CHAPTER 26
Traffic Status

26.1 Traffic Status Overview

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

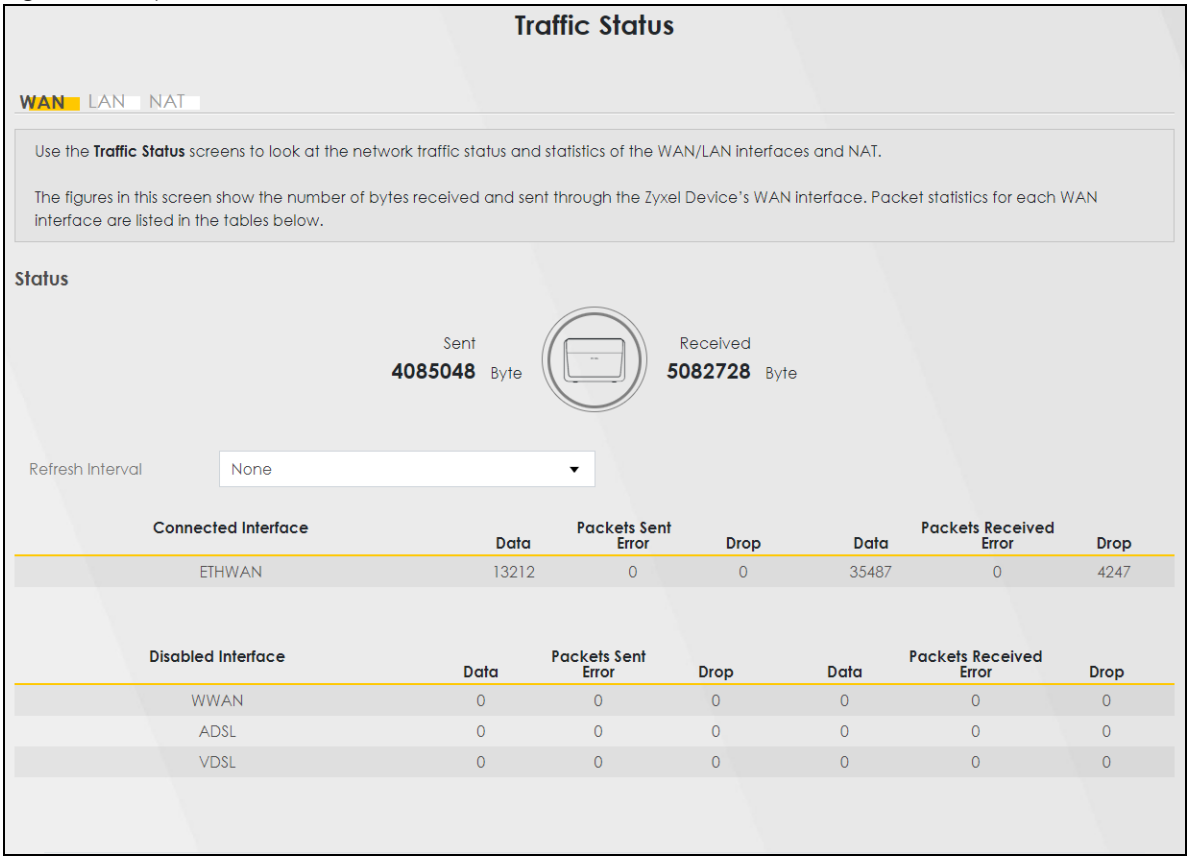
26.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 26.2 on page 365).
- Use the **LAN** screen to view the LAN traffic statistics (Section 26.3 on page 367).
- Use the **NAT** screen to view the NAT status of the Zyxel Device's clients (Section 26.4 on page 368).

26.2 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 Zyxel Device's WAN interface. The table below shows packet statistics for each WAN interface.

Figure 225 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 144 System Monitor > Traffic Status > WAN

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

Table 144 System Monitor > Traffic Status > WAN (continued)

LABEL	DESCRIPTION
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.

26.3 LAN Status

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

Figure 226 System Monitor > Traffic Status > LAN

The following table describes the fields in this screen.

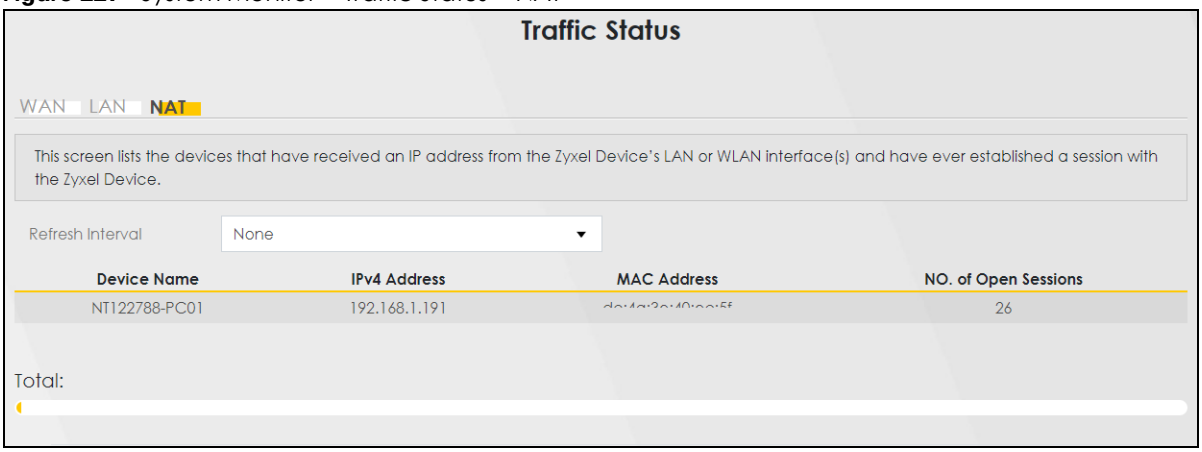
Table 145 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Interface	This shows the LAN or 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)	
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.

26.4 NAT Status

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

Figure 227 System Monitor > Traffic Status > NAT



The following table describes the fields in this screen.

Table 146 System Monitor > Traffic Status > NAT

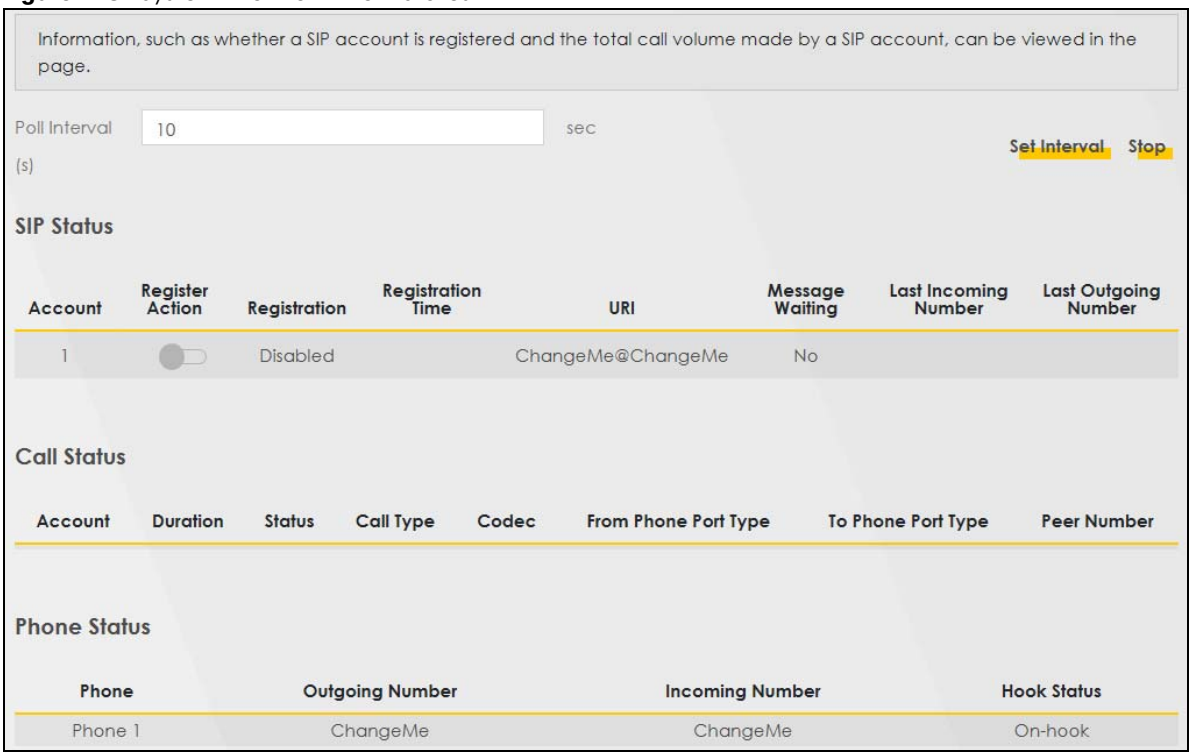
LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Device Name	This displays the name of the connected host.
IPv4 Address	This displays the IP address of the connected host.
MAC Address	This displays the MAC address of the connected host.
No. of Open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

CHAPTER 27
VoIP Status

27.1 VoIP Status Screen

Click **System Monitor** > **VoIP Status** to open the following screen. You can view the Voice over IP (VoIP) registration, current call status and phone numbers in this screen.

Figure 228 System Monitor > VoIP Status



The following table describes the labels in this screen.

Table 147 System Monitor > VoIP Status

LABEL	DESCRIPTION
Poll Interval	Enter the number of seconds the Device needs to wait before updating this screen and then click **Set Interval**. Click **Stop** to have the Device stop updating this screen.
SIP Status	
Account	This column displays each SIP account in the Device.
Register Action	Click on this switch to register/unregister the SIP account. This switch will turn blue if a registration attempt is successful; otherwise, it will revert to its unregistered setting. Unregistering an account does not delete the SIP account itself, but removes the mapping between your SIP identity and your IP address or domain name,
Registration Time	This field displays the last time the Device successfully registered the SIP account. The field is blank if the Device has never successfully registered this account.

Table 147 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
URI	This field displays the account number and service domain of the SIP account. You can change these in the **VoIP** > **SIP** screen.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the Device.
Duration	This field displays how long the current call has lasted.
Status	This field displays the current state of the phone call. **Idle** – There are no current VoIP calls, incoming calls or outgoing calls being made. **Dial** – The callee's phone is ringing. **Ring** – The phone is ringing for an incoming VoIP call. **Process** – There is a VoIP call in progress. **DISC** – The callee's line is busy, the callee hung up or your phone was left off the hook.
Call Type	This field displays the call direction type of the current VoIP call. Outgoing Call – It is a SIP VoIP call made by local phone ports, and this SIP account is able to issue a (SIP-based) call setup to the SIP account of remote peers for a VoIP call establishment. This (SIP-based) call setup signal is sent to the SIP server first, and then the SIP server would relay it to the target peer after correctly resolving and locating the target peer. During the call setup (signaling) phase, Calling state is displayed in the Status field, and it turns to InCall state once the call is successfully established. Incoming Call – It is a SIP VoIP call made or originated by remote SIP accounts to connect to this local SIP account. One or more local phone ports can be configured to receive this type of call, see the Incoming Number below, and all of them should begin to ring during the call setup (signaling phase), see the Status above. Once some remote SIP accounts start to ring one local phone, answer by off-hook to the call, and the call is successfully established. The other ringing local phone ports will stop ringing and turning to InCall state in the Status field. Internal Call – It is a local VoIP call between two different local phone ports. No SIP signaling is needed and thus no SIP server is involved to establish this type of call. This type of call is established through the Internal and Non-SIP local setup signaling procedure between the call- originating and call-terminating local phone ports. In general, one or more local phone ports can be designed to receive this type of call, and once any of the ringing phones answer the call, the other ringing ones will stop ringing. During the call setup phase (signaling phase), Calling state is displayed in Status field, and turns to InCall state once the call is successfully established.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
From Phone Port Type	This field displays the phone ports type used to originate, start, or create the current VoIP call. Type Two possible type values will be displayed here: SIP – For the current call which is categorized as Incoming Call in the Call Type filed, this field will show the type SIP. FXS – As for the other cases: Outgoing Call and Internal Call, this field will show the corresponding local phone port type: FXS, the legacy analog phone port on the device.

Table 147 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
To Phone Port Type	This field displays the phone ports type used to receive the current VoIP call. Three possible type Type values will be displayed here: SIP – For the current call which is categorized as Outgoing Call in the Call Type field, this field will show the type SIP. FXS and Unknown – As for the other cases: Incoming Call and Internal Call, this field will show the corresponding local phone port type: FXS, the legacy analog phone port on the device. While the call is established, this field shows Unknown during the call setup phase (signaling phase). This is because one or more local phone ports can be configured or designed to receive these two types of calls, see the Call Type above, and the local phone port will answer the call that hasn't been determined yet at that time.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Phone	This field displays the name of a phone port on the Device.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP number that you use to receive calls on this phone port.
Hook Status	This field displays whether the phone is in the on or off hook status. **Off-Hook** means a telephone connected to one of the phone port has its receiver off the hook. **On-Hook** means a telephone connected to one of the phone port has its receiver on the hook.

CHAPTER 28
ARP Table

28.1 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.

28.1.1 How ARP Works

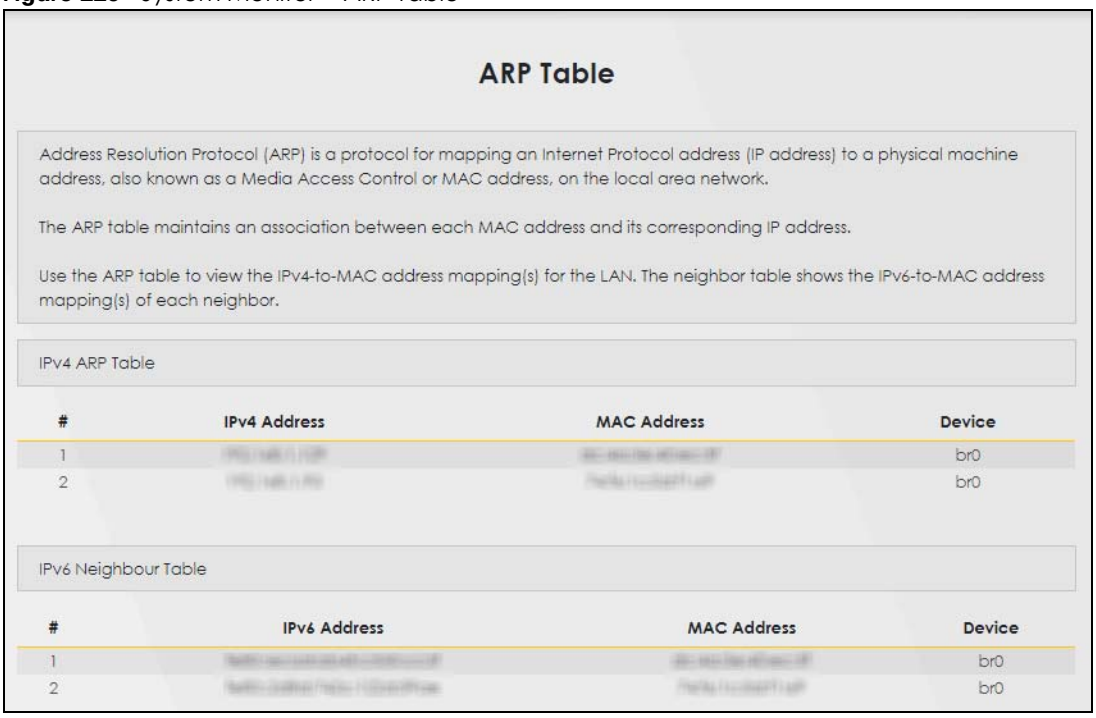
When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP table and, if it finds the address, sends it to the device.

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.

28.2 ARP Table

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 IPv6 neighbor. To open this screen, click **System Monitor** > **ARP Table**.

Figure 229 System Monitor > ARP Table



The following table describes the labels in this screen.

Table 148 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 Zyxel 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 29
Routing Table

29.1 Routing Table Overview

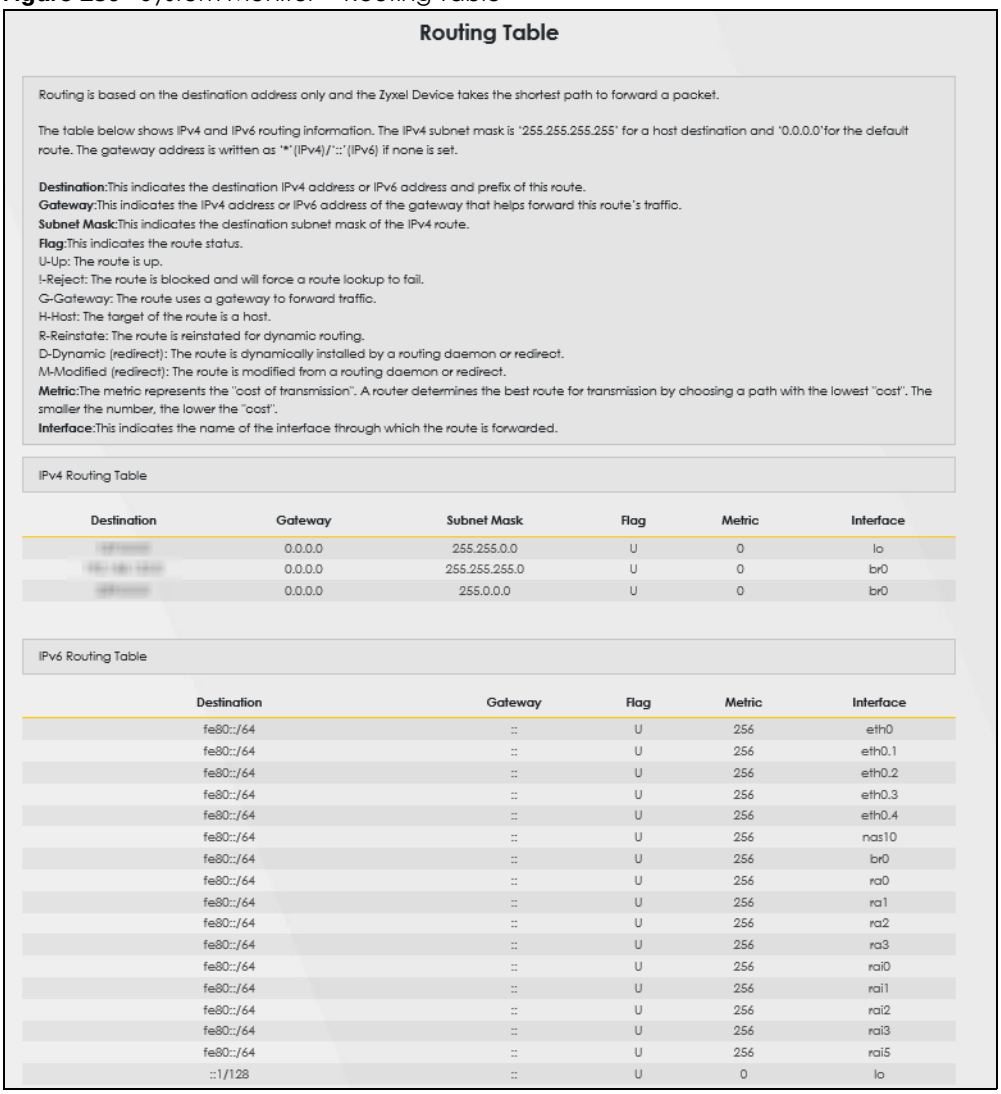
Routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet.

29.2 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 230 System Monitor > Routing Table



Routing Table

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

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

Destination:This indicates the destination IPv4 address or IPv6 address and prefix of this route.
Gateway:This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask:This indicates the destination subnet mask of the IPv4 route.
Flag:This indicates the route status.
U-Up: The route is up.
!-Reject: The route is blocked and will force a route lookup to fail.
G-Gateway: The route uses a gateway to forward traffic.
H-Host: The target of the route is a host.
R-Reinstate: The route is reinstated for dynamic routing.
D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect.
M-Modified (redirect): The route is modified from a routing daemon or redirect.
Metric:The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".
Interface:This indicates the name of the interface through which the route is forwarded.

