

CHAPTER 24

VoIP Status

24.1 The VoIP Status Screen

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

Figure 160 System Monitor > VoIP Status

Information, such as whether a SIP account is registered and the total call volume made by a SIP account, can be viewed in the page.

Poll Interval(s) sec [Set Interval](#) [Stop](#)

SIP Status

Account	Register Action	Registration	Registration Time	URI	Message Waiting	Last Incoming Number	Last Outgoing Number
1	<input type="checkbox"/>	Disabled		1122334455@VoIP-provider.com	No		
2	<input type="checkbox"/>	Disabled		ChangeMe@VoIP-provider.com	No		

Call Status

Account	Duration	Status	Call Type	Codec	From Phone Port Type	To Phone Port Type	Peer Number

Phone Status

Phone	Outgoing Number	Incoming Number
Phone 1	1122334455	1122334455
Phone 2	ChangeMe	ChangeMe

The following table describes the fields in this screen.

Table 118 System Monitor > VoIP Status

LABEL	DESCRIPTION
Poll Interval(s)	Enter the number of seconds the Zyxel Device needs to wait before updating this screen and then click Set Interval . Click Stop to have the Zyxel Device stop updating this screen.
SIP Status	
Account	This column displays the index number of each SIP account that has already configured in the Zyxel Device.

Table 118 System Monitor > VoIP Status (continued)



LABEL	DESCRIPTION
Register Action	<p>The switch is grayed out and cannot be configured if the SIP account is disabled.</p> <p>If the SIP account is not registered, you can click the switch to turn it on  to have the Zyxel Device attempt to register the SIP account with the SIP server.</p> <p>If the SIP account is already registered with a SIP server, setting the switch to off  will delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name.</p>
Registration	<p>This field displays the current registration status of the SIP account.</p> <p>Registered - The SIP account is activated and has <u>been</u> registered with a SIP server. <u>You can use it to make a VoIP call.</u></p> <p>Unregistered - The <u>SIP account</u> is activated, <u>but the last time the Zyxel Device</u> tried to register the SIP account with the SIP server, the attempt failed. <u>Use the Register Action switch to register the account again.</u> The Zyxel Device will <u>also</u> automatically try to register the SIP account again after a period of time <u>that you configured</u> in VoIP > SIP > SIP Service Provider > Add/Edit > SIP Register Fail Re-Try Timer.</p> <p>Disabled - The SIP account is not active. <u>Make sure the corresponding SIP Service Provider and SIP Account are both enabled</u> for proper activation. You can activate them in VoIP > SIP > SIP Service Provider > Add/Edit and VoIP > SIP > SIP Account > Add/Edit.</p>
Registration Time	<p>This field displays the last time the Zyxel Device successfully registered the SIP account <u>with</u> the SIP server. The field is blank if the SIP has not yet successfully registered this account <u>is never successfully registered.</u></p>
URI	<p>This field displays the account number and service domain of the SIP account, which is used to identify the SIP account on the SIP server. You can change these in the VoIP > SIP > SIP Service Provider > Add/Edit > SIP Service Domain and VoIP > SIP > SIP Account > Add/Edit > SIP Account Number screens.</p>
Message Waiting	<p>This field indicates whether or not there are any new voice messages <u>in the SIP account.</u> You have to enable the MWI function in the VoIP > SIP > SIP Account > Add/Edit > Enable MWI screen, and the SIP server your VoIP service provider should also support the voice mailbox function <u>voice mail system and MWI feature.</u></p>
Last Incoming Number	<p>Regardless of the status of the incoming call to this local SIP account, this field will display the SIP account number of the remote peer at the last incoming VoIP call. This field displays the last SIP number the peer device used to call the SIP account. The field is blank if there is never an <u>incoming call for the SIP account.</u></p>
Last Outgoing Number	<p>Regardless of the status of the outgoing call, this field will display the last phone number you dialed to make an outgoing VoIP call via this SIP account. This field displays the last SIP number <u>that you called via this SIP account.</u> The field is blank if you never dialed a number using the SIP account.</p> <p>Note: <u>An outgoing number is recorded only after SIP outgoing call signaling procedure starts.</u> The dialed number is recorded in this field only during the outgoing (SIP-based) call setup signaling procedure. If you dial numbers and on hook quickly as well as making the outgoing call before the outgoing (SIP-based) call signaling procedure starts, the numbers you dial here will not be recorded.</p>
Call Status (This table displays the status of all active and ongoing calls <u>only</u> .)	
Account	<p>This field displays the SIP number used to make an Outgoing Call or receive an Incoming Call <u>through a SIP server.</u> It shows the <u>phone port number</u> for an Internal call without a SIP server.</p>
Duration	<p>This field displays how long the current call has lasted.</p> <p>Note: The time calculation starts from the beginning of the call setup signaling procedure, rather than the moment when the call is successfully established.</p>

Table 118 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
Status	<p>This field displays the current call progress or state of the phone call.</p> <p>Calling - <u>The Zyxel Device sends an INVITE request to make an Outgoing Call or Internal Call. The callee's phone is ringing.</u></p> <p>Ringing - <u>There is an Incoming call. The phone attached to the Zyxel Device's phone port associated with the SIP account is ringing.</u></p> <p>InCall - <u>There is a call in progress. Voice data is exchanged between both parties.</u></p> <p>Hold - <u>An Outgoing Call or Incoming Call is placed on hold.</u></p>
Call Type	<p>This field displays the type of the current VoIP call.</p> <p>Outgoing Call - <u>This is a call that you originated using a SIP account.</u></p> <p>Incoming Call - <u>This is a call that you received for a SIP account.</u></p> <p>Internal Call - <u>This is a VoIP call between two phone ports without a SIP server. When you have phones attached to both of the Zyxel Device's phone ports, you can dial "####" to place a call to the phone(s) connected to the other port.</u></p>
Codec	<p>This field displays what voice codec is being used for a current VoIP call through a phone port. <u>It shows Unknown when Status is Calling or Ringing (before both parties agree on a codec).</u></p>
From Phone Port Type	<p>This field displays the phone ports type used to originate the current VoIP call. <u>It shows SIP for an Incoming Call and FXS for an Outgoing Call or Internal Call.</u></p> <p>SIP—For the current call which is categorized as Incoming Call in the Call Type field, this field will show the type SIP.</p> <p>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.</p>
To Phone Port Type	<p>This field displays the phone ports type used to receive the current VoIP call. <u>It shows SIP for an Outgoing Call and FXS for an Incoming Call or Internal Call. When an Incoming Call's Status is Ringing, the phone port type is Unknown.</u></p> <p>SIP—For the current call which is categorized as Outgoing Call in the Call Type field, this field will show the type SIP.</p> <p>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.</p>
Peer Number	<p><u>This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port. It shows #### for an Internal Call.</u></p> <p>This field displays the phone Number for the Outgoing Call and Internal Call cases or the SIP account number for the Incoming Call case of the remote party that's engaged in the current VoIP call.</p>
Phone Status (This table displays the name and the SIP account binding relationship of different local phone ports. The SIP account binding relationship can be configured in VoIP > Phone > Phone Device .)	
Phone	This field displays the name of each local phone port on the Zyxel Device.
Outgoing Number	This field displays the single-SIP account number that you use to make outgoing calls on this phone port.
Incoming Number	This field displays the SIP account number that you use to receive incoming calls on this phone port.

