS server extensions through the DNS proxy feature.

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

8.8.3 LAN TCP/IP

The WE 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 WE 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 WE 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 WE 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 WE 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.

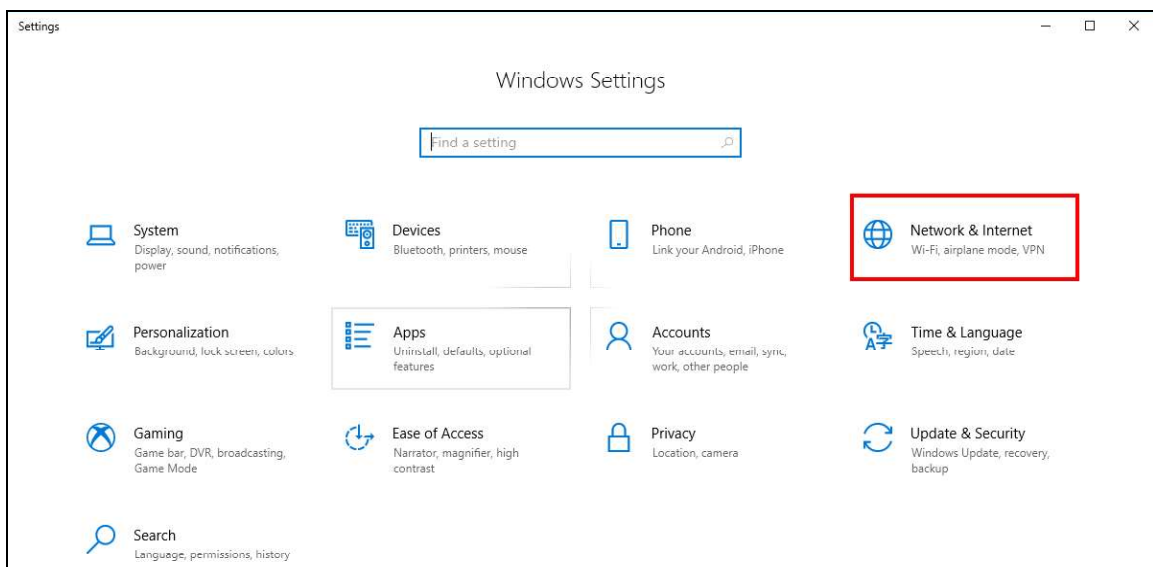
Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space".

8.9 Turn on UPnP in Windows 10 Example

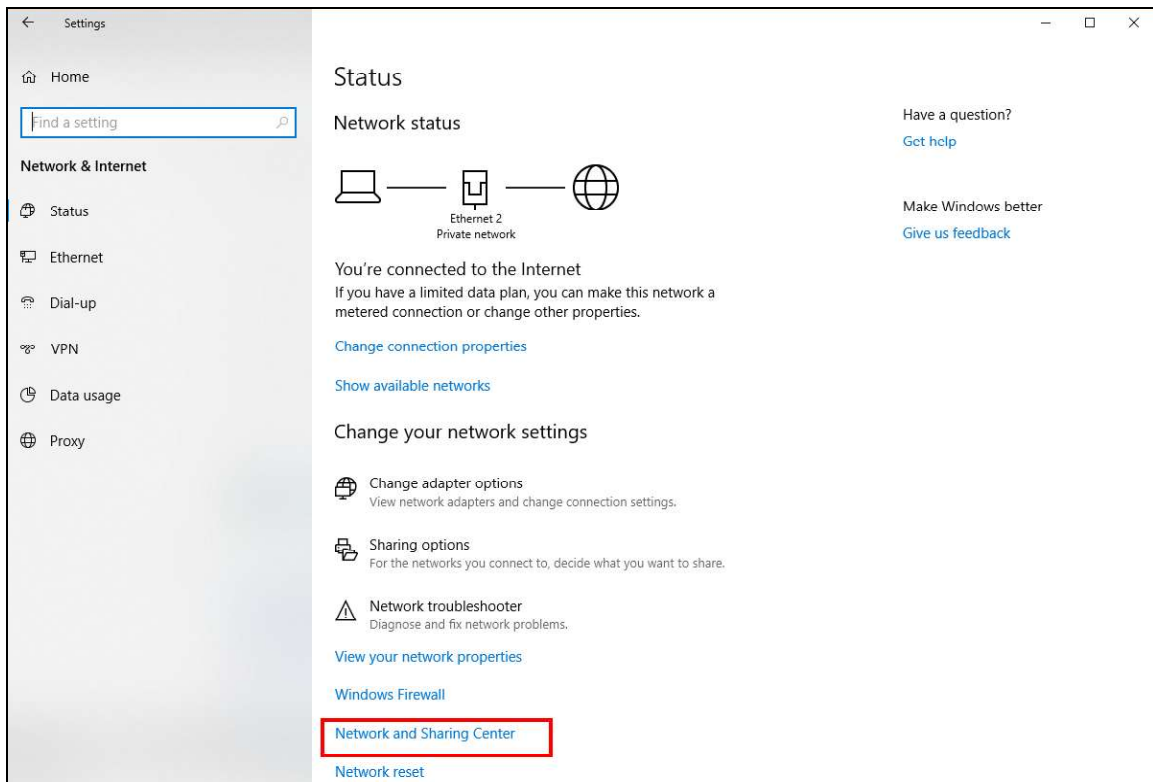
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the WE Device by clicking **Network Setting > Home Networking > UPnP**.

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

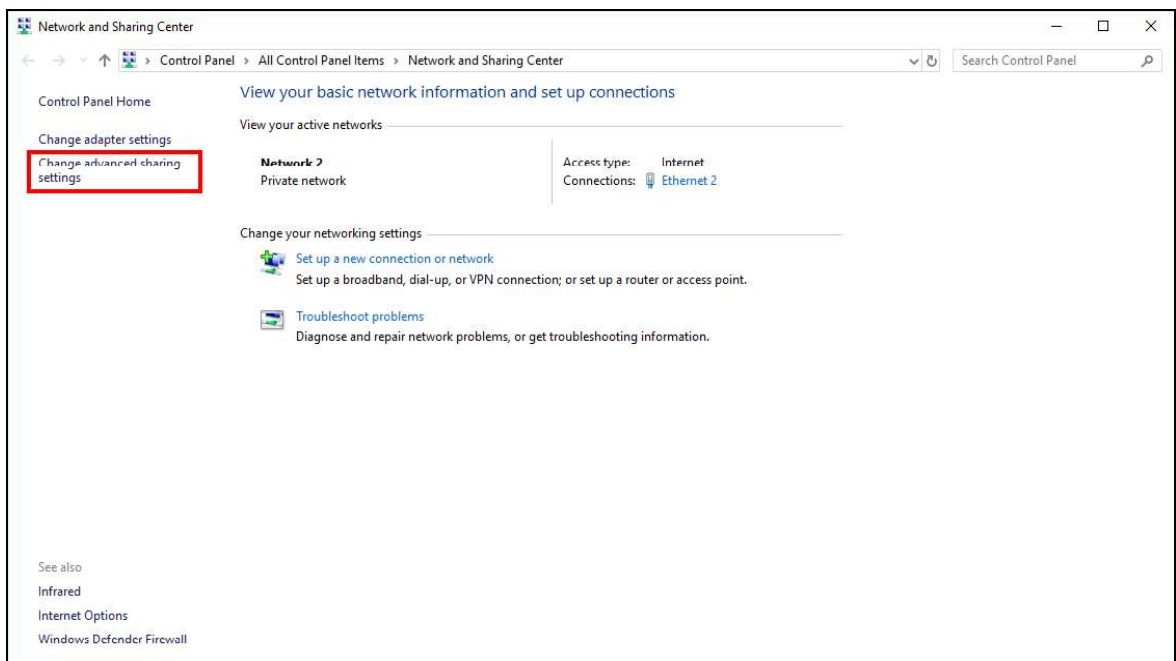
- 1 Click the start icon, **Settings** and then **Network & Internet**.



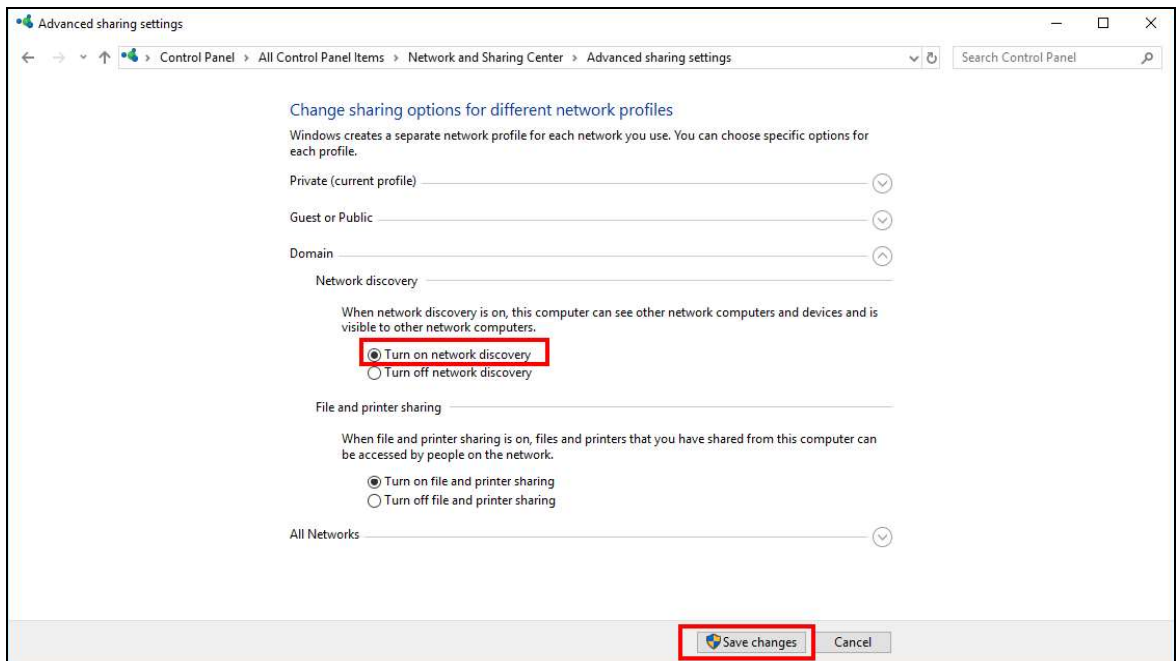
- 2 Click **Network and Sharing Center**.



3 Click **Change advanced sharing settings**.



4 Under **Domain**, select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.



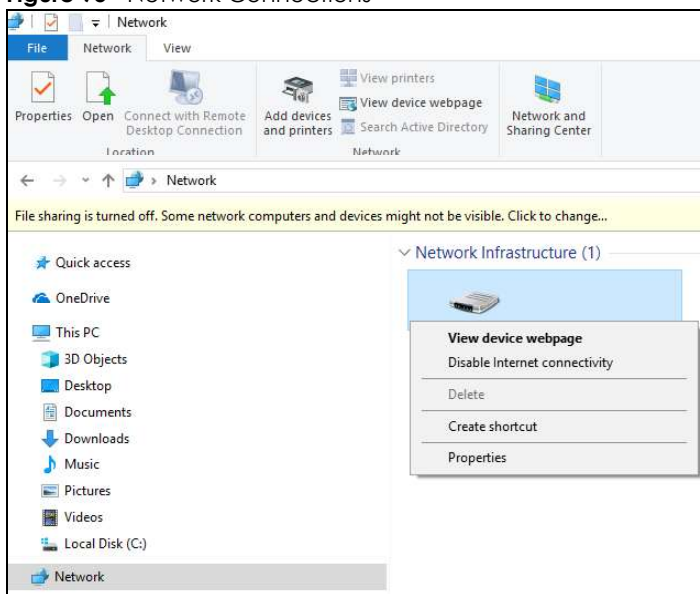
8.9.1 Auto-discover Your UPnP-enabled Network Device

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

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

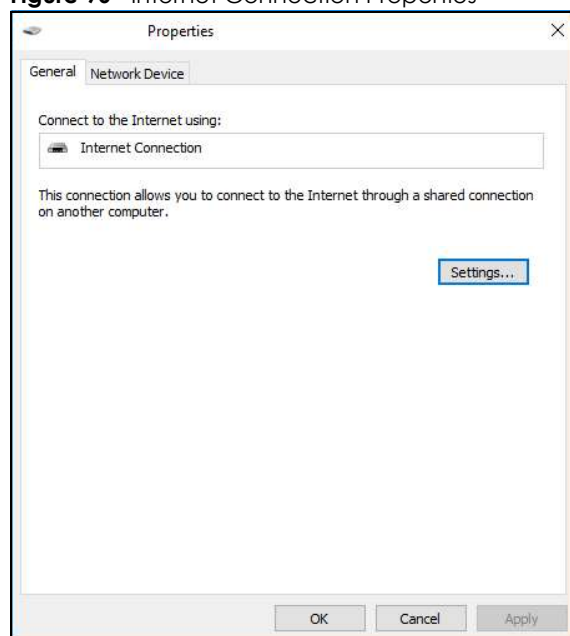
- 1 Open **File Explorer** and click **Network**.
- 2 Right-click the WE Device icon and select **Properties**.

Figure 95 Network Connections



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

Figure 96 Internet Connection Properties



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

Figure 97 Internet Connection Properties: Advanced Settings

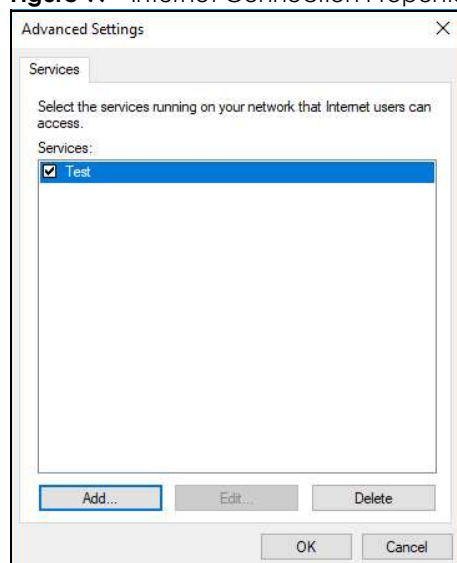
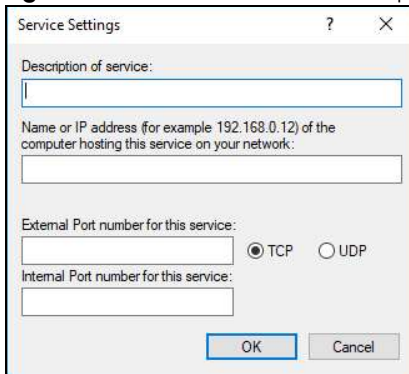


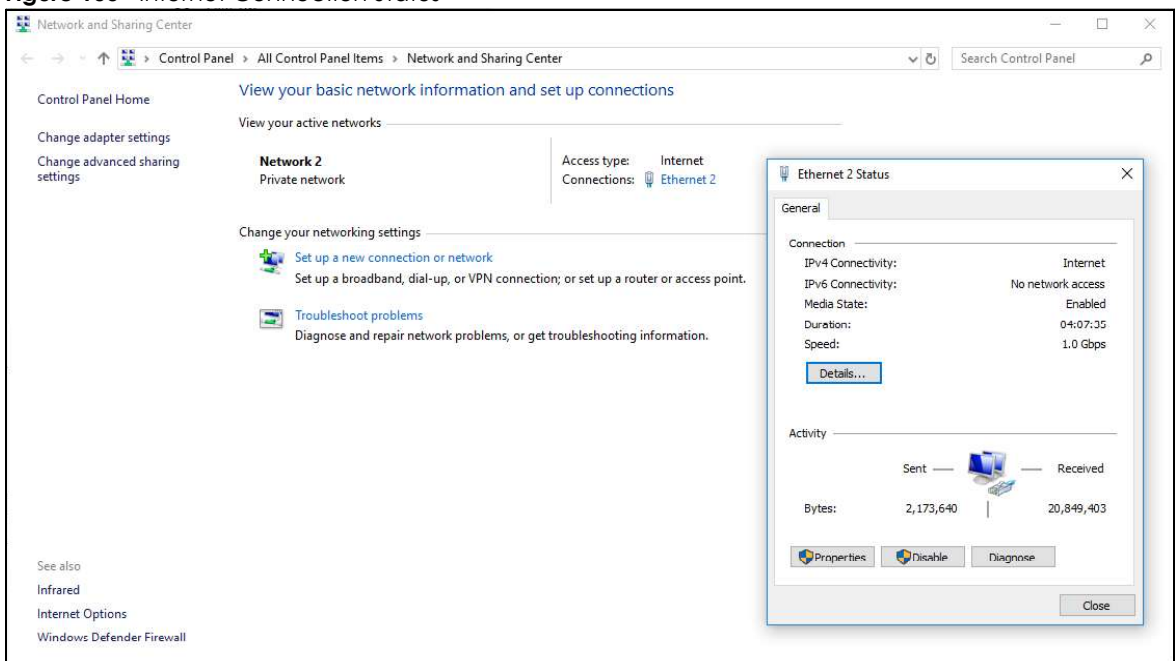
Figure 98 Internet Connection Properties: Advanced Settings: Add

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 99 System Tray Icon

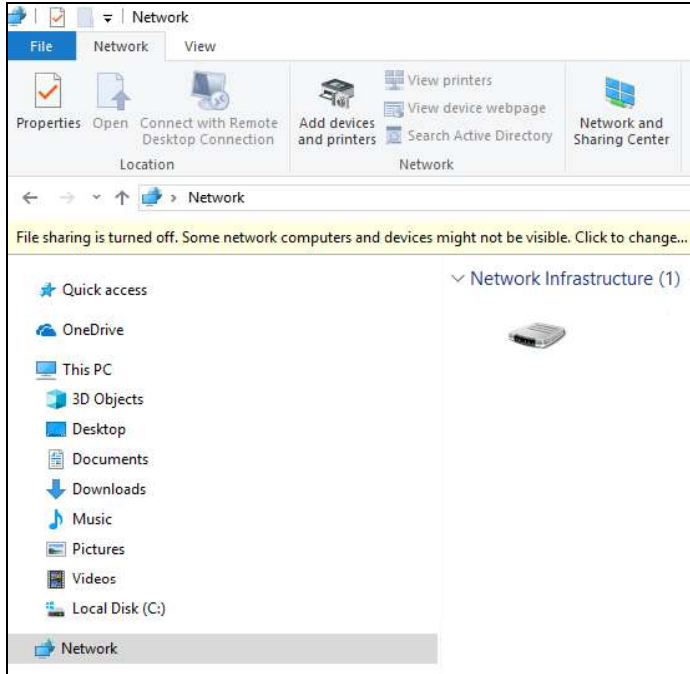
- 6 To see more details about your current Internet connection status, right click the network icon in the system tray and click **Open Network & Internet settings**. Click **Network and Sharing Center** and click the **Connections**.

Figure 100 Internet Connection Status

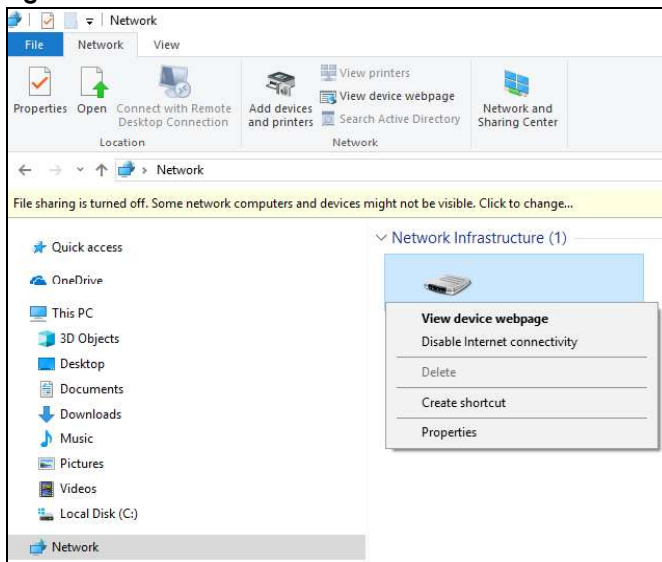
8.10 Web Configurator Access with UPnP in Windows 10

Follow the steps below to access the Web Configurator.

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

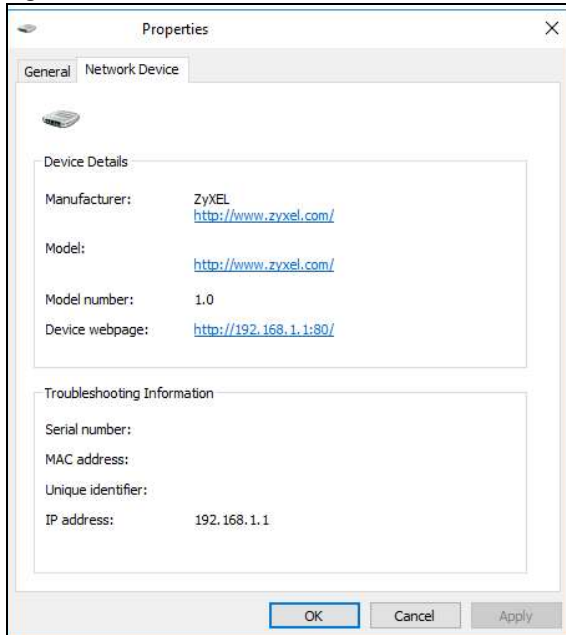
Figure 101 Network Connections

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

Figure 102 Network Connections: Network Infrastructure

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

Figure 103 Network Connections: Network Infrastructure: Properties: Example



CHAPTER 9

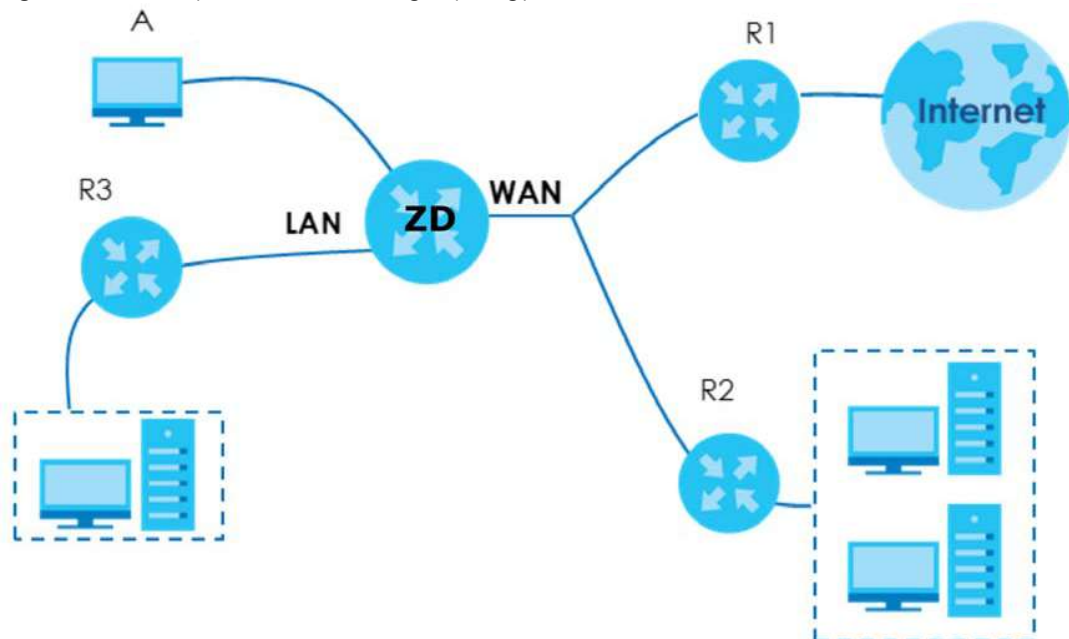
Routing

9.1 Routing Overview

The WE Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the WE 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 WE Device's LAN interface. The WE Device routes most traffic from **A** to the Internet through the WE 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 104 Example of Static Routing Topology



9.2 Configure Static Route

Use this screen to view and configure static route rules on the WE 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 105 Network Setting > Routing > Static Route

Routing

Static Route DNS Route Policy Route RIP

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
Note Maximum of 20 IPv4/IPv6 entries can be added.							