IPv4 Routing Table

Destination	Gateway	Subnet Mask	Flag	Metric	Interface
[redacted]	0.0.0.0	255.255.0.0	U	0	lo
[redacted]	0.0.0.0	255.255.255.0	U	0	br0
[redacted]	0.0.0.0	255.0.0.0	U	0	br0

IPv6 Routing Table

Destination	Gateway	Flag	Metric	Interface
fe80::/64	::	U	256	eth0
fe80::/64	::	U	256	eth0.1
fe80::/64	::	U	256	eth0.2
fe80::/64	::	U	256	eth0.3
fe80::/64	::	U	256	eth0.4
fe80::/64	::	U	256	nas10
fe80::/64	::	U	256	br0
fe80::/64	::	U	256	ra0
fe80::/64	::	U	256	ra1
fe80::/64	::	U	256	ra2
fe80::/64	::	U	256	ra3
fe80::/64	::	U	256	rai0
fe80::/64	::	U	256	rai1
fe80::/64	::	U	256	rai2
fe80::/64	::	U	256	rai3
fe80::/64	::	U	256	rai5
::1/128	::	U	0	lo

The following table describes the labels in this screen.

Table 149 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 149 System Monitor > Routing Table (continued)

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

CHAPTER 30
Multicast Status

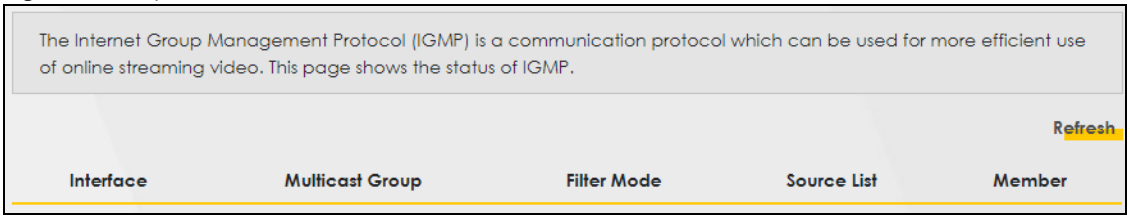
30.1 Multicast Status Overview

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

30.2 The IGMP Status Screen

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

Figure 231 System Monitor > Multicast Status > IGMP Status



The following table describes the labels in this screen.

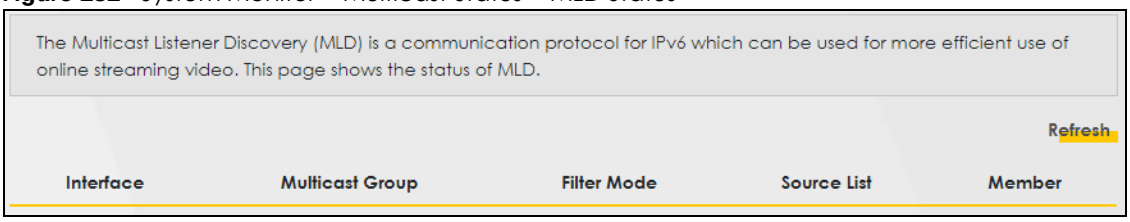
Table 150 System Monitor > Multicast Status > IGMP Status

LABEL	DESCRIPTION
Refresh	Click this button to update the information on this screen.
Interface	This field displays the name of an interface on the Zyxel 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.

30.3 The MLD Status Screen

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

Figure 232 System Monitor > Multicast Status > MLD Status



The following table describes the labels in this screen.

Table 151 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 Zyxel 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 31
WLAN Station Status

31.1 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 Zyxel 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 233 System Monitor > WLAN Station Status (For 2.4G and 5G models)

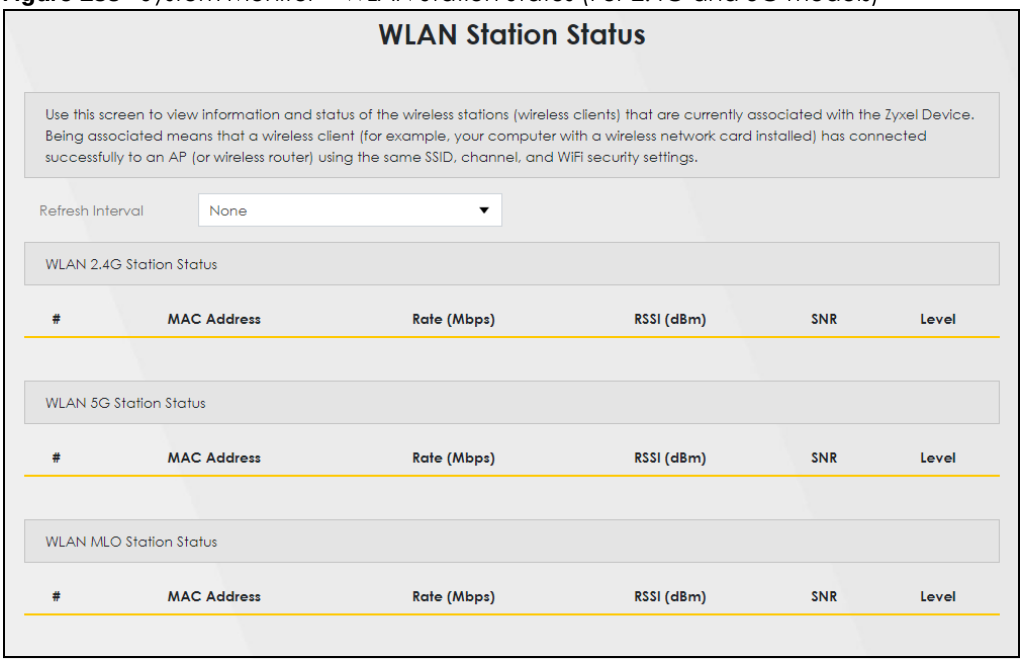
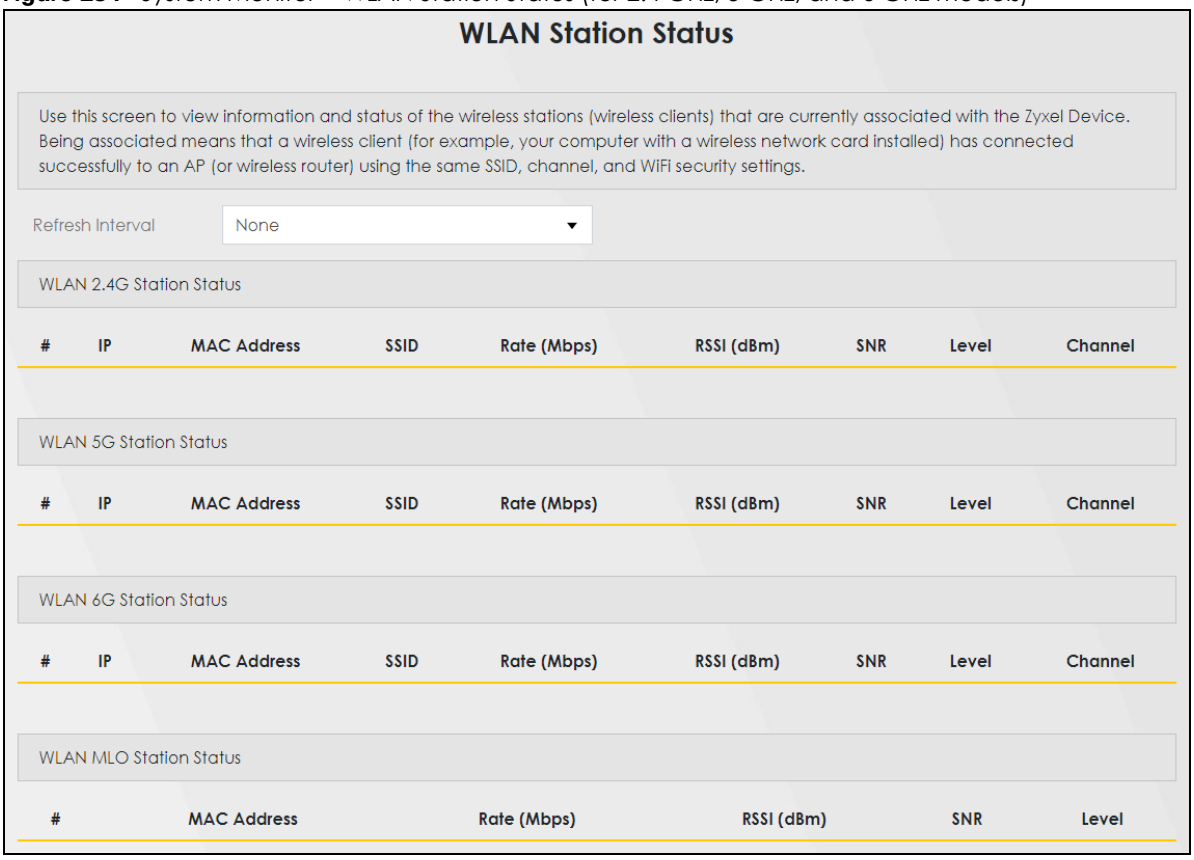


Figure 234 System Monitor > WLAN Station Status (for 2.4 GHz, 5 GHz, and 6 GHz models)



The following table describes the labels in this screen.

Table 152 System Monitor > WLAN Station Status

LABEL	DESCRIPTION
#	This is the index number of an associated WiFi station.
IP	This field displays the IP address of an associated WiFi station.
MAC Address	This field displays the MAC address of an associated WiFi station.
SSID	This field displays the SSID (Service Set IDentifier) this WiFi station is associated with.
Rate (Mbps)	This field displays the transmission rate of WiFi traffic between an associated WiFi station and the Zyxel Device.
RSSI (dBm)	The RSSI (Received Signal Strength Indicator) field shows the WiFi signal strength of the station's WiFi connection. The normal range is –30dBm to –79dBm. If the value drops below –80dBm, try moving the associated WiFi station closer to the Zyxel 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 greater the number, the better the quality of WiFi. The normal range is 15 to 40. If the value drops below 15, try moving the associated WiFi station closer to the Zyxel Device to get better quality WiFi.

Table 152 System Monitor > WLAN Station Status (continued)

LABEL	DESCRIPTION
Level	This field displays a number which represents the strength of the WiFi signal between an associated WiFi station and the Zyxel Device. The Zyxel Device uses the RSSI and SNR values to determine the strength of the WiFi signal. **5** means the Zyxel Device is receiving an excellent WiFi signal. **4** means the Zyxel Device is receiving a very good WiFi signal. **3** means the Zyxel Device is receiving a weak WiFi signal, **2** means the Zyxel Device is receiving a very weak WiFi signal. **1** means the Zyxel Device is not receiving a WiFi signal.
Channel	This field displays the wireless channel bandwidth of an associated WiFi station.

CHAPTER 32
Cellular Statistics

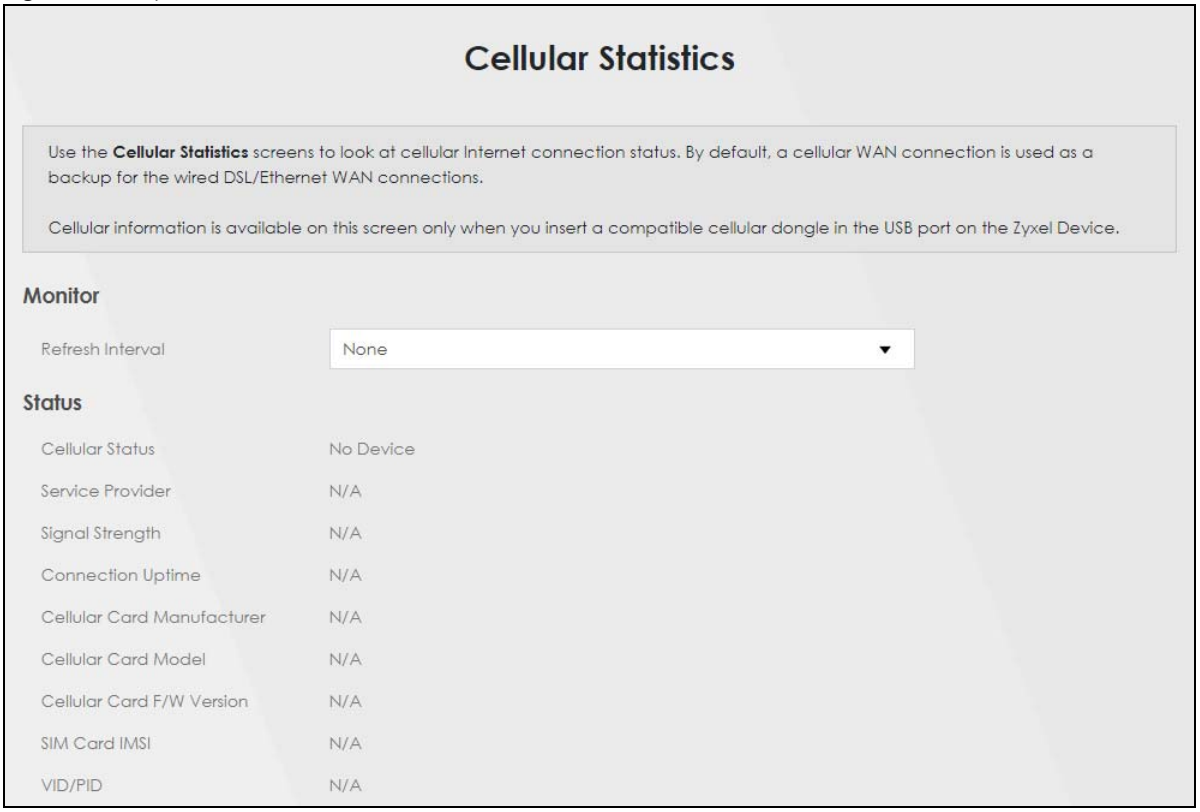
32.1 Cellular Statistics Overview

Use the **Cellular Statistics** screens to look at cellular Internet connection status. By default, a cellular WAN connection is used as a backup for the wired DSL or Ethernet WAN connections.

32.2 Cellular Statistics Settings

To open this screen, click **System Monitor** > **Cellular Statistics**. Cellular information is available on this screen only when you insert a compatible cellular dongle in the USB port on the Zyxel Device.

Figure 235 System Monitor > Cellular Statistics



The following table describes the labels in this screen.

Table 153 System Monitor > Cellular Statistics

LABEL	DESCRIPTION
Monitor	
Refresh Interval	Select how often you want the Zyxel Device to update this screen. Select **None** to stop refreshing.
Status	
Cellular Status	This field displays the status of the cellular Internet connection. This field can display: **GSM** – Global System for Mobile Communications, 2G **GPRS** – General Packet Radio Service, 2.5G **EDGE** – Enhanced Data rates for GSM Evolution, 2.75G **WCDMA** – Wideband Code Division Multiple Access, 3G **HSDPA** – High-Speed Downlink Packet Access, 3.5G **HSUPA** – High-Speed Uplink Packet Access, 3.75G **HSPA** – HSDPA+HSUPA, 3.75G
Service Provider	This field displays the name of the service provider.
Signal Strength	This field displays the strength of the signal in dBm.
Connection Uptime	This field displays the time the connection has been up.
Cellular Card Manufacturer	This field displays the manufacturer of the cellular card.
Cellular Card Model	This field displays the model name of the cellular card.
Cellular Card F/W Version	This field displays the firmware version of the cellular card.
SIM Card IMSI	The International Mobile Subscriber Identity or IMSI is a unique identification number associated with all cellular networks. This number is provisioned in the SIM card.
VID/PID	This field displays the USB Vendor ID and Product ID of the cellular card.

CHAPTER 33
Optical Signal Status

33.1 Overview

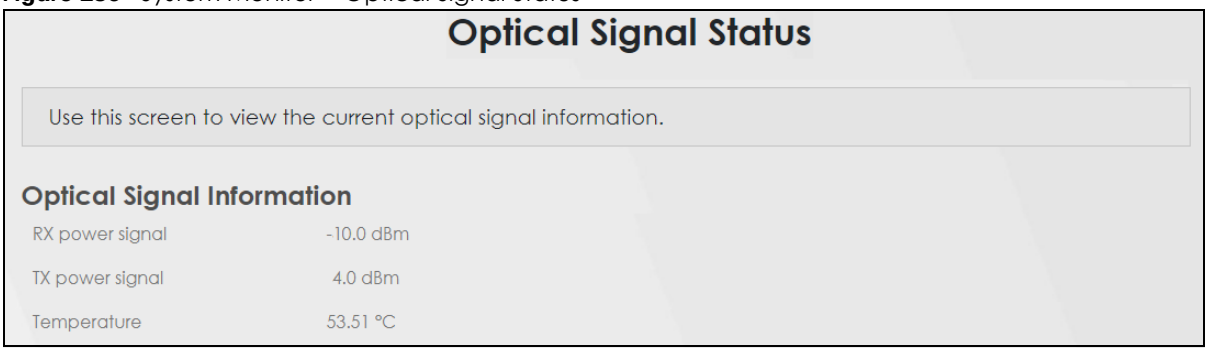
Use this screen to view the PON (Passive Optical Network) transceiver's TX power and RX power level and temperature.

33.2 The Optical Signal Status Screen

Click **System Monitor** > **Optical Signal Status** to open the **Optical Signal Status** screen to see the real-time DDMI (Digital Diagnostics Monitoring Interface) parameters.

The PON transceiver's support for the DDMI function lets you monitor the PON transceiver's parameters to perform component monitoring, fault isolation, and failure prediction tasks. This allows proactive, preventative network maintenance to help ensure service continuity.

Figure 236 System Monitor > Optical Signal Status



The following table describes the labels in this screen.

Table 154 System Monitor > Optical Signal Status

LABEL	DESCRIPTION
Optical Signal Information	
RX power signal	This displays the PON transceiver's receiving power in dBm. The normal range is –9 to –28 dBm. The lower the value, the stronger the signal as there is less background noise. For example, –28 dBm is a stronger signal than –9 dBm.
TX power signal	This displays the PON transceiver's transmitting power in dBm. The normal range is 4 to 9 dBm.
Temperature	This displays the PON transceiver's temperature in degrees Celsius. The normal range is 0 to 85 degrees Celsius (185 degrees Fahrenheit).

Note: Make sure the fiber optic cable is well connected to the PON port.

Note: If the TX and RX power signals of the DDMI are out of range, inspect the fiber optic cable for dirt, any fiber optic cable bends or excessive curves. If the fiber optic cable is clean and undamaged, use the power meter to measure whether the actual RX power signal of the Zyxel Device falls within the range of –9.0 to –28 dBm.

CHAPTER 34
System

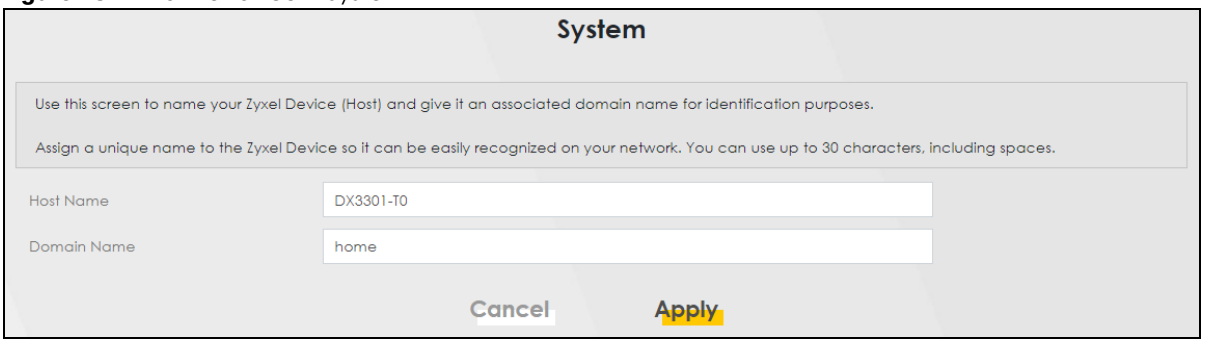
34.1 System Overview

Use this screen to name your Zyxel Device (Host) and give it an associated domain name for identification purposes.