CHAPTER 25

ARP Table

25.1 ARP Table Overview

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

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

25.1.1 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.

25.2 ARP Table Settings

Use the ARP table to view the IPv4-to-MAC address mapping(s) for ~~the client devices on the LAN or WLAN~~ for each device connected to the Zyxel Device. The neighbor table shows the IPv6-to-MAC address mapping(s) of each neighbor. To open this screen, click **System Monitor > ARP Table**.

Figure 161 System Monitor > ARP Table

ARP Table displays the IPv4 address and MAC address of each DHCP connection. Neighbour Table displays the IPv6 address and MAC address of each Neighbour.			
IPv4 ARP Table			
#	IPv4 Address	MAC Address	Device
1	192.168.1.100	dc:4a:3e:40:ec:67	br0
IPv6 Neighbour Table			
#	IPv6 Address	MAC Address	Device

The following table describes the labels in this screen.

Table 119 System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the index number of the ARP or neighbor table entry.
IPv4/IPv6 Address	This is the learned IPv4 or IPv6 IP address of a device connected to a port on the Zyxel Device .
MAC Address	This is the MAC address of the device with the listed IP address.
Device	This is the type name of the Zyxel Device's interface to which the device is connected.

CHAPTER 26

Routing Table

26.1 Routing Table Overview

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

26.2 Routing Table Settings

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

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

Figure 162 System Monitor > Routing Table

Routing Table					
Destination: The destination network or destination host. Gateway: The gateway address or *(IPv4)/:(IPv6) if none set. Subnet Mask (IPv4): The netmask for the destination net: '255.255.255.255' for a host destination and '0.0.0.0' for the default route. Flags: U - up, ! - reject, G - gateway, C - cache, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect). Metric: the distance to the target (usually counted in hops). Interface: Interface to which packets for this route will be sent.					
IPv4 Routing Table					
Destination	Gateway	Subnet Mask	Flag	Metric	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	br0
IPv6 Routing Table					
Destination	Gateway	Flag	Metric	Interface	
fe80::/64	::	U	256	eth3.0	
fe80::/64	::	U	256	br0	
::1/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::10:18ff:fe01:1/128	::	U	0	lo	
fe80::10:18ff:fe01:1/128	::	U	0	lo	
ff02::1/128	::	UC	0	br0	
ff02::16/128	::	UC	0	br0	
ff00::/8	::	U	256	eth3.0	
ff00::/8	::	U	256	br0	

The following table describes the labels in this screen.

Table 120 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.
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.

Table 120 System Monitor > Routing Table (continued)

LABEL	DESCRIPTION
Metric	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".
Interface	This indicates the name of the interface through which the route is forwarded. brx indicates a LAN interface where x can be 0~3 to represent LAN1 to LAN4 respectively. ethx indicates an Ethernet WAN interface using IPoE or in bridge mode. ppp0 indicates a WAN interface using PPPoE. wlx indicates a wireless interface where x can be 0~1. For some models, wl1 indicates 5 GHz wireless interface, and wl0 indicates 2.4 GHz wireless interface. For the other models, wl1 indicates 5 GHz wireless interface, and wl0 indicates 2.4 GHz wireless interface.

CHAPTER 27

Multicast Status

27.1 Multicast Status Overview

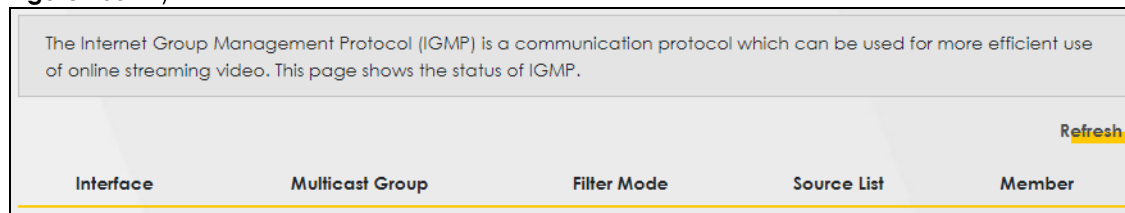
Use the **Multicast Status** screens to ~~look at view IGMP/MLD IPv4 or IPv6 multicast group information status and traffic statistics.~~

27.2 IGMP Status

Use this screen to look at the current list of [IPv4](#) multicast groups the Zyxel Device manages through IGMP. [Internet Group Multicast Protocol \(IGMP\) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. You can configure IGMP settings in Network Setting > IGMP/MLD.](#)

To open this screen, click **System Monitor > Multicast Status > IGMP Status**.

Figure 163 System Monitor > Multicast Status > IGMP Status



The following table describes the labels in this screen.

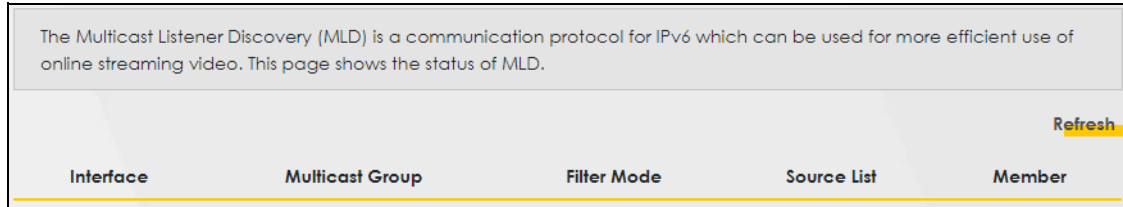
Table 121 System Monitor > Multicast Status > IGMP Status

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

27.3 MLD Status

Use this screen to look at the current list of IPv6 multicast groups the Zyxel Device manages through MLD. [Multicast Listener Discovery \(MLD\) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3. You can configure MLD settings in Network Setting > IGMP/MLD.](#) To open this screen, click **System Monitor > Multicast Status > MLD Status**.