The following table describes the labels in this screen.

Table 46 Network Setting > Routing > Static Route

LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the WE 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 WE Device. Click the Delete icon to remove a static route from the WE Device.

9.2.1 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 106 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 wan ▼

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 47 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 WE 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.

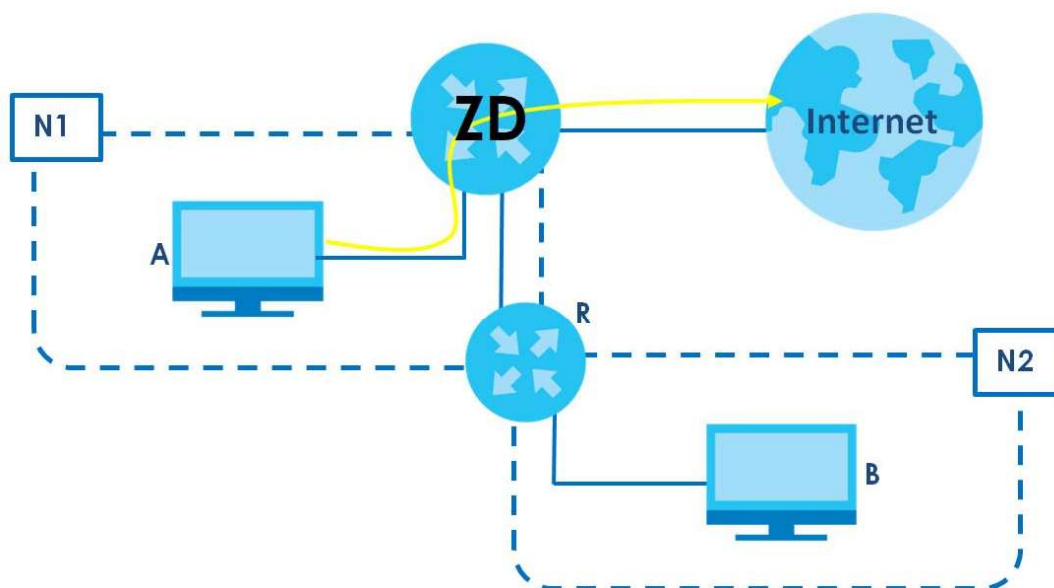
Table 47 Network Setting > Routing > Static Route > Add New Static Route (continued)

LABEL	DESCRIPTION
Use Gateway IP Address	The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. Click this switch to enable or disable the gateway IP address. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Gateway IP Address	Enter the IP address of the gateway.
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.

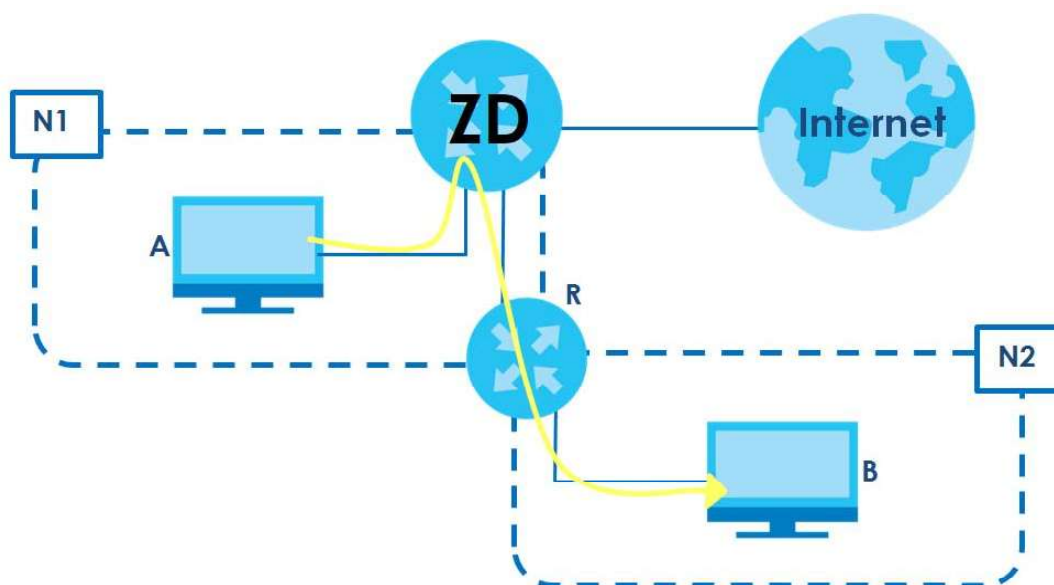
9.2.1.1 An Example of Adding a Static Route

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the WE 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 WE Device's WAN default gateway by default. In this case, **B** will never receive the traffic.

In the following figure, router **R** is connected to the WE 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 WE 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 WE Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the WE Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

Table 48 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The WE Device's WAN	172.16.1.1
The WE Device's LAN	192.168.1.1
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 WE Device's Web Configurator.
- 2 Click **Network Setting > Routing**.
- 3 Click **Add new Static Route** in the **Static Route** screen.

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

[+ Add New Static Route](#)

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

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

9.3 DNS Route

Use this screen to view and configure DNS routes on the WE Device. A DNS route entry defines a policy for the WE 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 107 Network Setting > Routing > DNS Route

Routing

Static Route **DNS Route** Policy Route RIP

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 49 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 WE Device. Click the Delete icon to remove a DNS route from the WE Device.

9.3.1 Add or Edit DNS Route

You can manually add the WE 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 108 Network Setting > Routing > DNS Route > Add New DNS Route

The following table describes the labels in this screen.

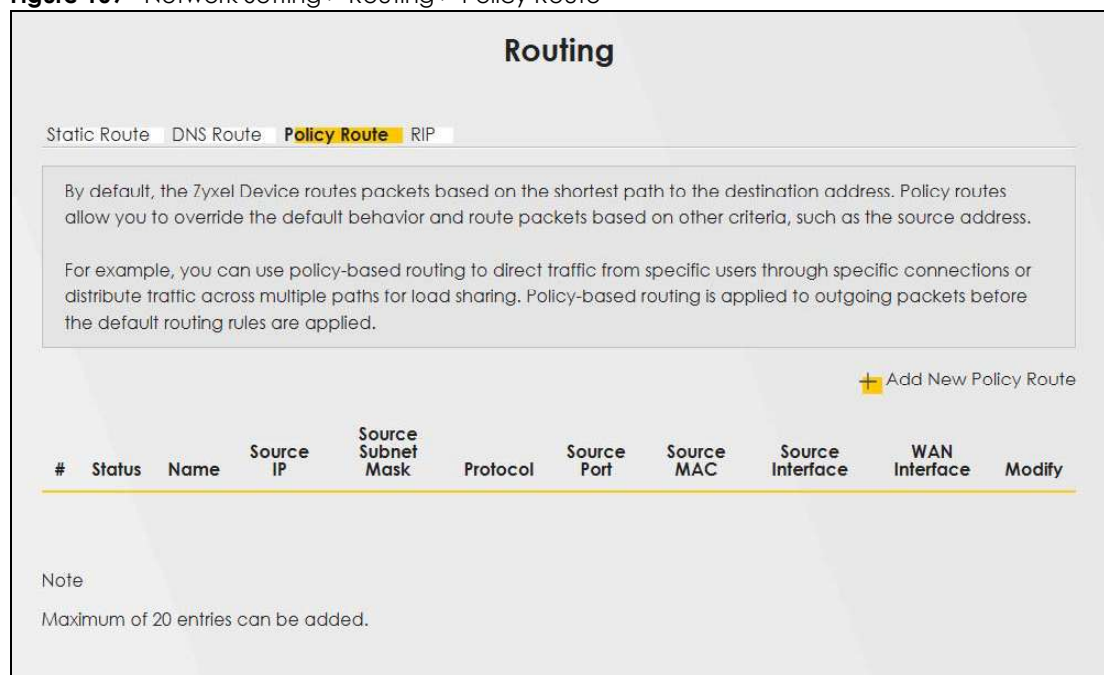
Table 50 Network Setting > Routing > DNS Route > Add New DNS Route

LABEL	DESCRIPTION
Active	Enable DNS route in your WE 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 WE 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.

9.4 Policy Route

By default, the WE 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 WE Device. Click **Network Setting > Routing > Policy Route** to open the following screen.

Figure 109 Network Setting > Routing > Policy Route


Routing

Static Route DNS Route **Policy Route** RIP

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
Note Maximum of 20 entries can be added.										

The following table describes the labels in this screen.

Table 51 Network Setting > Routing > Policy Route

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

9.4.1 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 110 Network Setting > Routing > Policy Route: Add or Edit

The following table describes the labels in this screen.

Table 52 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.
SourceInterface (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.

9.5 RIP Overview

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

9.5.1 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 111 Network Setting > Routing > RIP

Routing

Static Route DNS Route Policy Route **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	wan	RIPv2	Active	☐	☐

Cancel Apply

The following table describes the labels in this screen.

Table 53 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 WE 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 WE Device will broadcast its routing table periodically and incorporate the RIP information that it receives
Operation	Select Passive to have the WE 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 WE 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 WE 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 WE Device.

CHAPTER 10

Network Address Translation (NAT)

10.1 NAT Overview

NAT (Network Address Translation – NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

10.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the servers on your local network ([Section 10.2 on page 175](#)).
- Use the **Port Triggering** screen to add and configure the WE Device's trigger port settings ([Section 10.3 on page 178](#)).
- Use the **DMZ** screen to configure a default server ([Section 10.4 on page 182](#)).
- Use the **ALG** screen to enable or disable the SIP ALG ([Section 10.5 on page 183](#)).
- Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use ([Section 10.6 on page 184](#)).

10.1.2 What You Need To Know

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

Inside/Outside and Global/Local

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

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

NAT

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

Port Forwarding

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

10.2 Port Forwarding

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

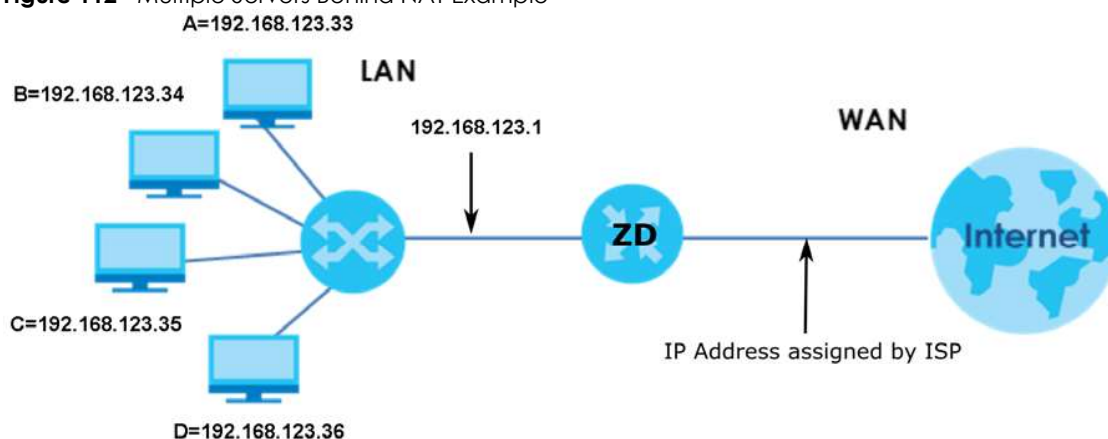
You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports. Please refer to RFC 1700 for further information about port numbers.

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

Configure Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example), a default server IP address of 192.168.1.35 to a third (**C** in the example), and a default server IP address of 192.168.1.36 to a fourth (**D** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 112 Multiple Servers Behind NAT Example

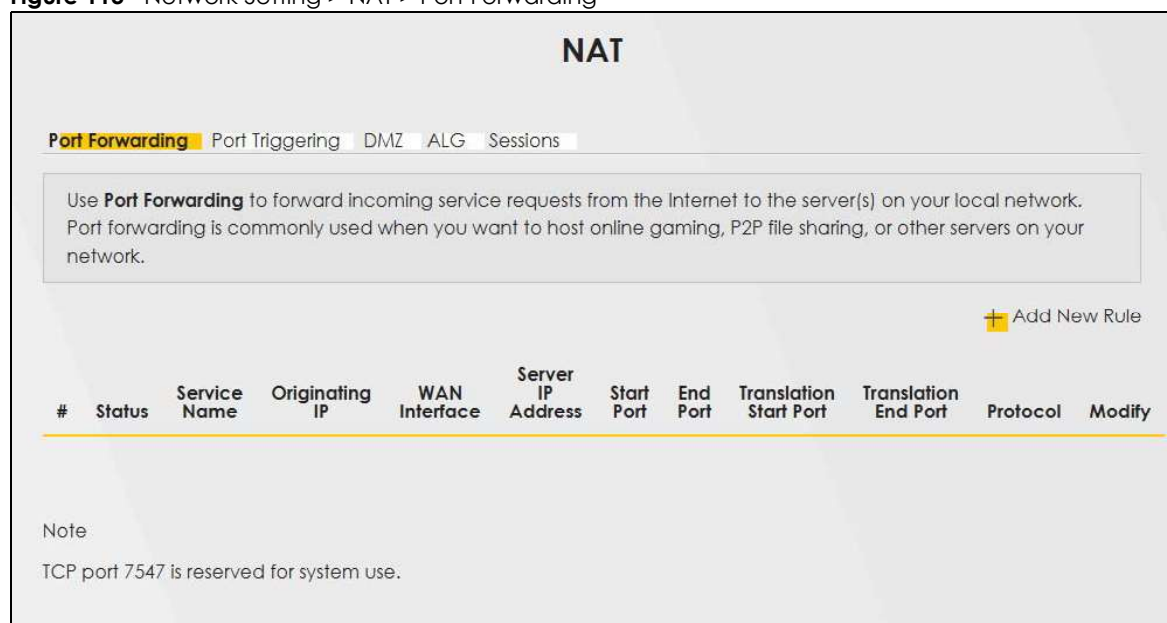


10.2.1 Port Forwarding

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

Note: TCP port 7547 is reserved for system use.

Figure 113 Network Setting > NAT > Port Forwarding



NAT

Port Forwarding Port Triggering DMZ ALG Sessions

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

+ Add New Rule

#	Status	Service Name	Originating IP	WAN Interface	Server IP Address	Start Port	End Port	Translation Start Port	Translation End Port	Protocol	Modify
Note TCP port 7547 is reserved for system use.											

The following table describes the fields in this screen.

Table 54 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add New Rule	Click this to add a new port forwarding rule.
#	This is the index number of the entry.
Status	This field indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This is the service's name. This shows User Defined if you manually added a service. You can change this by clicking the edit icon.
Originating IP	This is the source's IP address.
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.
Server IP Address	This is the server's IP address.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.
Protocol	This field displays the protocol (TCP, UDP, TCP+UDP) used to transport the packets for which you want to apply the rule.
Modify	Click the Edit icon to edit the port forwarding rule. Click the Delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.

10.2.2 Add or Edit Port Forwarding

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

Figure 114 Network Setting > NAT > Port Forwarding: Add or Edit

Add New Rule

Active ☒

Service Name

WAN Interface wan ▼

Start Port

End Port

Translation Start Port

Translation End Port

Server IP Address

Configure Originating IP ☐ Enable

Protocol TCP ▼

Note

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

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

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

2.TCP port 7547 is reserved for system use.

Cancel **OK**

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

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

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

Note: TCP port 7547 is reserved for system use.

The following table describes the labels in this screen.

Table 55 Network Setting > NAT > Port Forwarding: Add or Edit

LABEL	DESCRIPTION
Active	Click to turn the port forwarding rule on or off.
Service Name	Enter a name for the service to forward. You can use up to 256 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed.
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.
Start Port	Configure this for a user-defined entry. Enter the original destination port for the packets. To forward only one port, enter the port number again in the End Port field. To forward a series of ports, enter the start port number here and the end port number in the End Port field.
End Port	Configure this for a user-defined entry. Enter the last port of the original destination port range. To forward only one port, enter the port number in the Start Port field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the Start Port field above.
Translation Start Port	Configure this for a user-defined entry. This shows the port number to which you want the WE Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	Configure this for a user-defined entry. This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Configure Originating IP	Click the Enable checkbox to enter the source IP in the next field.
Originating IP	Enter the source IP address here.
Protocol	Select the protocol supported by this virtual server. Choices are TCP , UDP , or TCP/UDP .
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

10.3 Port Triggering

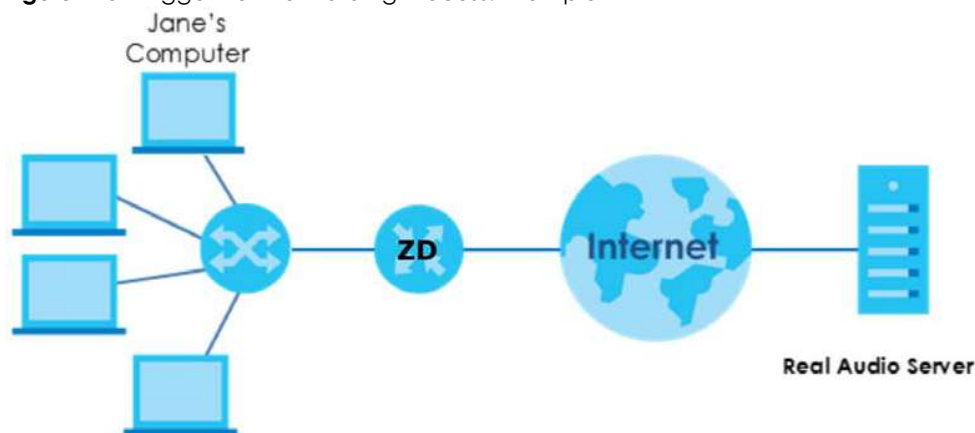
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding allows computers on the LAN to dynamically take turns using the service.

The WE Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the WE Device's WAN port receives a response with a specific port number and protocol ("open" port), the WE Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

Figure 115 Trigger Port Forwarding Process: Example



- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the WE Device to record Jane's computer IP address. The WE Device associates Jane's computer IP address with the "open" port range of 6970 – 7170.
- 3 The Real Audio server responds using a port number ranging between 6970 – 7170.
- 4 The WE Device forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The WE Device times out in 3 minutes with UDP (User Datagram Protocol) or 2 hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

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

Note: TCP port 7547 is reserved for system use.

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

Figure 116 Network Setting > NAT > Port Triggering

NAT

Port Forwarding **Port Triggering** DMZ ALG Sessions

Trigger port forwarding allows computers on the LAN to dynamically take turns using the service. The Zyxel Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the Zyxel Device's WAN port receives a response with a specific port number and protocol ("open" port), the Zyxel Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

+ Add New Rule

#	Status	Service Name	WAN Interface	Trigger Start Port	Trigger End Port	Trigger Proto.	Open Start Port	Open End Port	Open Protocol	Modify
Note TCP port 7547 is reserved for system use.										

The following table describes the labels in this screen.

Table 56 Network Setting > NAT > Port Triggering

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

10.3.1 Add or Edit Port Triggering Rule

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

Figure 117 Network Setting > NAT > Port Triggering: Add or Edit

The following table describes the labels in this screen.

Table 57 Network Setting > NAT > Port Triggering: Add or Edit

LABEL	DESCRIPTION
Active	Click this switch to activate this rule.
Service Name	Enter a name to identify this rule. You can use up to 256 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed.
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the WE Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Enter a port number or the starting port number in a range of port numbers.
Trigger End Port	Enter a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from TCP , UDP , or TCP/UDP .
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The WE Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Enter a port number or the starting port number in a range of port numbers.
Open End Port	Enter a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from TCP , UDP , or TCP/UDP .
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

10.4 DMZ

Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Triggering** screen. The DMZ (DeMilitarized Zone) is a network between the WAN and the LAN that is accessible to devices on both the WAN and LAN with firewall protection. Devices on the WAN can initiate connections to devices on the DMZ but not to those on the LAN.

You can put public servers, such as email and web servers, on the DMZ to provide services on both the WAN and LAN. To use this feature, you first need to assign a DMZ host. Click **Network Setting > NAT > DMZ** to open the **DMZ** screen.

Note: Use an IPv4 address for the DMZ server.

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

Figure 118 Network Setting > NAT > DMZ

NAT

Port Forwarding Port Triggering **DMZ** ALG Sessions

Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Triggering** screen. The DMZ (DeMilitarized Zone) is a network between the WAN and the LAN that is accessible to devices on both the WAN and LAN with firewall protection. Devices on the WAN can initiate connections to devices on the DMZ but not to those on the LAN.

You can put public servers, such as email, web, and FTP servers, on the DMZ to provide services on both the WAN and LAN. To use this feature, you first need to assign a DMZ host.

Default Server Address

Note

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

Cancel **Apply**

The following table describes the fields in this screen.

Table 58 Network Setting > NAT > DMZ

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

10.5 ALG

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

Click **Network Setting > NAT > ALG** to open the **ALG** screen. Use this screen to enable and disable the NAT Application Layer Gateway (ALG) in the WE Device.

Application Layer Gateway (ALG) allows certain applications such as Session Initiation Protocol (SIP) or file transfer in Instant Messaging (IM) applications to pass through the WE Device.

Figure 119 Network Setting > NAT > ALG

NAT

Port Forwarding Port Triggering DMZ **ALG** Sessions

Application Layer Gateway (ALG) allows customized NAT traversal filters to support address and port translation for certain applications such as File Transfer Protocol (FTP), Session Initiation Protocol (SIP), or file transfer in Instant Messaging (IM) applications. It allows SIP calls to pass through the Zyxel Device.

NAT ALG ☒

SIP ALG ☒

RTSP ALG ☒

PPTP ALG ☒

IPSEC ALG ☒

Cancel **Apply**

The following table describes the fields in this screen.

Table 59 Network Setting > NAT > ALG

LABEL	DESCRIPTION
NAT ALG	Enable this to make sure applications such as file transfer in IM applications work correctly with port-forwarding and address-mapping rules.
SIP ALG	Click this switch to enable SIP ALG to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
RTSP ALG	Click this switch to enable RTSP ALG to have the WE Device detect RTSP traffic and help build RTSP sessions through its NAT. The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
PPTP ALG	Click this switch to enable the PPTP ALG on the WE Device to detect PPTP traffic and help build PPTP sessions through the WE Device's NAT.
IPSEC ALG	Click this switch to enable IPsec ALG on the WE Device to detect IPsec traffic and help build IPsec sessions through the WE Device's NAT.

Table 59 Network Setting > NAT > ALG

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the WE Device.
Cancel	Click Cancel to restore your previously saved settings.

10.6 Sessions

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

Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use. Click **Network Setting > NAT > Sessions** to open the **Sessions** screen.

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

Figure 120 Network Setting > NAT > Sessions

NAT

Port Forwarding Port Triggering DMZ ALG **Sessions**

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

MAX NAT Session Per Host
(0 ~ 20480)

Note

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

Cancel **Apply**

The following table describes the fields in this screen.

Table 60 Network Setting > NAT > Sessions

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

10.7 Technical Reference

This part contains more information regarding NAT.