34.2 System

Click **Maintenance** > **System** to open the following screen. Assign a unique name to the Zyxel Device so it can be easily recognized on your network. You can use up to 30 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.

Figure 237 Maintenance > System



The following table describes the labels in this screen.

Table 155 Maintenance > System

LABEL	DESCRIPTION
Host Name	Enter a descriptive host name for your Zyxel Device. You can use up to 30 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. For some models, the supported maximum input length is 16 alphanumeric characters.
Domain Name	Enter a domain name for your host Zyxel Device. You can use up to 30 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Cancel	Click **Cancel** to abandon this screen without saving.
Apply	Click **Apply** to save your changes.

CHAPTER 35
User Account

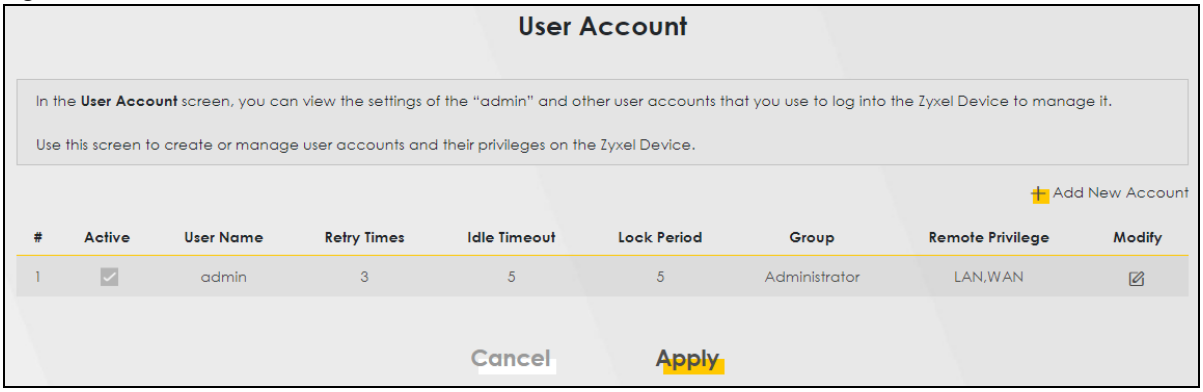
35.1 User Account Overview

In the **User Account** screen, you can view the settings of the "admin" that you use to log into the Zyxel Device to manage it.

35.2 User Account

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

Figure 238 Maintenance > User Account



The following table describes the labels in this screen.

Table 156 Maintenance > User Account

LABEL	DESCRIPTION
#	This is the index number.
Active	This indicates whether the user account is active or not. The checkbox is selected when the user account is enabled. It is cleared when it is disabled.
User Name	This displays the name of the account used to log into the Zyxel Device Web Configurator.
Retry Times	This displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	This displays the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	This field displays the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	This field displays this user has **Administrator** privileges.

Table 156 Maintenance > User Account (continued)

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

35.2.1 User Account Add or Edit

Add or change the name of the user account, set the security password and the retry times, and whether this user will have **Administrator** or **User** privileges. Click **Add New Account** or the **Edit** icon of an existing account in the **Maintenance** > **User Account** to open the following screen.

Figure 239 Maintenance > User Account: Add

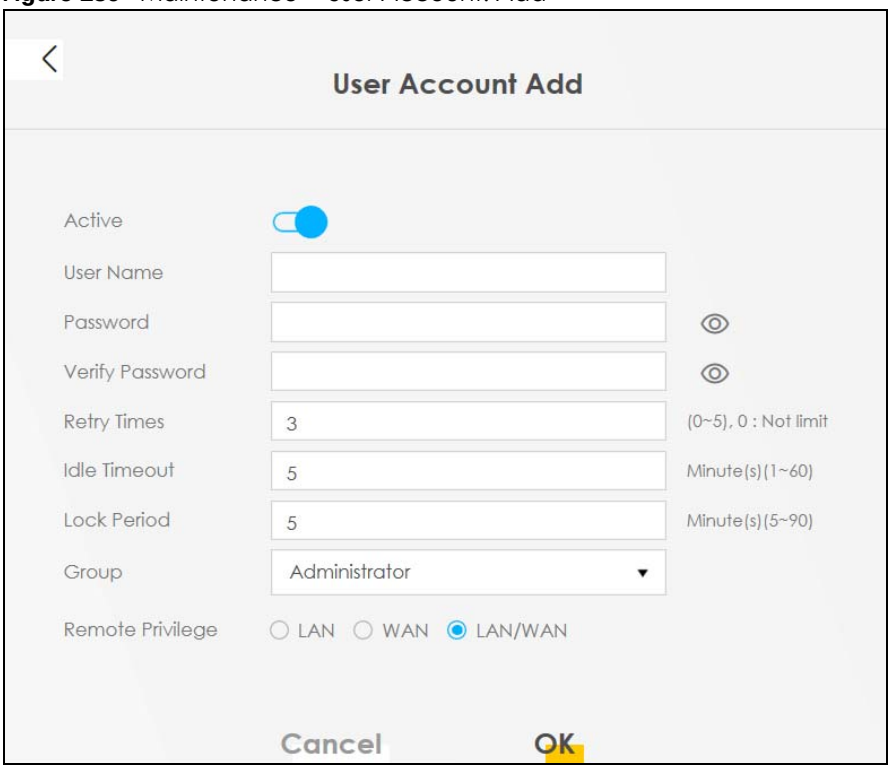
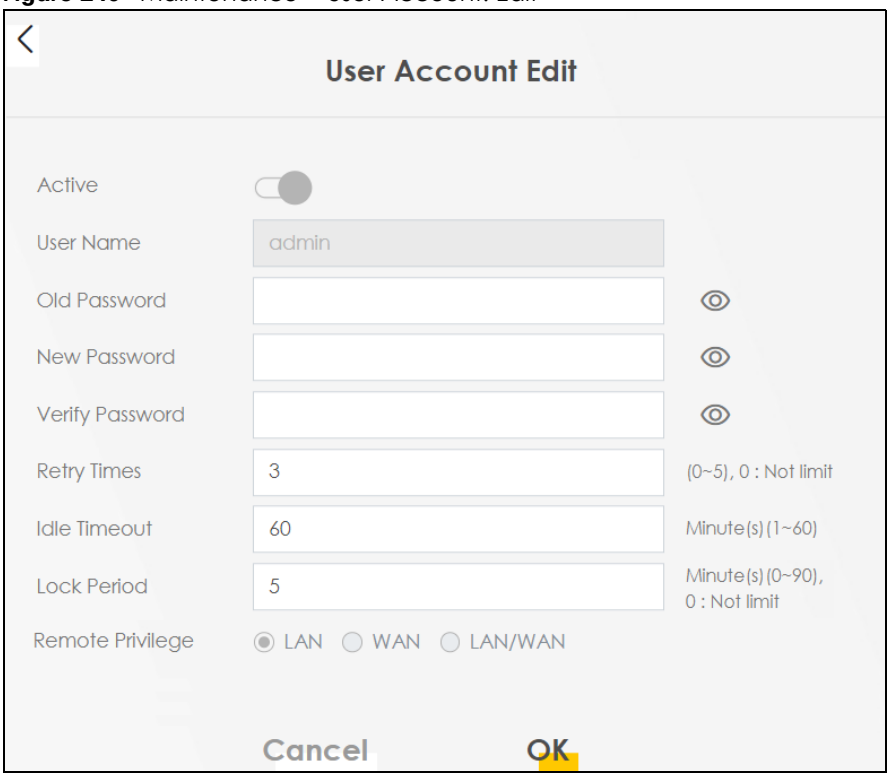


Figure 240 Maintenance > User Account: Edit



The following table describes the labels in this screen.

Table 157 Maintenance > User Account > User Account Add/Edit

LABEL	DESCRIPTION
Active	Click to enable (switch turns blue) or disable (switch turns gray) to activate or deactivate the user account.
User Name	Enter a name for this account. You can use up to 31 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Verify Password	Enter the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	Enter the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in **Retry Times**.
Cancel	Click **Cancel** to restore your previously saved settings.
OK	Click **OK** to save your changes.

CHAPTER 36
Remote Management

36.1 Remote Management Overview

Remote management controls through which interfaces, which web services (such as HTTPS, SSH, SNMP, and Ping) can access the Zyxel Device.

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

36.1.1 What You Can Do in this Chapter

- Use the **MGMT Services** screen to allow various approaches to access the Zyxel Device remotely from a WAN and/or LAN connection (Section 36.2 on page 390).
- Use the **Trust Domain** screen to enable users to permit access from local management services by entering specific IP addresses (Section 36.3 on page 392).

36.2 MGMT Services

Use this screen to configure the interfaces through which services can access the Zyxel Device. You can also specify service port numbers computers must use to connect to the Zyxel Device. Click **Maintenance** > **Remote Management** > **MGMT Services** to open the following screen.

Figure 241 Maintenance > Remote Management > MGMT Services

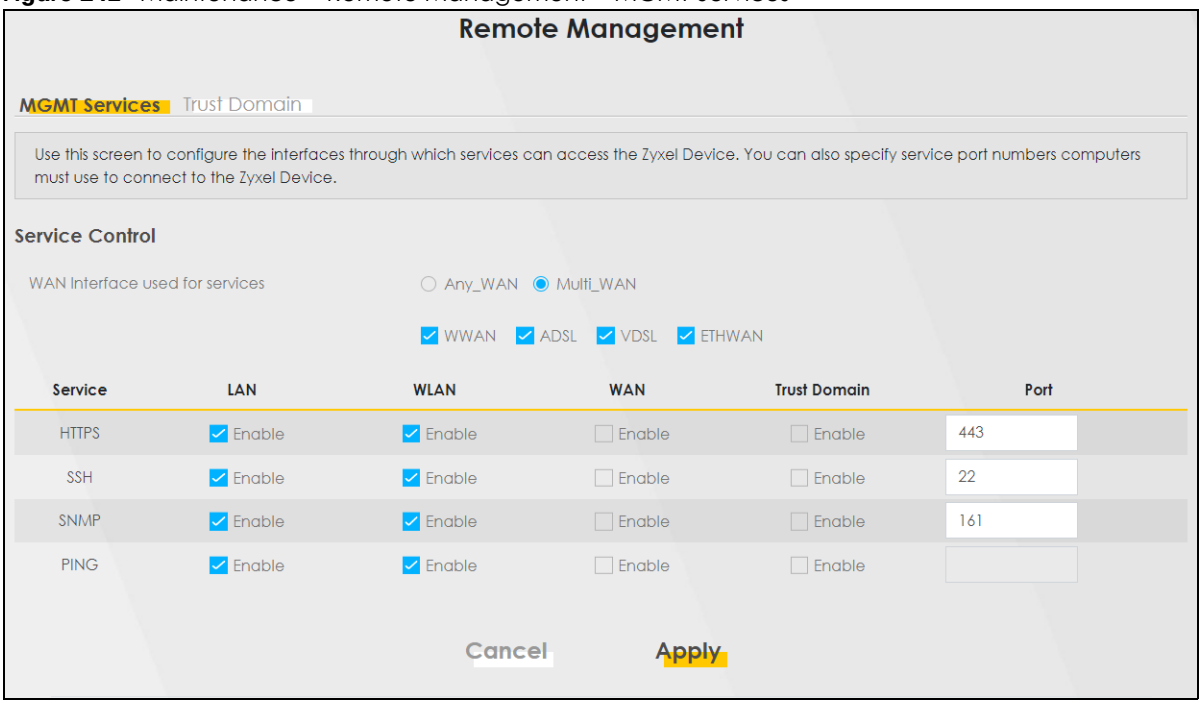
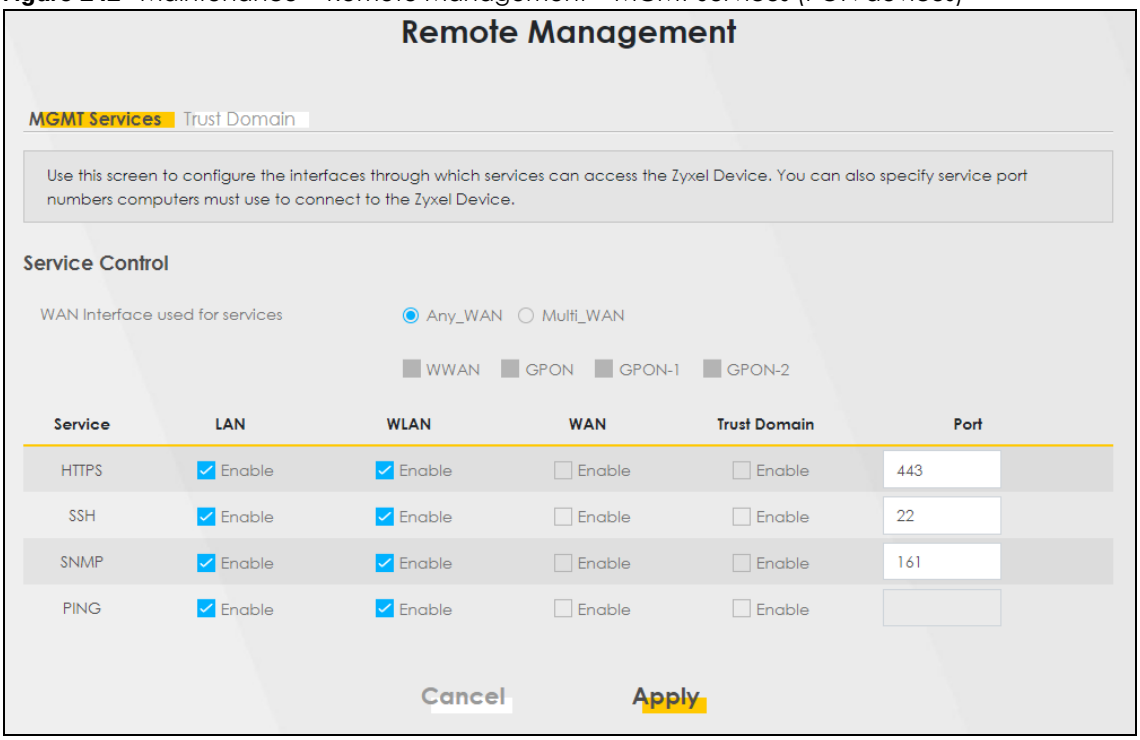


Figure 242 Maintenance > Remote Management > MGMT Services (PON devices)



The following table describes the fields in this screen.

Table 158 Maintenance > Remote Management > MGMT Services

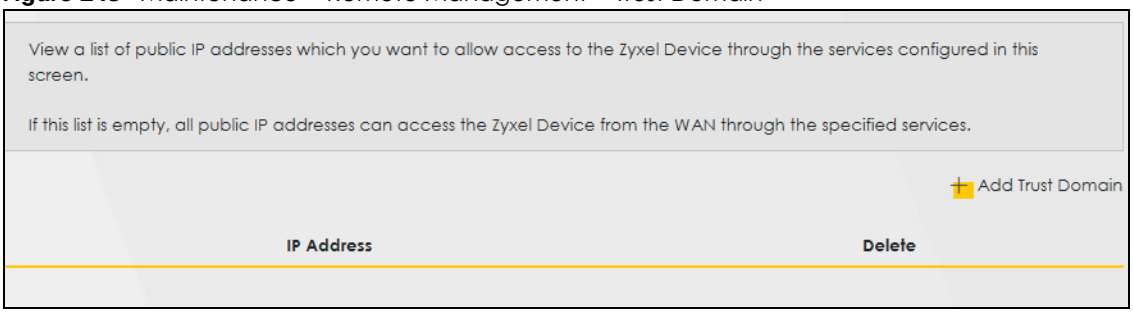
LABEL	DESCRIPTION
Service Control	
WAN Interface used for services	Select **Any_WAN** to have the Zyxel Device automatically activate the remote management service when any WAN connection is up. Select **Multi_WAN** and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up.
WWAN	Enable the WWAN (cellular) connection configured in **Network Setting** > **Broadband** > **Cellular Backup** to access the service on the Zyxel Device.
GPON	Enable the Gigabit Ethernet Passive Optical Network WAN connection configured in **Network Setting** > **Broadband** > **Add New WAN Interface** or **Modify** to access the service on the Zyxel Device.
Service	This is the service you may use to access the Zyxel Device.
LAN	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from the LAN.
WLAN	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from the WLAN.
WAN	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from the trusted host IP address.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Redirect	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server. For example, if you enter http://192.168.1.1 in your browser to access the Web Configurator, then the Zyxel Device will automatically change this to the more secure https://192.168.1.1 for access.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

36.3 Trust Domain

Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance** > **Remote Management** > **MGMT Services** screen. Click **Maintenance** > **Remote Management** > **Trust Domain** to open the following screen.

Note: Enter the IP address of the management station permitted to access the local management services. If specific services from the trusted hosts are allowed access but the trust domain list is empty, all public IP addresses can access the Zyxel Device from the WAN using the specified services.

Figure 243 Maintenance > Remote Management > Trust Domain



The following table describes the fields in this screen.

Table 159 Maintenance > Remote Management > Trust Domain

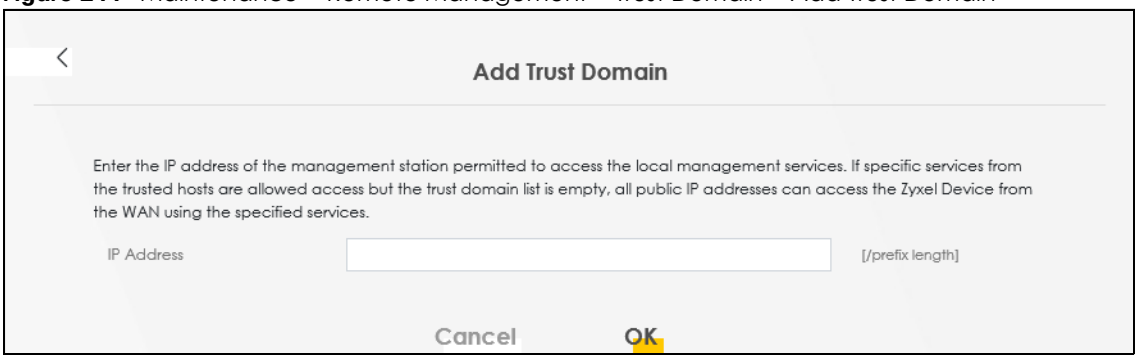
LABEL	DESCRIPTION
Add Trust Domain	Click this to add a trusted host IP address.
IP Address	This field shows a trusted host IP address.
Delete	Click the **Delete** icon to remove the trusted host IP address.

36.3.1 Add Trust Domain

Use this screen to add a public IP addresses or a complete domain name of a device which is allowed to access the Zyxel Device. Enter the IP address of the management station permitted to access the local management services. If specific services from the trusted-hosts are allowed access but the trust domain list is empty, all public IP addresses can access the Zyxel Device from the WAN using the specified services.

Click the **Add Trust Domain** button in the **Maintenance** > **Remote Management** > **Trust Domain** screen to open the following screen.

Figure 244 Maintenance > Remote Management > Trust Domain > Add Trust Domain



The following table describes the fields in this screen.