Figure 164 System Monitor > Multicast Status > MLD Status



The following table describes the labels in this screen.

Table 122 System Monitor > Multicast Status > MLD Status

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

CHAPTER 28

WLAN Station Status

28.1 WLAN Station Status Overview

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

Figure 165 System Monitor > WLAN Station Status

The screenshot shows the 'WLAN Station Status' interface. It features a title bar, a descriptive text box, and two data tables. The first table is for 'WLAN 2.4G Station Status' and the second is for 'WLAN 5G Station Status'. Both tables have columns for '#', 'MAC Address', 'Rate (Mbps)', 'RSSI (dBm)', 'SNR', and 'Level'.

WLAN Station Status					
WLAN Station Status lists associated wireless clients.					
WLAN 2.4G Station Status					
#	MAC Address	Rate (Mbps)	RSSI (dBm)	SNR	Level
WLAN 5G Station Status					
#	MAC Address	Rate (Mbps)	RSSI (dBm)	SNR	Level

The following table describes the labels in this screen.

Table 123 System Monitor > WLAN Station Status

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Rate (Mbps)	This field displays the transmission rate of WiFi traffic between an associated wireless station and the Zyxel Device .
RSSI (dBm)	This field displays the strength of the WiFi signal between an associated wireless station and an AP. The RSSI (Received Signal Strength Indicator) field shows the WiFi signal strength of the station's wireless connection. The normal range is -30dBm to -79dBm. If the value drops below -80dBm, try moving the associated wireless station closer to the Zyxel Device to get better signal strength.

Table 123 System Monitor > WLAN Station Status

LABEL	DESCRIPTION
SNR	<p>SNR (Signal to Noise Ratio) measures the strength of the WiFi signal and the background noise on the line. <u>The Signal-to-Noise Ratio (SNR) is the ratio between the received signal power and the received noise power.</u> The greater the number, the better the quality of WiFi.</p> <p>The normal range is 15 to 40. If the value drops below 15, try moving the associated wireless station closer to the Zyxel Device to get better quality WiFi.</p>
Level	<p>This field displays a number which represents the strength of the WiFi signal between an associated wireless station and an AP <u>the Zyxel Device</u>. The Zyxel Device uses the RSSI and SNR values to determine the strength of the WiFi signal.</p> <p>5 means the Zyxel Device is receiving an excellent WiFi signal.</p> <p>4 means the Zyxel Device is receiving a very good WiFi signal.</p> <p>3 means the Zyxel Device is receiving a weak WiFi signal,</p> <p>2 means the Zyxel Device is receiving a very weak WiFi signal.</p> <p>1 means the Zyxel Device is not receiving a WiFi signal.</p>

CHAPTER 29

xPON Status

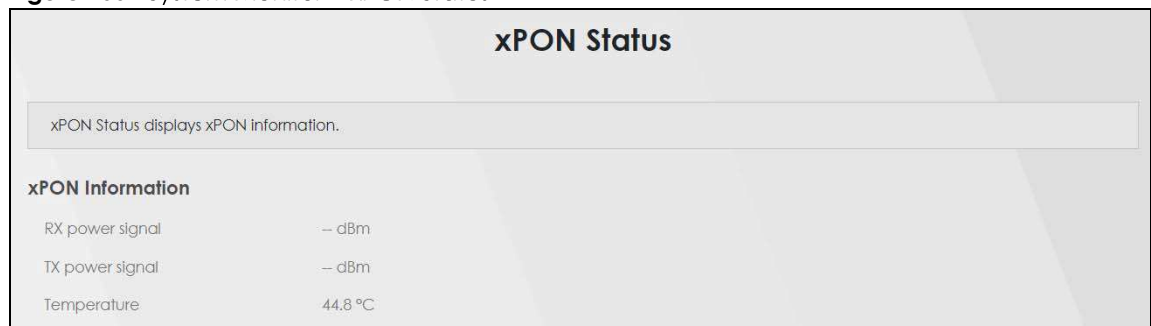
29.1 Overview

You can view the real-time optical transceiver information and operating parameters on the PON port. The parameters include, for example, transmitting and receiving power, and module temperature.

29.2 xPON Status Screen

Click **System Monitor > xPON Status** to open the following screen. Use this screen to view the current PON transceiver status.

Figure 166 System Monitor > xPON Status



The following table describes the labels in this screen.

Table 124 System Monitor > xPON Status

LABEL	DESCRIPTION
<u>xPON Information</u>	
<u>RX power signal</u>	<u>This displays the amount of power (in dBm) the PON transceiver is receiving from the fiber optic cable.</u>
<u>TX power signal</u>	<u>This displays the amount of power (in dBm) the PON transceiver is transmitting.</u>
<u>Temperature</u>	<u>This displays the temperature inside the PON transceiver in degrees Celsius.</u>

CHAPTER 30

System

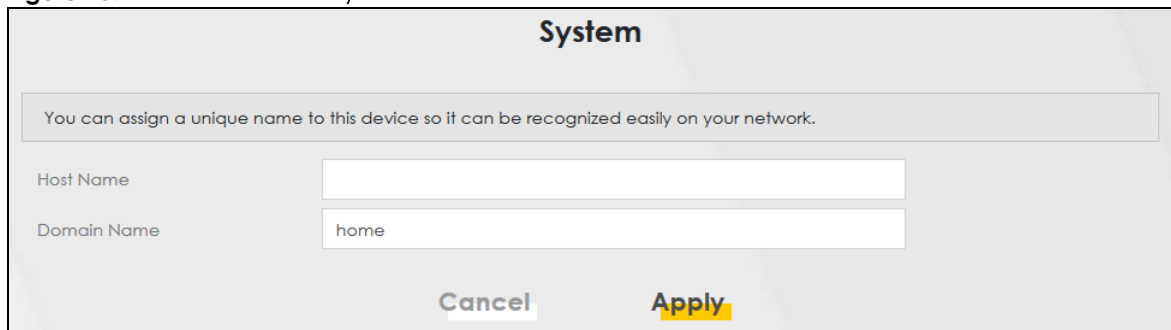
30.1 System Overview

In the **System** screen, you can name your Zyxel Device (Host) and give it an associated domain name for identification purposes.

30.2 System Settings

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

Figure 167 Maintenance > System



The screenshot shows a web interface titled "System". At the top, there is a message box that says "You can assign a unique name to this device so it can be recognized easily on your network." Below this, there are two input fields. The first is labeled "Host Name" and is currently empty. The second is labeled "Domain Name" and contains the text "home". At the bottom of the form, there are two buttons: "Cancel" and "Apply". The "Apply" button is highlighted in yellow.