10.7.1 NAT Definitions

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

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

Note that inside or outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 61 NAT Definitions

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

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

10.7.2 What NAT Does

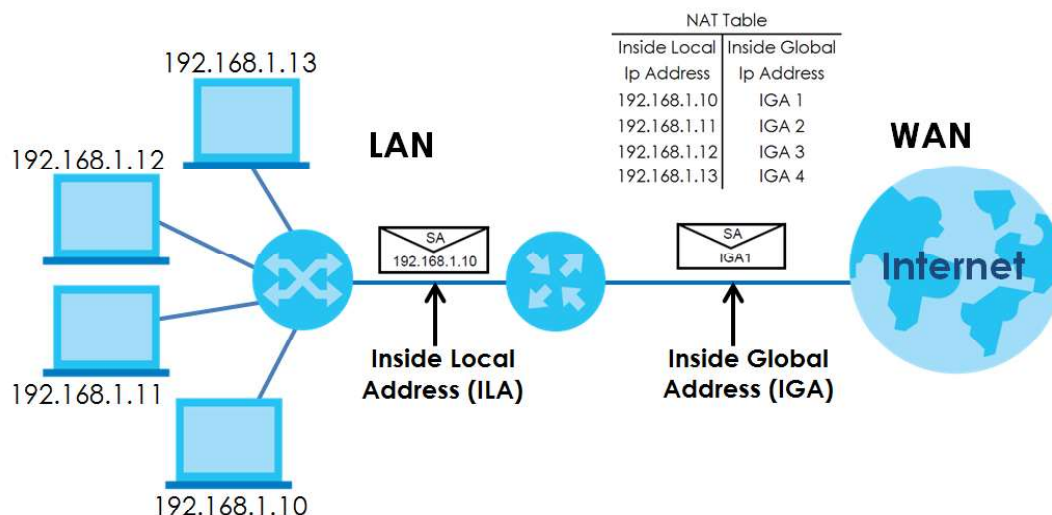
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

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

10.7.3 How NAT Works

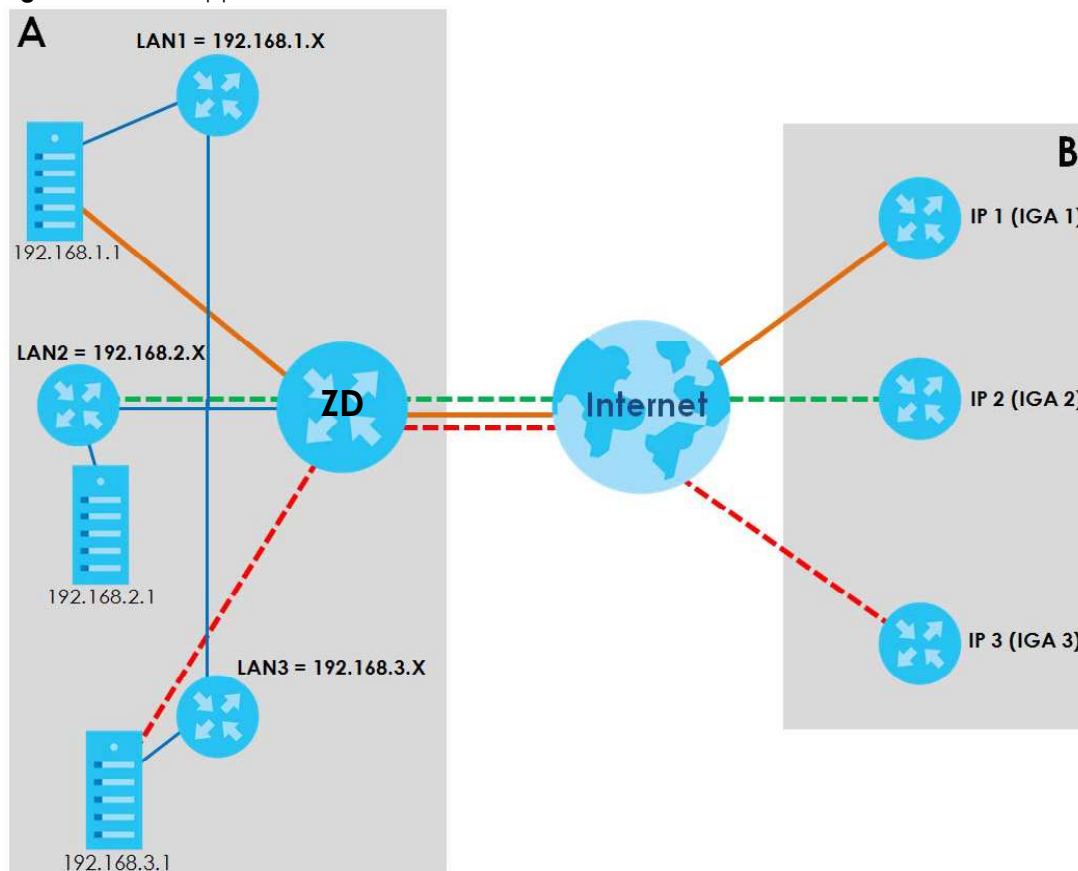
Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN,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

Figure 121 How NAT Works



10.7.4 NAT Application

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

Figure 122 NAT Application With IP Alias

Port Forwarding: Services and Port Numbers

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

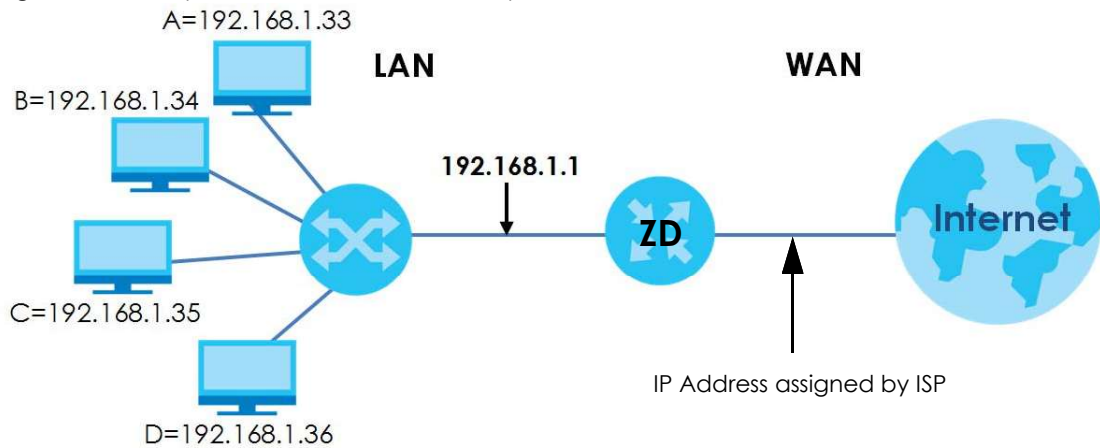
Table 62 Services and Port Numbers

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

Port Forwarding Example

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

Figure 123 Multiple Servers Behind NAT Example



CHAPTER 11

DNS

11.1 DNS Overview

DNS

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

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

Dynamic DNS

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

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

11.1.1 What You Can Do in this Chapter

- Use the **DNS Entry (DNS)** screen to view, configure, or remove DNS routes ([Section 11.2 on page 190](#)).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the WE Device ([Section 11.3 on page 191](#)).

11.1.2 What You Need To Know

DYNDNS Wildcard

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

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

11.2 DNS Entry (DNS)

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

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

Figure 124 Network Setting > DNS > DNS Entry

DNS

DNS Entry Dynamic DNS

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

+ Add New DNS Entry

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

The following table describes the fields in this screen.

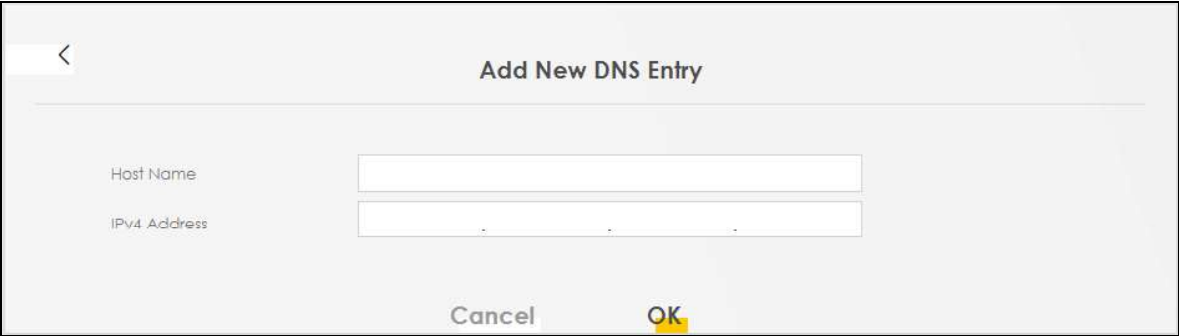
Table 63 Network Setting > DNS > DNS Entry

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

11.2.1 Add or Edit DNS Entry

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

Figure 125 Network Setting > DNS > DNS Entry: Add or Edit Network Setting > DNS: Add or Edit



The following table describes the labels in this screen.

Table 64 Network Setting > DNS > DNS Entry: Add or Edit or Network Setting > DNS: Add or Edit

LABEL	DESCRIPTION
Host Name	Enter the host name of the DNS entry. You can use up to 256 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.
IPv4 Address	Enter the IPv4 address of the DNS entry.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

11.3 Dynamic DNS

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

Figure 126 Network Setting > DNS > Dynamic DNS

DNS

DNS Entry **Dynamic DNS**

Dynamic DNS can update your current dynamic IP address mapping to a hostname. Use this screen to configure a DDNS service provider on your Zyxel Device.

Dynamic DNS Setup

Dynamic DNS ☐ Enable ☒ Disable (Settings are invalid when disable)

Service Provider

Host Name

Username

Password

Dynamic DNS Status

User Authentication Result

Last Updated Time

Current Dynamic IP

Cancel **Apply**

The following table describes the fields in this screen.

Table 65 Network Setting > DNS > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select Enable to use dynamic DNS.
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Host Name	Enter the domain name assigned to your WE Device by your Dynamic DNS provider. You can use up to 256 alphanumeric (0-9, a-z, A-Z) characters with hyphens [-] and periods [.]. You can specify up to two host names in the field separated by a comma (",").
Username	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select the checkbox to enable DynDNS Wildcard.
Enable Off Line Option (Only applies to custom DNS)	Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Dynamic DNS Status	
User Authentication Result	This shows Success if the account is correctly set up with the Dynamic DNS provider account.

Table 65 Network Setting > DNS > Dynamic DNS (continued)

LABEL	DESCRIPTION
Last Updated Time	This shows the last time the IP address the Dynamic DNS provider has associated with the hostname was updated.
Current Dynamic IP	This shows the IP address your Dynamic DNS provider has currently associated with the hostname.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

CHAPTER 12

IGMP/MLD

12.1 IGMP/MLD Overview

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

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

12.1.1 What You Need To Know

Multicast Listener Discovery (MLD)

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

- MLD allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.
- MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.
- MLD filtering controls which multicast groups a port can join.
- An MLD Report message is equivalent to an IGMP Report message, and an MLD Done message is equivalent to an IGMP Leave message.

IGMP Fast Leave

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

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

12.2 The IGMP/MLD Screen

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

Note: Some models only support IGMP/MLD **Default Version** configuration.

Note: For DX3300/3301-T0, IGMP/MLD are enabled by default and are not configurable. The default IGMP version is 3. The default MLD version is 2.

Figure 127 Network Setting > IGMP/MLD

The following table describes the labels in this screen.

Table 66 Network Setting > IGMP/MLD

LABEL	DESCRIPTION
IGMP/MLD Configuration	
Default Version	Enter the version of IGMP (1~3) and MLD (1~2) that you want the WE Device to use on the WAN.
Query Interval	Enter the number of seconds the WE Device sends a query message to hosts to get the group membership information.
Query Response Interval	Enter the maximum number of seconds the WE Device can wait for receiving a General Query message. Multicast routers use general queries to learn which multicast groups have members.
Last Member Query Interval	Enter the maximum number of seconds the WE Device can wait for receiving a response to a Group-Specific Query message. Multicast routers use group-specific queries to learn whether any member remains in a specific multicast group.
Robustness Value	Enter the number of times (1~7) the WE Device can resend a packet if packet loss occurs due to network congestion.
Maximum Multicast Groups	Enter a number to limit the number of multicast groups an interface on the WE Device is allowed to join. Once a multicast member is registered in the specified number of multicast groups, any new IGMP or MLD join report frames are dropped by the interface.
Maximum Multicast Data Sources(for IGMPv3)	Enter a number to limit the number of multicast data sources (1-24) a multicast group is allowed to have. Note: The setting only works for IGMPv3 and MLDv2.
Maximum Multicast Group Members	Enter a number to limit the number of multicast members a multicast group can have.
Fast Leave Enable	Select this option to set the WE Device to remove a port from the multicast tree immediately (without sending an IGMP or MLD membership query message) once it receives an IGMP or MLD leave message. This is helpful if a user wants to quickly change a TV channel (multicast group change) especially for IPTV applications.
LAN to LAN (Intra LAN) Multicast Enable	Select this to enable LAN to LAN IGMP snooping capability.

Table 66 Network Setting > IGMP/MLD (continued)

LABEL	DESCRIPTION
Membership Join Immediate (IPTV)	Select this to have the WE Device add a host to a multicast group immediately once the WE Device receives an IGMP or MLD join message.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes back to the WE Device.

CHAPTER 13

Firewall

13.1 Firewall Overview

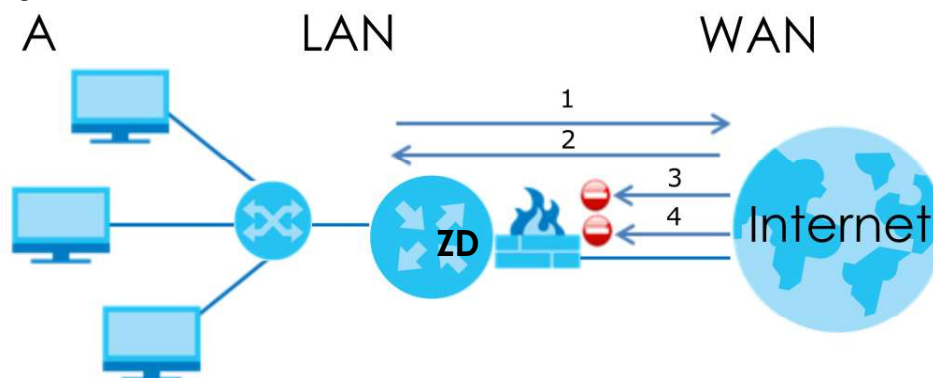
This chapter shows you how to enable the WE Device firewall. Use the firewall to protect your WE Device and network from attacks by hackers on the Internet and control access to it. The firewall:

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

By default, the WE Device blocks DoS attacks whether the firewall is enabled or disabled.

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

Figure 128 Default Firewall Action



13.1.1 What You Need to Know About Firewall

SYN Attack

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

DoS

Denial-of-Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access

to network resources. The WE Device is pre-configured to automatically detect and thwart all known DoS attacks.

DoS Thresholds

For DoS attacks, the WE Device uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions. You can use the default threshold values, or you can change them to values more suitable to your security requirements.

DDoS

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

ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

LAND Attack

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

Ping of Death

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

SPI

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

13.2 Firewall

Use the firewall to protect your WE Device and network from attacks by hackers on the Internet and control access to it.

13.2.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the WE Device ([Section 13.3 on page 199](#)).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules ([Section 13.4 on page 200](#)).

- Use the **Access Control** screen to view and configure incoming or outgoing filtering rules ([Section 13.5 on page 202](#)).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks ([Section 13.6 on page 205](#)).

13.3 General

Use the firewall to protect your WE Device and network from attacks by hackers on the Internet and control access to it. Use this screen to set the security level of the firewall on the WE Device. Firewall rules are grouped based on the direction of travel of packets. A higher firewall level means more restrictions on the Internet activities you can perform. Click **Security > Firewall > General** to display the following screen. Use the slider to select the level of firewall protection.

Figure 129 Security > Firewall > General

Firewall

General | Protocol | Access Control | Dos

Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. Use this screen to set the security level of the firewall on the Zyxel Device. Firewall rules are grouped based on the direction of travel of packets to which they apply. A higher firewall level means more restrictions on the Internet activities you can perform.

IPv4 Firewall ☒

IPv6 Firewall ☒

Low Medium (Recommended) High

	Low	Medium (Recommended)	High
LAN to WAN	☒	☒	☐
WAN to LAN	☒	☐	☐

Note

(1) LAN to WAN is your access to all Internet services. WAN to LAN is the access of other computers on the Internet to devices behind the Zyxel Device.

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

(3) We do not recommend you to disable the Firewall for your Zyxel device and network.

Note: LAN to WAN is your access to all Internet services. WAN to LAN is the access of other computers on the Internet to devices behind the WE Device. When the security level is set to **High**, Telnet, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and/or IPv6 ICMPv6 (Ping) traffic from the LAN are still allowed.

The following table describes the labels in this screen.

Table 67 Security > Firewall > General

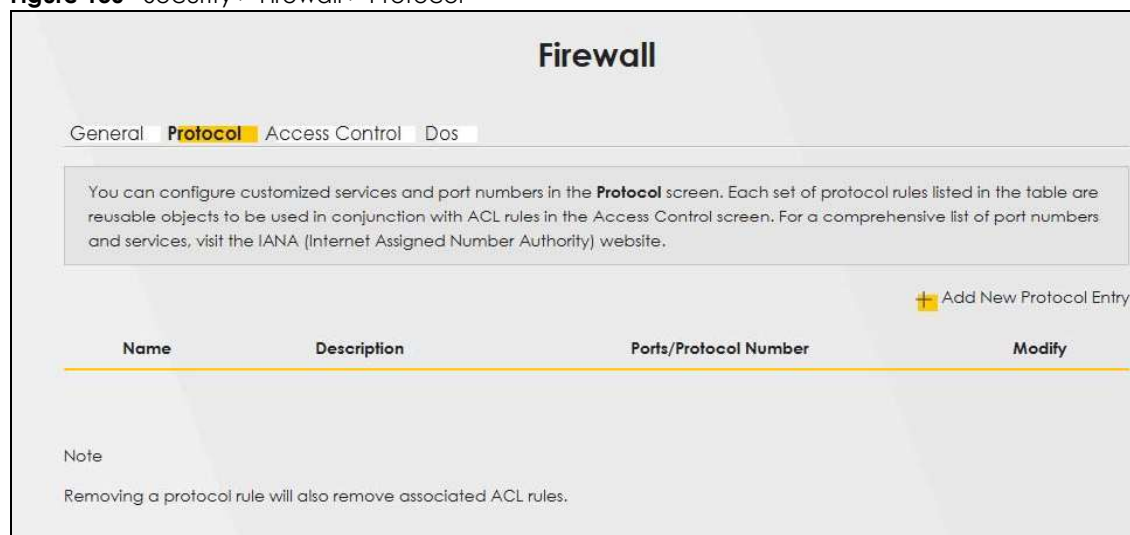
LABEL	DESCRIPTION
IPv4 Firewall	Enable firewall protection when using IPv4 (Internet Protocol version 4).
IPv6 Firewall	Enable firewall protection when using IPv6 (Internet Protocol version 6).
High	This setting blocks all traffic to and from the Internet. Only local network traffic and LAN to WAN service (Telnet, HTTP, HTTPS, DNS, POP3, SMTP) is permitted.
Medium	This is the recommended setting. It allows traffic to the Internet but blocks anyone from the Internet from accessing any services on your local network.
Low	This setting allows traffic to the Internet and also allows someone from the Internet to access services on your local network. This would be used with Port Forwarding, Default Server.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

13.4 Protocol

You can configure customized services and port numbers in the **Protocol** screen. Each set of protocol rules listed in the table are reusable objects to be used in conjunction with ACL rules in the Access Control screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. Click **Security > Firewall > Protocol** to display the following screen.

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

Figure 130 Security > Firewall > Protocol



Firewall

General **Protocol** Access Control Dos

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

+ Add New Protocol Entry

Name	Description	Ports/Protocol Number	Modify
Note Removing a protocol rule will also remove associated ACL rules.			

The following table describes the labels in this screen.

Table 68 Security > Firewall > Protocol

LABEL	DESCRIPTION
Add New Protocol Entry	Click this to configure a customized service.
Name	This is the name of your customized service.
Description	This is a description of your customized service.
Ports/Protocol Number	This shows the port number or range and the IP protocol (TCP or UDP) that defines your customized service.
Modify	Click this to edit a customized service.

13.4.1 Add New Protocol Entry

Add a customized rule or edit an existing rule by specifying the protocol and the port numbers. Click **Add New Protocol Entry** in the **Protocol** screen to display the following screen.

Figure 131 Security > Firewall > Protocol: Add New Protocol Entry

The following table describes the labels in this screen.

Table 69 Security > Firewall > Protocol: Add New Protocol Entry

LABEL	DESCRIPTION
Service Name	Enter a descriptive name for your customized service. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed.
Description	Enter a description for your customized service. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed.
Protocol	Select the protocol (TCP , UDP , ICMP , ICMPv6 , or Other) that defines your customized port from the drop down list box.
Protocol Number	Enter a single port number or the range of port numbers (0 – 255) that define your customized service.
Source Port	This field is displayed if you select either the TCP or UDP protocol. You may set it to Any , Single , or Range and enter the Port Number or range of Port Numbers for your source port.
Destination Port	This field is displayed if you select either the TCP or UDP protocol. You may set it to Any , Single , or Range and enter the Port Number or range of Port Numbers for your destination port.
ICMPv6type	This field is displayed if you select the ICMPv6 protocol. From the drop-down menu, select which type value you would like to use.

Table 69 Security > Firewall > Protocol: Add New Protocol Entry (continued)

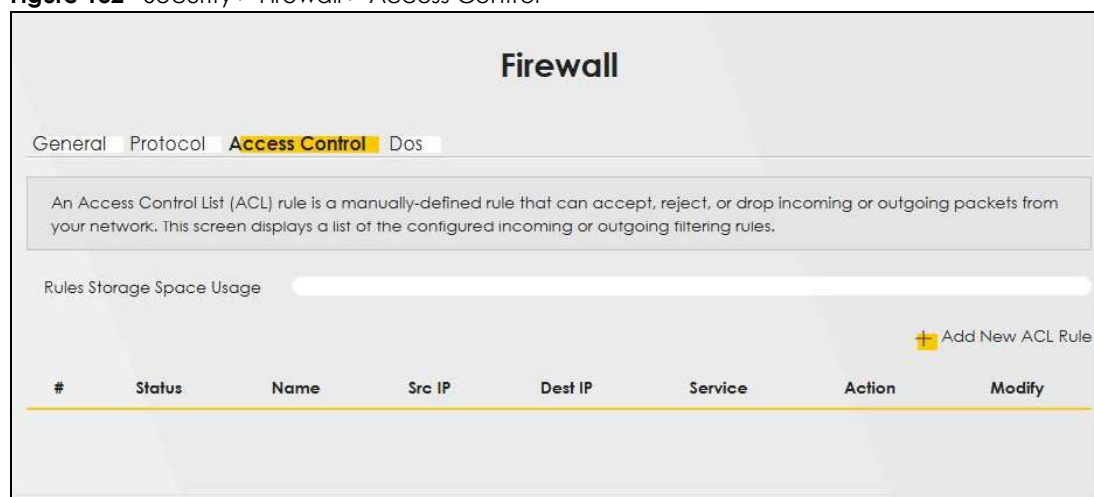
LABEL	DESCRIPTION
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

13.5 Access Control (Rules)

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

Note: The ordering of your rules is very important as rules are applied in turn.

Figure 132 Security > Firewall > Access Control



The following table describes the labels in this screen.