Table 160 Maintenance > Remote Management > Trust Domain > Add Trust Domain

LABEL	DESCRIPTION
IP Address	Enter a public IPv4/IPv6 IP address which is allowed to access the service on the Zyxel Device from the WAN.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

CHAPTER 37
Power Monitor

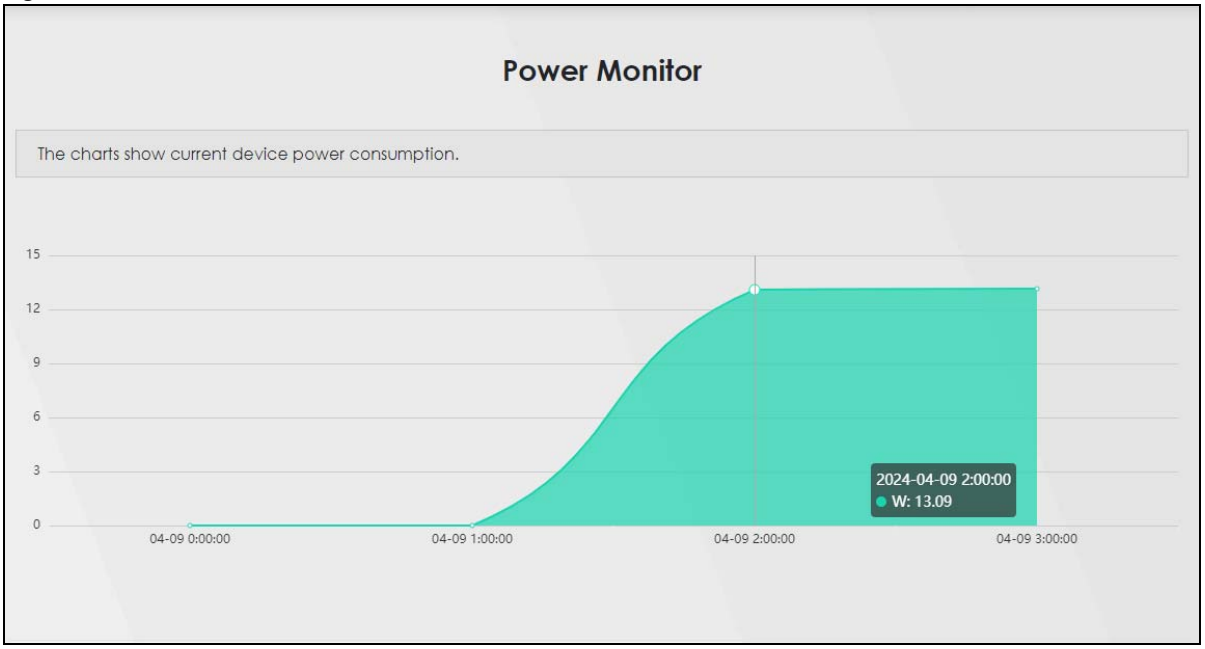
37.1 Power Monitor Overview

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

37.2 Power Monitoring

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

Figure 245 Maintenance > Power Monitor



The following table describes the fields in this screen.

Table 161 Maintenance > Power Monitor

LEGEND	DESCRIPTION
Y-axis	The y-axis shows the amount of power consumed by the Zyxel 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 Zyxel Device or when the Zyxel Device is reset to its factory default setting.

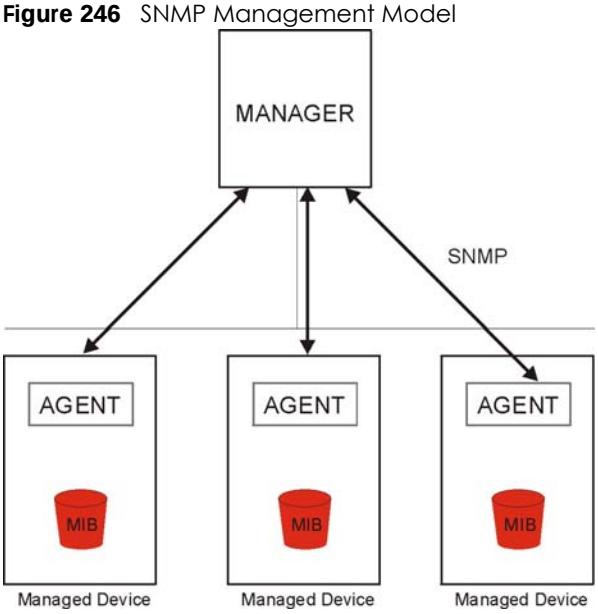
CHAPTER 38
SNMP

38.1 SNMP Overview

This chapter explains how to configure the SNMP settings on the Zyxel Device.

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Zyxel Device supports SNMP agent functionality, which allows a manager station to manage and monitor the Zyxel Device through the network. The Zyxel Device supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 246 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the Zyxel Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables or managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status, and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

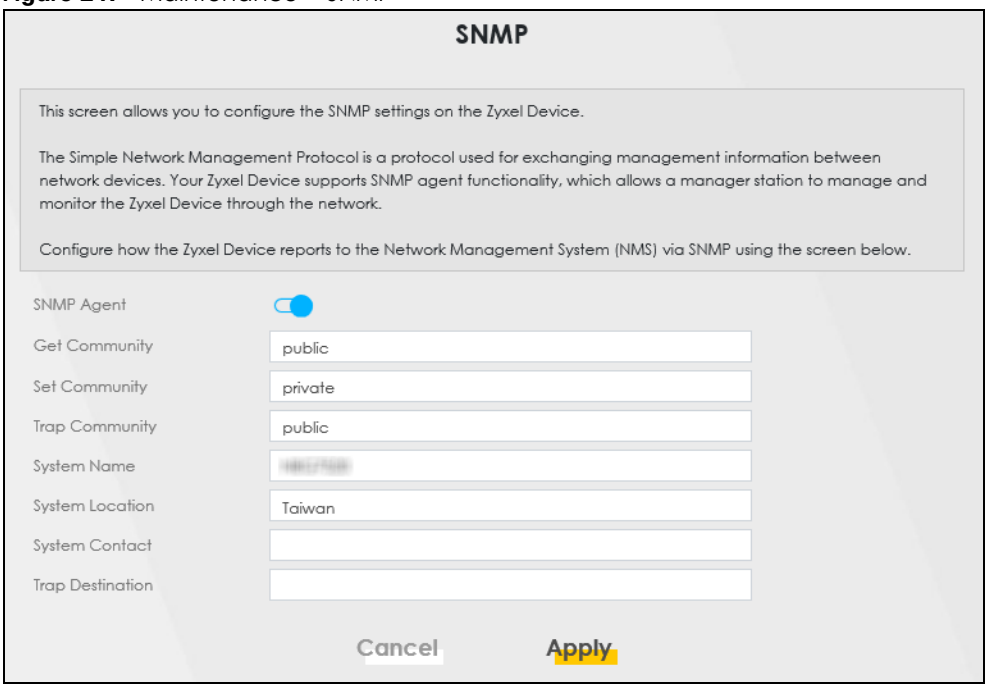
SNMP itself is a simple request/response protocol based on the manager or agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get – Allows the manager to retrieve an object variable from the agent.
- GetNext – Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set – Allows the manager to set values for object variables within an agent.
- Trap – Used by the agent to inform the manager of some events.

38.2 SNMP Settings

Click **Maintenance** > **SNMP** to open the following screen. Use this screen to configure the Zyxel Device SNMP settings.

Figure 247 Maintenance > SNMP



The following table describes the fields in this screen.

Table 162 Maintenance > SNMP

LABEL	DESCRIPTION
SNMP Agent	Click the switch (turns blue) to let the Zyxel Device act as an SNMP agent, which allows a manager station to manage and monitor the Zyxel Device through the network. Otherwise, click the switch (turns gray) to turn this feature off.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station.
Trap Community	Enter the **Trap Community**, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
System Name	Enter the SNMP system name.
System Location	Enter the SNMP system location.

Table 162 Maintenance > SNMP (continued)

LABEL	DESCRIPTION
System Contact	Enter the SNMP system contact.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click this to save your changes back to the Zyxel Device.
Cancel	Click this to restore your previously saved settings.

CHAPTER 39
Time Settings

39.1 Time Settings Overview

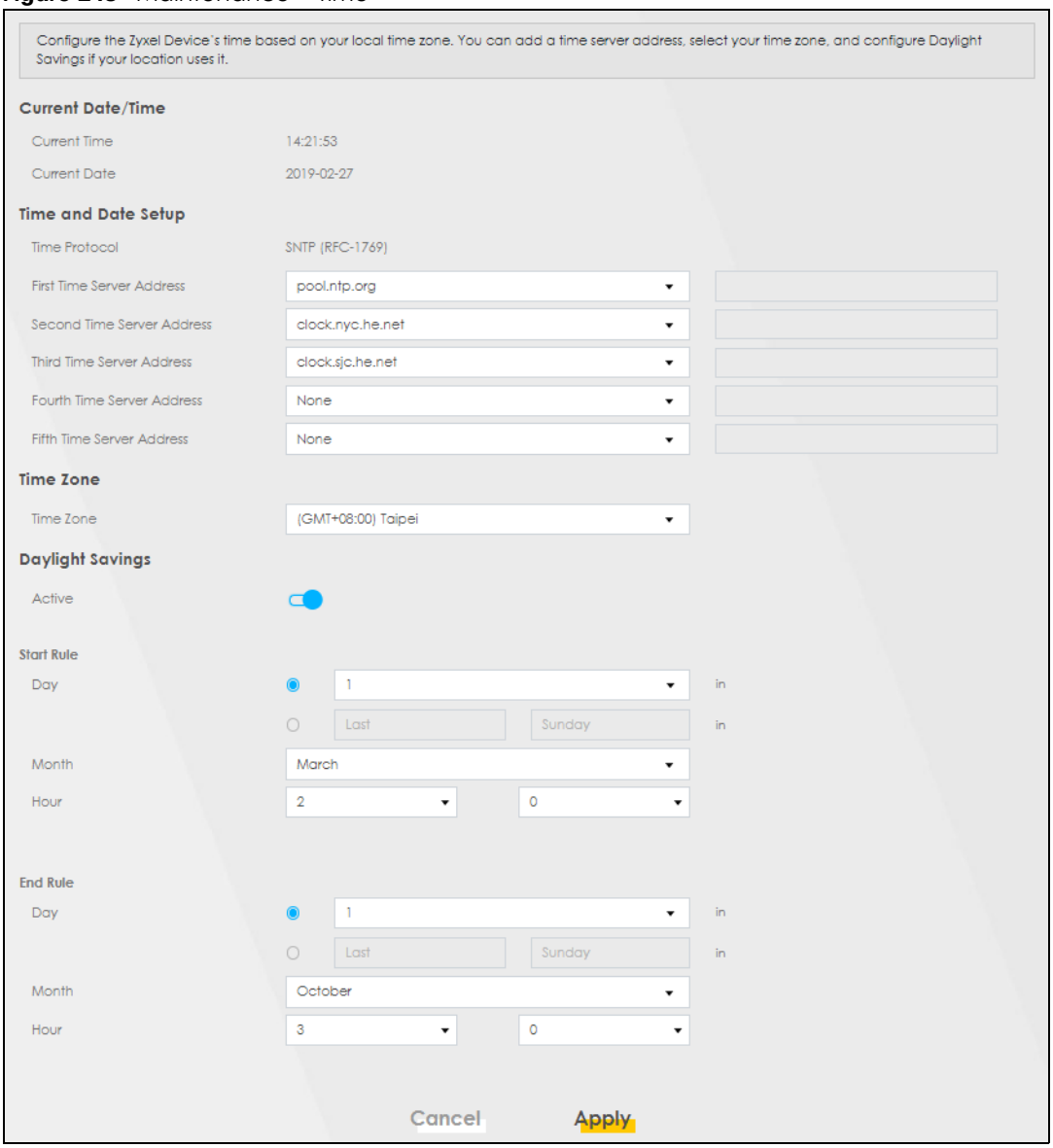
This chapter shows you how to configure system related settings, such as system date and time.

39.2 Time

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

To change your Zyxel Device's time and date, click **Maintenance** > **Time**. The screen appears as shown.

Figure 248 Maintenance > Time



The following table describes the fields in this screen.

Table 163 Maintenance > Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This displays the time of your Zyxel Device. Each time you reload this screen, the Zyxel Device synchronizes the time with the time server.
Current Date	This displays the date of your Zyxel Device. Each time you reload this screen, the Zyxel Device synchronizes the date with the time server.
Time and Date Setup	
Time Protocol	This displays the time protocol used by your Zyxel Device.

Table 163 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 printable 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 turns blue, 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 **Time** 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 **Time** 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 exit this screen without saving.
Apply	Click **Apply** to save your changes.

CHAPTER 40
Email Notification

40.1 Email Notification Overview

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

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

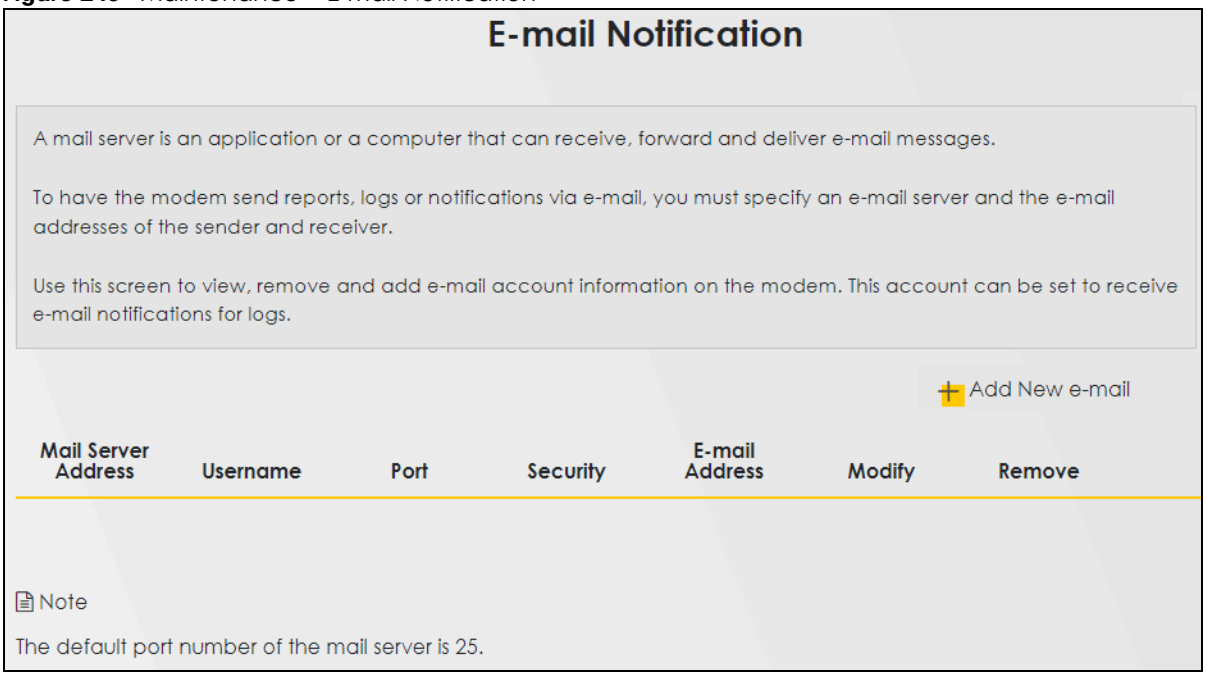
40.2 Email Notification

Use this screen to view, remove and add email account information on the Zyxel 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 249 Maintenance > E-mail Notification



The following table describes the labels in this screen.

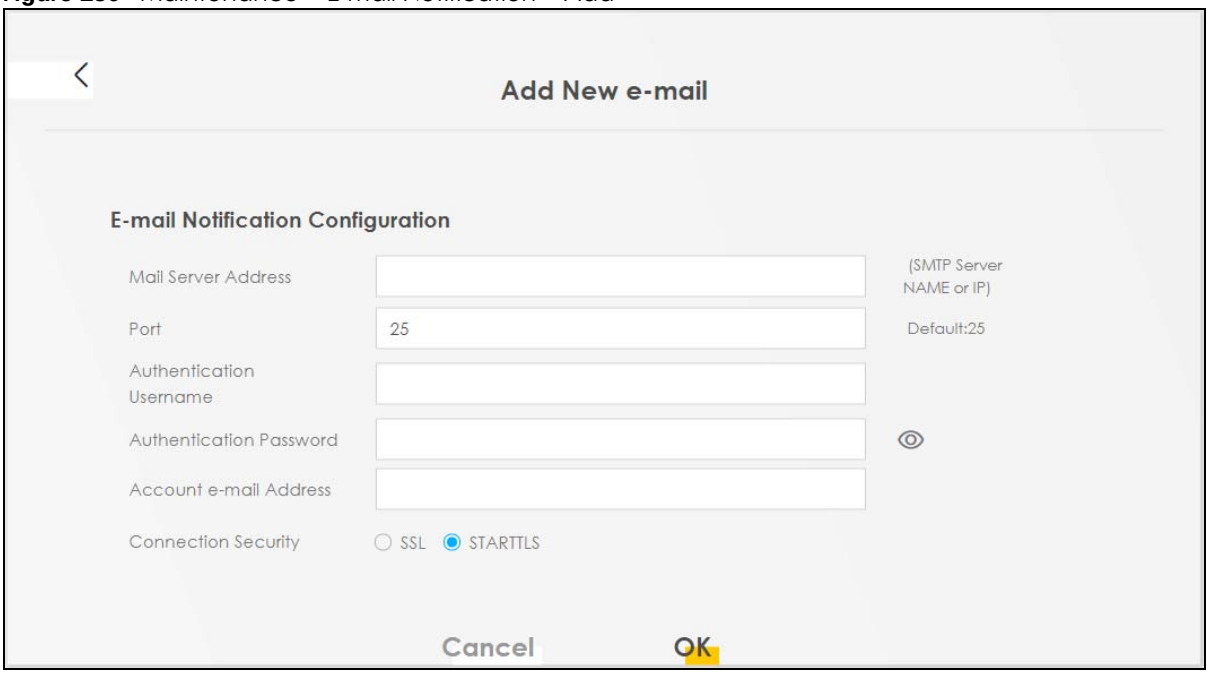
Table 164 Maintenance > E-mail Notification

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.
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 Zyxel 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.

40.2.1 E-mail Notification Edit

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

Figure 250 Maintenance > E-mail Notification > Add



The following table describes the labels in this screen.