The following table describes the labels in this screen.

Table 125 Maintenance > System

LABEL	DESCRIPTION
Host Name	Type a host name for your Zyxel Device. Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes.
Domain Name	Type a Domain name for your Zyxel Device.
Cancel	Click Cancel to restore your previously saved settings .
Apply	Click Apply to save your changes.

CHAPTER 31

User Account

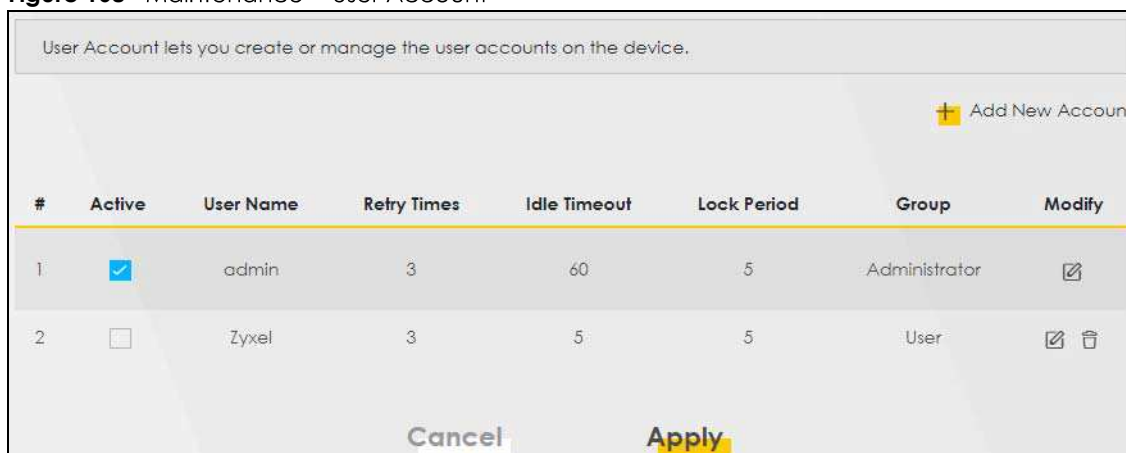
31.1 User Account Overview

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

31.2 User Account Settings

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

Figure 168 Maintenance > User Account



The following table describes the labels in this screen.

Table 126 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account.
#	This is the index number <u>of the user account</u> .
Active	This field indicates whether the user account is active or not. Clear the check box to disable the user account. Select the check box to enable it.
User Name	This field displays the name of the account used to log into the Zyxel Device web configurator.
Retry Times	This field displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	This field displays the length of inactive time before the Zyxel Device will automatically log the user out of the web configurator.

Table 126 Maintenance > User Account (continued)

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

31.2.1 User Account Add/Edit

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

Figure 169 Maintenance > User Account > Add/Edit

The following table describes the labels in this screen.

Table 127 Maintenance > User Account > Add/Edit

LABEL	DESCRIPTION
Active	Select Enable or Disable to activate or deactivate the user account.
User Name	Enter a new name for the account. This field displays the name of an existing account.
Password	Type your new system password (up to 256 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Zyxel Device.
Verify New Password	Type the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.

Table 127 Maintenance > User Account > Add/Edit (continued) (continued)

LABEL	DESCRIPTION
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 .
Group	Specify whether this user will have Administrator or User privileges.
Cancel	Click Cancel to restere your previously saved settings exit this screen without saving .
OK	Click OK to save your changes.

CHAPTER 32

Remote Management

32.1 Remote Management Overview

Use remote management to control through which interface(s), each service can access the Zyxel Device.

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

32.2 MGMT Services

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

Figure 170 Maintenance > Remote Management > MGMT Services

Remote MGMT enables various approaches to access this device remotely from a WAN and/or LAN connection.

Service Control

WAN Interface used for services: Any_WAN Multi_WAN

GPON test test2

Service	LAN/WLAN	WAN	Trust Domain	Port
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	80
HTTPS	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	443
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	21
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	23
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	22
SNMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	161
PING	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	

Cancel Apply

The following table describes the fields in this screen.

Table 128 Maintenance > Remote Management > MGMT Services

LABEL	DESCRIPTION
WAN Interface used for services	Select Any_WAN to have the Zyxel Device automatically activate the remote management service when any WAN connection is up. Select Multi_WAN and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up.
Service	This is the service you may use to access the Zyxel Device.
LAN/WLAN	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from the LAN/WLAN.
WAN	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from the trusted hosts configured in the Maintenance > Remote MGMT > Trust Domain screen. If you only want certain WAN connections to have access to the Zyxel Device using the corresponding services, then clear WAN , select Trust Domain and configure the allowed IP address(es) in the Trust Domain screen.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes back to the Zyxel Device.

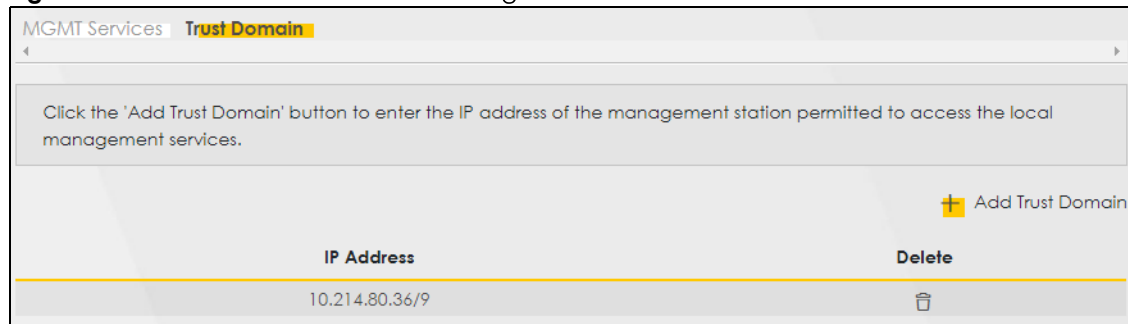
32.3 Trust Domain

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

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

Note: If specific services from the trusted hosts are allowed access but this the trust domain list is empty, all public IP addresses can access the Zyxel Device from the WAN through using the specified services.

Figure 171 Maintenance > Remote Management > Trust Domain



The following table describes the fields in this screen.

Table 129 Maintenance > Remote Management > Trust Domain

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

32.4 Add Trust Domain

Use this screen to configure a public IP address which is allowed to access the Zyxel Device. Click the **Add Trust Domain** button in the **Maintenance > Remote Management > Trust Domain** screen to open the following screen.