Table 70 Security > Firewall > Access Control

LABEL	DESCRIPTION
Rules Storage Space Usage	This read-only bar shows how much of the WE Device's memory is in use for recording firewall rules. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Add New ACL Rule	Select an index number and click Add New ACL Rule to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
#	This field displays the rule index number. The ordering of your rules is important as rules are applied in turn.
Status	This field displays the status of the ACL rule. A yellow bulb signifies that this ACL rule is active, while a gray bulb signifies that this ACL rule is not active.
Name	This field displays the rule name.
Src IP	This field displays the source IP addresses to which this rule applies.
Dest IP	This field displays the destination IP addresses to which this rule applies.

Table 70 Security > Firewall > Access Control (continued)

LABEL	DESCRIPTION
Service	This field displays the protocol (All, TCP, UDP, TCP/UDP, ICMP, ICMPv6, or any) used to transport the packets for which you want to apply the rule.
Action	Displays whether the firewall silently discards packets (Drop), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (Reject), or allow the passage of (Accept) packets that match this rule.
Modify	Click the Edit icon to edit the firewall rule. Click the Delete icon to delete an existing firewall rule.

13.5.1 Add New ACL Rule

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

Figure 133 Security > Firewall > Access Control > Add New ACL Rule

Add New ACL Rule

Active ☒

Filter Name

Order

Select Source IP Address

Source IP Address

Select Destination Device

Destination IP Address

MAC Address

IP Type

Select Service

Protocol

Custom Source Port -

Custom Destination Port -

Policy

Direction

Enable Rate Limit ☐

packet(s) per (1-512)

Scheduler Rules

Add New Rule

Cancel **OK**

The following table describes the labels in this screen.

Table 71 Security > Firewall > Access Control > Add New ACL Rule

LABEL	DESCRIPTION
Active	Click this switch to enable this ACL rule.
Filter Name	Enter a descriptive name for your filter rule. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed.
Order	Assign the order of your rules as rules are applied in turn.
Select Source IP Address	If you want the source to come from a particular (single) IP, select Specific IP Address . If not, select from a detected device.
Select Source Device	If you want the source to come from a particular (single) IP, select Specific IP Address . If not, select from a detected device.
Source IP Address	If you selected Specific IP Address in the previous item, enter the source device's IP address here. Otherwise this field will be hidden if you select the detected device.
Select Destination Device	If you want your rule to apply to packets with a particular (single) IP, select Specific IP Address . If not, select a detected device.
Destination IP Address	If you selected Specific IP Address in the previous item, enter the destination device's IP address here. Otherwise this field will be hidden if you select the detected device.
MAC Address	Enter the MAC addresses of the WiFi or wired LAN clients that are allowed access to the WE 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.
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 1038 IP addresses. The WE Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).
Select Service	Select a service from the Select Service box.
Protocol	Select the protocol (ALL , TCP/UDP , TCP , UDP , ICMP , or ICMPv6) used to transport the packets for which you want to apply the rule.
Custom Source Port	This is a single port number or the starting port number of a range that defines your rule.
Custom Destination Port	This is a single port number or the ending port number of a range that defines your rule.
TCP Flag	Select the TCP Flag (SYN, ACK, URG, PSH, RST, FIN). This appears when you select TCP/UDP or TCP in the Protocol field.
Type	This field is displayed only when you select Specific Protocol in Select Service and ICMPv6 in the protocol field. From the drop-down list box, select which ICMPv6 type you would like to use.
Policy	Use the drop-down list box to select whether to discard (Drop), deny and send an ICMP destination-unreachable message to the sender (Reject), or allow the passage of (Accept) packets that match this rule.
Direction	Select WAN to LAN to apply the rule to traffic from WAN to LAN. Select LAN to WAN to apply the rule to traffic from LAN to WAN. Select WAN to Router to apply the rule to traffic from WAN to router. Select LAN to Router to apply the rule to traffic from LAN to router.
Enable Rate Limit	Click this switch to enable the setting of maximum number of packets per maximum number of minute or second to limit the throughput of traffic that matches this rule. If not, the next item will be disabled.
Scheduler Rules	Select a schedule rule for this ACL rule from the drop-down list box. You can configure a new schedule rule by clicking Add New Rule . This will bring you to the Security > Scheduler Rules screen.
packet(s) per (1–512)	Enter the maximum number of packets (1 – 512) per minute or second.

Table 71 Security > Firewall > Access Control > Add New ACL Rule (continued)

LABEL	DESCRIPTION
Add New Rule	Select a schedule rule for this ACL rule from the drop-down list box. You can configure a new schedule rule by clicking Add New Rule .
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

13.6 DoS

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. Use the **DoS** screen to activate protection against DoS attacks.

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

Figure 134 Security > Firewall > DoS

Firewall

General Protocol Access Control **DoS**

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

Use the **DoS** screen to activate protection against DoS attacks.

Dos Protection Blocking ☒ Enable ☐ Disable (Settings are invalid when disable)

Cancel Apply

The following table describes the labels in this screen.

Table 72 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Enable this to protect against DoS attacks. The WE Device will drop sessions that surpass maximum thresholds.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

13.7 Firewall Technical Reference

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

13.7.1 Firewall Rules Overview

Your customized rules take precedence and override the WE Device's default settings. The WE Device checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the WE Device takes the action specified in the rule.

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to Router
- LAN to WAN
- WAN to LAN
- WAN to Router

By default, the WE Device's stateful packet inspection allows packets traveling in the following directions:

- LAN to Router

These rules specify which computers on the LAN can manage the WE Device (remote management).

Note: You can also configure the remote management settings to allow only a specific computer to manage the WE Device.

- LAN to WAN

These rules specify which computers on the LAN can access which computers or services on the WAN.

By default, the WE Device's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN

These rules specify which computers on the WAN can access which computers or services on the LAN.

Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN.

- WAN to Router

By default the WE Device stops computers on the WAN from managing the WE Device. You could configure one of these rules to allow a WAN computer to manage the WE Device.

Note: You also need to configure the remote management settings to allow a WAN computer to manage the WE Device.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a web server.

- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the source IP address, destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the WE Device's default rules.

13.7.2 Guidelines For Security Enhancement With Your Firewall

- 1 Change the default password through the Web Configurator.
- 2 Think about access control before you connect to the network in any way.
- 3 Limit who can access your router.
- 4 Do not enable any local service (such as telnet) that you do not use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

13.7.3 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the WE Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

- 1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC (Internet Relay Chat) is blocked, are there users that require this service?
- 2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- 3 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the Web Configurator screens.

CHAPTER 14

MAC Filter

14.1 MAC Filter Overview

You can configure the WE Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired 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 wired LAN client to configure this screen.

14.2 MAC Filter

Enable **MAC Address Filter** and add the host name and MAC address of a wired LAN client to the table if you wish to allow or deny them access to your network. You can choose to enable or disable the filters per entry; make sure that the checkbox under **Active** is selected if you want to use a filter. Select **Security > MAC Filter**. The screen appears as shown.

Figure 135 Security > MAC Filter

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 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.

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

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
-----	--------	-----------	-------------	--------

The following table describes the labels in this screen.

Table 73 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select Enable to activate the MAC filter function.
MAC Restrict Mode	Select Allow to only permit the listed MAC addresses access to the WE Device. Select Deny to permit anyone access to the WE Device except the listed MAC addresses.
Add New Rule	Click the Add button to create a new entry.
Add New Rule	Select an existing wired LAN client from the list to add as a new entry. Select Custom if you want to manually enter the Host Name and MAC Address . Click the Add button to create a new entry.
Set	This is the index number of the MAC address.
Active	Select Active to enable the MAC filter rule. The rule will not be applied if Allow is not selected under MAC Restrict Mode .
Host Name	Enter the host name of a wired LAN client that you want to allow access to the WE Device. You can use up to 17 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed.
MAC Address	Enter the MAC address of a wired LAN client that you want to allow access to the WE Device. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Delete	Click the Delete icon to delete an existing rule.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

14.2.1 Add New Rule

You can choose to enable or disable the filters per entry; make sure that the checkbox under **Active** is selected if you want to use a filter, as shown in the example below. Select **Security > MAC Filter > Add New Rule**. The screen appears as shown.

Figure 136 Security > MAC Filter > Add New Rule

Set	Active	Host Name	MAC Address	Delete
1	☒	test	BC - 22 - 33 - 11 - 66 - AA	
2	☒	Test	BC - 88 - 99 - 00 - 11 - 22	

The following table describes the labels in this screen.

Table 74 Security > MAC Filter > Add New Rule

LABEL	DESCRIPTION
Set	This is the index number of the MAC address.
Active	Select Active to enable the MAC filter rule. The rule will not be applied if Allow is not selected under MAC Restrict Mode .
Host Name	Enter the host name of a wired LAN client that you want to allow access to the WE Device. You can use up to 17 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed.
MAC Address	Enter the MAC addresses of a wired LAN client that you want to allow access to the WE 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.

Table 74 Security > MAC Filter > Add New Rule (continued)

LABEL	DESCRIPTION
Delete	Click the Delete icon to delete an existing rule.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

CHAPTER 15

Home Security

15.1 Home Security Overview

The WE Device supports URL (Uniform Resource Locator) filtering that allows you to block user access to specific websites containing inappropriate or harmful content. Users on your network will not be able to enter the websites with URL domain names, keywords or full URLs you specify.

15.2 Home Security

Use this screen to configure URL filtering settings to block users on your network from accessing certain websites. To access this screen, click **Security > Home Security**.

Figure 137 Security > Home Security

Connected Home Security

You may be more specific by adding URL into the list. The website under the specific domain will be blocked.

Enter Website URL

example.com

Block

Block List

examplewebsite X

The following table describes the labels in this screen.

Table 75 Security > Home Security

LABEL	DESCRIPTION
Enter Website URL	Enter the URL of a website or URL keyword to which the WE Device blocks access. Click Block to add the website to the Block List. Use keywords, domain names, or full URLs to block websites. For example, if you want to block a website with the domain name "www.exampleWeb.com", you can use the following input formats: • http://exampleWeb.com • https://exampleWeb.com • exampleWeb.com • www.exampleWeb.com • example
Block List	The WE Device prohibits users on your network from viewing the websites with the URLs/keywords in this block list. Click x to remove the entry from the list.

CHAPTER 16

Parental Control

16.1 Parental Control Overview

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

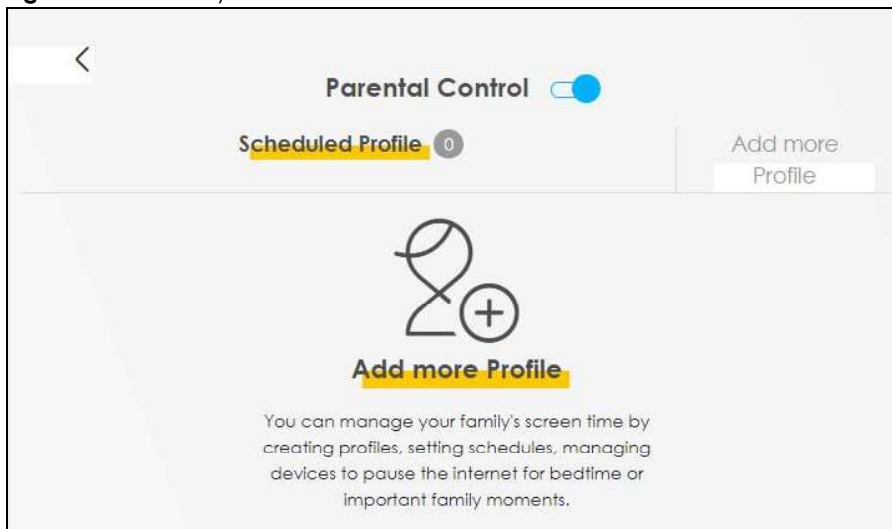
16.2 Parental Control Schedule

Use this screen to enable parental control and view parental control rules and schedules. You can limit the time a user can access the Internet. These rules are defined in a Parental Control Profile (PCP).

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

Note: For some WE Device models, you need to disable MESH to add a new parental control profile.

Figure 138 Security > Parental Control



The following table describes the fields in this screen.

Table 76 Security > Parental Control

LABEL	DESCRIPTION
Parental Control	Click this switch to enable or disable parental control.

Table 76 Security > Parental Control (continued)

LABEL	DESCRIPTION
Scheduled Profile	This screen shows all the created profiles.
Add more Profile	Click this button to create a new profile.

16.2.1 Add or Edit a Parental Control Profile

Click **Add more Profile** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule.

Figure 139 Security > Parental Control > Add more Profile: Select Device

The following table describes the fields in this screen.

Table 77 Security > Parental Control > Add more Profile: Select Device

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 or disable 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.
Next	Click Next to go to the next step to set a schedule for this profile.

16.2.2 Define a Schedule

This screen allow you to define time periods and days during which Internet access is blocked on the profile devices. Finish the settings in the **Select Device** step and click **Next** to access this screen.

Figure 140 Security > Parental Control > Add more Profile: Time limits

The screenshot shows the 'Parental Control' interface with the 'Time limits' step selected. The left sidebar contains profile settings, and the main area shows the scheduling options for blocking internet access.

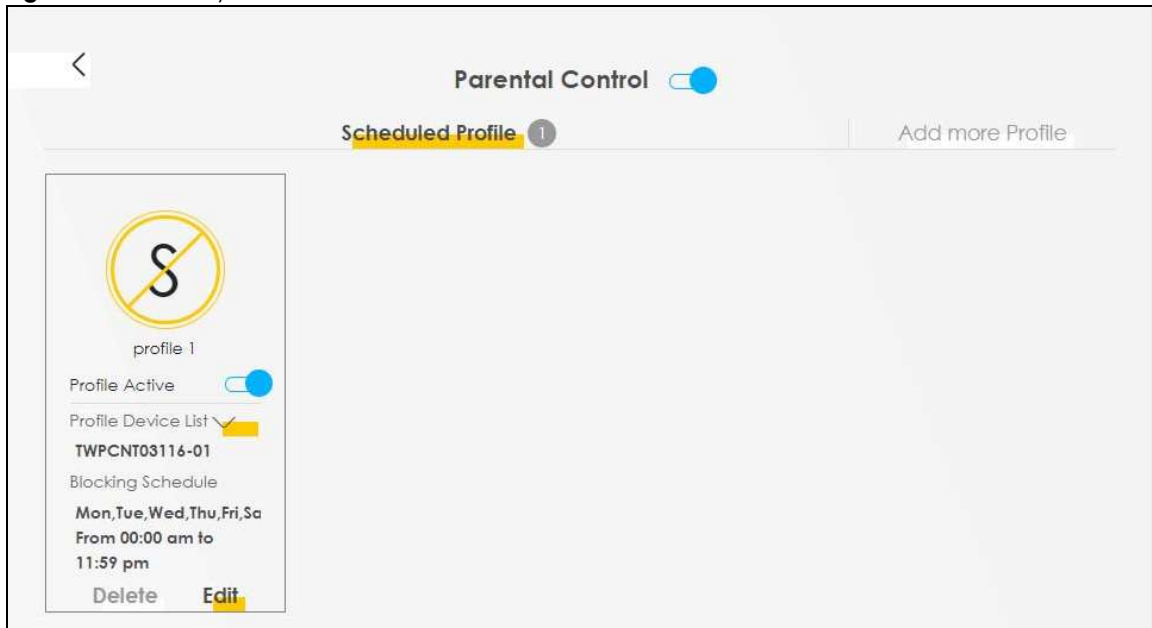
The following table describes the fields in this screen.

Table 78 Security > Parental Control > Add more Profile: Time limits

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile.
Profile Active	Click this switch to enable or disable this profile. When the switch goes to the right ( , this profile is active. 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 devices.
Schedule	
Add New Schedule	Click this to add a new block for scheduling.
Start/End blocking	Select the time period when Internet access is blocked on the profile devices.
Repeat On	Select the days when Internet access is blocked on the profile devices. Select Whole Week and the scheduler rule will be activated for the whole week.
Back	Click Back to return to the previous screen.
Save	Click Save to save your changes.

16.2.3 Parental Control Scheduled Profile

Use this screen to view and manage the created parental control profiles.

Figure 141 Security > Parental Control > Scheduled Profile

The following table describes the fields in this screen.

Table 79 Security > Parental Control > Scheduled Profile

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

CHAPTER 17

Certificates

17.1 Certificates Overview

The WE Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

17.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to view and import the WE Device's CA-signed (Certification Authority) certificates ([Section 17.3 on page 217](#)).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the WE Device. You can also export the certificates to a computer ([Section 17.4 on page 221](#)).

17.2 What You Need to Know

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

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the WE Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

17.3 Local Certificates

Use this screen to view the WE Device's summary list of certificates, generate certification requests, and import signed certificates. You can import the following certificates to your WE Device:

- Web Server – This certificate secures HTTP connections.
- SSH – This certificate secures remote connections.

Click **Security** > **Certificates** to open the **Local Certificates** screen.

Figure 142 Security > Certificates > Local Certificates

Certificates

Local Certificates Trusted CA

The Zyxel Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Use this screen to view the Zyxel Device's summary list of certificates, generate certification requests, and import signed certificates.

Replace PrivateKey/Certificate file in PEM format

☐ Private Key is protected by password

Choose File No file chosen

Import Certificate Create Certificate Request

Current File	Subject	Issuer	Valid From	Valid To	Modify
--------------	---------	--------	------------	----------	--------

The following table describes the labels in this screen.

Table 80 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Replace Private Key/Certificate file in PEM format	
Private Key is protected by password	Select the checkbox and enter the private key into the text box to store it on the WE Device. The private key should not exceed 63 ASCII characters (not including spaces).
Choose File	Click this button to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the WE Device.
Create Certificate Request	Click this button to go to the screen where you can have the WE Device generate a certification request.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have a unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the View icon to open a screen with an in-depth list of information about the certificate. For a certification request, click Load Signed to import the signed certificate. Click the Remove icon to remove the certificate (or certification request). A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.

17.3.1 Create Certificate Request

Click **Security > Certificates > Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the WE Device generate a certification request. To create a certificate signing request, you need to enter a common name, organization name, state or province name, and the default US two-letter country code (The US country code is by default and not changeable when sold in the U.S.) for the certificate.

Figure 143 Create Certificate Request

The following table describes the labels in this screen.

Table 81 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select Auto to have the WE Device configure this field automatically. Or select Customize to enter it manually. Type the IP address (in dotted decimal notation), domain name or email address in the field provided. The domain name or email address can be up to 63 ASCII characters. The domain name or email address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the WE Device drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the WE Device drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

17.3.2 View Certificate Request

Use this screen to view in-depth information about the certificate request. The **Certificate** is used to verify the authenticity of the certification authority. The **Private Key** serves as your digital signature for authentication and must be safely stored. The **Signing Request** contains the certificate signing request value that you will copy upon submitting the certificate request to the CA (certificate authority).

Click the **View** icon in the **Local Certificates** screen to open the following screen.

Figure 144 Certificate Request: View

The screenshot shows a window titled "View Certificate" with a close button in the top right corner. The window contains a "Certificate Details" section with the following fields:

- Name:** Test
- Type:** none
- Subject:** /CN=588BF3-VMG8825-B50B-S172V48000015/O=Zyxel/ST=Hsinchu/C=TW

Below these fields are three large text areas:

- Certificate:** A large empty box for the certificate content.
- Private Key:** A text area containing a long string of alphanumeric characters, including "hGEzXjrkPkeJHmKBehzvdv", "KGLNbx22N1C0qtl++BwFFzOK8xTshyNxGW27goeOY", "1QpuD2RQy1FB+Ky9zVNCrUP", "6C1korOCNOwp2Mds4udfazEzEefm7ysyC0P2etwd7", "AbLBM49P1qUsWbGWR9snO74", "Myqhf+kCc2R801HUQvWX7XbHzTG+8RKTpV/oCkLZy", "cUBlyq0IY2f6FkWQBxp9C2H", "xteLLgB6SXDfK5vTyQTcj0spmPNdj4ZkxKhqtuLwM8E3", "bzHCdujBwvzZXnf6NxAZ", and "fAdmacECaYEA+SlZJoWxoB90BopN1JP3t//IOLPznbs".
- Signing Request:** A text area containing a long string of alphanumeric characters, including "-----BEGIN CERTIFICATE REQUEST-----", "MIICoDCCAYgCAQAwWzEgMCgGA1UEAwwhNlg4", "QkYzLVZNRzg4MjU0UjUwQl11TMTcy", "VjQ4MDAwMDE1MQ4wDAYDVQQKDAVaeXhibDEQ", "MA4GA1UECAwHSHNpbm11NodTElMAkG", "A1UEBhMCVfcwggEIMA0GCSqGSIb3DQEBAQUAAI", "BDwAwggEKAoIBAQDMCB3HK+Su", "PeKUpWid2QkPL4qsQsYXhL7chlIWxCYAFw9QQYXP", "NDQm4l3bS9rfwLqUMFck3F4HQ", and "-----END CERTIFICATE REQUEST-----".

At the bottom of the window is a yellow button labeled "Back".

The following table describes the fields in this screen.

Table 82 Certificate Request: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).

Table 82 Certificate Request: View (continued)

LABEL	DESCRIPTION
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution.
Private Key	This field displays the private key of this certificate.
Signing Request	This field displays the CSR (Certificate Signing Request) information of this certificate. The CSR will be provided to a certificate authority, and it includes information about the public key, organization name, domain name, location, and country of this certificate.
Back	Click Back to return to the previous screen.

17.4 Trusted CA

Click **Security > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the WE Device to accept as trusted. The WE Device accepts any valid certificate signed by a certification authority on this list as being trustworthy, which means you do not need to import any certificate that is signed by one of these certification authorities.

Note: A maximum of ten certificates can be added.

Figure 145 Security > Certificates > Trusted CA

The following table describes the labels in this screen.

Table 83 Security > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the WE Device.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have a unique subject information.

Table 83 Security > Certificates > Trusted CA (continued)

LABEL	DESCRIPTION
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Modify	Click the View icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the Remove icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

17.5 Import Trusted CA Certificate

Click **Import Certificate** in the **Trusted CA** screen to open the **Import Certificate** screen. The WE Device trusts any valid certificate signed by any of the imported trusted CA certificates. Certificates should be in one of the following formats: Binary X.509, PEM (base-64) encoded, Binary PKCS#7, or PEM (base-64) encoded PKCS#7.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 146 Security > Certificates > Trusted CA > Import Certificates

The following table describes the labels in this screen.

Table 84 Security > Certificates > Trusted CA > Import Certificates

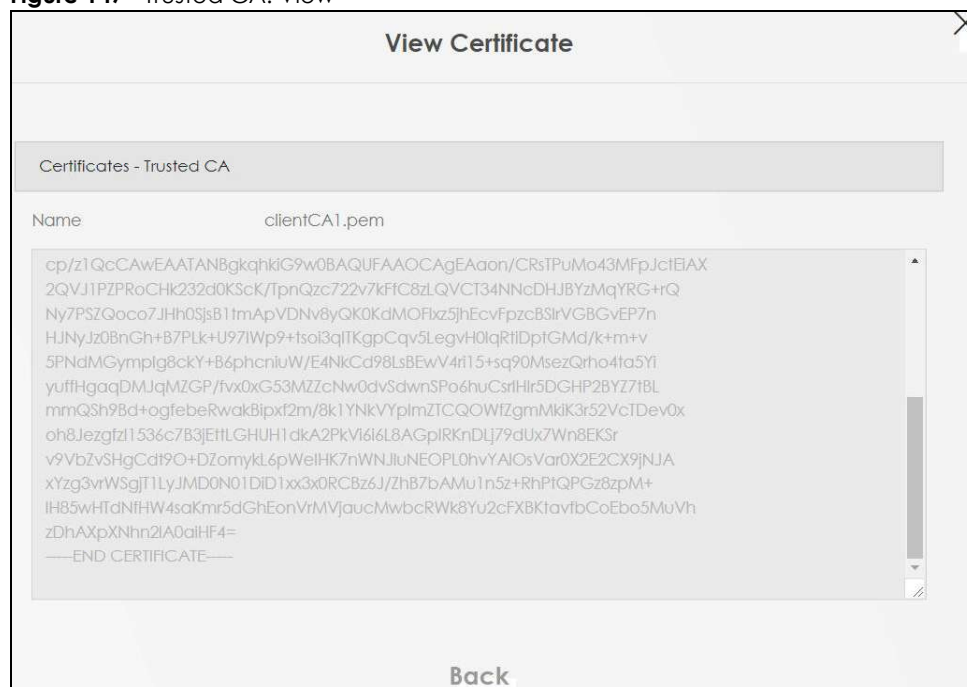
LABEL	DESCRIPTION
Certificate File Path	Type in the location of the file you want to upload in this field or click Choose File / Browse... to find it.
Choose File	Click this button to find the certificate file you want to upload.
OK	Click this to save the certificate on the WE Device.
Cancel	Click this to exit this screen without saving.