Table 165 Maintenance > E-mail Notification > Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the email address specified in the **Account e-mail Address** field. If this field is left blank, reports, logs or notifications will not be sent through email.
Port	Enter the same port number here as is on the mail server for mail traffic.
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 email 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 Zyxel Device sends. If you activate SSL/TLS authentication, the email address must be able to be authenticated by the mail server as well.
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 41
Log Setting

41.1 Log Setting Overview

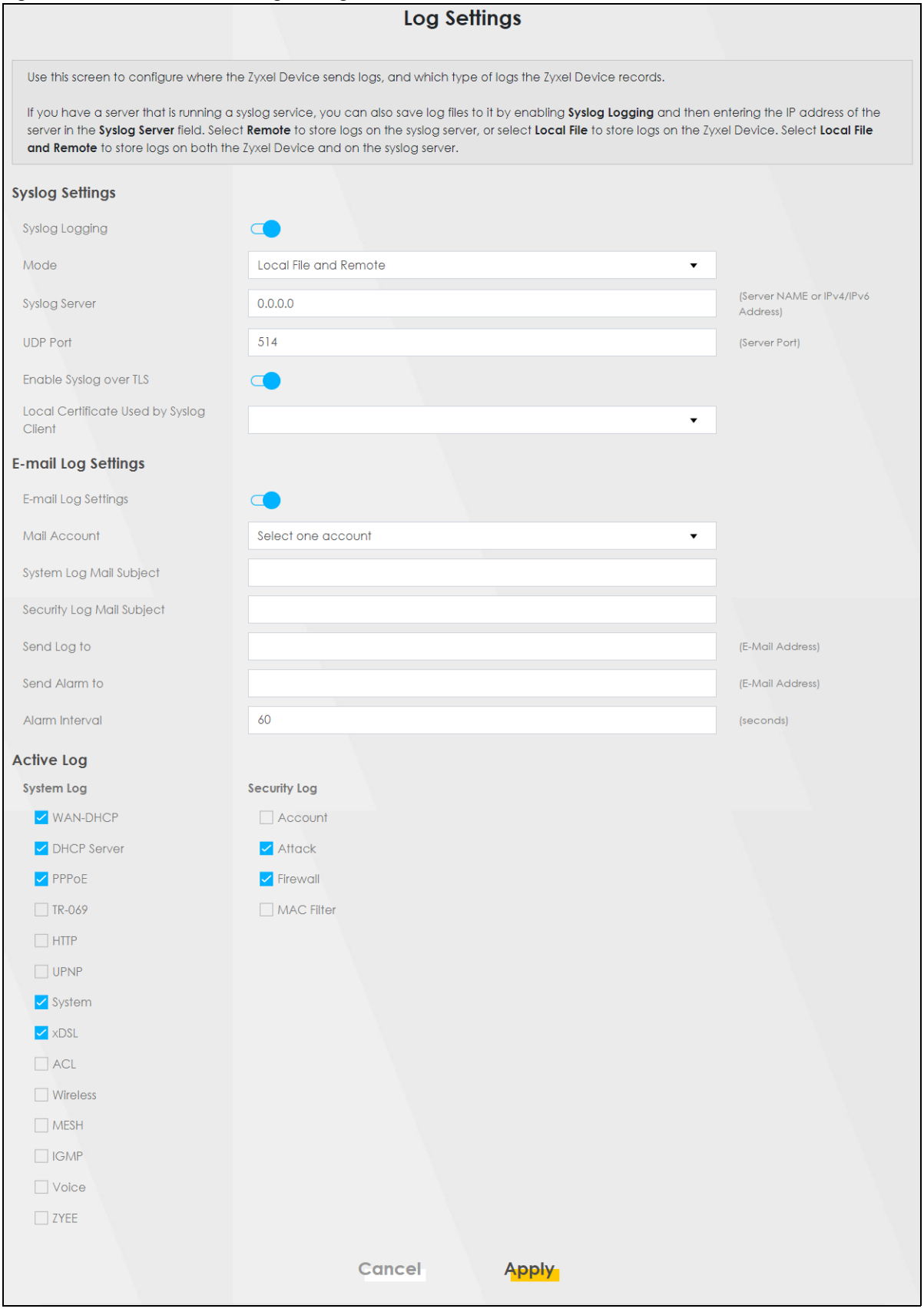
You can configure where the Zyxel Device sends logs and which type of logs the Zyxel Device records in the **Logs Setting** screen.

41.2 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 the syslog server. To change your Zyxel Device's log settings, click **Maintenance** > **Log Setting**. The screen appears as shown.

Figure 251 Maintenance > Log Setting



The following table describes the fields in this screen.

Table 166 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 Zyxel Device send it to an external syslog server. Select **Local File** to have the Zyxel Device save the log file on the Zyxel Device itself. Select **Local File and Remote** to have the Zyxel Device save the log file on the Zyxel 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.
UDP Port	Enter the port number used by the syslog server.
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 Log**s that you want to record.
Security Log	Select the categories of **Security Log**s that you want to record.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

41.2.1 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 252 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 42
Firmware Upgrade

42.1 Firmware Upgrade Overview

This chapter explains how to upload new firmware to your Zyxel Device if you get new firmware releases from your service provider.

42.2 Firmware Upgrade

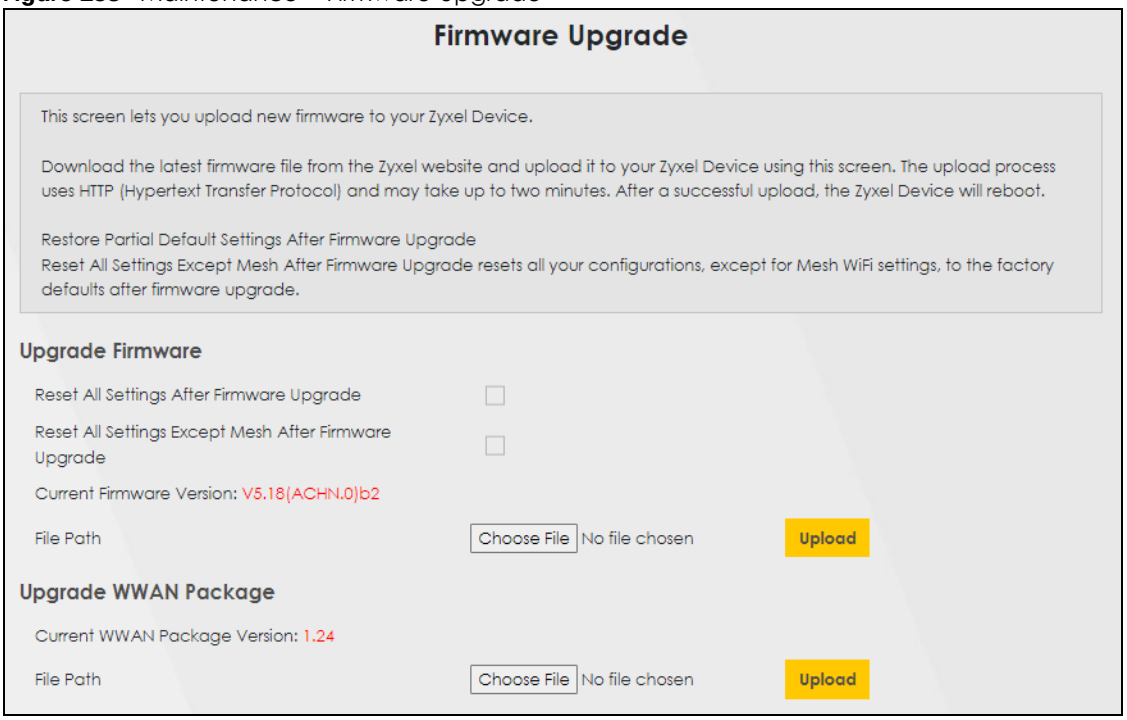
This screen lets you upload new firmware to your Zyxel Device.

Get the latest firmware from your service provider. Then upload the firmware file to your Zyxel Device. The upload process uses HTTP (Hypertext Transfer Protocol). The upload may take up to 3 minutes. After a successful upload, the Zyxel Device will reboot.

Click **Maintenance** > **Firmware Upgrade** to open the **following** screen.

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

Figure 253 Maintenance > Firmware Upgrade



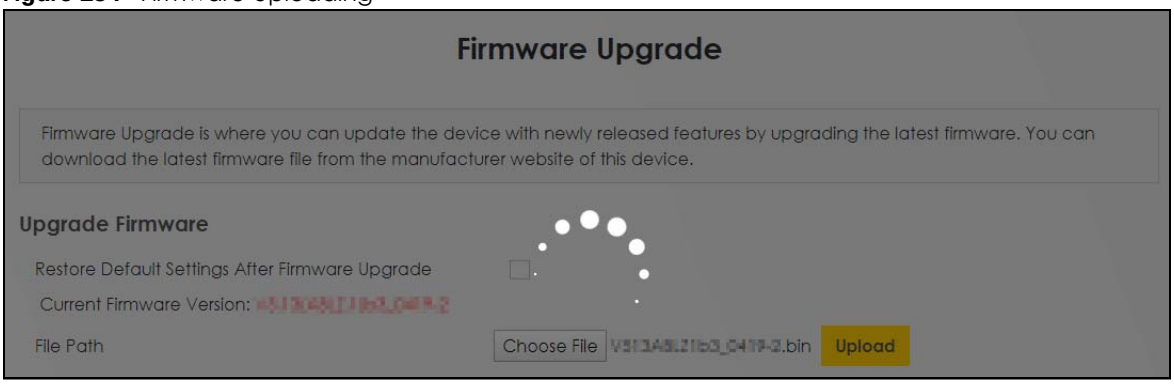
The following table describes the labels in this screen.

Table 167 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Select this to reset all your configurations, including Mesh WiFi settings, to the factory defaults after firmware upgrade. Otherwise, make sure this is cleared if you do not want the Zyxel Device to lose all its current configurations and return to the factory defaults. Note: Make sure to back up the Zyxel Device's configuration settings first in case the reset all settings process is not successful.
Current Firmware Version	This is the current firmware version.
File Path	Enter the location of the file you want to upload in this field or click **Choose File**/**Browse** to find it.
Choose File/ Browse	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 3 minutes. Note: Only use firmware for your Zyxel Device's specific model. Refer to the label on the bottom of your Zyxel Device. For example, if the Zyxel Device's current firmware version is V5.70(ACDZ.0)B4, you must upload the firmware file containing "ACDZ".

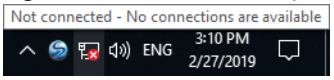
After you see the firmware updating screen, wait a few minutes before logging into the Zyxel Device again.

Figure 254 Firmware Uploading



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

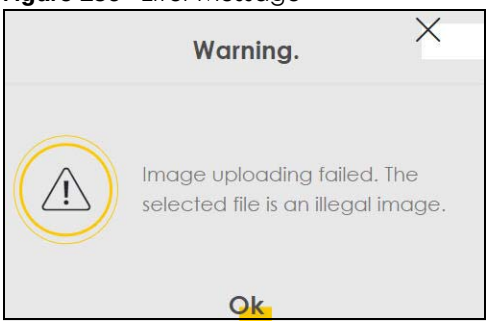
Figure 255 Network Temporarily Disconnected



After 2 minutes, log in again and check your new firmware version in the **Connection Status** screen.

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

Figure 256 Error Message



42.3 Online Upgrade

This screen lets you check for new firmware for your Zyxel Device by checking online for the latest firmware file now or scheduling when the Zyxel Device will check online for the latest firmware file.

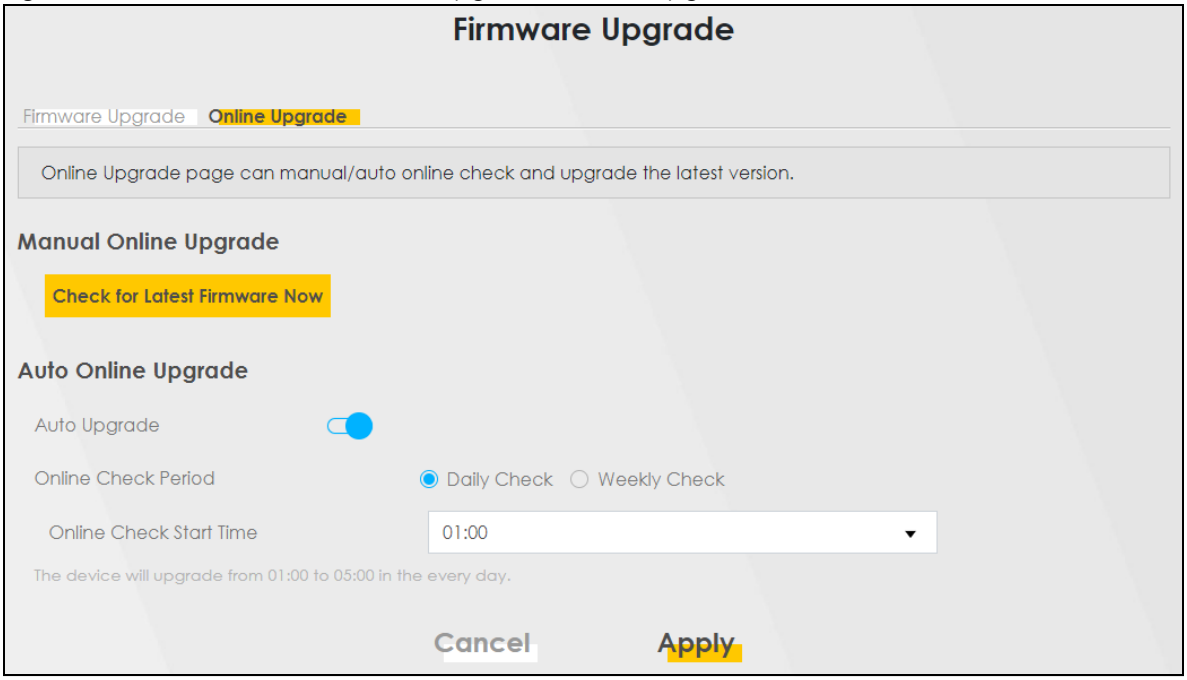
Note: Make sure your Zyxel Device is connected to the Internet.

The upload process uses HTTP (Hypertext Transfer Protocol) and may take more than 3 minutes. After a successful upload, the Zyxel Device will reboot automatically.

Click **Maintenance** > **Firmware Upgrade** > **Online Upgrade** to open the **following** screen.

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

Figure 257 Maintenance > Firmware Upgrade > Online Upgrade



The following table describes the labels in this screen.

Table 168 Maintenance > Firmware Upgrade > Online Upgrade

LABEL	DESCRIPTION
Manual Online Upgrade	
Check for Latest Firmware Now	Click this to have the Zyxel Device check for new firmware immediately. If a newer firmware is available, follow the online prompt to upload the new firmware to your Zyxel Device.
Auto Online Upgrade	
Auto Upgrade	Click the switch to the right to activate automatic firmware upgrade. Note: To minimize disruption to your network, the Zyxel Device will upgrade the firmware from 01:00 to 05:00 by default.
Online Check Period	Select **Daily Check** when you want the Zyxel Device to check online for new firmware everyday. Select **Weekly Check** when you want the Zyxel Device to check online for new firmware once a week.
The day of every week	Select the day that you want the Zyxel Device to check for new firmware. Note: This field only appears when you select **Weekly Check** in **Online Check Period**.
Online Check Start Time	Select the hour of the day that you want the Zyxel Device to check for new firmware.
Cancel	Click **Cancel** to close the window with changes unsaved.
Apply	Click **Apply** to save the changes back to the Zyxel Device.

CHAPTER 43
Backup/Restore

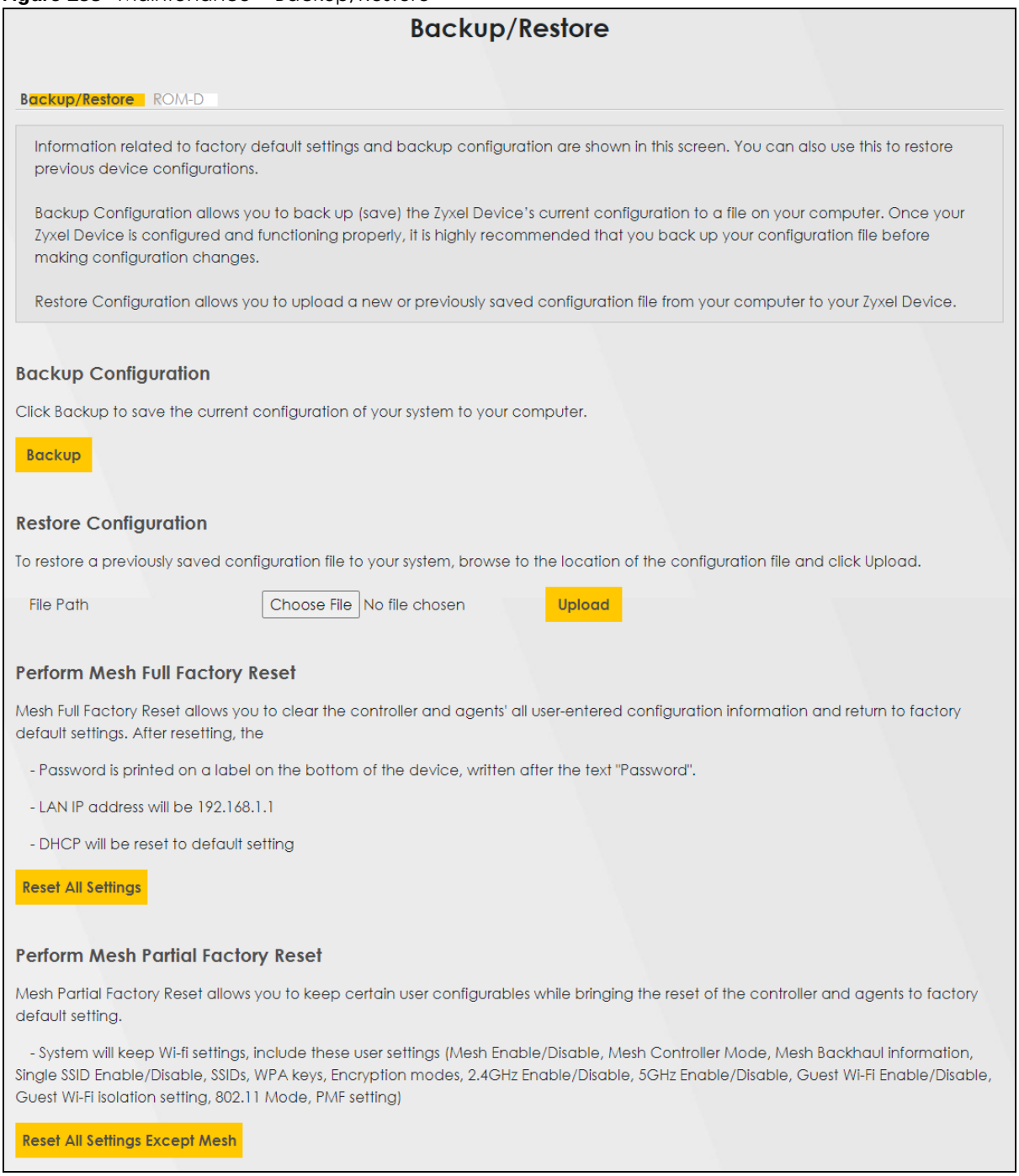
43.1 Backup/Restore Overview

Information related to factory default settings and backup configuration are shown in this screen. You can also use this to restore Zyxel Device's previous configurations.

43.2 Backup/Restore

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

Figure 258 Maintenance > Backup/Restore



Backup Configuration

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

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

Restore Configuration

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

Table 169 Maintenance > Backup/Restore: Restore Configuration

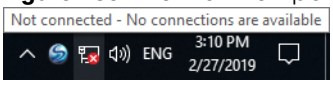
LABEL	DESCRIPTION
File Path	Enter in the location of the file you want to upload in this field or click **Choose File** / **Browse** to find it.
Choose File / Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.
Reset	Click this to reset your settings back to the factory default.

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

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

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

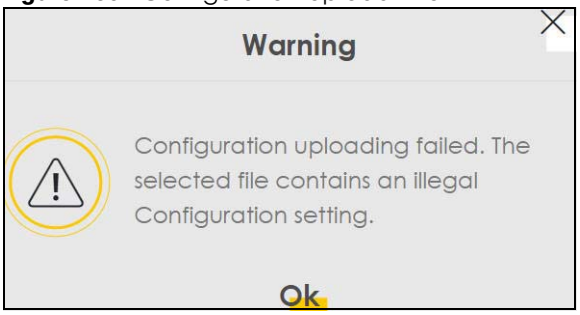
Figure 259 Network Temporarily Disconnected



If you restore the default configuration, you may need to change the IP address of your computer to be in the same subnet as that of the default Zyxel Device IP address (192.168.1.1 – 192.168.225.225).

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Configuration** screen.