Figure 172 Maintenance > Remote Management > Trust Domain > Add Trust Domain

Enter the IP address of the management station permitted to access the local management services, and click 'Apply'.

IP Address [prefix length]

Cancel OK

The following table describes the fields in this screen.

Table 130 Maintenance > Remote Management > Trust Domain > Add Trust Domain

LABEL	DESCRIPTION
IP Address	Enter a public IPv4 IP address which is allowed to access the service on the Zyxel Device from the WAN. <u>You can enter an IPv4 or IPv6 address and subnet mask or prefix length.</u>
Cancel	Click Cancel to restore your previously saved settings <u>exit this screen without saving.</u>
OK	Click OK to save your changes back to the Zyxel Device.

CHAPTER 33

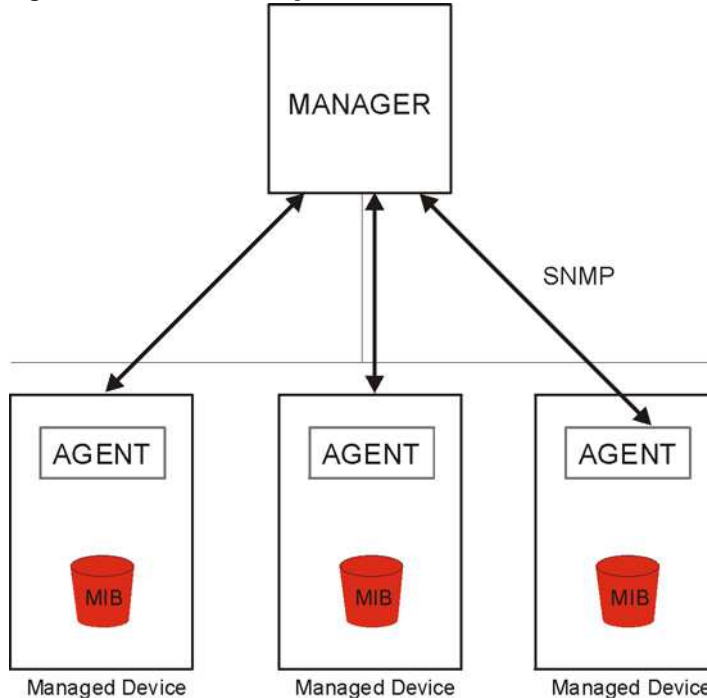
SNMP

33.1 SNMP Overview

This screen allows you to configure the SNMP settings on the Zyxel Device.

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

Figure 173 SNMP Management Model



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

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

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

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

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

Trap - Used by the agent to inform the manager of some events.

33.2 SNMP Settings

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

Configure how the Zyxel Device reports to the Network Management System (NMS) via SNMP using the screen below.

Figure 174 Maintenance > SNMP

The following table describes the fields in this screen.

Table 131 Maintenance > SNMP


LABEL	DESCRIPTION
SNMP Agent	Enable this switch to let the Zyxel Device act as an SNMP agent, which allows a manager station to manage and monitor the Zyxel Device through the network. Click on this switch to enable/disable it. When the switch goes to the right  , the function is enabled.
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station.

Table 131 Maintenance > SNMP

LABEL	DESCRIPTION
Set Community	Enter the Set Community , which is the password for the incoming Set requests from the management station.
Trap Community	Enter the Trap Community , which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
System Name	Enter the SNMP system name.
System Location	Enter the SNMP system location.
System Contact	Enter the SNMP system contact.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes back to the Zyxel Device.

CHAPTER 34

Time Settings

34.1 Time Settings Overview

This chapter shows you how to configure ~~system related settings, such as~~ the Zyxel Device's system date and time.

34.2 Time

~~To change your Zyxel Device's time and date, click **Maintenance > Time**. The screen appears as shown. 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 ~~add~~ enter a time server address, select ~~your~~ the time zone where the Zyxel Device is physically located, and configure Daylight Savings settings if ~~your location uses it~~ needed.

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

Figure 175 Maintenance > Time

In order to get a correct time for the device, fill in a time server address, select the time zone where this device is physically located, and complete the daylight saving settings if needed.

Current Date/Time

Current Time 09:21:28
Current Date 2018-04-16

Time and Date Setup

Time Protocol SNTP (RFC-1769)

First Time Server Address pool.ntp.org
Second Time Server Address clock.nyc.he.net
Third Time Server Address clock.sjc.he.net
Fourth Time Server Address None
Fifth Time Server Address None

Time Zone

Time Zone (GMT-12:00) International Date Line West

Daylight Savings

Active

Start Rule

Day 1 in
 Last Sunday in
Month April
Hour 2 : 0


End Rule

Day 1 in
 Last Sunday in
Month November
Hour 3 : 0

Cancel Apply

The following table describes the fields in this screen.

Table 132 Maintenance > Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your Zyxel Device. Each time you reload this page, the Zyxel Device synchronizes the time with the time server.
Current Date	This field displays the date of your Zyxel Device. Each time you reload this page, the Zyxel Device synchronizes the date with the time server.
Time and Date Setup	
First ~ Fifth Time Server Address	Select an NTP time server from the drop-down list box. Otherwise, select Other and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select None if you don't want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Active	Click this switch to enable or disable Daylight Saving Time. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Start Rule	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The TimeHour 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 TimeHour 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 restore your previously saved settings.
Apply	Click Apply to save your changes.

CHAPTER 35

Email Notification

35.1 Email Notification Overview

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

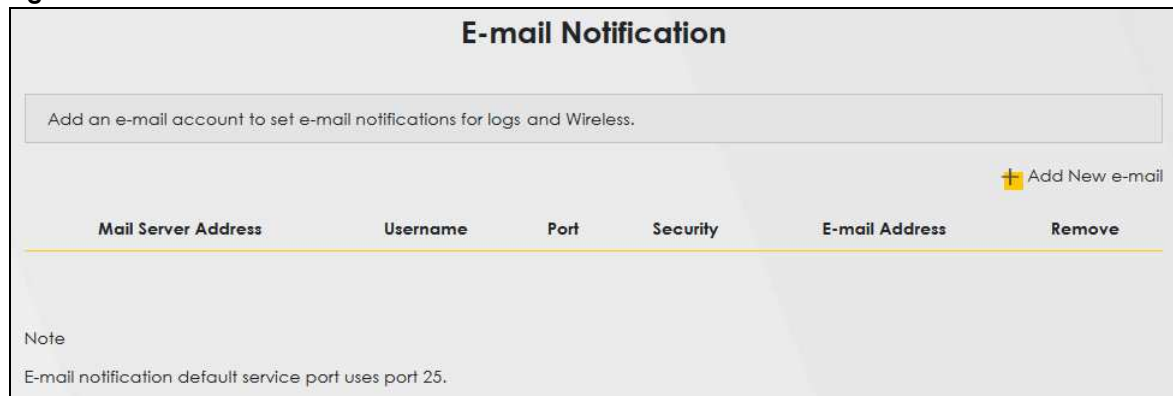
To have the Zyxel Device send reports, logs or notifications via email, you must specify an email server and the email addresses of the sender and receiver.