17.6 View Trusted CA Certificate

Use this screen to view in-depth information about the certification authority's certificate. The certificate text box is read-only and can be distributed to others.

Click **Security > Certificates > Trusted CA** to open the **Trusted CA** screen. Click the **View** icon to open the **View Certificate** screen.

Figure 147 Trusted CA: View



The following table describes the labels in this screen.

Table 85 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (through USB thumb drive for example).
Back	Click this to return to the previous screen.

17.7 Certificates Technical Reference

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

Certification Authorities

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities.

Public and Private Keys

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

- 1 Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.
- 2 Tim keeps the private key and makes the public key openly available.
- 3 Tim uses his private key to encrypt the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to decrypt it.
- 5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The WE Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

Advantages of Certificates

Certificates offer the following benefits.

- The WE Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Certificate File Format

The certification authority certificate that you want to import has to be in PEM (Base-64) encoded X.509 file format. This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.

17.7.1 Verify a Certificate

Before you import a trusted CA or trusted remote host certificate into the WE Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the WE Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

- 1 Browse to where you have the certificate saved on your computer.

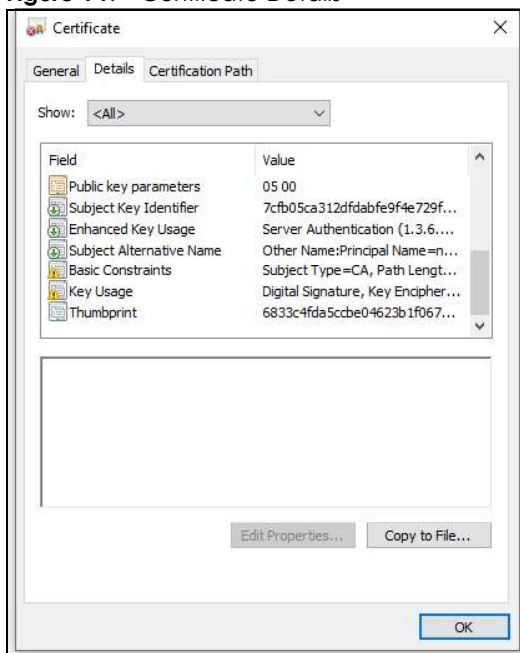
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 148 Certificates on Your Computer



- 3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 149 Certificate Details



Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

CHAPTER 18

Log

18.1 Log Overview

These screens allow you to determine the categories of events that the WE Device logs and then display these logs or have the WE Device send them to an administrator (through email) or to a syslog server.

18.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs ([Section 18.2 on page 227](#)).
- Use the **Security Log** screen to see the security-related logs for the categories that you select ([Section 18.3 on page 228](#)).

18.1.2 What You Need To Know

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

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 86 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.

Table 86 Syslog Severity Levels (continued)

CODE	SEVERITY
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

18.2 System Log Settings

Use the **Log** screen to see the system logs. You can filter the entries by selecting a severity level and/or category. Click **System Monitor > Log > System Log** to open the **System Log** screen.

Figure 150 System Monitor > Log > System Log

The following table describes the fields in this screen.

Table 87 System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the WE Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to save the current list of logs to your computer.
E-mail Log Now	Click this to send the log files to the email address you specified in the Maintenance > Log Setting screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

18.3 Security Log

Use the **Security Log** screen to see the security-related logs for the categories that you select. You can filter the entries by selecting a severity level and/or category. Click **System Monitor > Log > Security Log** to open the following screen.

Figure 151 System Monitor > Log > Security Log

The following table describes the fields in this screen.

Table 88 System Monitor > Log > Security Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the WE Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected logs.
E-mail Log Now	Click this to send the log files to the email address you specify in the Maintenance > Log Setting screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the WE Device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

CHAPTER 19

Traffic Status

19.1 Traffic Status Overview

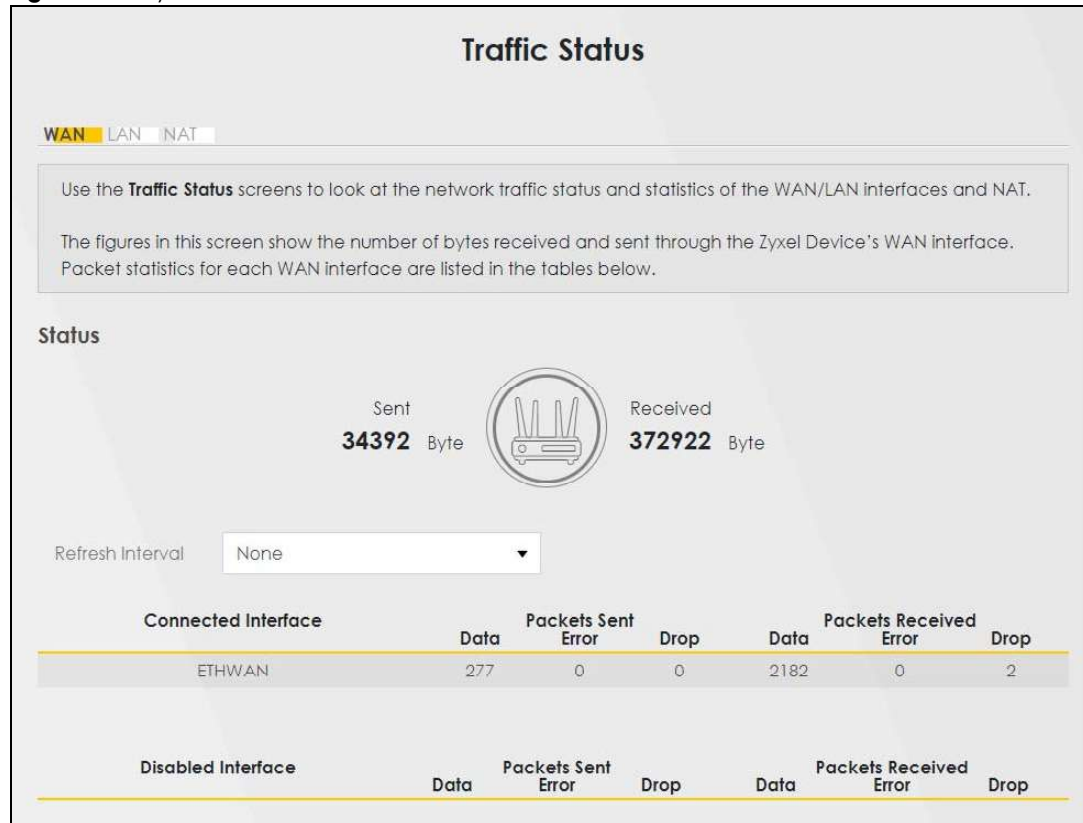
Use the **Traffic Status** screens to look at the network traffic status and statistics of the WAN/LAN interfaces and NAT.

19.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics ([Section 19.2 on page 229](#)).
- Use the **LAN** screen to view the LAN traffic statistics ([Section 19.3 on page 231](#)).
- Use the **NAT** screen to view the NAT status of the WE Device's clients ([Section 19.4 on page 232](#)).

19.2 WAN Status

Click **System Monitor > Traffic Status** to open the **WAN** screen. The figures in this screen show the number of bytes received and sent through the WE Device's WAN interface. The table below shows packet statistics for each WAN interface.

Figure 152 System Monitor > Traffic Status > WAN

The following table describes the fields in this screen.

Table 89 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the WE Device to update this screen.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.
Disabled Interface	This shows the name of the WAN interface that is currently disabled.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	

Table 89 System Monitor > Traffic Status > WAN (continued)

LABEL	DESCRIPTION
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

19.3 LAN Status

Click **System Monitor > Traffic Status > LAN** to open the following screen. This screen allows you to view packet statistics for each LAN or WLAN interface on the WE Device.

Figure 153 System Monitor > Traffic Status > LAN

Traffic Status							
WAN LAN NAT							
This screen allows you to view packet statistics for each LAN or WLAN interface on the Zyxel Device.							
Refresh Interval		None					
Interface		LAN1	LAN2	LAN3	2.4G WLAN	5G WLAN	6GHz WLAN
Bytes Sent		40852582	0	0	4139620	1009256	1030231
Bytes Received		7480980	0	0	0	0	0

Interface		LAN1	LAN2	LAN3	2.4G WLAN	5G WLAN	6GHz WLAN
Sent (Packet)	Data	75641	0	0	41274	10080	10283
	Error	0	0	0	0	0	0
	Drop	0	0	0	0	0	0
Received (Packet)	Data	67598	0	0	0	0	0
	Error	0	0	0	0	0	0
	Drop	0	0	0	0	0	0

The following table describes the fields in this screen.

Table 90 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the WE Device to update this screen.
Interface	This shows the LAN or WLAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN or WLAN interfaces.
Sent (Packets)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packets)	

Table 90 System Monitor > Traffic Status > LAN (continued)

LABEL	DESCRIPTION
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

19.4 NAT Status

Click **System Monitor > Traffic Status > NAT** to open the following screen. This screen lists the devices that have received an IP address from the WE Device LAN or WLAN interfaces and have ever established a session with the WE Device.

Figure 154 System Monitor > Traffic Status > NAT

The following table describes the fields in this screen.

Table 91 System Monitor > Traffic Status > NAT

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the WE Device to update this screen.
Device Name	This displays the name of the connected host.
IPv4 Address	This displays the IP address of the connected host.
MAC Address	This displays the MAC address of the connected host.
No. of Open Sessions	This displays the number of NAT sessions currently opened for the connected host.
Total	This displays what percentage of NAT sessions the WE Device can support is currently being used by all connected hosts. You can also see the number of active NAT sessions and the maximum number of NAT sessions the WE Device can support

CHAPTER 20

ARP Table

20.1 ARP Table Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol (IP) address to a physical machine address, known as a Media Access Control (MAC) address, on the local area network.

An IP version 4 address is 32 bits long. MAC addresses are 48 bits long. The ARP table maintains an association between each MAC address and its corresponding IP address.

20.1.1 How ARP Works

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

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP table for future reference and then sends the packet to the MAC address that replied.

20.2 ARP Table

Use the ARP table to view the IPv4-to-MAC address mappings for each device connected to the WE Device. The neighbor table shows the IPv6-to-MAC address mappings of each IPv6 neighbor. To open this screen, click **System Monitor > ARP Table**.

Figure 155 System Monitor > ARP Table

ARP Table			
Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol (IP) address to a physical machine address, known as a Media Access Control (MAC) address, on the local area network. An IPv4 address is 32 bits long. MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address. Use the ARP table to view the IPv4-to-MAC address mappings for each device connected to the Zyxel Device. The neighbor table shows the IPv6-to-MAC address mappings of each neighbor.			
IPv4 ARP Table			
#	IPv4 Address	MAC Address	Device
1			br-lan
2			br-lan
IPv6 Neighbour Table			
#	IPv6 Address	MAC Address	Device
1			br-lan

The following table describes the labels in this screen.

Table 92 System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the ARP table entry number.
IPv4 / IPv6 Address	This is the learned IPv4 or IPv6 IP address of a device connected to the WE Device.
MAC Address	This is the MAC address of the connected device with the listed IP address.
Device	This is the type of interface used by the connected device. You can click the device type to go to its configuration screen.

CHAPTER 21

Routing Table

21.1 Routing Table Overview

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

21.2 Routing Table

The table below shows IPv4 and IPv6 routing information. The IPv4 subnet mask is '255.255.255.255' for a host destination and '0.0.0.0' for the default route. The gateway address is written as '*' (IPv4) / '::' (IPv6) if none is set.

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

Figure 156 System Monitor > Routing Table

Routing Table					
Routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet. The table below shows IPv4 and IPv6 routing information. The IPv4 subnet mask is '255.255.255.255' for a host destination and '0.0.0.0' for the default route. The gateway address is written as '*' (IPv4) / '::' (IPv6) if none is set. Destination: This indicates the destination IPv4 address or IPv6 address and prefix of this route. Gateway: This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic. Subnet Mask: This indicates the destination subnet mask of the IPv4 route. Flag: This indicates the route status. U-Up: The route is up. I-Reject: The route is blocked and will force a route lookup to fail. G-Gateway: The route uses a gateway to forward traffic. H-Host: The target of the route is a host. R-Reinstate: The route is reinstated for dynamic routing. D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect. M-Modified (redirect): The route is modified from a routing daemon or redirect. Metric: The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost". Interface: This indicates the name of the interface through which the route is forwarded.					
IPv4 Routing Table					
Destination	Gateway	Subnet Mask	Flag	Metric	Interface
			U	0	br-lan
			U	0	br-lan200
			U	0	br-lan300
			U	0	br-lan400
IPv6 Routing Table					
Destination	Gateway	Flag	Metric	Interface	
	::	In	-1	lo	
	::	In	2147483647	lo	
	::	U	256	br-lan	
	::	U	256	wlan0.4	

The following table describes the labels in this screen.

Table 93 System Monitor > Routing Table

LABEL	DESCRIPTION
IPv4 / IPv6 Routing Table	
Destination	This indicates the destination IPv4 address or IPv6 address and prefix of this route.
Gateway	This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of the IPv4 route.

Table 93 System Monitor > Routing Table (continued)

LABEL	DESCRIPTION
Flag	This indicates the route status. U–Up: The route is up. !–Reject: The route is blocked and will force a route lookup to fail. G–Gateway: The route uses a gateway to forward traffic. H–Host: The target of the route is a host. R–Reinstate: The route is reinstated for dynamic routing. D–Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect. M–Modified (redirect): The route is modified from a routing daemon or redirect.
Metric	The metric represents the "cost of transmission." A router determines the best route for transmission by choosing a path with the lowest "cost." The smaller the number, the lower the "cost."
Interface	This indicates the name of the interface through which the route is forwarded. • brx indicates a LAN interface where x can be 0 – 3 to represent LAN1 to LAN4 respectively. • ptm0 indicates a VDSL (including G.fast) WAN interface using IPoE or in bridge mode. • atm0 indicates an ADSL WAN interface using IPoE or in bridge mode. • ethx indicates an Ethernet WAN interface using IPoE or in bridge mode. • ppp0 indicates a WAN interface using PPPoE. • wlx indicates a wireless interface where x can be 0 – 1.
Interface	This indicates the name of the interface through which the route is forwarded. • brx indicates a LAN interface where x can be 0 – 3 to represent LAN1 to LAN4 respectively.

CHAPTER 22

Multicast Status

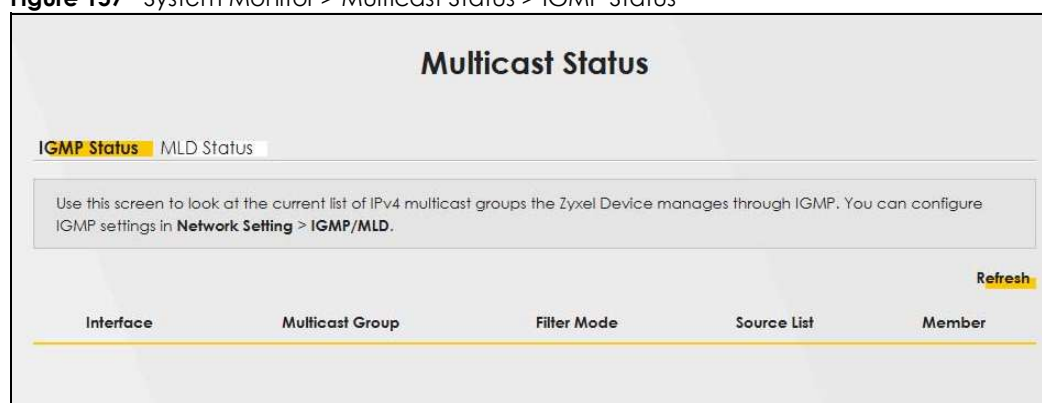
22.1 Multicast Status Overview

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

22.2 The IGMP Status Screen

Use this screen to look at the current list of multicast groups the WE Device manages through IGMP. Configure IGMP in **Network Setting > IGMP/MLD**. To open this screen, click **System Monitor > Multicast Status > IGMP Status**.

Figure 157 System Monitor > Multicast Status > IGMP Status



The following table describes the labels in this screen.

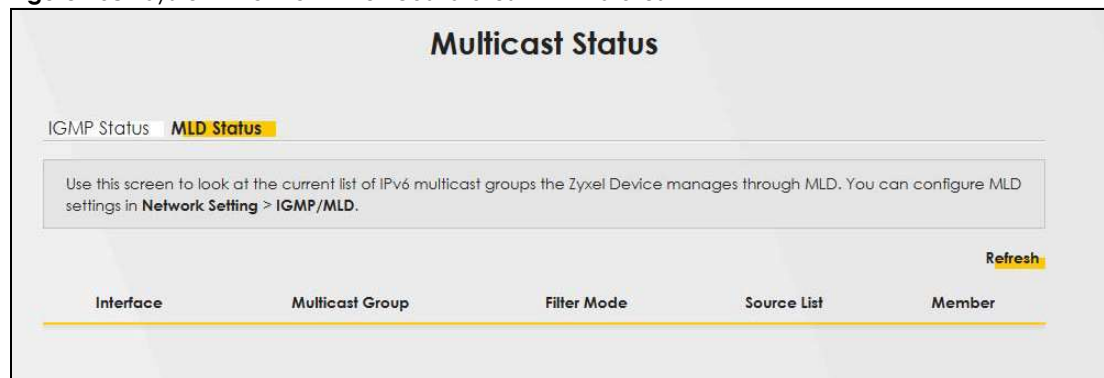
Table 94 System Monitor > Multicast Status > IGMP Status

LABEL	DESCRIPTION
Refresh	Click this button to update the information on this screen.
Interface	This field displays the name of an interface on the WE Device that belongs to an IGMP multicast group.
Multicast Group	This field displays the name of the IGMP multicast group to which the interface belongs.
Filter Mode	INCLUDE means that only the IP addresses in the Source List get to receive the multicast group's traffic. EXCLUDE means that the IP addresses in the Source List are not allowed to receive the multicast group's traffic but other IP addresses can.
Source List	This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode.
Member	This is the list of the members of the multicast group.

22.3 The MLD Status Screen

Use this screen to look at the current list of multicast groups the WE Device manages through MLD. Configure MLD in **Network Setting > IGMP/MLD**. To open this screen, click **System Monitor > Multicast Status > MLD Status**.

Figure 158 System Monitor > Multicast Status > MLD Status



The following table describes the labels in this screen.

Table 95 System Monitor > Multicast Status > MLD Status

LABEL	DESCRIPTION
Refresh	Click this button to update the status on this screen.
Interface	This field displays the name of an interface on the WE Device that belongs to an MLD multicast group.
Multicast Group	This field displays the name of the MLD multicast group to which the interface belongs.
Filter Mode	INCLUDE means that only the IP addresses in the Source List get to receive the multicast group's traffic. EXCLUDE means that the IP addresses in the Source List are not allowed to receive the multicast group's traffic but other IP addresses can.
Source List	This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode.
Member	This is the list of members in the multicast group.

CHAPTER 23

WLAN Station Status

23.1 WLAN Station Status Overview

Click **System Monitor > WLAN Station Status** to open the following screen. Use this screen to view information and status of the WiFi stations (WiFi clients) that are currently associated with the WE Device. Being associated means that a WiFi client (for example, your computer with a WiFi network card installed) has connected successfully to an AP (or WiFi router) using the same SSID, channel, and WiFi security settings.

Figure 159 System Monitor > WLAN Station Status

WLAN Station Status

Use this screen to view information and status of the wireless stations (wireless clients) that are currently associated with the Zyxel Device. Being associated means that a wireless client (for example, your computer with a wireless network card installed) has connected successfully to an AP (or wireless router) using the same SSID, channel, and WiFi security settings.

Refresh Interval

WLAN 2.4G Station Status

#	MAC Address	Rate (Mbps)	RSSI (dBm)	SNR	Level
---	-------------	-------------	------------	-----	-------

WLAN 5G Station Status

#	MAC Address	Rate (Mbps)	RSSI (dBm)	SNR	Level
---	-------------	-------------	------------	-----	-------

WLAN MLO Station Status

#	MAC Address	Rate (Mbps)	RSSI (dBm)	SNR	Level
---	-------------	-------------	------------	-----	-------

The following table describes the labels in this screen.

Table 96 System Monitor > WLAN Station Status

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the WE Device to update this screen.
#	This is the index number of an associated WiFi station.
MAC Address	This field displays the MAC address of an associated WiFi station.
Rate (Mbps)	This field displays the transmission rate of WiFi traffic between an associated WiFi station and the WE Device.

Table 96 System Monitor > WLAN Station Status (continued)

LABEL	DESCRIPTION
RSSI (dBm)	The RSSI (Received Signal Strength Indicator) field shows the WiFi signal strength of the station's WiFi connection. The normal range is –30 dBm to –79 dBm. If the value drops below –80 dBm, try moving the associated WiFi station closer to the WE Device to get better signal strength.
SNR	The Signal-to-Noise Ratio (SNR) is the ratio between the received signal power and the received noise power. The normal range is 15 to 40. If the value drops below 15, try moving the associated WiFi station closer to the WE Device to get better quality WiFi.
Level	This field displays a number which represents the strength of the WiFi signal between an associated WiFi station and the WE Device. The WE Device uses the RSSI and SNR values to determine the strength of the WiFi signal. 5 means the WE Device is receiving an excellent WiFi signal. 4 means the WE Device is receiving a very good WiFi signal. 3 means the WE Device is receiving a weak WiFi signal. 2 means the WE Device is receiving a very weak WiFi signal. 1 means the WE Device is not receiving a WiFi signal.

CHAPTER 24

Operation Mode

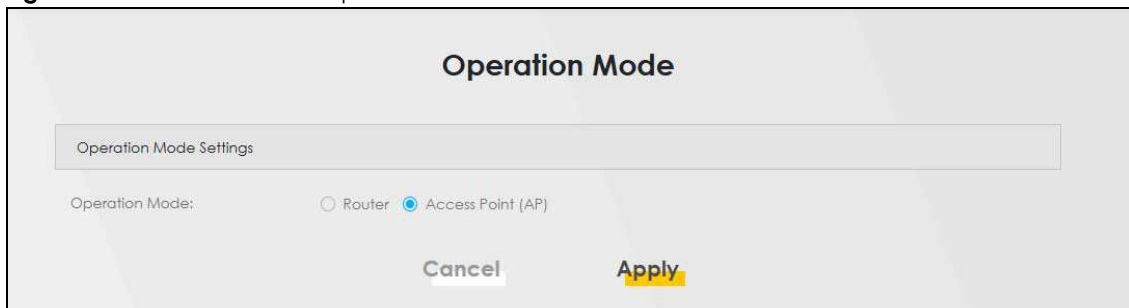
24.1 Operation Mode Overview

In this screen, you can select the operation mode for the WE Device when it is operated as Mesh controller role.

24.2 Operation Mode Settings

Click **Maintenance > Operation Mode** to open the following screen. Select **Router** or **Access Point (AP)** mode for the WE Device.