Figure 260 Configuration Upload Error

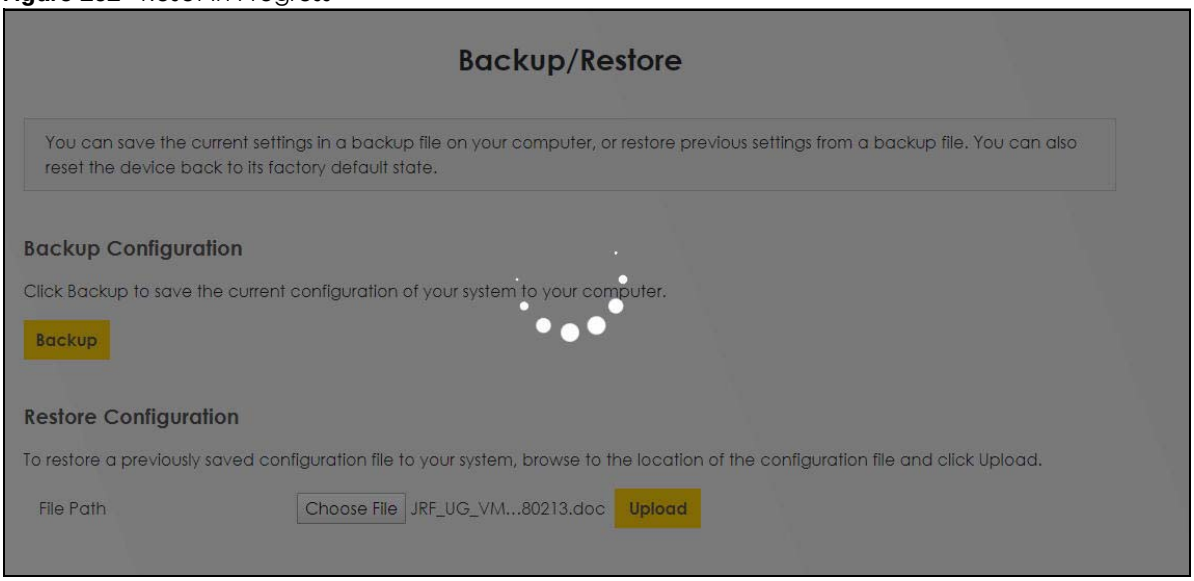


Back to Factory Default Settings

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

Figure 261 Reset Warning Message

Figure 262 Reset In Progress



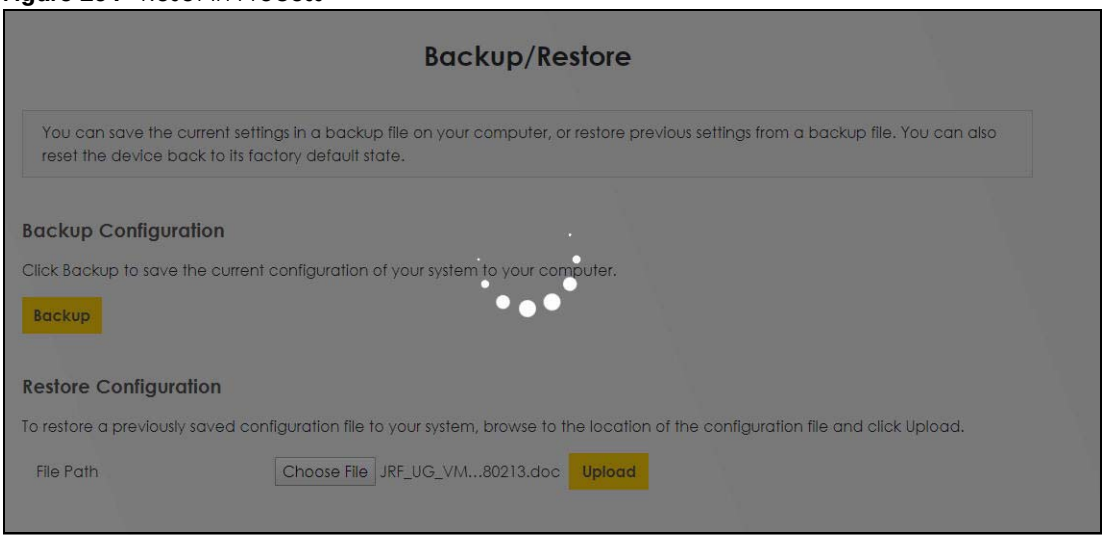
You can also press the **RESET** button on the panel to reset the Zyxel Device to the factory defaults.

Perform Partial Factory Reset

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

Figure 263 Reset Warning Message

Figure 264 Reset In Process

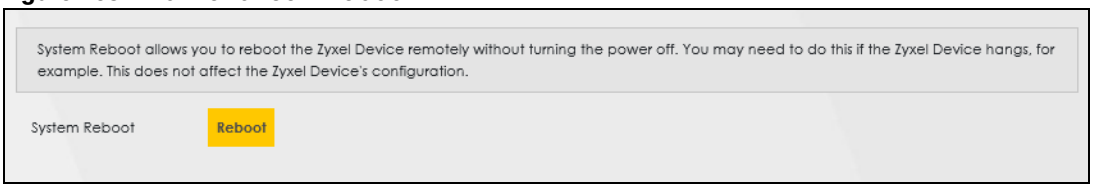


43.3 Reboot

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

Click **Maintenance** > **Reboot**. Click **Reboot** to have the Zyxel Device restart.

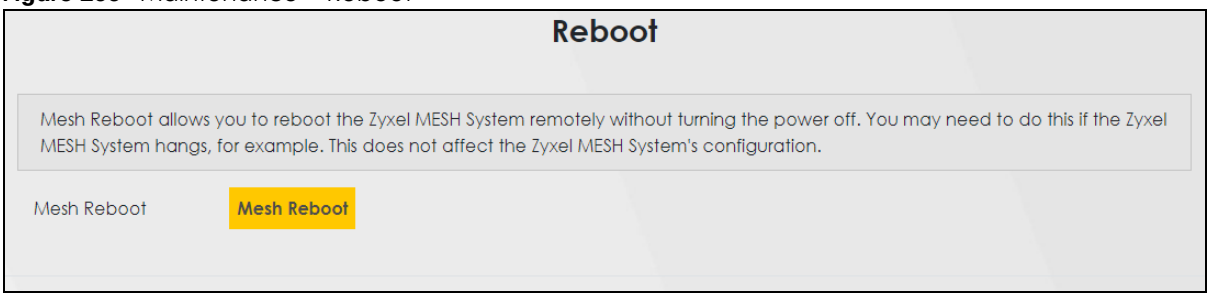
Figure 265 Maintenance > Reboot



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 reboot.

Figure 266 Maintenance > Reboot



CHAPTER 44
Diagnostic

44.1 Diagnostic Overview

The **Diagnostic** screen displays information to help you identify Internet connection problems with the Zyxel Device.

The route between an Ethernet 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.

44.1.1 What You Can Do in this Chapter

- The **Ping&Traceroute&Nslookup** screen lets you ping an IP address or trace the route packets take to a host (Section 44.3 on page 419).

44.2 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.

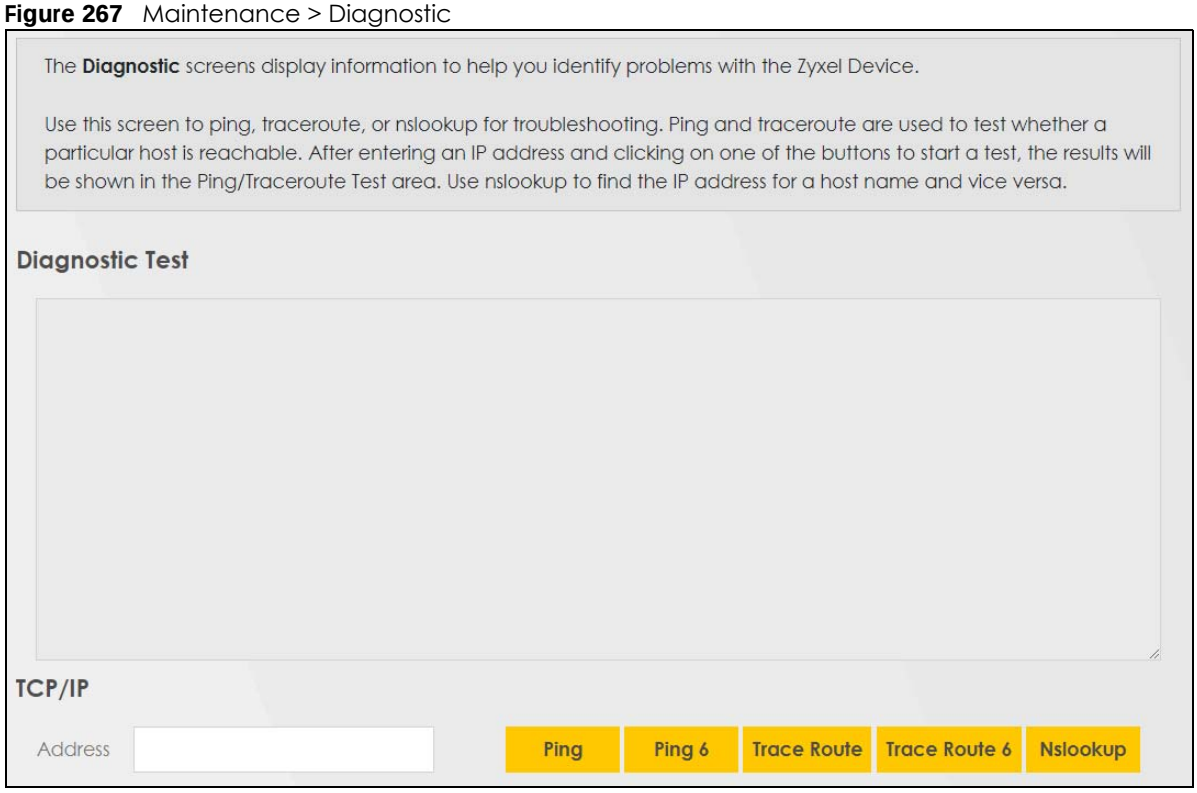
- Loopback test – checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test – provides additional connectivity fault analysis to get more information 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.

44.3 Diagnostic

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 one of the buttons to start a test, the results will be shown in the screen. Use nslookup to find the IP address for a host name and the host name for an IP address.

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

Figure 267 Maintenance > Diagnostic



The following table describes the fields in this screen.

Table 170 Maintenance > Diagnostic

LABEL	DESCRIPTION
Diagnostic Test	The result of tests is shown here in the info area.
Select Test Method	
Ping	Select this to perform a ping test on the IPv4 address or host name in order to test a connection. The ping statistics will show in the info area.
Ping 6	Select this to perform a ping test on the IPv6 address or host name in order to test a connection. The ping statistics will show in the info area.
Trace Route	Select this to perform the IPv4 trace route function. This determines the path a packet takes to the specified host.
Trace Route 6	Select this to perform the IPv6 trace route function. This determines the path a packet takes to the specified host.
Nslookup	Select this to perform a DNS lookup on the IP address or host name.
TCP/IP	

Table 170 Maintenance > Diagnostic (continued)

LABEL	DESCRIPTION
Address	Enter the IP address of a computer that you want to perform ping, trace route or nslookup in order to test a connection.
Start Test	Click this to perform the selected test method.

PART III
Troubleshooting and Appendices

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

CHAPTER 45
Troubleshooting

45.1 Troubleshooting Overview

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

- Power and Hardware Problems
- Device Access Problems
- Internet Problems
- WiFi Problems
- USB Problems
- VoIP Problems
- UPnP Problems

45.2 Power and Hardware Problems

The Zyxel Device does not turn on.

1. Make sure you are using the power adapter included with the Zyxel Device.
2. Make sure the power adapter is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adapter to the Zyxel Device.
4. Make sure you have pressed the **POWER** button to turn on the Zyxel Device.
5. If the problem continues, contact the vendor.

The LED 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 Zyxel Device off and on.

5 If the problem continues, contact the vendor.

45.3 Device Access Problems

I do not know the IP address of the Zyxel Device.

1 The default IP address is 192.168.1.1.

2 If you changed the IP address, you might be able to find the IP address of the Zyxel Device by looking up the IP address of your computer's default gateway. To do this in Microsoft Windows, click **Start** > **Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Zyxel Device, depending on your network environment.

3 If this does not work, reset the Zyxel Device to its factory defaults.

- Locate a small hole labeled **RESET** on the Zyxel Device.
- Use a paperclip or a similar tool to press and hold the **RESET** button for more than 5 seconds.
- Release the button, and the Zyxel Device will reset to its default settings, including the default IP address, user name, and password.

Note: Resetting the Zyxel Device will erase all your custom settings, so you need to reconfigure it.

I forgot the admin password.

1 See the Zyxel Device label or this document's cover page for the default admin password.

2 If you changed the password from default and cannot remember the new one, you have to reset the Zyxel Device to its factory default settings.

I cannot access the Web Configurator login screen.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten the new address, see the troubleshooting suggestions for I do not know the IP address of the Zyxel Device.

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 JavaScript and Java enabled.

4 Clear the Internet browser cache and try accessing the Web Configurator login screen again.

5 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance** > **Remote Management**).

6 Reset the Zyxel Device to its factory default, and try to access the Zyxel Device with the default IP address.

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

Advanced Suggestions

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the Zyxel Device using another service, such as Telnet. If you can access the Zyxel Device, check the remote management settings and firewall rules to find out why the Zyxel Device does not respond to HTTP.

I cannot log into the Zyxel Device.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**. These both user name and password are case-sensitive, so make sure [Caps Lock] is not on.

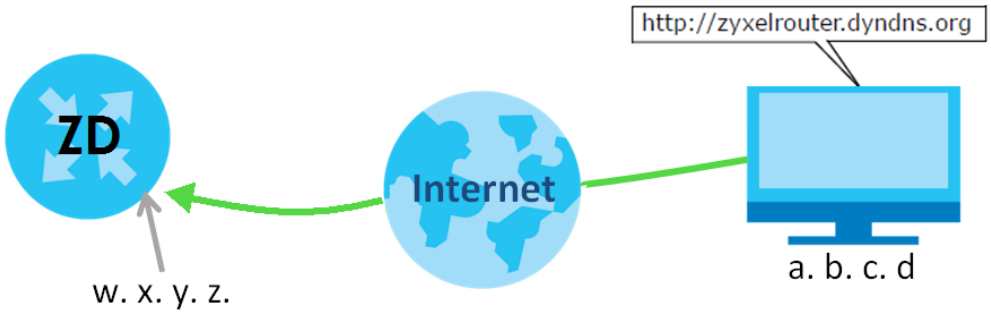
2 You cannot log in to the Web Configurator while someone is using Telnet to access the Zyxel Device. Log out of the Zyxel Device in the other session, or ask the person who is logged in to log out.

3 Turn the Zyxel Device off and on.

4 If this does not work, you have to reset the Zyxel Device to its factory default.

I cannot log into the Zyxel Device using DDNS.

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



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

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

Here are the three steps to use a domain name to log in the Web Configurator:

Step 1 Register for a DDNS Account on www.dyndns.org

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

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

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

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

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

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

Step 2 Configure DDNS on Your Zyxel Device

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

- Select **Enable Dynamic DNS**.
- Select **www.DynDNS.com** as the service provider.
- Enter **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**). Click **Apply**.

Step 3 Test the DDNS Setting

Now you should be able to access the Zyxel Device from the Internet. To test this:

1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.

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

3 The Zyxel Device's login page should appear. You can then log into the Zyxel Device and manage it.

I cannot connect to the Zyxel Device using Telnet, SSH, or Ping.

1 See the Remote Management section for details on allowing web services (such as HTTPS, Telnet, SSH and Ping) to access the Zyxel Device.

2 Check the server **Port** number field for the web service in the **Maintenance** > **Remote Management** screen. You must use the same port number in order to use that web service for remote management.

3 Try the troubleshooting suggestions for I cannot access the Web Configurator login screen. Ignore the suggestions about your browser.

I cannot access the Zyxel Device from outside the network (WAN).

To test if this is due to CGNAT, follow these steps:

1 Log in to your Zyxel Device's Web Configurator using the default IPv4 address (for example, 192.168.1.1).

2 Locate the WAN IP address on the **Dashboard** screen. You can find this information in the Network or WAN settings.

3 Go to a website that can show you the public IP address of your network (for example, https://whatsmyip.com). When you access this site, it will display your public IP address.

4 Compare the WAN IP address displayed on the **Dashboard** screen with the public IP address shown on the https://whatsmyip.com website.

- If both IP addresses are the same, your ISP is not using Carrier-Grade NAT, and you should be able to access your Zyxel Device from the WAN (outside).
- If the IP addresses are different, it indicates that your ISP is using Carrier-Grade NAT, and your Zyxel Device has a shared public IP address. As a result, remote access to your Zyxel Device from the WAN will not be possible.

If you discover that your Zyxel Device is behind a Carrier-Grade NAT and you need remote access, you must contact your ISP and request a public IP address for your SIM card or Zyxel Device.

The SIM card cannot be detected.

1 Disconnect the Zyxel Device from the power supply.

2 Remove the SIM card from its slot.

3 Clean the SIM card slot of any loose debris using compressed air.

4 Clean the gold connectors on the SIM card with a clean lint-free cloth.

5 Insert the SIM card into its slot and connect the Zyxel Device to the power supply to restart it.

I get an **Invalid** SIM card alert.

1 Make sure you have an active plan with your ISP.

2 Make sure that the Zyxel Device is in the coverage area of a cellular network.

3 Enable **Data Roaming** in **Network Setting** > **Broadband** > **Cellular WAN** to keep the Zyxel Device connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered, such as a different country. Then, restart the Zyxel Device.

45.4 Internet Problems

I cannot access the Internet.

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

2 Make sure you entered your ISP account information correctly on the **Network Setting** > **Broadband** screen. Fields on this screen are case-sensitive, so check if [Caps Lock] is on of off.

3 If you are trying to access the Internet wirelessly, make sure that you enabled the WiFi in the Zyxel Device and your WiFi client and that the WiFi settings in the WiFi client are the same as the settings in the Zyxel Device.

4 Disconnect all the cables from your Zyxel Device and reconnect them.

5 If the problem continues, contact your ISP.

I cannot connect to the Internet using an Ethernet connection.

1 Make sure you have the Ethernet WAN port connected to a Modem or Router.

2 Make sure you configured a proper Ethernet WAN interface (**Network Setting** > **Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.

3 Check that the WAN interface you are connected to is in the same interface group as the Ethernet connection (**Network Setting** > **Interface Group**).

4 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **Network Setting** > **Home Networking** > **LAN Setup** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot connect to the Internet using a Fiber connection.

1 Make sure the Fiber/SFP port has a compatible SFP/SFP+ transceiver installed with a fiber/Ethernet cable connected to it.

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

The **PON** LED is off if the optical transceiver has malfunctioned or the fiber cable is not connected or is broken or damaged enough to break the PON connection.

The **LOS** LED is red if the GPON Device is not receiving an optical signal.

The **LOS** LED blinks red if the GPON Device is receiving a weak optical signal.

3 Disconnect all the cables from your device and reconnect them. Make sure the fiber cable is not curved too much.

4 If that does not work, restart your Zyxel Device.

5 If the problems continues, contact your ISP.

I cannot connect to the Internet using a cellular connection.

1 The DSL and Ethernet connections have priority in that order. If the DSL or Ethernet connection is up, then the cellular connection will be down.

2 Make sure you have connected a compatible cellular dongle to the USB port, if required.

3 Make sure you have configured **Network Setting** > **Broadband** > **Cellular Backup** correctly.

4 Check that the Zyxel Device is within range of a cellular base station.

The Zyxel Device cannot assign individual IP addresses to the connected client devices.

1 Make sure to select **Bridge** in **Network Setting** > **Broadband** > **Add/Edit New WAN Interface**: **Mode**.

2 Make sure to reboot the Zyxel Device after changing to **Bridge** mode.

3 Make sure the Zyxel Device can get an IP address dynamically (DHCP) from the router controller.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. If the Zyxel Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 If your Zyxel Device keeps alternating between ISPs, then choose a fixed ISP. Go to the **Network Setting** > **Cellular PLMN** screen, disable **PLMN Auto Selection** and then choose your preferred ISP.

3 Turn the Zyxel Device off and on.

4 If the problem continues, contact the network administrator or vendor, or try the advanced suggestions in I cannot access the Web Configurator login screen.

Note: If your Zyxel Device is an outdoor-type, inclement weather like rain and hot weather may affect cellular signals.

What should I do if my Zyxel Device is under attack?

A slow Internet speed, a web browser that keeps redirecting you, suspicious activity alerts from your ISP, and increased pop-ups on the Zyxel Device; could be signs that your Zyxel Device is under attack. If you suspect that your Zyxel Device is under attack, do the following:

1 Create an ACL (Access Control List) rule to block the ports being targeted. See Section 18.5 on page 304 for more information on using ACL. See also Section 5.5.1 on page 90 for more information on configuring a firewall rule. Go to **System Monitor** > **Log** > **Security Log** to view the security-related logs to determine which ports are being targeted. See Section 25.3 on page 364 for more information on security logs.