35.2 Email Notification Settings

Click **Maintenance > Email Notification** to open the **Email Notification** screen. Use this screen to view, remove and add Email account information on the Zyxel Device. This account can be set to receive email notifications for logs.

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

Figure 176 Maintenance > Email Notification



The following table describes the labels in this screen.

Table 133 Maintenance > Email Notification

LABEL	DESCRIPTION
Add New e-mail	Click this button to create a new entry.
Mail Server Address	This field displays the server name or the IP address of the mail server.
Username	This field displays the user name of the sender's mail account.
Port	This field displays the port number of the mail server.
Security	This field displays the protocol used for encryption.

Table 133 Maintenance > Email Notification (continued)

LABEL	DESCRIPTION
Email Address	This field displays the email address that you want to be in the from/sender line of the email that the Zyxel Device sends.
Remove	Click this button to delete the selected entry(ies) entry.

35.2.1 Email Notification Edit

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

Figure 177 Email Notification > Add

The following table describes the labels in this screen.

Table 134 Email 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 Email Address field. If this field is left blank, reports, logs or notifications will not be sent via email.
Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication Username	Enter the user name (up to 32 characters). 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 Email Address	Enter the email address that you want to be in the from/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.
Connection Security	Select SSL to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the Zyxel Device. Select STARTTLS to upgrade a plain text connection to a secure connection using SSL/TLS.

Table 134 Email Notification > Add (continued)

LABEL	DESCRIPTION
Cancel	Click this button to begin configuring this screen afresh <u>exit this screen without saving</u> .
OK	Click this button to save your changes and return to the previous screen.

CHAPTER 36

Log Setting

36.1 Logs Setting Overview

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

36.2 Log Settings

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

If you have a LAN client on your network or a remote server that is running a syslog utility, you can also save its log files by enabling **Syslog Logging**, selecting **Remote** or **Local File and Remote** in the **Mode** field, and entering the IP address of the LAN client in the **Syslog Server** field. **Remote** allows you to store logs on a syslog server, while **Local File** allows you to store them on the Zyxel Device. **Local File and Remote** means your logs are stored both on the Zyxel Device and on a syslog server.

Figure 178 Maintenance > Log Setting

Log Setting

Log Setting defines which types of logs and which log levels you want to record. If you have a LAN client on your network that is running a syslog utility, you can also save the log files there by enabling Syslog Logging and enter the IP address of that LAN client.

Syslog Setting

Syslog Logging

Mode Local File

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

UDP Port 514 (Server Port)

E-mail Log Settings

E-mail Log Settings

Mail Account Select one account

System Log Mail Subject

Security Log Mail Subject

Send Log to (E-Mail Address)

Send Alarm to (E-Mail Address)

Alarm Interval 60 (seconds)

Active Log

System Log

WAN-DHCP

DHCP Server

PPPoE

TR-069

HTTP

UPNP

System

ACL

Wireless

Security Log

Account

Attack

Firewall

MAC Filter


Cancel
Apply

The following table describes the fields in this screen.

Table 135 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Setting	
Syslog Logging	The Zyxel Device sends a log to an external syslog server. Click this switch to enable or disable to enable syslog logging. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Mode	Select the syslog destination from the drop-down list box. If you select Remote , the log(s) will be sent to a remote syslog server. If you select Local File , the log(s) will be saved in a local file. If you want to send the log(s) to a remote syslog server and save it in a local file, select Local File and Remote .
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.

Table 135 Maintenance > Log Setting (continued)

LABEL	DESCRIPTION
UDP Port	Enter the port number used by the syslog server.
Email Log Settings	
Email Log Settings	Click this switch to have the Zyxel Device send logs and alarm messages to the configured email addresses. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Mail Account	Select a mail account from which you want to send logs. You can configure mail accounts in the Maintenance > Email Notification screen.
System Log Mail Subject	Type a title that you want to be in the subject line of the system log email message that the Zyxel Device sends.
Security Log Mail Subject	Type a title that you want to be in the subject line of the security log email message that the Zyxel Device sends.
Send Log to	The Zyxel Device sends logs to the email address specified in this field. If this field is left blank, the Zyxel Device does not send logs via email.
Send Alarm to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the email address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via email.
Alarm Interval	Specify how often the alarm should be updated.
Active Log	
System Log	Select the categories of system logs that you want to record.
Security Log	Select the categories of security logs that you want to record.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

36.2.1 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 179 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 37

Firmware Upgrade

37.1 Firmware Upgrade Overview

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

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

37.2 Firmware Upgrade Settings

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

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

Figure 180 Maintenance > Firmware Upgrade

Firmware Upgrade

Firmware Upgrade is where you can update the device with newly released features by upgrading the latest firmware. You can download the latest firmware file from the manufacturer website of this device.

Upgrade Firmware

Restore Default Settings After Firmware Upgrade

Current Firmware Version: V5.15(ABQX.0)b3_0618

File Path No file selected.

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

Table 136 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Select the check box to have the Zyxel Device automatically reset itself after the new firmware is uploaded.
Current Firmware Version	This is the present Firmware version and the date created.

Table 136 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
File Path	Type the location of the file you want to upload in this field or click Browse to find it.
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 two minutes.