Figure 160 Maintenance > Operation Mode



The following table describes the labels in this screen.

Table 97 Maintenance > Operation Mode

LABEL	DESCRIPTION
Operation Mode	Select Router or Access Point (AP) mode for the WE Device. In Router mode, the WE Device acts as the controller in router mode. In Access Point (AP) mode, the WE Device could act as either mesh controller or mesh agent in bridge mode. Use Router mode if you want the WE Device to use routing functions such as DHCP Server. You will need to reconfigure your network if you have an existing router. Use Access Point (AP) mode to pass the ISP-assigned IP address(es) to your devices connected to the LAN port. All traffic from the Internet passes through the WE Device directly to devices connected to the LAN port. Use this mode if you already have a router with routing functions in your network.
Cancel	Click Cancel to restore the default or previously saved settings.
Apply	Click Apply to save your changes.

CHAPTER 25

System

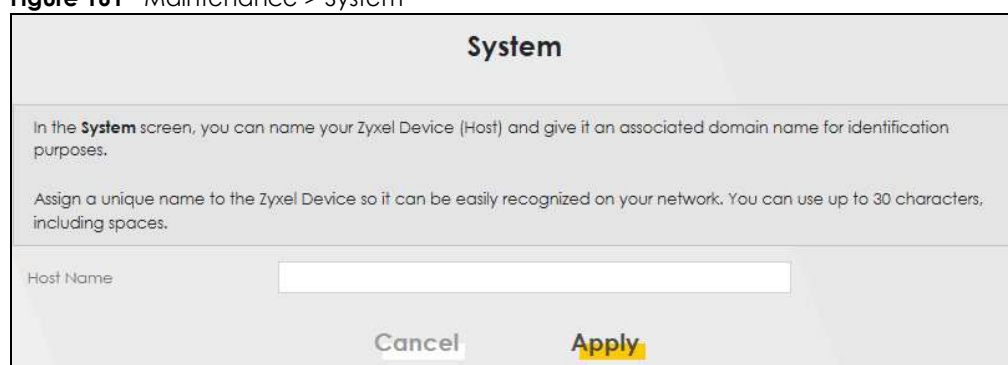
25.1 System Overview

In the **System** screen, you can name your WE Device (Host) and give it an associated domain name. Domain is the name given to a network. It will be required to reach a network from an external point (like the Internet). Knowing the domain name will allow you to reach a particular network, and knowing the host name will allow you to reach a particular device. For this reason, accessing a device from another device within a network may work with just the host name (without the use of the domain name).

25.2 System Settings

Click **Maintenance > System** to open the following screen. Assign a unique name to the WE Device so it can be easily recognized on your network. You can use up to 30 characters, including spaces.

Figure 161 Maintenance > System



The following table describes the labels in this screen.

Table 98 Maintenance > System

LABEL	DESCRIPTION
Host Name	Type a host name for your WE Device. Enter a descriptive name of up to 30 alphanumeric characters, not including spaces, underscores, and dashes.
Cancel	Click Cancel to restore the default or previously saved settings.
Apply	Click Apply to save your changes.

CHAPTER 26

User Account

26.1 User Account Overview

In the **User Account** screen, you can view the settings of the 'admin' and other user accounts that you use to log into the WE Device to manage it.

26.2 User Account Settings

Click **Maintenance > User Account** to open the following screen. Use this screen to create or manage user accounts and their privileges on the WE Device.

Figure 162 Maintenance > User Account

User Account

In the **User Account** screen, you can view the settings of the "admin" and other user accounts that you use to log into the Zyxel Device.

Use this screen to create or manage user accounts and their privileges on the Zyxel Device.

[+ Add New Account](#)

#	Active	User Name	Retry Times	Idle Timeout	Lock Period	Group	Modify
1	☒	admin	0	60	5	Administrator	
2	☒	Zyxel	3	5	5	User	

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

The following table describes the labels in this screen.

Table 99 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account.
#	This is the index number of the user account.
Active	This field indicates whether the user account is active or not. Clear the checkbox to disable the user account. Select the checkbox to enable it.
User Name	This field displays the name of the account used to log into the WE Device Web Configurator.
Retry Times	This field displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.

Table 99 Maintenance > User Account (continued)

LABEL	DESCRIPTION
Idle Timeout	This field displays the length of inactive time before the WE Device will automatically log the user out of the Web Configurator.
Lock Period	This field displays the length of time a user must wait before attempting to log in again after a number if consecutive wrong passwords have been entered as defined in Retry Times .
Group	This field displays whether this user has Administrator or User privileges.
Modify	Click the Edit icon to configure the entry. Click the Delete icon to remove the entry.
Cancel	Click Cancel to restore the default or previously saved settings.
Apply	Click Apply to save your changes.

26.2.1 User Account Add/Edit

Click **Add New Account** or the **Edit** icon of an existing account in the **Maintenance > User Account** to open the following screen.

Figure 163 Maintenance > User Account > Add/Edit

The following table describes the labels in this screen.

Table 100 Maintenance > User Account > Add/Edit

LABEL	DESCRIPTION
Active	Select Enable or Disable to activate or deactivate the user account.
User Name	Enter a new name for the account. You can use up to 31 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [:]. Spaces are allowed.
Password	Type your new system password. The new Password must be at least 8 characters, must contain at least one uppercase letter, one lowercase letter, one number, and one special character. Please see the password requirement displayed on the screen.
Verify Password	Type the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.

Table 100 Maintenance > User Account > Add/Edit (continued)

LABEL	DESCRIPTION
Idle Timeout	Enter the length of inactive time before the WE Device will automatically log the user out of the Web Configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in Retry Times .
Group	Specify whether this user will have Administrator or User privileges. Administrator and User privileges are mostly the same, but the following menu items will only display when you log in as an Administrator. • Network Setting • Security • Maintenance > System
Cancel	Click Cancel to exit this screen without saving any changes.
OK	Click OK to save your changes.

CHAPTER 27

Remote Management

27.1 Remote Management Overview

Use remote management to control what services you can use through which interface(s) in order to manage the WE Device.

27.1.1 What You Can Do in this Chapter

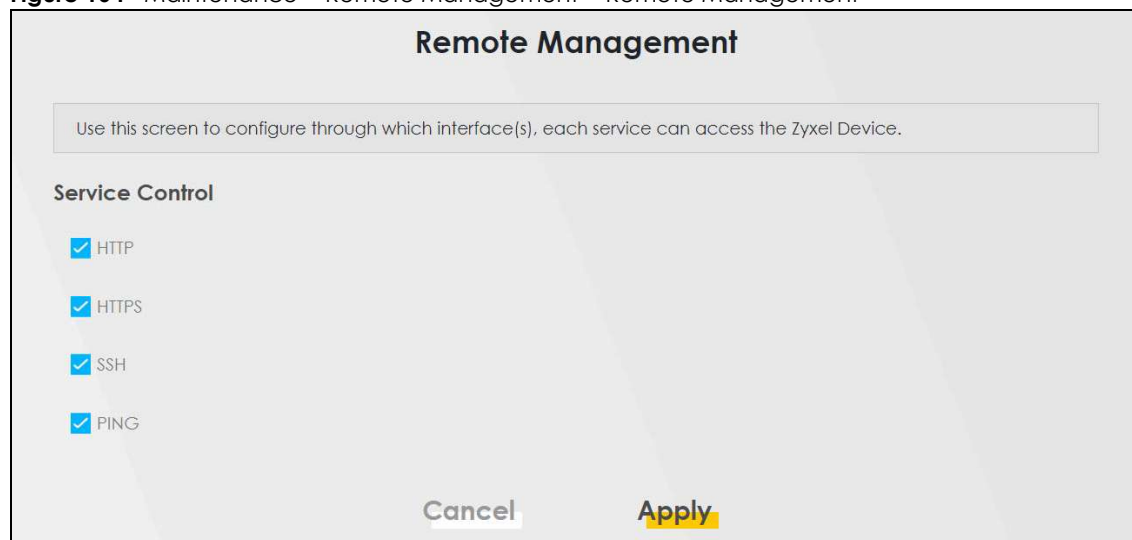
Use the **Remote Management** screen to allow various approaches to access the WE Device remotely from a LAN connection ([Section 27.2 on page 247](#)).

Note: The WE Device is managed using the Web Configurator.

27.2 Management Services

Use this screen to configure through which interface(s), each service can access the WE Device. You can also specify service port numbers computers must use to connect to the WE Device. Click **Maintenance > Remote Management > Remote Management** to open the following screen.

Figure 164 Maintenance > Remote Management > Remote Management



Remote Management

Use this screen to configure through which interface(s), each service can access the Zyxel Device.

Service Control

- ☒ HTTP
- ☒ HTTPS
- ☒ SSH
- ☒ PING

Cancel Apply

The following table describes the fields in this screen.

Table 101 Maintenance > Remote Management > Remote Management

LABEL	DESCRIPTION
Service Control	This is the service list you may use to access the WE Device. • HTTP allows you to access the WE Device through a web browser. • HTTPS is a secured version of HTTP that provides a secure connection through encryption. • SSH is a secure protocol for remote command-line access. • Telnet is a protocol for remote command-line access. • Ping can test if the WE Device is reachable and measure response time.
Cancel	Click Cancel to restore the default or previously saved settings.
Apply	Click Apply to save your changes back to the WE Device.

CHAPTER 28

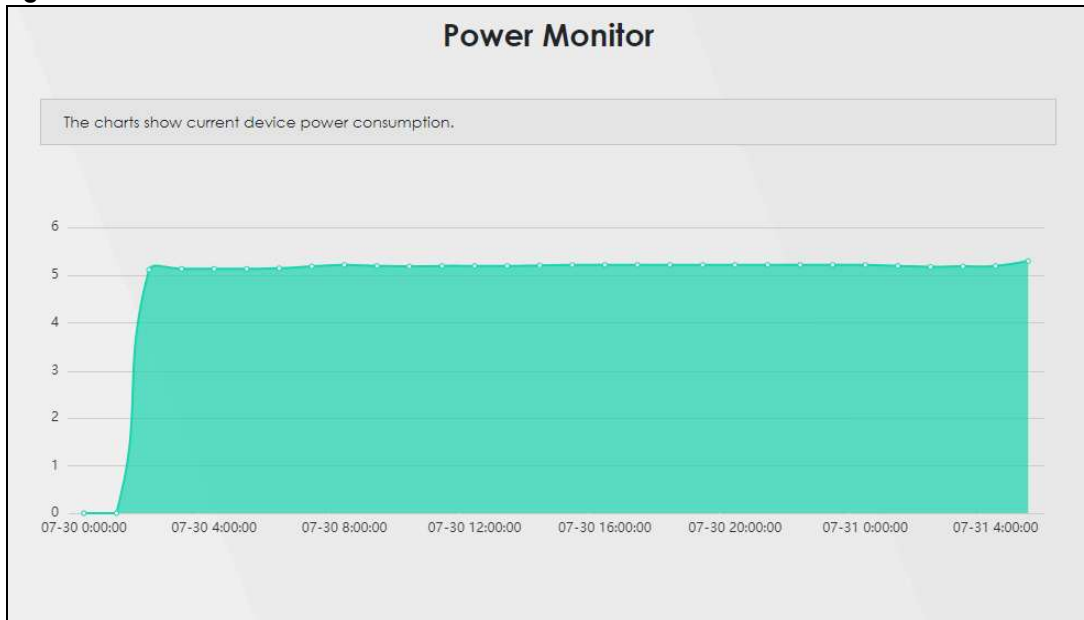
Power Monitor

28.1 Power Monitor Overview

This chapter explains how to monitor the power consumption of the WE Device.

Click **Maintenance > Power Monitor** to open the following screen. Use this screen to view the current and past amount of power consumed by the WE Device.

Figure 165 Maintenance > Power Monitor



The following table describes the fields in this screen.

Table 102 Maintenance > Power Monitor

LABEL	DESCRIPTION
Y-axis	The y-axis shows the amount of power consumed by the WE Device in watts.
X-axis	The x-axis shows the period over which the power consumption is recorded. The maximum period for recording is 48 hours. After 48 hours, the power consumption data wraps around and new ones replace the earliest ones.

Note: The power consumption data is lost when you turn off the power to your WE Device or when the WE Device is reset to its factory default setting.

CHAPTER 29

Time Settings

29.1 Time Settings Overview

This chapter shows you how to configure the WE Device's system date and time.

29.2 Time

For effective scheduling and logging, the WE Device's system time must be accurate. Use this screen to configure the WE Device's time based on your local time zone. You can enter a time server address, select the time zone where the WE Device is physically located, and configure Daylight Savings settings if needed.

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

Figure 166 Maintenance > Time

Configure the Zyxel Device's time based on your local time zone. You can add a time server address, select your time zone, and configure Daylight Savings if your location uses it.

Current Date/Time

Current Time

14:21:53

Current Date

2019-02-27

Time and Date Setup

Time Protocol

SNTP (RFC-1769)

First Time Server Address

pool.ntp.org

Second Time Server Address

clock.nyc.he.net

Third Time Server Address

clock.sjc.he.net

Fourth Time Server Address

None

Fifth Time Server Address

None

Time Zone

Time Zone

(GMT+08:00) Taipei

Daylight Savings

Active

☒

Start Rule

Day

☒ 1

☐ Last

☐ Sunday

in

Month

March

Hour

2

0

End Rule

Day

☒ 1

☐ Last

☐ Sunday

in

Month

October

Hour

3

0

Cancel

Apply

The following table describes the fields in this screen.

Table 103 Maintenance > Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your WE Device. Each time you reload this page, the WE Device synchronizes the time with the time server.
Current Date	This field displays the date of your WE Device. Each time you reload this page, the WE Device synchronizes the date with the time server.
Time and Date Setup	

Table 103 Maintenance > Time (continued)

LABEL	DESCRIPTION
First – Fifth Time Server Address	Select an NTP time server from the drop-down list box. Otherwise, select Other and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select None if you do not want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Active	Click this switch to enable or disable Daylight Saving Time. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Start Rule	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The Hour field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to Second, Sunday, the month to March and the time to 2 in the Hour field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to Last, Sunday and the month to March. The time you select in the o'clock field depends on your time zone. In Germany for instance, you would select 2 in the Hour field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Rule	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The Hour field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would set the day to First, Sunday, the month to November and the time to 2 in the Hour field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to Last, Sunday, and the month to October. The time you select in the o'clock field depends on your time zone. In Germany for instance, you would select 2 in the Hour field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Cancel	Click Cancel to restore the default or previously saved settings.
Apply	Click Apply to save your changes.

CHAPTER 30

Email Notification

30.1 Email Notification Overview

A mail server is an application or a computer that can receive, forward and deliver email messages.

To have the WE Device send reports, logs or notifications through email, you must specify an email server and the email addresses of the sender and receiver.

30.2 Email Notification

Use this screen to view, remove and add email account information on the WE Device. This account can be set to send email notifications for logs.

Click **Maintenance > E-mail Notification** to open the **E-mail Notification** screen.

Note: The default port number of the mail server is 25.

Figure 167 Maintenance > E-mail Notification

E-mail Notification

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

To have the Zyxel Device send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

Use this screen to view, remove and add e-mail account information on the Zyxel Device. This account can be set to receive e-mail notifications for logs.

 Add New e-mail

Mail Server Address	Username	Port	Security	E-mail Address	Remove
---------------------	----------	------	----------	----------------	--------

The following table describes the labels in this screen.

Table 104 Maintenance > E-mail Notification

LABEL	DESCRIPTION
Add New e-mail	Click this button to create a new entry (up to 32 can be created).
Mail Server Address	This displays the server name or the IP address of the mail server.
Username	This displays the user name of the sender's mail account.

Table 104 Maintenance > E-mail Notification (continued)

LABEL	DESCRIPTION
Port	This field displays the port number of the mail server.
Security	This field displays the protocol used for encryption.
E-mail Address	This field displays the email address that you want to be in the from or sender line of the email that the WE Device sends.
Modify	Click the Edit icon to configure the entry. Click the Delete icon to remove the entry.
Remove	Click this button to delete the selected entries.

30.2.1 Add New e-mail

Click the **Add New e-mail** button in the **E-mail Notification** screen. Use this screen to configure the required information for sending email through a mail server.

Figure 168 Maintenance > E-mail Notification > Add New e-mail

The following table describes the labels in this screen.

Table 105 Maintenance > E-mail Notification > Add New e-mail

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the Account e-mail Address field. If this field is left blank, reports, logs or notifications will not be sent through e-mail.
Port	Enter the same port number here as is on the mail server for mail traffic.

Table 105 Maintenance > E-mail Notification > Add New e-mail (continued)

LABEL	DESCRIPTION
Authentication Username	Enter the user name. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed. This is usually the user name of a mail account you specified in the Account e-mail Address field.
Authentication Password	Enter the password associated with the user name above.
Account e-mail Address	Enter the email address that you want to be in the from or sender line of the email notification that the WE Device sends. If you activate SSL/TLS authentication, the email address must be able to be authenticated by the mail server as well.
Connection Security	Select SSL to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the WE Device. Select STARTTLS to upgrade a plain text connection to a secure connection using SSL/TLS. Select NONE to disable the connection security.
Cancel	Click this button to begin configuring this screen afresh.
OK	Click this button to save your changes and return to the previous screen.

CHAPTER 31

Log Setting

31.1 Log Setting Overview

You can configure where the WE Device sends logs and which type of logs the WE Device records in the **Logs Setting** screen.

31.2 Log Setting

Use this screen to configure where the WE Device sends logs, and which type of logs the WE Device records.

If you have a server that is running a syslog service, you can also save log files to it by enabling **Syslog Logging**, and then entering the IP address of the server in the **Syslog Server** field. Select **Remote** to store logs on the syslog server, or select **Local File** to store logs on the WE Device. Select **Local File and Remote** to store logs on both the WE Device and the syslog server. To change your WE Device's log settings, click **Maintenance > Log Setting**. The screen appears as shown.

Figure 169 Maintenance > Log Setting

Use this screen to configure where the Zyxel Device sends logs, and which type of logs the Zyxel Device records.

If you have a server that is running a syslog service, you can also save log files to it by enabling **Syslog Logging** and then entering the IP address of the server in the **Syslog Server** field. Select **Remote** to store logs on the syslog server, or select **Local File** to store logs on the Zyxel Device. Select **Local File and Remote** to store logs on both the Zyxel Device and on the syslog server.

Syslog Settings

Syslog Logging ☒

Mode Local File ▼

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

UDP Port 514 (Server Port)

E-mail Log Settings

E-mail Log Settings ☒

Mail Account Select one account ▼

System Log Mail Subject

Send Log to (E-Mail Address)

Send Alarm to (E-Mail Address)

Alarm Interval 60 (seconds)

Active Log

System Log

- ☒ WAN-DHCP
- ☒ TR-069
- ☒ Wireless

Cancel Apply

The following table describes the fields in this screen.

Table 106 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Slide the switch to the right to enable syslog logging.
Mode	Select Remote to have the WE Device send it to an external syslog server. Select Local File to have the WE Device save the log file on the WE Device itself. Select Local File and Remote to have the WE Device save the log file on the WE Device itself and send it to an external syslog server. Note: A warning appears upon selecting Remote or Local File and Remote. Just click OK to continue.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.

Table 106 Maintenance > Log Setting (continued)

LABEL	DESCRIPTION
UDP Port	Enter the port number used by the syslog server.
Enable Syslog over TLS	Use Syslog over TLS to securely send logs from the WE Device to the syslog server using TLS encryption. On the WE Device, first generate a certificate for syslog authentication of the WE Device. The CN (Certificate Name) must match the IP address of the WE Device's interface to the syslog server. Go to Security > Certificates > Local CA and import a certificate for syslog authentication. This is required.
Local Certificate Used by Syslog Client	Optionally, the Syslog server may also request a certificate from the WE Device for mutual authentication. Go to Security > Certificates > Local Certificate and import a WE Device certificate that the syslog server can use to verify the WE Device.
E-mail Log Settings	
E-mail Log Settings	Slide the switch to the right to allow the sending through email the system and security logs to the email address specified in Send Log to . Note: Make sure that the Mail Server Address field is not left blank in the Maintenance > E-mail Notifications screen.
Mail Account	Select a server specified in Maintenance > E-mail Notifications to send the logs to.
System Log Mail Subject	This field allows you to enter a descriptive name for the system log email (for example Zyxel System Log). Up to 127 printable characters are allowed for the System Log Mail Subject including special characters inside the square brackets [!#%()*+,-./:=?@[\\{}~].
Security Log Mail Subject	This field allows you to enter a descriptive name for the security log email (for example Zyxel Security Log). Up to 127 printable characters are allowed for the Security Log Mail Subject including special characters inside the square brackets [!#%()*+,-./:=?@[\\{}~].
Send Log to	This field allows you to enter the log's designated email recipient. The log's format is plain text file sent as an email attachment.
Send Alarm to	This field allows you to enter the alarm's designated e-mail recipient. The alarm's format is plain text file sent as an email attachment.
Alarm Interval	Select the frequency of showing of the alarm.
Active Log	
System Log	Select the categories of System Logs that you want to record.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

31.2.1 Example Email Log

An 'End of Log' message displays for each mail in which a complete log has been sent. The following is an example of a log sent by email.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- 'End of Log' message shows that a complete log has been sent.

Figure 170 Email Log Example

```

Subject:
        Firewall Alert From
Date:
        Fri, 07 Apr 2000 10:05:42
From:
        user@zyxel.com
To:
        user@zyxel.com
1|Apr 7 00 |From:192.168.1.1      To:192.168.1.255  |default policy  |forward
  | 09:54:03 |UDP      src port:00520 dest port:00520  |<1,00>         |
2|Apr 7 00 |From:192.168.1.131    To:192.168.1.255  |default policy  |forward
  | 09:54:17 |UDP      src port:00520 dest port:00520  |<1,00>         |
3|Apr 7 00 |From:192.168.1.6      To:10.10.10.10    |match           |forward
  | 09:54:19 |UDP      src port:03516 dest port:00053  |<1,01>         |
.....{snip}.....
.....{snip}.....
126|Apr 7 00 |From:192.168.1.1      To:192.168.1.255  |match           |forward
   | 10:05:00 |UDP      src port:00520 dest port:00520  |<1,02>         |
127|Apr 7 00 |From:192.168.1.131    To:192.168.1.255  |match           |forward
   | 10:05:17 |UDP      src port:00520 dest port:00520  |<1,02>         |
128|Apr 7 00 |From:192.168.1.1      To:192.168.1.255  |match           |forward
   | 10:05:30 |UDP      src port:00520 dest port:00520  |<1,02>         |

End of Firewall Log

```

CHAPTER 32

Firmware Upgrade

32.1 Firmware Upgrade Overview

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

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

32.2 Firmware Upgrade Settings

Click **Maintenance > Firmware Upgrade** to open the following screen. Download the latest firmware file from the Zyxel website and upload it to your WE Device using this screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to 2 minutes. After a successful upload, the WE Device will reboot.

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

Figure 171 Maintenance > Firmware Upgrade

The screenshot shows the 'Firmware Upgrade' screen. At the top, the title 'Firmware Upgrade' is centered. Below it, a text box explains the purpose of the screen and provides instructions on downloading the latest firmware from the Zyxel website and uploading it to the device. It also mentions that the upload process uses HTTP and may take up to two minutes, after which the device will reboot. Below this, there is a section titled 'Reset All Settings Except Mesh After Firmware Upgrade' which lists the settings that will be kept (Wi-Fi settings, Mesh settings, etc.) and those that will be reset. Underneath, there are two checkboxes: 'Reset All Settings After Firmware Upgrade' and 'Reset All Settings Except Mesh After Firmware Upgrade', both of which are currently unchecked. Below these checkboxes, the 'Current Firmware Version' is displayed as 'V5.70(ACKA.0)b3'. At the bottom, there is a 'File Path' field with a 'Choose File' button next to it, which currently shows 'No file chosen'. To the right of the 'File Path' field is an orange 'Upload' button.