2 Contact your ISP to report the attack and seek assistance.

3 When possible, turn off the Zyxel Device for 24 hours, then turn it on again.

4 Request the ISP to change your IP address.

45.5 WiFi Problems

I cannot connect to the Zyxel Device WiFi.

1 Check the WiFi LED status to make sure the Zyxel Device WiFi is on.

2 Make sure your WiFi client is within transmission range of the Zyxel Device.

3 Make sure you entered the correct SSID and password. See the Zyxel Device back label for the default SSID and password.

4 Make sure your WiFi client is using the same WiFi security type (WPA2-PSK, WPA3-SAE, or none) as the Zyxel Device.

5 Make sure the WiFi adapter on your WiFi client is working properly. Right-click your computer's network adapter then select **Properties** to check your network adapter status.

6 Make sure the WiFi adapter on your WiFi client is IEEE 802.11-compatible and supports the same WiFi standard as the Zyxel Device radio.

Note: To check if it is your Zyxel Device that is causing the problem and not your WiFi connection, try using a wired connection.

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 wireless devices.

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

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

45.6 USB Problems

The Zyxel Device fails to detect my USB device.

1 Disconnect the USB device.

2 Reboot the Zyxel Device.

3 If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

4 Reconnect your USB device to the Zyxel Device.

45.7 VoIP Problems

I cannot make phone calls through the phone connected to the Zyxel Device.

1 Pick up the phone and check the phone tone. You should hear the dial tone if your configuration on the Zyxel Device is correct, and your phone is successfully connected to the SIP server.

2 Check that the settings from your VoIP service are entered correctly on the Zyxel Device.

3 Make sure your phone is connected to the Zyxel Device phone port through an RJ-11 cable. Check the Zyxel Device phone LED for the corresponding phone status.

4 Make sure the Zyxel Device has an Internet connection. See Section 45.4 on page 427 for more information.

5 Make sure your SIP account is registered and your SIP service plan is valid. Use the **System Monitor** > **VoIP Status** screen to check the account **Registration** status.

6 Make sure your SIP server settings (in the **VoIP** > **SIP** > **SIP Service Provider** and the **VoIP** > **SIP** > **SIP Account** screens) use the correct information from your SIP service provider. For example, your SIP service provider name, SIP account and password.

7 Make sure your phone settings (in the **VoIP** > **Phone** > **Phone Device** screen) are correct.

8 Contact the SIP server administrator and make sure your SIP server is not down.

I am experiencing echoes during calls.

Go to **VoIP > SIP > SIP Account > SIP Account Entry Edit**. Click **Enable G.168 (Echo Cancellation)** to eliminate echo during calls.

45.8 UPnP Problems

My computer cannot detect UPnP settings from the Zyxel Device.

1. Make sure that UPnP is enabled in your computer.
2. On the Zyxel Device, make sure that UPnP is enabled on the **Network Settings** > **Home Networking** > **UPnP** screen.
3. Disconnect the Ethernet cable from the Zyxel Device's Ethernet port or from your computer.
4. Reconnect the Ethernet cable.
5. Restart your computer.

45.9 Getting More Troubleshooting Help

Search for support information for your model at *https://service-provider.zyxel.com/global/en/tech-support* and *community.zyxel.com* for more troubleshooting suggestions.

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 Zyxel 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
Wireless LANs

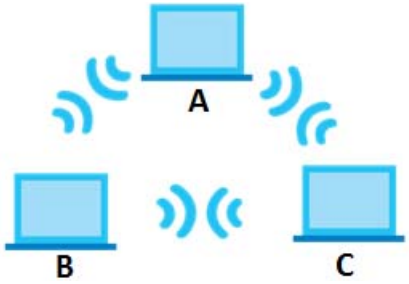
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 268 Peer-to-Peer Communication in an Ad-hoc Network

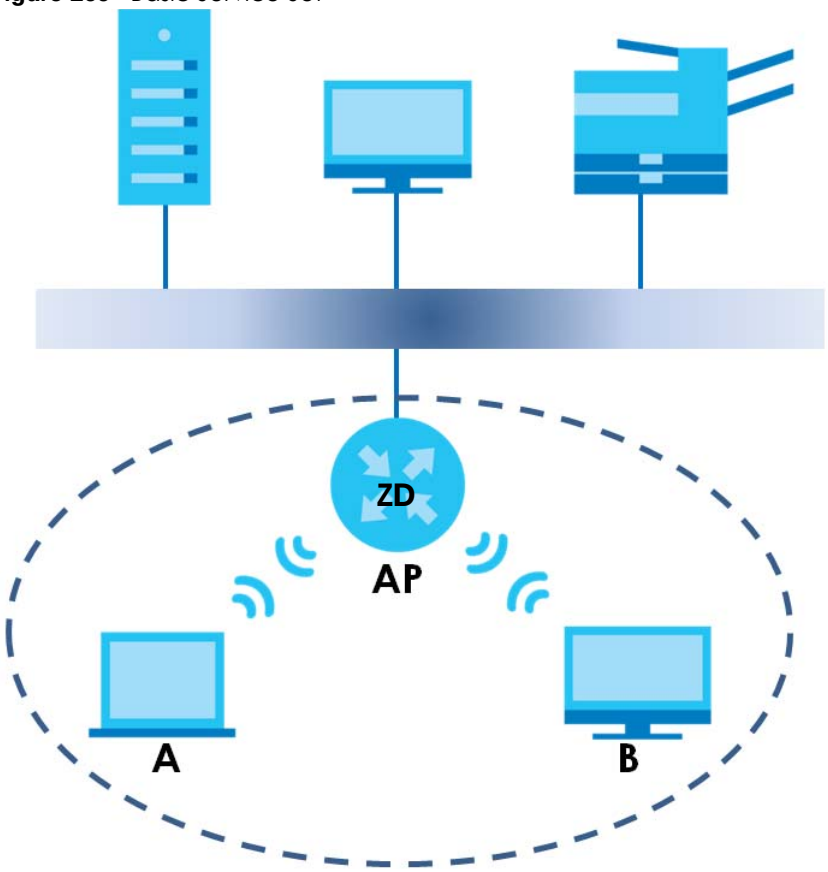


BSS

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

Intra-BSS traffic is traffic between WiFi clients in the BSS. When Intra-BSS is enabled, WiFi client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, WiFi client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 269 Basic Service Set



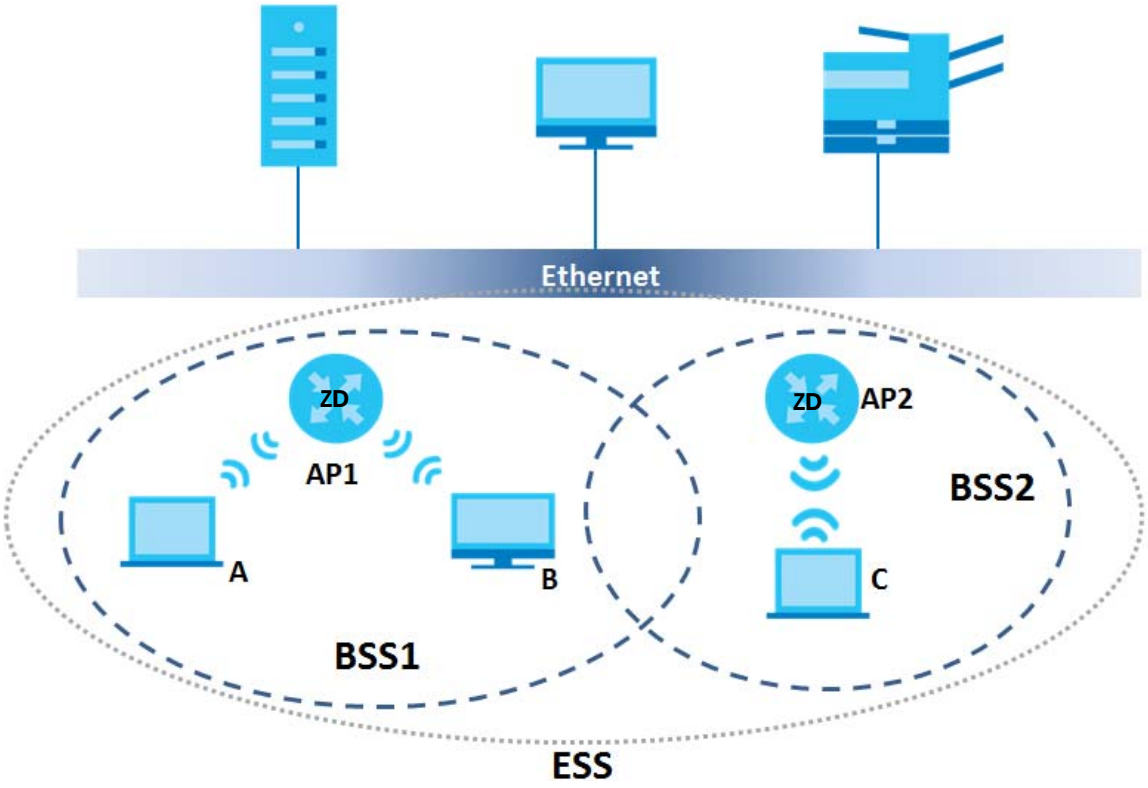
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated WiFi clients within the same ESS must have the same ESSID in order to communicate.

Figure 270 Infrastructure WLAN



Channel

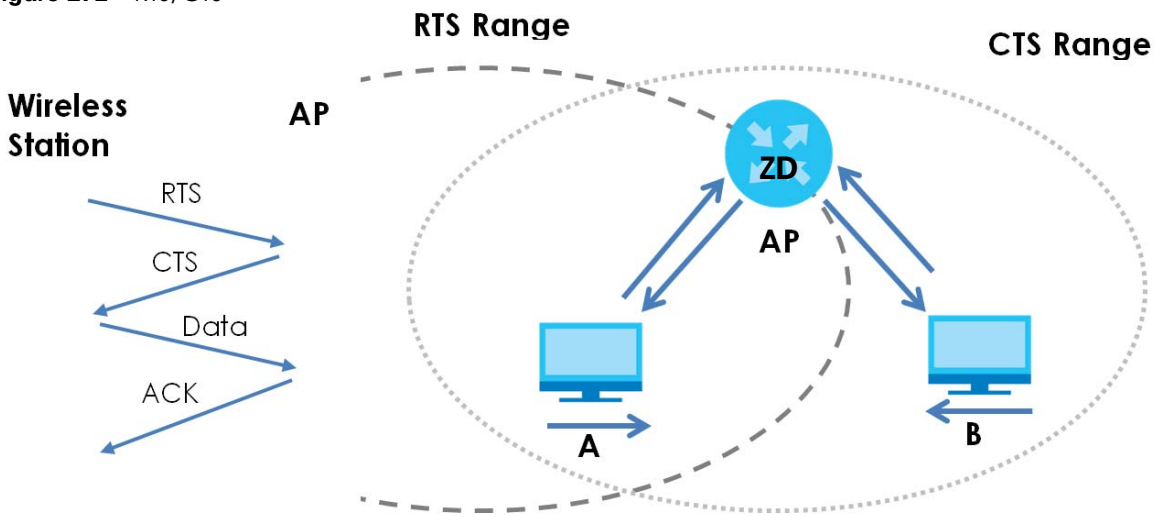
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 271 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 171 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between WiFi clients, access points and the wired network.

Wireless security methods available on the Zyxel Device are data encryption, WiFi client authentication, restricting access by device MAC address and hiding the Zyxel Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your Zyxel Device.

Table 172 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	WiFi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the Zyxel Device and on all WiFi clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.

- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the WiFi clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the WiFi client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the WiFi client. The WiFi client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the WiFi clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2

and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 173 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

WiFi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the WiFi clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and WiFi client. As long as the passwords match, a WiFi client will be granted access to a WLAN.

If the AP or the WiFi clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or WiFi clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice..

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the WiFi clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a WiFi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP).

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate WiFi clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a WiFi client to store the PMK it derived through a successful authentication with an AP. The WiFi client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the WiFi client (already connected to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

WiFi Client WPA Supplicants

A WiFi client supplicant is the software that runs on an operating system instructing the WiFi client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

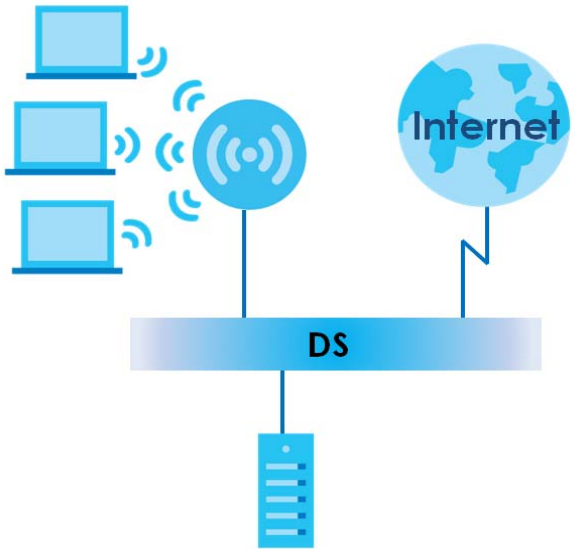
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" WiFi client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the WiFi client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the WiFi clients.

Figure 272 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

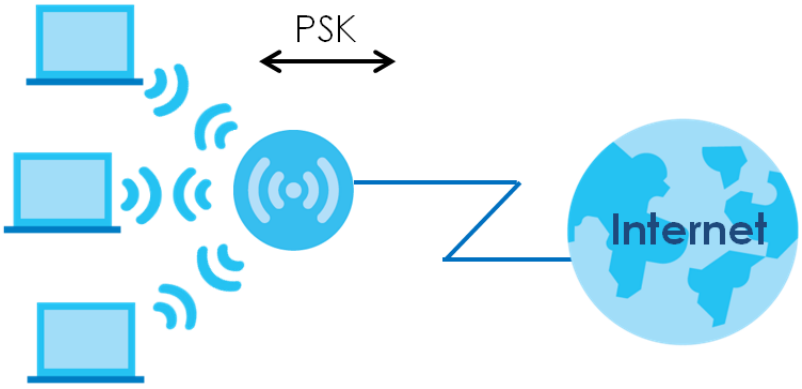
1. First enter identical passwords into the AP and all WiFi clients. The Pre-Shared Key (PSK) must consist of between 8 to 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces.

2 The AP checks each WiFi client's password and allows it to join the network only if the password matches.

3 The AP and WiFi clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and WiFi clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 273 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 174 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4 GHz (IEEE 802.11b and IEEE 802.11g) or 5 GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WiFi

There are two types of antennas used for WiFi applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

APPENDIX C
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 x 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 175 Link-local Unicast Address Format

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

Global Address

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

Unspecified Address

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

Loopback Address

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

Multicast Address

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

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

Table 176 Predefined Multicast Address

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

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

Table 177 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
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

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

Interface ID

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

EUI-64

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

Table 178

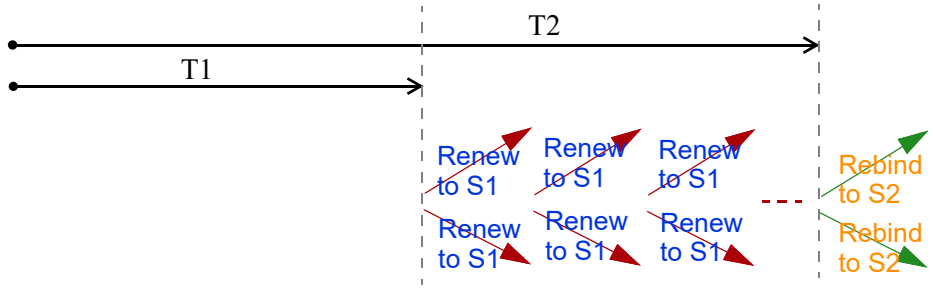
MAC	00	:	13	:	49	:	12	:	34	:	56

Table 179

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

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

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

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

Prefix Delegation

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

ICMPv6

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

Neighbor Discovery Protocol (NDP)

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

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

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Zyxel Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Zyxel Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Zyxel Device also sends out a neighbor solicitation message. When the Zyxel Device

receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Zyxel Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Zyxel Device creates an entry in the default router list cache if the router can be used as a default router.

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

Multicast Listener Discovery

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

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

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

MLD filtering controls which Multicast groups a port can join.

MLD Messages

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

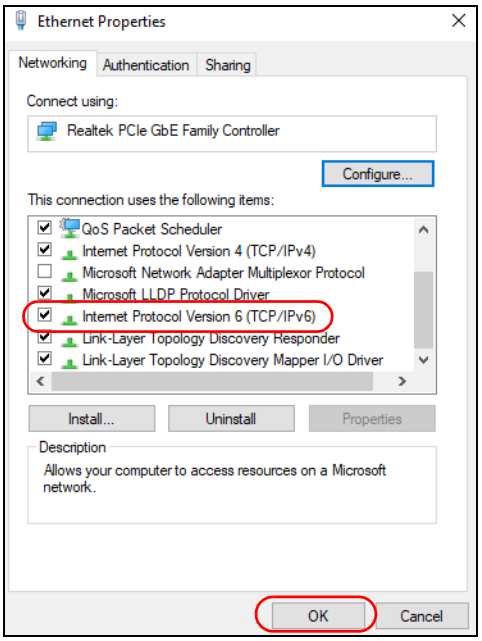
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a Multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected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

Example – Enabling IPv6 on Windows 10

Windows 10 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 10 computer.

To enable IPv6 in Windows 10:

1. Click the start icon, **Settings** and then **Network & Internet**.
2. Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
3. Click **OK** to save the change.