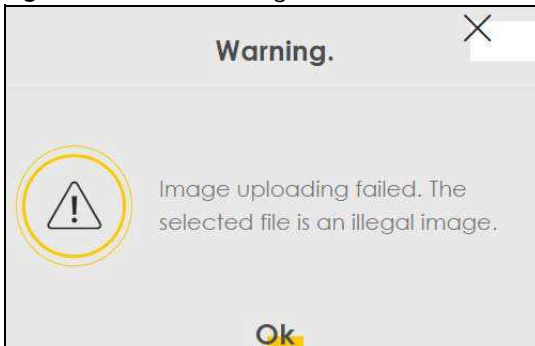
Figure 181 Firmware Uploading



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

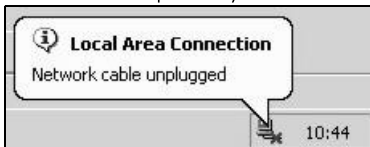
If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 182 Error Message



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

Network Temporarily Disconnected



CHAPTER 38

Backup Restore

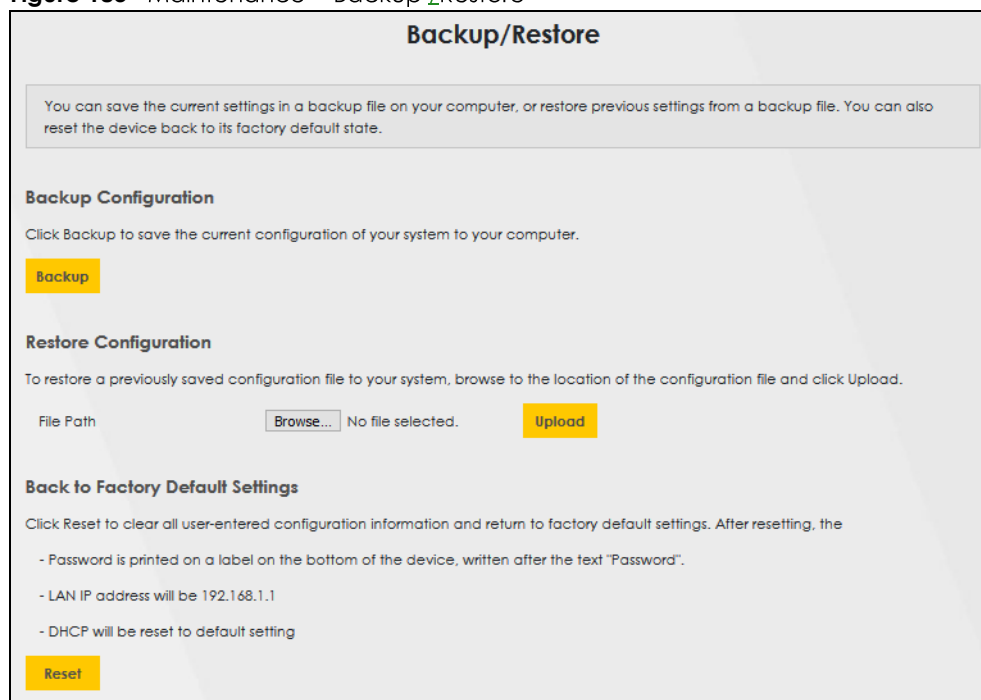
38.1 Backup/Restore Overview

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

38.2 Backup/Restore Settings

Click **Maintenance > Backup/Restore**. Information related to factory default settings and backup configuration are shown in this screen. You can also use this to restore previous device configurations.

Figure 183 Maintenance > Backup/Restore



The screenshot shows the 'Backup/Restore' web interface. At the top, there is a title 'Backup/Restore' and a descriptive paragraph: 'You can save the current settings in a backup file on your computer, or restore previous settings from a backup file. You can also reset the device back to its factory default state.' Below this, there are three main sections: 'Backup Configuration' with a 'Backup' button; 'Restore Configuration' with a 'File Path' field, a 'Browse...' button, 'No file selected.' text, and an 'Upload' button; and 'Back to Factory Default Settings' with a 'Reset' button and a list of default settings: '- Password is printed on a label on the bottom of the device, written after the text "Password".', '- LAN IP address will be 192.168.1.1', and '- DHCP will be reset to default setting'.

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 137 Restore Configuration

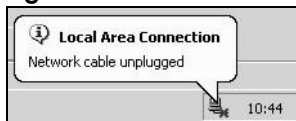
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload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

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

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

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

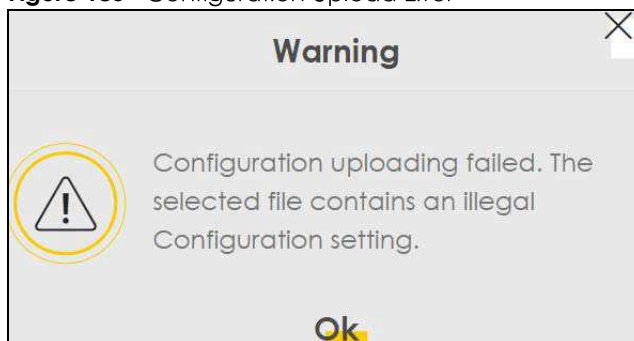
Figure 184 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

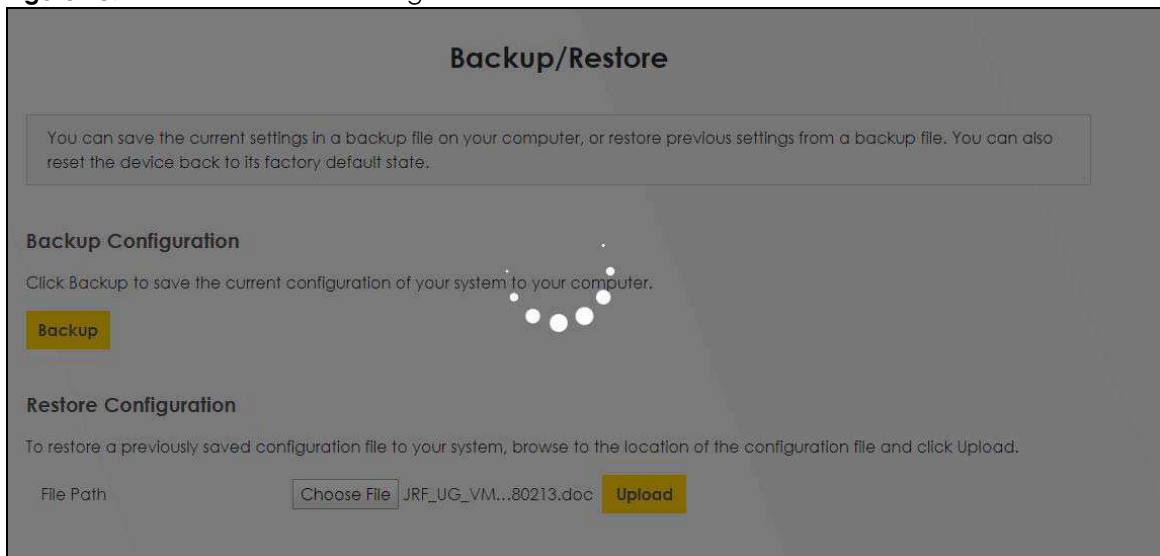
If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Configuration Backup/Restore** screen.