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.

Reset All Settings Except Mesh After Firmware Upgrade
- System will keep Wi-Fi settings, include these user settings (Mesh Enable/Disable, Mesh Controller Mode, Mesh Backhaul information, Single SSID Enable/Disable, MLO 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)

Upgrade Firmware

Reset All Settings After Firmware Upgrade ☐

Reset All Settings Except Mesh After Firmware Upgrade ☐

Current Firmware Version: V5.70(ACKA.0)b3

File Path No file chosen

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

Table 107 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Reset All Settings After Firmware Upgrade	Select the checkbox to have the WE Device automatically reset itself after the new firmware is uploaded.
Reset All Settings Except Mesh After Firmware Upgrade	Select this to reset all your configurations, except for Mesh WiFi settings, to the factory defaults after firmware upgrade. This minimizes interruption to your Mesh WiFi network after upgrading firmware. Mesh WiFi settings include: • Controller/Agent Mode • Mesh Internet Access • Main and Guest SSIDs including Guest WiFi isolation • 2.4GHz & 5GHz Radios • 802.11 Mode • Protected Management Frames • Encryption and WPA keys
Current Firmware Version	The firmware on each WE Device is identified by the firmware trunk version, followed by a unique code which identifies the model, and then the release number after the period. For example, 5.70(ACKA.0) is a firmware for the 5.70 version trunk, the ACKA code identifies the specific WE Device model, and .0 is the first firmware release for this model.
File Path	Enter the location of the file you want to upload in this field or click Choose File to find it.
Choose File	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.

Figure 172 Firmware Uploading

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.

Reset All Settings Except Mesh After Firmware Upgrade
 - System will keep Wi-fi settings, include these user settings (Mesh Enable/Disable, Mesh Controller Mode, Mesh Backhaul Information, Single SSID Enable/Disable, MLO 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)

Upgrade Firmware

Reset All Settings After Firmware Upgrade ☐

Reset All Settings Except Mesh After Firmware Upgrade ☐

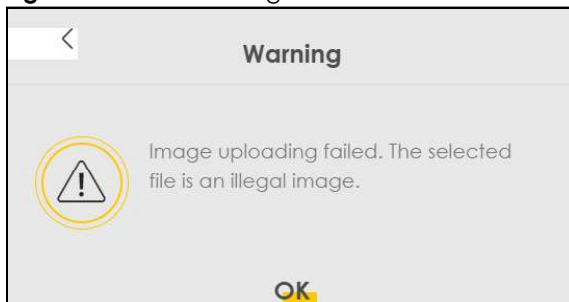
Current Firmware Version: V5.70(ACKA.0)b3

File Path

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

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

Figure 173 Error Message



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



CHAPTER 33

Backup/Restore

33.1 Backup/Restore Overview

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

33.2 Backup/Restore Settings

Click **Maintenance > Backup/Restore**. Information related to factory default settings, backup configuration and restoring configuration appears in this screen.

Figure 174 Maintenance > Backup/Restore

Backup/Restore

Backup/Restore ROM-D

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

Choose File

No file chosen

Upload

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 192.168.1.2

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

Backup Configuration

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

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

Restore Configuration

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

Table 108 Maintenance > Backup/Restore: Restore Configuration

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

Do NOT turn off the WE Device while configuration file upload is in progress.

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

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

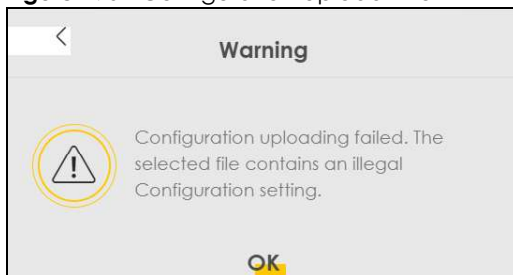
Figure 175 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default WE Device IP address (192.168.1.2).

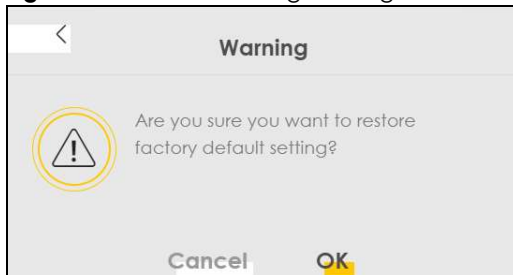
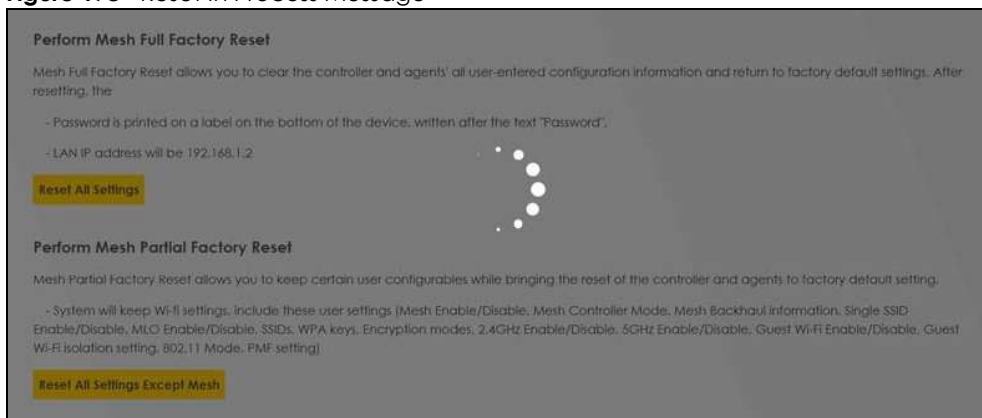
If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Backup/Restore** screen.

Figure 176 Configuration Upload Error



Reset to Factory Defaults

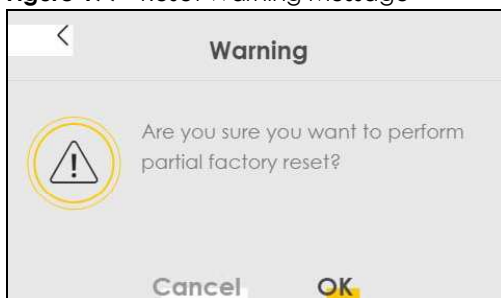
Click the **Reset All Settings** button to clear all user-entered configuration information and return the WE Device to its factory defaults. The following warning screen appears.

Figure 177 Reset Warning Message**Figure 178** Reset In Process Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your WE Device. Refer to [Section 2.5 on page 41](#) for more information on the **RESET** button.

Perform Partial Factory Reset

Click the **Reset All Settings Except Mesh** button to clear all user-entered configuration information and return the WE Device to its factory defaults except for Mesh WiFi settings. The following warning screen appears.

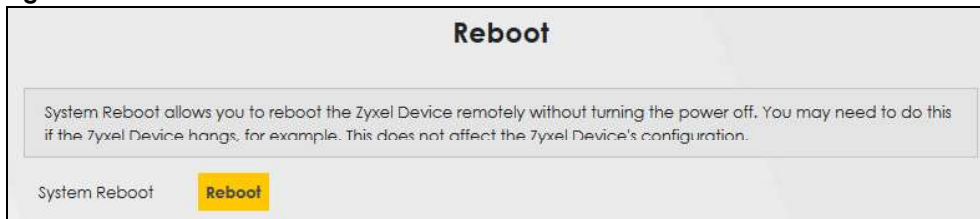
Figure 179 Reset Warning Message

33.3 Reboot

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

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

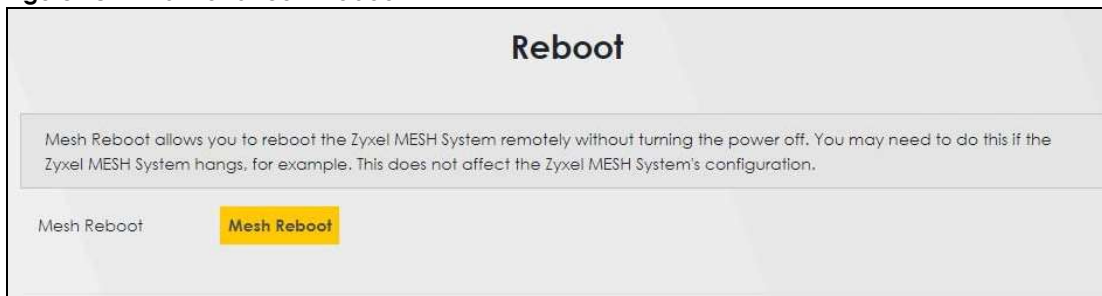
Figure 180 Maintenance > Reboot



Mesh Reboot allows you to reboot the Zyxel Mesh system remotely without turning the power off. You may need to do this if the Mesh system hangs, for example. This does not affect the Zyxel Mesh system's configuration.

Click **Maintenance > Reboot**. Click **Mesh Reboot** to have the Zyxel Mesh system to reboot.

Figure 181 Maintenance > Reboot



Note: **Mesh Reboot** is only available when **MPro Mesh** in **Network Setting > Wireless > MESH** is enabled and the WE Device is set as **Controller**.

CHAPTER 34

Diagnostic

34.1 Diagnostic Overview

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

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

34.1.1 What You Can Do in this Chapter

The **Diagnostic** screen lets you ping an IP address or trace the route packets take to a host ([Section 34.3 on page 269](#)).

34.2 What You Need to Know

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

How CFM Works

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

CFM provides two tests to discover connectivity faults.

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

34.3 Diagnostic Test

Use this screen use ping, traceroute, or nslookup for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking on one of the buttons to start a test, the results will be shown in the Ping/Traceroute Test area. Use nslookup to find the IP address for a host name and vice versa. Click **Maintenance > Diagnostic** to open the screen shown next.

Figure 182 Maintenance > Diagnostic

Diagnostic

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

Use this screen to ping, traceroute, or nslookup for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking on one of the buttons to start a test, the results will be shown in the Ping/Traceroute Test area. Use nslookup to find the IP address for a host name and vice versa.

Diagnostic Test

TCP/IP

Address

Ping Ping 6 Trace Route Trace Route 6 Nslookup

The following table describes the fields in this screen.

Table 109 Maintenance > Diagnostic

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

PART III

Troubleshooting and Appendices

Appendices contain general information. Some information may not apply to your WE Device.

CHAPTER 35

Troubleshooting

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

- [Accessibility and Compatibility Problems](#)
- [Power and Hardware Problems](#)
- [Device Access Problems](#)
- [Internet Problems](#)
- [WiFi Problems](#)
- [Resetting the WE Device to Its Factory Defaults](#)
- [Zyxel One App Problems](#)
- [Daisy Chain Problems](#)

35.1 Accessibility and Compatibility Problems

[Screen reader not reading content.](#)

- Ensure the latest version of the screen reader is installed.
- Check if the screen reader's accessibility settings are enabled.

[Web browser not displaying correctly.](#)

- Clear your web browser cache.
- Ensure that JavaScript is enabled.
- Try using a different supported web browser.

35.2 Power and Hardware Problems

[The WE Device does not turn on. None of the LEDs turn on.](#)

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

[One of the LEDs does not behave as expected.](#)

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

35.3 Device Access Problems

[I do not know the IP address of the WE Device.](#)

- 1 The default LAN IP address is 192.168.1.2.
- 2 If your router assigns an IP address to the WE Device, you can find your new IP address on the Zyxel One app or on your router's Web Configurator.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 35.6 on page 275](#).

[I forgot the admin password.](#)

- 1 See the cover page for the default login names and associated passwords.
- 2 If those do not work, you have to reset the device to its factory defaults. See [Section 35.6 on page 275](#).

I cannot access the Web Configurator screen.

- 1 Make sure you are using the correct IP address.
 - The default IP address is [192.168.1.2](#).
 - If you changed the IP address, use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I do not know the IP address of the WE Device](#).
 - Make sure your computer has an IP address in the same subnet as the WE Device. Your computer should have an IP address from 192.168.1.3 to 192.168.1.254. See [Section 35.6 on page 275](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected.
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
- 4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance > Remote Management**).
- 5 Reset the device to its factory defaults, and try to access the WE Device with the default IP address. See [Section 35.6 on page 275](#).
- 6 If the problem continues, contact the network administrator or vendor, or try the advanced suggestion.

Advanced Suggestion

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.

I cannot log into the WE Device.

- 1 Make sure you have entered the password correctly. See the cover page for the default login names and associated passwords. The field is case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the Web Configurator while someone is using Telnet to access the WE Device. Log out of the WE Device in the other session, or ask the person who is logged in to log out.
- 3 Turn the WE Device off and on.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 35.6 on page 275](#).

35.4 Internet Problems

[I cannot access the Internet.](#)

- 1 Check the hardware connections. Make sure the LEDs are behaving as expected. See the **Quick Start Guide**.
- 2 Make sure you entered your ISP account information correctly in the **Network Setting > Home Networking** screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 If you are trying to access the Internet wirelessly, make sure that you enable WiFi on the WE Device (the WE Device's WiFi is enabled by default) and your WiFi client, and that the WiFi settings in the WiFi client are the same as the settings in the WE Device.
- 4 Disconnect all the cables from your device and reconnect them.
- 5 If the problem continues, contact your ISP.

[I cannot connect to the Internet using an Ethernet cable.](#)

- Make sure you have the Ethernet LAN port connected to a modem or router. To see more details about how to set up the router and the WE Device, please go to the link of the Zyxel One app tutorial in [Section 1.6 on page 27](#).

35.5 WiFi Problems

[The WiFi connection is slow and intermittent.](#)

The following factors may cause interference:

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

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

- Move your WiFi device closer to the AP if the signal strength is low.
- Reduce WiFi interference that may be caused by other WiFi networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the WiFi client. Avoid placing the WE Device inside any type of box that might block WiFi signals.

- Reduce the number of WiFi clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the WiFi client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

I cannot access the WE Device using WiFi.

- Make sure the WE Device is working in AP or Repeater mode and WiFi is enabled on the WE Device.
- Make sure the WiFi adapter on the WiFi client is working properly.
- Make sure the WiFi adapter installed on your computer is IEEE 802.11 compatible and supports the same WiFi standard as the WE Device.
- Make sure your computer (with a WiFi adapter installed) is within the transmission range of the WE Device.
- Check that both the WE Device and your WiFi station are using the same WiFi and WiFi security settings.

35.6 Resetting the WE Device to Its Factory Defaults

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

You will lose all of your changes when you reset the WE Device to its factory defaults.

- You can back up the configuration you made before resetting the WE Device.

To reset the WE Device,

- Make sure the power LED is on.
- Press the **RESET** button for longer than 5 seconds, the Power LED begins to blink, to set the WE Device back to its factory-default configuration.

OR

Click **Maintenance** > **Restore** and then click **Reset**.

- If the WE Device restarts automatically, wait for the WE Device to finish restarting, and log in to the Web Configurator. The password is in the device label.

If the WE Device does not restart automatically, disconnect and reconnect the WE Device. Then, follow the directions above again.

- You can upload a previously saved configuration file from your computer to the WE Device after resetting the device.

35.7 Zyxel One App Problems

[I cannot use the Zyxel One app to manage my WiFi network.](#)

- Make sure you connect your mobile device to the WiFi network of the controller (The Mesh Router or the WE Device) in order to manage the WiFi network. Go to the link of the Zyxel One app tutorial in [Section 1.6 on page 27](#) for more information.
- Make sure you enable Mesh on your Mesh Router, so your mobile device can find the Mesh Router through the Zyxel One app. To enable Mesh, log into the Mesh Router's web configurator and go to **Network Setting > Wireless > MESH**. Click the **MPro Mesh** switch to the right. Please see the Mesh Router's User's Guide for more information.
- Make sure you use the controller's (The Mesh Router or the WE Device) SSID and wireless key when logging in with the app.

35.8 Daisy Chain Problems

[I cannot add another WE Device to my daisy chain network.](#)

- Check your device mode. The mode of your WE Device will affect how you add another WE Device to your network. For more information on modes, see [Section 1.1 on page 17](#). For more information on how to set your device in AP or Repeater mode, see [Section 1.1.1 on page 17](#).
- If you are using the WPS PBC (Push Button Configuration) method, make sure you press the WPS button in the right way. For more information on adding WE Devices using WPS button, see [Section 2.4.1 on page 40](#).
- If you are using the Zyxel One app for adding a WE Device to your network, make sure you choose the right scenario.

For more information about how to set up the WE Device with the Zyxel One app, please go to the link of the Zyxel One app tutorial in [Section 1.6 on page 27](#) to add WE Devices to your network.

APPENDIX A

Customer Support

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

For Zyxel Communication offices, see <https://service-provider.zyxel.com/global/en/contact-us> for the latest information.

For Zyxel Network offices, see <https://www.zyxel.com/index.shtml> for the latest information.

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

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- <https://www.zyxel.com>

Asia

China

- Zyxel Communications Corporation–China Office
- <https://www.zyxel.com/cn/sc>

India

- Zyxel Communications Corporation–India Office
- <https://www.zyxel.com/in/en-in>

Kazakhstan

- Zyxel Kazakhstan
- <https://www.zyxel.com/ru/ru>

Korea

- Zyxel Korea Co., Ltd.
- <http://www.zyxel.kr/>

Malaysia

- Zyxel Communications Corp.
- <https://www.zyxel.com/global/en>

Philippines

- Zyxel Communications Corp.
- <https://www.zyxel.com/global/en>

Singapore

- Zyxel Communications Corp.
- <https://www.zyxel.com/global/en>

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- <https://www.zyxel.com/tw/zh>

Thailand

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

Vietnam

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

Europe

Belarus

- Zyxel Communications Corp.
- <https://www.zyxel.com/ru/ru>

Belgium (Netherlands)

- Zyxel Benelux
- <https://www.zyxel.com/nl/nl>
- <https://www.zyxel.com/fr/fr>

Bulgaria

- Zyxel Bulgaria

- <https://www.zyxel.com/bg/bg>

Czech Republic

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

Denmark

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

Finland

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

France

- Zyxel France
- <https://www.zyxel.com/fr/fr>

Germany

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

Hungary

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

Italy

- Zyxel Communications Italy S.r.l.
- <https://www.zyxel.com/it/it>

Norway

- Zyxel Communications A/S
- <https://www.zyxel.com/no/no>

Poland

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

Romania

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

Russian Federation

- Zyxel Communications Corp.
- <https://www.zyxel.com/ru/ru>

Slovakia

- Zyxel Slovakia
- <https://www.zyxel.com/sk/sk>

Spain

- Zyxel Iberia
- <https://www.zyxel.com/es/es>

Sweden

- Zyxel Communications A/S
- <https://www.zyxel.com/se/sv>

Switzerland

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

Turkey

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

UK

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

Ukraine

- Zyxel Ukraine
- <https://www.zyxel.com/ua/uk-ua>

South America

Argentina

- Zyxel Communications Corp.
- <https://www.zyxel.com/co/es-co>

Brazil

- Zyxel Communications Brasil Ltda.

- <https://www.zyxel.com/br/pt>

Colombia

- Zyxel Communications Corp.
- <https://www.zyxel.com/co/es-co>

Ecuador

- Zyxel Communications Corp.
- <https://www.zyxel.com/co/es-co>

South America

- Zyxel Communications Corp.
- <https://www.zyxel.com/co/es-co>

Middle East

Israel

- Zyxel Communications Corp.
- <https://il.zyxel.com>

North America

USA

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

APPENDIX B

IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses.

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

Prefix and Prefix Length

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

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

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

Link-local Address

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

Table 110 Link-local Unicast Address Format

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

Global Address

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

Unspecified Address

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

Loopback Address

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

Multicast Address

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

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

Table 111 Predefined Multicast Address

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

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

Table 112 Reserved Multicast Address

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

Table 112 Reserved Multicast Address (continued)

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

Subnet Masking

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

Interface ID

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

EUI-64

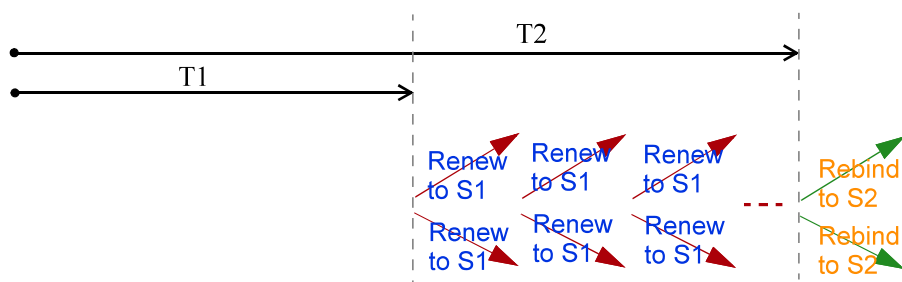
The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits ffe between the third and fourth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

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

Identity Association

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

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



DHCP Relay Agent

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

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

Prefix Delegation

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

ICMPv6

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

Neighbor Discovery Protocol (NDP)

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

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.

- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The WE Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the WE Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the WE Device also sends out a neighbor solicitation message. When the WE Device receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the WE Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The WE Device creates an entry in the default router list cache if the router can be used as a default router.

When the WE Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the WE Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is on-link, the address is considered as the next hop. Otherwise, the WE Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the WE Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the WE Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

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

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

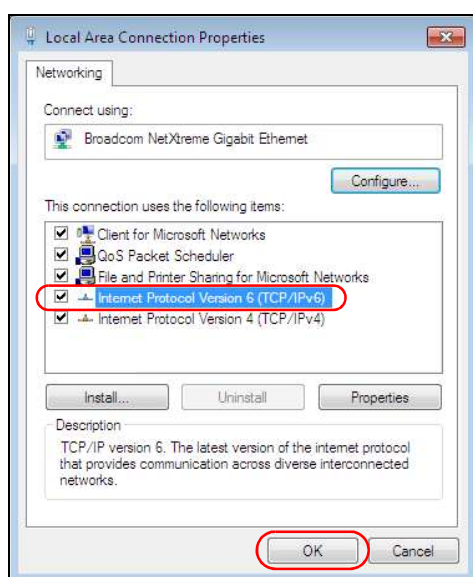
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example – Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

- 1 Select **Control Panel > Network and Sharing Center > Local Area Connection**.
- 2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
- 3 Click **OK** to save the change.