4 Click the Search icon ( ) and then enter "cmd" in the search box.

5 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:f
```

APPENDIX D
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 180 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.
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.
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.

Table 180 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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 email 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.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).

Table 180 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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 E
Legal Information

Copyright

Disclaimer

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

Regulatory Notice and Statement

United States of America

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

FCC Statement

- The device complies with Part 15 of the 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 equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

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 Radio Frequency (RF) radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 50 cm (EE6510-10) and 20 cm (all other models) 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.

Canada

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

CAN ICES(B) / NMB(B)

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

  (1) this device may not cause interference, and

  (2) this device must accept any interference, including interference that may cause undesired operation of the device.
- L'émetterur/récepteur exempt de licence contenu dans le prés ent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio ex empts de licence.
  L'exploitation est autorisée aux deux condi tions suivantes:

  (1) l'appareil ne doit pas produire de brouillage;

  (2) L'appareil doit accepter tout brouillage radioélectrique su bi, même si le brouillage est susc eptible d'en compromettre le fonctionnement.
- For 2.4 G WLAN, only channels 1-11 are operational. Selection of other channels is NOT possible.
- Pour le WLAN 2,4 G, seuls les canaux 1 à 11 sont opérationnels. La sélection d'autres canaux n'est PAS possible.
- The device operating in the 5150-5250 MHZ band is only for indoor use to reduce the potential for harmful interference to co-channal mobile statellite systems.
- Where applicable, antenna type(s), antenna model(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set force in Section 6.2.2.3 of RSS 247 shall be clearly indicated.
- Les dispositifs fonctionnant dans la bande de 5150 à 5250 MHz so nt réservés uniquement pour une utilisation à l'intérieur af in de réduire les risques de brouillage préjudiciable aux systémes de satellites mobiles utilisant les mêmes canaux;
- Lorsq'ily a lieu, les types d'antnnes(s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inc linaison nécessaires pour rester confirme à la limite de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doi vent être clairement indiqués.

Industry Canada radiation exposure statement

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 23 cm (EE6601-00), 29 cm (EE6510-10), and 20 cm (all other models) between the radiator and your body.

Déclaration d'exposition aux radiations

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 23 cm (EE6601-00), 29 cm (EE6510-10), et 20 cm (tous les autres modèles) de distance entre la source de rayonnement et votre corps.

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

RLAN Devices

- Devices shall not be used for control of or communications with unmanned aircraft systems.
- Devices shall not be used on oil platforms.
- Devices shall not be used on aircraft, except for the low-power indoor access points, indoor subordinate devices, low-power client devices, and very low-power devices operating in the 5925-6425 MHz band, that may be used on large aircraft as defined in the Canadian Aviation Regulations, while flying above 3,048 metres (10,000 feet).
- Devices shall not be used on automobiles.
- Devices shall not be used on trains.
- Devices shall not be used on maritime vessels.

Les dispositifs RLAN

- Les dispositifs ne doivent pas être utilisés pour commander des systèmes d'aéronef sans pilote ni pour communiquer avec de tels systèmes;
- Les dispositifs ne doivent pas être utilisés sur les plateformes de forage pétrolier;
- Les dispositifs ne doivent pas être utilisés dans les aéronefs, à l'exception des points d'accès intérieurs de faible puissance, des dispositifs subordonnés intérieurs, des dispositifs clients de faible puissance et des dispositifs de très faible puissance fonctionnant dans la bande de 5 925 à 6 425 MHz, qui peuvent être utilisés dans les gros aéronefs tel qu'il est défini dans le Règlement de l'aviation canadien, et ce, lorsqu'ils volent à une altitude supérieure à 3 048 mètres (10 000 pieds).
- Les dispositifs ne doivent pas être utilisés dans les automobiles;
- Les dispositifs ne doivent pas être utilisés dans les trains;
- Les dispositifs ne doivent pas être utilisés sur les navires maritimes.

Low-power indoor access points and indoor subordinate devices

- Operation shall be limited to indoor use only.

Points d'accès intérieurs de faible puissance et dispositifs subordonnés intérieurs

- Le fonctionnement doit être limitée à une utilisation à l'intérieur seulement.

Europe and the United Kingdom

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

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED) and UK Radio Equipment Regulations 2017

Model List: EE6601-00, PE5301-00

- Compliance information for wireless products relevant to the EU, United Kingdom, and other Countries following the EU Directive 2014/53/EU (RED) and UK Radio Equipment Regulations 2017. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and United Kingdom without any limitation except for the countries mentioned below table:
- In the majority of the EU, United Kingdom, 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 operates in the 5150 to 5350 MHz band, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20cm between the radio equipment and your body.
- The maximum RF operating power for each band is as follows:
- EE6601-00
  - 83.95 mW for the 2,400 to 2,483.5 MHz band
  - 165.58 mW for the 5,150 to 5,350 MHz band
  - 749.89 mW for the 5,470 to 5,725 MHz band
  - 170.22 mW for the 5,725 to 5,850 MHz band (UK only)
  - 165.96 mW for the 5,945 to 6,425 MHz band
- PE5301-00
  - 88.92 mW for the 2,400 to 2,483.5 MHz band
  - 176.20 mW for the 5,150 to 5,350 MHz band
  - 887.16 mW for the 5,470 to 5,725 MHz band
  - 177.42 mW for the 5,725 to 5,850 MHz band (UK only)

Belgium (English) België (Flemish) Belgique (French)	**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.
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
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 deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.

Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
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 şi alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените 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
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, has extreme temperatures, or that blocks the device ventilation slots. These conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for power rating of the device and operating temperature.
- There is a remote risk of electric shock from lightning: (1) Do not use the device outside, and make sure all the connections are indoors. (2) Do not install or service this device during a thunderstorm.
- 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 Zyxel Device. Opening or removing the device 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 connected cables carefully so that no one will step on them or stumble over them.
- 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 the power adaptor or cord 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 the damaged power adaptor or cord from the device and the power source. Contact your local vendor to order a new one.
- CAUTION: There is a risk of explosion if you replace the device battery with an incorrect one. Dispose of used batteries according to the instructions. 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.
- Do not leave a battery in an extremely high temperature environment or surroundings since it can result in an explosion or the leakage of flammable liquid or gas.
- Do not subject a battery to extremely low air pressure since it may result in an explosion or the leakage of flammable liquid or gas.
- 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 a permanently connected device, a readily accessible method to disconnect the device shall be incorporated externally to the device;

  – For a pluggable device, the socket-outlet shall be installed near the device and shall be easily accessible.
- This product is intended to be supplied by a DC power source marked 'L.P.S' or `Limited Power Source'. The rating for each model is as follows:
  - EE6510-10 / EE6601-00: 12 Vdc / 3.5 A / Tma 40 °C
  - PE5301-00: 12 Vdc / 3 A / Tma 40 °C

The following information applies for products with SFP:

- CLASS 1 LASER PRODUCT & "IEC 60825-1:2014"
- CLASS 1 CONSUMER LASER PRODUCT & "EN 50689:2021"
- Caution – Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.
- Complies with 21 CFR 1040.10 and 1040.11 except for conformance with IEC 60825-1 Ed. 3., as described in Laser Notice No. 56, dated May 8, 2019.

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.
- Attention: L'utilisation des commandes ou reglages ou l'execution des procedures autres que celles specifiees dans les presents exigences peuvent etre la cause d'une exposition a un rayonnement dangereux

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU and United Kingdom market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC and UK regulation 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 < 8 W, and/or
- Off mode power consumption < 0.5 W, and/or
- Standby mode power consumption < 0.5 W.

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

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

- 取得審驗證明之低功率射頻器材，非經核准，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。
- 低功率射頻器材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。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材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。
- 本機限在不干擾合法電台與不被干擾保障條件下於室內使用。本產品使用時建議應距離人體 20 cm 以上。
- 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。
- 請使用隨貨提供或指定的連接線 / 電源線 / 電源變壓器，將其連接到合適的供應電壓 （如：台灣供應電壓 110 伏特）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。

- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  – 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  – 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

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

Explanation of the Symbols

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

Viewing Certifications

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

Zyxel Limited Warranty

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

Note

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

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

Registration

Register your product online at *www.zyxel.com* to receive e-mail notices of firmware upgrades and related information.

Open Source Licenses

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

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

Index

Numbers

6rd
IPv6 128

A

access
troubleshooting 423
Access Control (Rules) screen 304
ACK message 354
activation
firewalls 302
media server 299
SSID 175
Address Resolution Protocol 372
antenna
directional 449
gain 449
omni-directional 449
Any_WAN
Remote Management 392
AP (access point) 440
Application Layer Gateway (ALG) 264
applications
media server 298
activation 299
iTunes server 298
applications, NAT 272
ARP Table 372
Asynchronous Transfer Mode 127
ATM 127
authentication 187

B

backup
configuration 413
backup configuration 413
Backup/Restore screen 412
bandwidth capacity
cable type 25
Basic Service Set, See BSS 438
Basic Service Set, see BSS
blinking LEDs 29
Bridge mode 137, 147
broadband 125
Broadband screen
overview 125
broadcast 164
BSS 189, 438
example 189
button
WLAN 36, 39
BYE request 354

C

CA 327, 444
cable type
Ethernet 25
call hold 359, 361
call service mode 359, 360
call transfer 360, 361
call waiting 360, 361
Canonical Format Indicator See CFI
CCMs 418
certificate
details 329
factory default 321
file format 328
file path 326
import 321, 325
public and private keys 327
verification 328
Certificate Authority
See CA.

certificate request
create 321
view 323
certificates 320
advantages 328
authentication 320
CA 320, 327
creating 322
public key 320
replacing 321
storage space 321
thumbprint algorithms 328
trusted CAs 325
verifying fingerprints 328
Certification Authority 320
Certification Authority, see CA
certifications 464
viewing 467
CFI 163
CFM 418
CCMs 418
link trace test 418
loopback test 418
MA 418
MD 418
MEP 418
MIP 418
channel 440
interference 440
Class of Service 357
Class of Service, see CoS
client list 202
client-server protocol 351
comfort noise generation 356
configuration
backup 413
firewalls 302
restoring 414
static route 275
Connectivity Check Messages, see CCMs
contact information 433
copyright 461
CoS 250, 357
CoS technologies 234
Create Certificate Request screen 322
creating certificates 322
CTS (Clear to Send) 441
CTS threshold 182, 187
customer support 433
customized service 303
add 304
customized services 304

D

data fragment threshold 182, 187
DDoS 301
Denials of Service, see DoS
DHCP 196, 212
DHCP Server Lease Time 200
DHCP Server State 200
diagnostic 418
diagnostic screens 418
differentiated services 358
Differentiated Services, see DiffServ 250
DiffServ 250
marking rule 251
DiffServ (Differentiated Services) 357
code points 357
marking rule 358
digital IDs 320
disclaimer 461
distance maximum
cable type 25
DLNA 298
DMZ screen 263
DNS 196, 212
DNS server address assignment 164
DNS Values 200
Domain Name 273
domain name system, see DNS
DoS 300
thresholds 301
DoS protection blocking
enable 307
DS field 251, 358
DS, see differentiated services
DSCP 250, 357
Dual Stack Lite 128

dual/tri-radios 22
dual-band application 21
dual-band gateway 21
dual-radio application 22
dynamic DNS 274
  wildcard 274
Dynamic Host Configuration Protocol, see DHCP
dynamic WEP key exchange 445
DYNDNS wildcard 274

E

EAP Authentication 444
ECHO 273
echo cancellation 356
email
  log example 406
  log setting 406
Encapsulation 160
  MER 160
  PPP over Ethernet 161
encapsulation
  RFC 1483 161
encapsulation method
  technical reference 160
encryption 446
ESS 439
Ether Type 242
Europe type call service mode 359
Extended Service Set IDentification 171, 177
Extended Service Set, See ESS 439

F

factory defaults
  reset 414
factory-default configuration
  reload 41
Fast Leave 281
fiber cable
  connecting 40
  removal 40
file sharing 26
filters
  MAC address 178, 188
Finger services 273
firewall
  enhancing security 309
  LAND attack 301
  security considerations 309
  traffic rule direction 307
Firewall DoS screen 307
Firewall General screen 302
firewall rules
  direction of travel 308
firewalls 300, 302
  actions 307
  configuration 302
  customized service 303
  customized services 304
  DDoS 301
  DoS 300
    thresholds 301
  ICMP 301
  Ping of Death 301
  rules 308
  security 309
  SYN attack 300
firmware 408
Firmware Upgrade screen 408, 410
firmware upload 408, 410
firmware version
  check 409
flash key 359
flashing 359
fragmentation threshold 182, 187, 441

G

G.168 356
General wireless LAN screen 167
Guide
  Quick Start 2

H

hidden node 440
Home Security URL filtering 312
HTTP 273

I

IBSS 438
ICMP 301
ICMPv6 279
IEEE 802.11ax 167
IEEE 802.11g 442
IEEE 802.1Q 163
IGA 271
IGMP 164
  multicast group list 280, 377, 378
  version 164
IGMP Fast Leave 279
IGMPv2 279
IGMPv3 279
ILA 271
Import Certificate screen 325
importing trusted CAs 325
Independent Basic Service Set
  See IBSS 438
initialization vector (IV) 446
Inside Global Address, see IGA
Inside Local Address, see ILA
interface group 285
Internet
  no access 427
  wizard setup 56
Internet access
  wizard setup 56
Internet access application
  Ethernet WAN 20
Internet Blocking 109
Internet connection
  add or edit 130, 141
  slow or erratic 429
Internet Control Message Protocol, see ICMP
Internet Protocol version 6 127
Internet Protocol version 6, see IPv6
Intra LAN Multicast 281
IP address 213
  private 213
  WAN 126
IP address assignment 163
IP alias
  NAT applications 272
IP over Ethernet 160
IP packet
  transmission method 164
IPoE technical reference 160
IPv4 firewall 303
IPv6 127, 451
  addressing 127, 164, 451
  EUI-64 453
  global address 451
  interface ID 453
  link-local address 451
  Neighbor Discovery Protocol 451
  ping 451
  prefix 127, 165, 451
  prefix and length 127
  prefix delegation 129
  prefix length 127, 165, 451
  subnet mask 127
  unspecified address 452
IPv6 address
  abbreviation method 164
IPv6 firewall 303
IPv6 rapid deployment 128
iTunes server 298
ITU-T 356

K

key combinations 362
keypad 362

L

LAN 195
  client list 202
  DHCP 212

DNS 212
IP address 213
MAC address 203
status 114, 121
subnet mask 197, 213
LAN IP address 200
LAN IPv6 Mode Setup 201
LAN Setup screen 197
LAN subnet mask 200
LAN to LAN multicast 281
LAND attack 301
LBR 418
LED description 31, 32
LED indicators 29
limitations
wireless LAN 189
WPS 194
link trace 418
Link Trace Message, see LTM
Link Trace Response, see LTR
listening port 341
Local Area Network, see LAN
Local Certificates screen 320
log setting 404
Log Setting screen 404
login 42
password 43
Login screen
no access 423
logs 363
Loop Back Response, see LBR
loopback 418
LTM 418
LTR 418

M

MA 418
MAC address 203
filter 178, 188
LAN 203
MAC Authentication screen 178
MAC Filter 310
Maintenance Association, see MA
Maintenance Domain, see MD
Maintenance End Point, see MEP
Management Information Base (MIB) 395
managing the device
good habits 27
Maximum Burst Size (MBS) 162
MBSSID 190
MD 418
media server 298
activation 299
iTunes server 298
MEP 418
MESH
enable 185
MGMT Services screen 390
MLD 279
MLDv1 279
MLDv2 279
MTU (Multi-Tenant Unit) 163
Multi_WAN
Remote Management 392
multicast 164
Multicast Listener Discovery, see MLD
multi-gigabit 24
multimedia 350
Multiple BSS, see MBSSID
multiplexing 161
LLC-based 161
VC-based 161
multiprotocol encapsulation 161

N

NAT 270, 271
applications 272
IP alias 272
default server 263
DMZ host 263
example 272
global 271
IGA 271
ILA 271
inside 271

local 271
multiple server example 256
outside 271
port number 273
services 273
NAT ALG screen 264, 267
NAT example 273
Network Address Translation, see NAT
network disconnect
temporary 409
network map 109
NNTP 273
Nslookup test 419

O

OK response 354, 355
online firmware 410
Optical Signal Status screen 384
Others screen 182

P

Packet Transfer Mode 127
Pairwise Master Key (PMK) 446, 448
parental control
schedule setup 315, 317
password 43
admin 423
lost 423
user 423
PBC 191
Peak Cell Rate (PCR) 161
Per-Hop Behavior, see PHB 251
PHB 251, 358
phone functions 362
PIN, WPS 191
Ping of Death 301
Ping test 419
Ping/TraceRoute/Nslookup screen 419
Point-to-Point Tunneling Protocol, see PPTP
POP3 273
port forwarding rule
add/edit 257
Port Forwarding screen 257
Port Triggering
add new rule 261
Port Triggering screen 259
ports 29
POWER button 34, 36, 38
POWER LED 30
PPPoE 161
Benefits 161
technical reference 161
PPTP 273
preamble 183, 187
preamble mode 190
prefix delegation 129
private IP address 213
problems 422
Protocol (Customized Services) screen 303
Protocol Entry
add 304
PSK 446
PTM 127
Push Button Configuration, see PBC
push button, WPS 191

Q

QoS 233, 250, 357
marking 234
setup 233
tagging 234
versus CoS 234
Quality of Service, see QoS
Quick Start Guide 2

R

RADIUS 443
message types 443
messages 443
shared secret key 443
Real time Transport Protocol, see RTP

Reboot screen 416
reset 41
RESET button 34, 36, 39
  using 41
reset to factory defaults 414
restart system 416
restoring configuration 414
RFC 1058, see RIP
RFC 1389, see RIP
RFC 1483 161
RFC 1631 255
RFC 1889 353
RIP 231
Routing Information Protocol, see RIP
routing table 374
RTP 353
RTS (Request To Send) 441
  threshold 440, 441
RTS threshold 182, 187

S

security
  network 309
  wireless LAN 187
Security Log 364
Security Parameter Index, see SPI
service access control 393
Service Set 171, 177
services
  port forwarding 273
Session Initiation Protocol, see SIP
setup
  firewalls 302
  static route 275
silence suppression 356
Simple Network Management Protocol, see SNMP
Single Rate Three Color Marker, see srTCM
SIP 350
  account 350
  call progression 353
  client 351
  identities 350
  INVITE request 354, 355
  number 350
  OK response 355
  proxy server 351
  redirect server 352
  register server 353
  servers 351
  service domain 350
  URI 350
  user agent 351
SMTP 273
SNMP 395
  agents 395
  Get 396
  GetNext 396
  Manager 395
  managers 395
  MIB 395
  network components 395
  Set 396
  Trap 396
  versions 395
SPI 301
srTCM 253
SSH
  unusable 426
SSID 188
  activation 175
  MBSSID 190
static DHCP 202
  configuration 204
Static DHCP screen 202
static route 222, 231
  configuration 275
status 109
  LAN 114, 121
  WAN 113
  wireless LAN 114
status indicators 29
subnet mask 213
supplementary services 358
Sustained Cell Rate (SCR) 162
SYN attack 300
syslog logging
  enable 406
syslog server
  name or IP address 406
system

firmware 408
online firmware 410
password 43
reset 41
status 109
LAN 114, 121
WAN 113
wireless LAN 114
time 398

T

Telnet
unusable 426
three-way conference 360, 361
thresholds
data fragment 182, 187
DoS 301
RTS/CTS 182, 187
time 398
ToS 357
TPID 163
Trace Route test 419
traffic shaping 161
transmission speed
cable type 25
troubleshooting 422
trTCM 253
Trust Domain
add 393
Trust Domain screen 392
Trusted CA certificate
view 326
Trusted CA screen 324
Two Rate Three Color Marker, see trTCM
TWT (Target Wakeup Time) 167
Type of Service, see ToS

U

unicast 164
Uniform Resource Identifier 350
Universal Plug and Play, see UPnP
upgrading firmware 408
upgrading online firmware 410
UPnP 204
forum 197
NAT traversal 196
security issues 197
state 205
usage confirmation 196
UPnP screen 204
UPnP-enabled Network Device
auto-discover 216
USA type call service mode 360
USB feature
Media Server 27
USB features 26

V

VAD 356
Vendor ID 208
Virtual Circuit (VC) 161
Virtual Local Area Network See VLAN
VLAN 163
Introduction 163
VLAN ID 163
VLAN tag 163
voice activity detection 356
voice coding 355
VoIP 350

W

Wake on LAN 208
WAN
status 113
Wide Area Network, see WAN 125
WAN IP address 126
warranty
note 467
Web Configurator
login 42
password 43
WEP 173

WEP Encryption 173
WiFi
MBSSID 190
Wi-Fi Protected Access 445
WiFi standards
comparison table 167
WiFi6 introduction 167
wireless client WPA supplicants 447
Wireless General screen 168
wireless LAN 166
authentication 187
BSS 189
example 189
example 186
fragmentation threshold 182, 187
limitations 189
MAC address filter 178, 188
preamble 183, 187
RTS/CTS threshold 182, 187
security 187
SSID 188
activation 175
status 114
WPS 190, 191
example 192
limitations 194
PIN 191
push button 191
wireless security 442
wizard setup
Internet 56
WLAN
interference 440
security parameters 448
WMM screen 181
WPA 173, 445
key caching 446
pre-authentication 446
user authentication 446
vs WPA-PSK 446
wireless client supplicant 447
with RADIUS application example 447
WPA2 173, 445
user authentication 446
vs WPA2-PSK 446
wireless client supplicant 447
with RADIUS application example 447
WPA2-Pre-Shared Key 445
WPA2-PSK 173, 445, 446
application example 447
WPA3-SAE (Simultaneous Authentication of Equals handshake) 173
WPA-PSK 445, 446
application example 447
WPA-PSK (WiFi Protected Access-Pre-Shared Key) 173
WPS 190, 191
activate 41
example 192
limitations 194
PIN 191
push button 191
WPS button 34, 36, 39
using 41
WPS screen 179

Z

Zyxel Device
managing 27