Figure 185 Configuration Upload Error



Reset to Factory Defaults

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

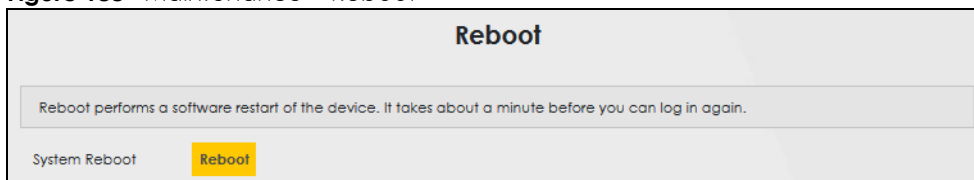
Figure 186 Reset Warning Message**Figure 187** Reset In Process Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your Zyxel Device. Refer to [Section 1.5.4 on page 23](#) for more information on the **RESET** button.

38.3 Reboot

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

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

Figure 188 Maintenance > Reboot

CHAPTER 39

Diagnostic

39.1 Diagnostic Overview

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

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

39.1.1 What You Can Do in this Chapter

- The **Ping & TraceRoute & Nslookup Diagnostic** screen lets you ping an IP address or trace the route packets take to a host (Section 39.3 on page 304).
- The **802.1ag** screen lets you perform CFM actions (Section on page 307).
- The **802.3ah** screen lets you configure link OAM port parameters (Section 39.5 on page 306).

39.2 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.

39.3 ~~Ping & TraceRoute & Nslookup~~ Diagnostic Screen

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

Figure 189 Maintenance > Diagnostic > ~~Ping&TraceRoute&Nslookup~~

Ping and TraceRoute are network utilities used to test whether a particular host is reachable. Enter either an IP address or a host name and click one of the buttons to start a Ping or TraceRoute test. The test result will be shown in the Info area.

Ping/TraceRoute Test

TCP/IP

Address

Ping Ping 6 Trace Route Trace Route 6 Nslookup

The following table describes the fields in this screen.

Table 138 Maintenance > Diagnostic > ~~Ping & TraceRoute & Nslookup~~

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

39.4 ~~802.1ag (CFM)~~

Click **Maintenance > Diagnostic > ~~802.1ag~~** to open the following screen. Use this screen to configure and perform Connectivity Fault Management (CFM) actions as defined by the IEEE 802.1ag standard. CFM protocols include Continuity Check Protocol (CCP), Link Trace (LT), and Loopback (LB).

Figure 190 Maintenance > Diagnostic > 802.1ag

The following table describes the fields in this screen.

Table 139 Maintenance > Diagnostic > 802.1ag



LABEL	DESCRIPTION
802.1ag Connectivity Fault Management	
IEEE 802.1ag-CFM	Click this switch to enable or disable the IEEE802.1ag CFM specification, which allows network administrators to identify and manage connection faults. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Y.1731	Click this switch to enable or disable Y.1731, which monitors Ethernet performance. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Interface	Select the interface on which you want to enable the IEEE 802.1ag CFM.
Maintenance Domain (MD) Level	Select a level (0-7) under which you want to create an MA.
MD Name	Enter a descriptive name for the MD (Maintenance Domain). This field only appears if the Y.1731 field is disabled.

Table 139 Maintenance > Diagnostic > 802.1ag (continued)

LABEL	DESCRIPTION
MA ID	Enter a descriptive name to identify the Maintenance Association. This field only appears if the Y.1731 field is disabled.
MEG ID	Enter a descriptive name to identify the ????. This field only appears if the Y.1731 field is enabled.
802.1Q-VLAN ID	Type a VLAN ID (1-4094) for this MA.
Local MEP ID	Enter the local Maintenance Endpoint Identifier (1-8191).
CCM	Select Enable to continue sending MEP information by CCM (Connectivity Check Messages). When CCMs are received the Zyxel Device will always process it, whether CCM is enabled or not.
Remote MEP ID	Enter the remote Maintenance Endpoint Identifier (1-8191).
Test the connection to another Maintenance End Point (MEP)	
Destination-MAC Address	Enter the target device's MAC address to which the Zyxel Device performs a CFM loopback and linktrace test.
Test Result	
Loopback-Message (LBM)	This shows Pass if a Loop-Back Messages (LBMs) responses are received. If LBMs do not get a response it shows Fail .
Linktrace-Message (LTM)	This shows the MAC address of MEPs that respond to the LTMs.
Apply	Click this button to save your changes.
Send Loopback	Click this button to have the selected MEP send the LBM (Loop-Back Message) to a specified remote end point.
Send Linktrace	Click this button to have the selected MEP send the LTMs (Link-Trace Messages) to a specified remote end point.

39.5 802.3ah (OAM)

Click **Maintenance > Diagnostic > 802.3ah** to open the following screen. Link layer Ethernet OAM (Operations, Administration and Maintenance) as described in IEEE 802.3ah is a link monitoring protocol. It utilizes OAM Protocol Data Units (OAM-PDU's) to transmit link status information between directly connected Ethernet devices. Both devices must support IEEE 802.3ah.

Figure 191 Maintenance > Diagnostic > 802.3ah

IEEE 802.3ah Configuration

IEEE 802.3ah Ethernet OAM

Interface: eth4

OAM ID: 0



Auto Event:

Features: Variable Retrieval Link Events Remote Loopback Active Mode

Apply

The following table describes the labels in this screen:

Table 140 Maintenance > Diagnostics > 802.3ah

LABEL	DESCRIPTION
IEEE 802.3ah Ethernet OAM	Click this switch to enable or disable the Ethernet OAM on the specified interface. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Interface	Select the interface on which you want to enable the IEEE802.3ah.
OAM ID	Enter a positive integer to identify this node.
Auto Event	Click this switch to detect link status and send a notification when an error (such as errors in symbol, frames, or seconds) is detected. Otherwise, disable this and you will not be notified. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Features	<p>Select Variable Retrieval so the Zyxel Device can respond to requests for information, such as requests for Ethernet counters and statistics, about link events.</p> <p>Select Link Events so the Zyxel Device can interpret link events, such as link fault and dying asp. Link events are set in event notification PDUs (Protocol Data Units), and indicate when the number of errors in a certain given interval (time, number of frames, number of symbols, or number of error frame seconds) exceeds a specified threshold. Organizations may create organization-specific link event TLVs as well.</p> <p>Select Remote Loopback so the Zyxel Device can accept loopback control PDUs to convert Zyxel Device into loopback mode.</p> <p>Select Active Mode so the Zyxel Device initiates OAM discovery, send information PDUs; and may send event notification PDUs, variable request/response PDUs, or loopback control PDUs.</p>
Apply	Click this button to save your changes.