- 4 Click **Close** to exit the **Local Area Connection Status** screen.
- 5 Select **Start > All Programs > Accessories > Command Prompt**.
- 6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:b021:2d::1000
    Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
    IPv4 Address. . . . . : 172.16.100.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::213:49ff:feaa:7125%11
                                172.16.100.254
```

APPENDIX C

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**.
 - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 113 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by email.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol – a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for email.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.

Table 113 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
NFS	UDP	2049	Network File System – NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one email server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.

Table 113 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
VDOLIVE	TCP UDP	7000 user- defined	A videoconferencing solution. The UDP port number is specified in the application.

APPENDIX D

Legal Information

Copyright

Copyright © 2025 by Zyxel and/or its affiliates.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

United States of America



The following information applies if you use the product within USA area.

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference, and
 - (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful

interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

The following information applies to products with wireless functions.

- For 2.4G WLAN, only channels 1~11 are operational. Selection of other channels is not possible.
- Operation of this device is restricted to indoor use only, unless the relevant user's manual states that this device can be installed outdoors.

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

The following information applies for products operating in the 5.925-7.125 GHz band.

Low-power Indoor Access Point

- FCC regulations restrict the operation of this device to indoor use only.
- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet in the 5.925-6.425 GHz band.
- Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Standard Power Access Point

- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft.
- Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Europe and the United Kingdom



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

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

Model List: WE3300-00, WE4600-00

- Compliance information for wireless products relevant to the EU, United Kingdom, and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5 GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5 GHz wireless LANs.
- If this device for operation in the band 5150 – 5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20 cm between the radio equipment and your body.
- The maximum RF power operating for each band as follows:
- WE3300-00:
 - The band 2400 to 2483.5 MHz is 20 dBm.
 - The band 5150 to 5350 MHz is 23 dBm.
 - The band 5470 to 5725 MHz is 30dBm.
 - The band 5725 to 5850 MHz is 23 dBm. (UK only)
- WE4600-00:
 - The band 2400 to 2483.5 MHz is 98.175 mW.
 - The band 5150 to 5350 MHz is 171.791 mW.
 - The band 5470 to 5725 MHz is 465.586 mW.
 - The band 5725 to 5850 MHz is 157.398 mW. (UK only)
 - The band 5945 to 6425 MHz is 190.546 mW.

United Kingdom



UK Declaration of Conformity

Zyxel hereby declares that the device is in compliance with the essential requirements and other relevant provisions of the Radio Equipment Regulations 2017.

The original UK Declaration of Conformity may be found at <https://service-provider.zyxel.com/global/en/tech-support>.

National Restrictions

Attention: This device may only be used indoors in Great Britain.



Belgium (English)	National Restrictions - The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details. - Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens. - Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.
België (Flemish)	
Belgique (French)	
Čeština (Czech)	
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Ζyxel ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. National Restrictions - This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check https://www.mise.gov.it/it/ for more details. - Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare https://www.mise.gov.it/it/ per maggiori dettagli.

Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoją, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществениите изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.

Notes:

- Not all European states that implement EU Directive 2014/53/EU are European Union (EU) members.
- The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not put the device in a place that is humid, dusty or has extreme temperatures as these conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for the power rating of the device and operating temperature.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- The Power Supply is not waterproof, avoid contact with liquid. Handle the Power Supply with care; do not pry open, nor pull or press the pins on it.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/adaptors. Connect it to the right supply voltage (for example, 120V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adaptor or cord is prohibited. Contact your local vendor to order a new one.

- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
 - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
 - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Important Safety Instructions

- Caution! The RJ-45 jacks are not used for telephone line connection.
- Caution! Do not use this product near water, for example a wet basement or near a swimming pool.
- Caution! Avoid using this product (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Caution! Always disconnect all telephone lines from the wall outlet before servicing or disassembling this product.
- Attention: Les prises RJ-45 ne sont pas utilisés pour la connexion de la ligne téléphonique.
- Attention: Ne pas utiliser ce produit près de l'eau, par exemple un sous-sol humide ou près d'une piscine.
- Attention: Évitez d'utiliser ce produit (autre qu'un type sans fil) pendant un orage. Il peut y avoir un risque de choc électrique de la foudre.
- Attention: Toujours débrancher toutes les lignes téléphoniques de la prise murale avant de réparer ou de démonter ce produit.

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless setting, please refer to the chapter about wireless settings for more detail.)

European Union – Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣



以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 第十二條 經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

- 第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
- 前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 – 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
 - 任何液體 – 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
 - 灰塵及污物 – 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
 - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
 - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor.

Enquiries

Go to <https://www.zyxel.com/service-provider/global/en/download-enquiry> to request a User's Guide for configuration assistance and related safety warnings.

General enquiry

Sales enquiry

Media enquiry

Download enquiry

Download enquiry

Please use this enquiry form if you are an internet service provider (ISP) or system integrator. We will respond shortly after your submission.

First name *

Last name

Email *

Phone

Job title

Company *

Country *

Model *

- Select your country -

Select the materials you need

☐ Datasheet

☐ Quick start guide

☐ Users Guide

Message

☐ I have read the Privacy Policy. *
Information [here](#).

☐ Sign up for exclusive networking insights, news, and special offers.

Submit

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses, please go to: <https://service-provider.zyxel.com/global/en/gpl-oss-software-notice>.

Index

Numbers

6rd
 IPv6 [87](#)
802.11 mode [60](#)

A

Access Control (Rules) screen [202](#)
access point [125](#)
 coverage area [22](#)
Access Point (AP) mode [18](#)
activation
 firewalls [199](#)
 SSID [111](#)
Address Resolution Protocol [233](#)
ad-hoc type
 network [125](#)
Antenna [17](#)
AP controller [22](#)
AP Mode [40](#)
 Web Configurator access [42](#)
AP steering [20](#)
APC mode [40](#)
Apple Store [2](#), [27](#)
Application Layer Gateway (ALG) [183](#)
applications, NAT [186](#)
ARP Table [233](#)
Arrow icon [55](#), [57](#)
Asynchronous Transfer Mode [86](#)
ATM [86](#)
authentication [127](#), [128](#)
 RADIUS server [128](#)

B

backup

 configuration [264](#)
Backup/Restore screen [79](#)
Band select [72](#)
band steering [20](#)
band steering application [21](#)
bandwidth capacity
 cable type [20](#)
bandwidth usage
 optimize [20](#)
Basic Service Set, see BSS
Basic Service Sets (BSSs) [130](#)
bridge [125](#)
Bridge mode [95](#)
broadband [85](#)
Broadband screen
 overview [85](#)
broadcast [101](#)
BSS [129](#)
 example [130](#)
button
 power [37](#), [38](#)
 RESET [37](#), [38](#), [39](#), [41](#)
 WPS [37](#), [38](#), [39](#), [40](#), [72](#)

C

CA [223](#)
cable type
 Ethernet [20](#)
Canonical Format Indicator See CFI
CCMs [268](#)
certificate
 details [225](#)
 factory default [218](#)
 file format [224](#)
 file path [222](#)
 import [218](#), [221](#)
 public and private keys [224](#)
 verification [224](#)

- certificate request
 - create [218](#)
 - view [219](#)
- certificates [217](#)
 - advantages [224](#)
 - authentication [217](#)
 - CA [217](#), [223](#)
 - creating [219](#)
 - public key [217](#)
 - replacing [218](#)
 - storage space [218](#)
 - thumbprint algorithms [225](#)
 - trusted CAs [222](#)
 - verifying fingerprints [224](#)
- Certification Authority [217](#)
- Certification Authority, see CA
- certifications [296](#)
 - viewing [301](#)
- CFI [100](#)
- CFM [268](#)
 - CCMs [268](#)
 - link trace test [268](#)
 - loopback test [268](#)
 - MA [268](#)
 - MD [268](#)
 - MEP [268](#)
 - MIP [268](#)
- channel
 - WiFi [126](#)
- channel number [60](#)
- Channel Status screen [117](#)
- Check icon [54](#)
- configuration
 - back up [79](#)
 - backup [264](#)
 - firewalls [199](#)
 - reset [265](#)
 - restore [80](#)
 - restoring [265](#)
 - static route [190](#)
- Connection Status screen
 - overview [54](#)
- connection status screen [44](#)
- Connectivity Check Messages, see CCMs
- contact information [277](#)
- controller
 - network [22](#)

- copyright [292](#)
- coverage area
 - access point [22](#)
 - repeater [22](#)
- CPU usage percentage [59](#)
- Create Certificate Request screen [219](#)
- creating certificates [219](#)
- CTS threshold [127](#)
- customer support [277](#)
- customized service [200](#)
 - add [201](#)
- customized services [201](#)
- CyberTrust [217](#)

D

- daisy chain [40](#)
 - form [26](#)
- data encryption [110](#), [113](#)
- data fragment threshold [127](#)
- DDoS [198](#)
- Denials of Service, see DoS
- device label [41](#)
- DFS channel [117](#)
- DHCP [139](#), [154](#)
- DHCP Server Lease Time [145](#)
- DHCP Server State [145](#)
- digital IDs [217](#)
- disclaimer [292](#)
- distance limitation
 - cable type [20](#)
- distance maximum
 - cable type [20](#)
- DMZ screen [182](#)
- DNS [154](#)
- DNS server address assignment [101](#)
- DNS Values [145](#)
- Domain Name [187](#)
- DoS [197](#)
 - thresholds [198](#)
- DoS protection blocking
 - enable [205](#)
- Dual Stack Lite [87](#)

dual-band application [23, 24](#)
dual-band WiFi [23](#)
dual-band WiFi extender [17](#)
dynamic DNS [189](#)
 wildcard [189](#)
Dynamic Host Configuration Protocol, see DHCP
DYNDNS wildcard [189](#)

E

ECHO [187](#)
Edit icon [56](#)
email
 log example [258](#)
 log setting [258](#)
Encapsulation [97](#)
 MER [97](#)
 PPP over Ethernet [98](#)
encapsulation
 RFC 1483 [98](#)
encapsulation method
 technical reference [97](#)
encryption [128](#)
 type [109](#)
Extended Service Set IDentification [108, 112](#)
Eye icon [60](#)

F

factory-default configuration file
 reload [41](#)
Fast Leave [195](#)
filters
 MAC address [114, 128](#)
Finger services [187](#)
firewall
 enhancing security [207](#)
 LAND attack [198](#)
 security considerations [207](#)
 traffic rule direction [204](#)
Firewall DoS screen [205](#)
Firewall General screen [199](#)
firewall rules

 direction of travel [206](#)
firewalls [197, 199](#)
 actions [204](#)
 configuration [199](#)
 customized service [200](#)
 customized services [201](#)
 DDoS [198](#)
 DoS [197](#)
 thresholds [198](#)
 ICMP [198](#)
 Ping of Death [198](#)
 rules [206](#)
 security [207](#)
 SYN attack [197](#)
firmware [260](#)
 download [79](#)
 upload [79](#)
 version [59](#)
Firmware Upgrade screen [79](#)
fragmentation threshold [127](#)
front panel [28](#)

G

General screen [70, 104](#)
gigabit Ethernet LAN port [17](#)
Google Play [2, 27](#)
guest WiFi network
 configure [110](#)
 enable [63](#)
guest WiFi settings
 configuring [63](#)
Guest/More AP screen [76, 110](#)
Guest/More AP settings
 edit [111](#)

H

home networking
 example [138](#)
Home Networking screen [140](#)
Home Security URL filtering [211](#)
HTTP [187](#)

I

ICMP [198](#)
ICMPv6 [194](#)
icon
 Arrow [55, 57](#)
 Check [54](#)
 Edit [56](#)
 Eye [60](#)
 Language [52](#)
 layout [54](#)
 Logout [52](#)
 menu [45](#)
 Restart [52](#)
 Theme [52](#)
IEEE 802.11 compliant [130](#)
IEEE 802.11a/b/g/n/ac/ax [23](#)
IEEE 802.11ax [104](#)
IEEE 802.1Q [100](#)
IGA [185](#)
IGMP [101](#)
 multicast group list [194, 238, 239](#)
 version [101](#)
IGMP Fast Leave [194](#)
IGMPv2 [194](#)
IGMPv3 [194](#)
ILA [185](#)
Import Certificate screen [222](#)
importing trusted CAs [222](#)
infrastructure type
 network [125](#)
Inside Global Address, see IGA
Inside Local Address, see ILA
Internet connection
 add or edit [90](#)
Internet Control Message Protocol, see ICMP
Internet Protocol version 6 [86](#)
Internet Protocol version 6, see IPv6
Intra LAN Multicast [195](#)
Intra-BSS traffic [129](#)
IP address [138, 155](#)
 ping [269](#)
 private [155](#)
 view [56](#)
 WAN [86](#)

IP address assignment [100](#)
IP alias
 NAT applications [187](#)
IP over Ethernet [97](#)
IP packet
 transmission method [101](#)
IPoE technical reference [97](#)
IPv4 address [60](#)
 LAN [65](#)
IPv4 firewall [200](#)
IPv6 [86, 282](#)
 addressing [86, 101, 282](#)
 EUI-64 [284](#)
 global address [282](#)
 interface ID [284](#)
 link-local address [282](#)
 Neighbor Discovery Protocol [282](#)
 ping [282](#)
 prefix [86, 102, 282](#)
 prefix and length [86](#)
 prefix delegation [88](#)
 prefix length [86, 102, 282](#)
 subnet mask [87](#)
 unspecified address [283](#)
IPv6 address [60](#)
 abbreviation method [101](#)
IPv6 firewall [200](#)
IPv6 rapid deployment [87](#)

J

Java permission [42](#)
JavaScript [42](#)

K

key
 default [41](#)

L

LAN

- DHCP [154](#)
- DNS [154](#)
- IP address [138](#), [140](#), [155](#)
- MAC address [148](#)
- overview [138](#)
- status [60](#), [65](#)
- subnet mask [139](#), [140](#), [142](#), [155](#)
- LAN Ethernet adapter [60](#)
- LAN IP address
 - view [65](#)
- LAN IPv6 Mode Setup [146](#)
- LAN port [17](#)
- LAN setup [65](#)
- LAN Setup screen [142](#)
- LAN subnet mask [145](#)
- LAN to LAN multicast [195](#)
- LAND attack [198](#)
- Language icon [52](#)
- Layout icon [54](#)
- LBR [268](#)
- LED
 - Link [29](#), [31](#), [34](#)
 - POWER [29](#), [31](#), [34](#)
 - WiFi [30](#), [32](#), [33](#), [35](#)
- LED table [28](#)
- LEDs [28](#)
- limitations
 - WiFi [129](#)
 - WPS [136](#)
- Link LED [29](#), [31](#), [34](#), [40](#)
- link rate
 - maximum [104](#)
- link trace [268](#)
- Link Trace Message, see LTM
- Link Trace Response, see LTR
- link-local address [60](#)
- List view screen [56](#)
- Local Certificates screen [217](#)
- Log Setting screen [256](#)
- login [43](#)
- login screen [43](#)
- Logout icon [52](#)
- logs [226](#), [256](#)
- Loop Back Response, see LBR
- loopback [268](#)

- LTM [268](#)
- LTR [268](#)

M

- MA [268](#)
- MAC (Media Access Control) address [60](#), [113](#)
- MAC address [148](#)
 - add [114](#)
 - add/edit [115](#)
 - filter [114](#), [128](#)
 - LAN [148](#)
 - view [56](#)
- MAC authentication [114](#)
- MAC authentication rule
 - edit [115](#)
- MAC Authentication screen [114](#), [115](#)
- MAC Filter [208](#)
- MAC filter rule
 - add [114](#)
- MAC filter settings [114](#)
- Maintenance Association, see MA
- Maintenance Domain, see MD
- Maintenance End Point, see MEP
- malware (malicious software) [127](#)
- management frame protection (MFP) [108](#), [110](#), [113](#)
- Maximum Burst Size (MBS) [99](#)
- MBSSID [130](#)
- MBSSID (Multiple Basic Service Set Identifier) [130](#)
- MD [268](#)
- menu icon [45](#)
- MEP [268](#)
- Mesh [20](#), [40](#)
- Mesh application [22](#)
- MLD [194](#)
- MLDv1 [194](#)
- MLDv2 [194](#)
- mobile app [17](#)
- mode
 - select [40](#)
- model number [59](#)
- models
 - WE Series [17](#)

MTU (Multi-Tenant Unit) [100](#)
multicast [101](#)
Multicast Listener Discovery, see MLD
multicast traffic [108](#)
multi-gigabit (IEEE 802.3bz) [19](#)
multi-gigabit application [20](#)
Multiple BSS, see MBSSID
multiplexing [98](#)
 LLC-based [98](#)
 VC-based [98](#)
multiprotocol encapsulation [98](#)
MU-MIMO [17](#)

N

NAT [185](#)
 applications [186](#)
 IP alias [187](#)
 default server [182](#)
 DMZ host [182](#)
 example [186](#)
 global [185](#)
 IGA [185](#)
 ILA [185](#)
 inside [185](#)
 local [185](#)
 multiple server example [175](#)
 outside [185](#)
 port number [187](#)
 services [187](#)
NAT ALG screen [183, 184](#)
NAT example [188](#)
navigation panel [46](#)
Network Address Translation, see NAT
network connection status
 view [55](#)
network map [46, 47](#)
NNTP [187](#)

O

Others screen [72](#)

P

Packet Transfer Mode [86](#)
parental control
 schedule setup [214, 216](#)
password [41](#)
 configure [61](#)
 reset [41](#)
PBC [131](#)
 WPS [72](#)
Peak Cell Rate (PCR) [98](#)
PIN
 WPS [131](#)
PIN (Personal Identification Number) [131](#)
PIN (Personal Identification Number) [72](#)
PIN configuration [72](#)
 WPS [72](#)
PIN, WPS
 example [133](#)
Ping of Death [198](#)
Point-to-Point Tunneling Protocol, see PPTP
POP3 [187](#)
port forwarding rule
 add/edit [177](#)
Port Forwarding screen [175, 177](#)
Port Triggering
 add new rule [181](#)
Port Triggering screen [178](#)
Power Button [37, 38](#)
power cable
 connect [37, 38, 39](#)
Power LED [40, 41](#)
PPPoE [98](#)
 Benefits [98](#)
 technical reference [98](#)
PPTP [187](#)
preamble [127](#)
preamble type [130](#)
prefix delegation [88](#)
Pre-Shared Key (PSK) [109](#)
private IP address [155](#)
Protocol (Customized Services) screen [200](#)
Protocol Entry
 add [201](#)
PTM [86](#)

Push Button Configuration

WPS [72](#)

Push Button configuration (PBC) [132](#)

Push Button Configuration (PBC) method [115](#)

Push Button Configuration, see PBC

Push Button, WPS [131](#)

Q

QR code [60](#)

R

RADIUS server [128](#)

RAM usage percentage [59](#)

Repeater [18](#)

repeater

coverage area [22](#)

Repeater (RP) mode [18](#)

Repeater mode [40](#)

Web Configurator access [42](#)

reset [265](#)

RESET button [37](#), [38](#), [39](#), [41](#)

reset the WE Device [41](#)

restart [266](#)

Restart icon [52](#)

restoring configuration [265](#)

RFC 1058, see RIP

RFC 1389, see RIP

RFC 1483 [98](#)

RFC 1631 [174](#)

RFC 3164 [226](#)

RIP [173](#)

router controller [22](#)

Routing Information Protocol, see RIP

routing table [235](#)

RTS threshold [127](#)

S

screen order

arrange [54](#)

screen resolution recommended [42](#)

secure WiFi [40](#)

security

network [207](#)

WiFi [127](#)

Security Log [228](#)

security mode [60](#), [70](#)

Security Parameter Index, see SPI

security settings [103](#)

serial number [59](#)

service access control [247](#)

service set [108](#), [112](#)

services

port forwarding [187](#)

setup

firewalls [199](#)

static route [190](#)

SMTP [187](#)

SNMP [187](#)

SNMP trap [187](#)

SPI [198](#)

SSID [60](#), [128](#)

activation [111](#)

configure [61](#)

hide [62](#)

MBSSID [130](#)

SSID (Service Set Identifier) [111](#)

SSID (Service Set IDentity) [62](#)

static DHCP

configuration [149](#)

Static DHCP screen [148](#)

static route [163](#), [173](#)

configuration [190](#)

status [54](#)

firmware version [59](#)

LAN [60](#), [65](#)

WiFi [60](#)

Status screen [79](#)

subnet

same [18](#)

subnet mask [60](#), [65](#), [139](#), [155](#)

- view [65](#)
- Sustained Cell Rate (SCR) [99](#)
- SYN attack [197](#)
- syslog
 - protocol [226](#)
 - severity levels [226](#)
- syslog logging
 - enable [257](#)
- syslog server
 - name or IP address [257](#)
- system
 - firmware [260](#)
 - firmware version [59](#)
 - status [54](#)
 - LAN [65](#)
 - time [250](#)
- system Information
 - detailed information [58, 59](#)
- system information
 - view [57](#)
- system status
 - LAN [60](#)
 - WiFi [60](#)
- system uptime [59](#)

T

- Theme icon [52](#)
- thresholds
 - data fragment [127](#)
 - DoS [198](#)
 - RTS/CTS [127](#)
- time [250](#)
- Topology view screen [55](#)
- TPID [100](#)
- traffic shaping [98](#)
- transmission speed
 - cable type [20](#)
- Trusted CA certificate
 - view [223](#)
- Trusted CA screen [221](#)
- TWT (Target Wakeup Time) [104](#)

U

- unicast [101](#)
- unicast traffic [108](#)
- Universal Plug and Play, see UPnP
- upgrading firmware [260](#)
- uplink connection [26](#)
 - WiFi [26](#)
 - wired [26](#)
- UPnP [149](#)
 - forum [139](#)
 - NAT traversal [139](#)
 - security issues [139](#)
 - state [150](#)
 - usage confirmation [139](#)
- UPnP screen [149](#)
- UPnP-enabled Network Device
 - auto-discover [158](#)

V

- Vendor ID [153](#)
- VeriSign [217](#)
- Virtual Circuit (VC) [98](#)
- Virtual Local Area Network See VLAN
- VLAN [100](#)
 - Introduction [100](#)
- VLAN ID [100](#)
- VLAN tag [100](#)

W

- wall mount [17](#)
- WAN
 - Wide Area Network, see WAN [85](#)
- WAN IP address [86](#)
- warranty
 - note [301](#)
- WE Device
 - features comparison [17](#)
- WE Series [17](#)
- web browser recommended [42](#)
- Web Configurator [27](#)

- accessing [42](#)
- layout [45](#)
- login [43](#)
- overview [42](#)
- web server [217](#)
- WEP encryption [109](#)
- Wi-Fi
 - encryption [128](#)
 - fragmentation threshold [127](#)
 - MAC address filter [128](#)
 - MBSSID [130](#)
 - preamble [127](#)
 - RADIUS server [128](#)
 - RTS/CTS threshold [127](#)
 - SSID [128](#)
 - SSID activation [111](#)
 - WPS [131](#), [133](#)
 - WPS example [134](#)
 - WPS limitations [136](#)
 - WPS PIN [131](#)
 - WPS Push Button [131](#)
- WiFi
 - authentication [127](#), [128](#)
 - BSS [129](#)
 - BSS example [130](#)
 - channel [126](#)
 - limitations [129](#)
 - MAC address filter [114](#)
 - security [127](#)
 - status [60](#)
- WiFi adapter [130](#)
- Wi-Fi adapter utility [73](#)
- Wi-Fi Alliance [40](#), [131](#)
- Wi-Fi basics [103](#)
- Wi-Fi channel [275](#)
- Wi-Fi client [125](#)
- Wi-Fi connection
 - set up [103](#)
- Wi-Fi coverage
 - extend [17](#)
- Wi-Fi DoS attack
 - prevent [108](#), [110](#), [113](#)
- WiFi extender [17](#)
- Wi-Fi LED [30](#), [32](#), [33](#), [35](#)
- Wi-Fi network
 - example [125](#)
 - overview [125](#)
 - secure setup [66](#)
 - set up [70](#)
 - set up using WPS [72](#)
 - set up without WPS [73](#)
- WiFi network group
 - set up [73](#)
- WiFi network name [63](#)
- WiFi network settings
 - configure [60](#)
- WiFi overview [103](#)
- WiFi password [64](#)
- WiFi Protected Setup (WPS) [40](#), [115](#), [131](#)
- WiFi security
 - troubleshooting [275](#)
- WiFi setting
 - configuration [61](#), [62](#)
- WiFi standards [104](#)
- WiFi terms [127](#)
- WiFi tutorial [72](#)
- WiFi6 introduction [104](#)
- Wired Equivalent Protocol (WEP) [127](#)
- wireless LAN [275](#)
- Wireless screens [103](#)
- WPA encryption standard [109](#)
- WPA2-PSK [70](#), [104](#)
- WPS [17](#), [40](#), [60](#), [131](#), [133](#)
 - disable [62](#)
 - example [134](#)
 - limitations [136](#)
 - PIN [131](#)
 - example [133](#)
 - Push Button [131](#)
- WPS button [37](#), [38](#), [39](#), [40](#), [72](#), [131](#)
 - using [40](#)
- WPS LED [40](#)
- WPS methods
 - tutorial [72](#)
- WPS screen [72](#), [115](#)

Z

- Zyxel One app [2](#), [27](#)