

# CHAPTER 22

## ARP Table

### 22.1 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.

#### 22.1.1 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.

## 22.2 ARP Table Settings

The ARP Table displays the IPv4 address and MAC address of each DHCP connection. The Neighbour Table displays the IPv6 address and MAC address of a device in the same IP domain. To open this screen, click **System Monitor > ARP Table**.

**Figure 142** 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 100 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 a port.
MAC Address	This is the MAC address of the device with the listed IP address.
Device	This is the type of interface used by the device. You can click on the device type to go to its configuration screen.
<a href="#">IPv6 Neighbour Table</a>	<a href="#">This is the IPv6 address and MAC address of a device in the same IP domain.</a>

# CHAPTER 23

## Routing Table

### 23.1 Routing Table Overview

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

### 23.2 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 143** 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 101 System Monitor &gt; 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. <b>U-Up:</b> The route is up. <b>!-Reject:</b> The route is blocked and will force a route lookup to fail. <b>G-Gateway:</b> The route uses a gateway to forward traffic. <b>H-Host:</b> The target of the route is a host. <b>R-Reinstate:</b> The route is reinstated for dynamic routing. <b>D-Dynamic (redirect):</b> The route is dynamically installed by a routing daemon or redirect. <b>M-Modified (redirect):</b> The route is modified from a routing daemon or redirect.

Table 101 System Monitor &gt; 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.  <b>brx</b> indicates a LAN interface where x can be 0~3 to represent LAN1 to LAN4 respectively.  <b>ethx</b> indicates an Ethernet WAN interface using IPoE or in bridge mode.  <b>ppp0</b> indicates a WAN interface using PPPoE.  <b>wlx</b> indicates a wireless interface where x can be 0~1. For some models, <b>wl1</b> indicates 5 GHz wireless interface, and <b>wl0</b> indicates 2.4 GHz wireless interface. For the other models, <b>wl1</b> indicates 5 GHz wireless interface, and <b>wl0</b> indicates 2.4 GHz wireless interface.

# CHAPTER 24

## Multicast Status

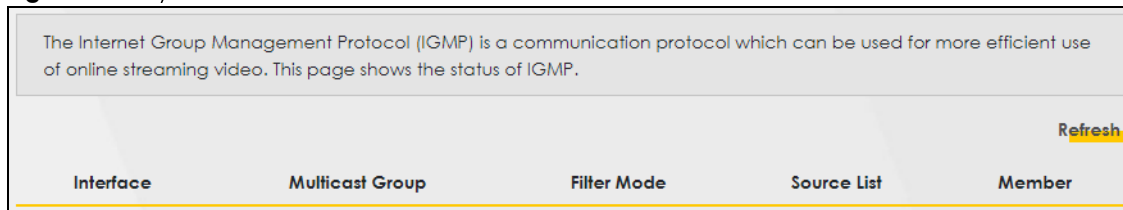
### 24.1 Multicast Status Overview

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

### 24.2 IGMP Status

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 144** System Monitor > Multicast Status > IGMP Status



The following table describes the labels in this screen.

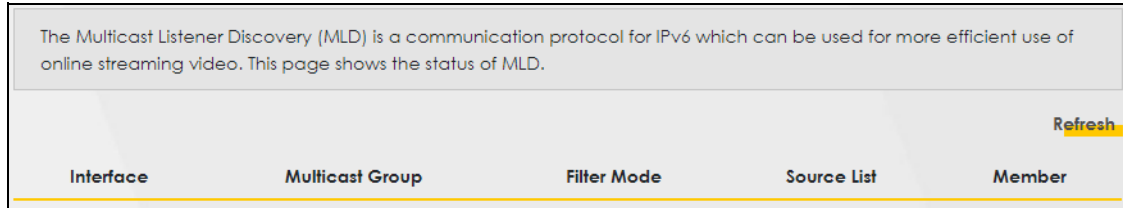
Table 102 System Monitor > Multicast Status > IGMP Status

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	<b>INCLUDE</b> means that only the IP addresses in the <b>Source List</b> get to receive the multicast group's traffic. <b>EXCLUDE</b> means that the IP addresses in the <b>Source List</b> 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.

## 24.3 MLD Status

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 145** System Monitor > Multicast Status > MLD Status



The following table describes the labels in this screen.

Table 103 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	<b>INCLUDE</b> means that only the IP addresses in the <b>Source List</b> get to receive the multicast group's traffic. <b>EXCLUDE</b> means that the IP addresses in the <b>Source List</b> 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 25

## xDSL Statistics

### 25.1 xDSL Statistics

Use this screen to view detailed **DSL statistics**. Click **System Monitor > xDSL Statistics** to open the following screen.

**Figure 146** System Monitor > xDSL Statistics

**xDSL Statistics**

xDSL Statistics displays the DSL information.

**Monitor**

Refresh Interval: No Refresh

Line: Line 0

**Status**

```
=====
+-----+
xDSL Training Status: Idle
Mode: G.DMT
Traffic Type: Inactive
Link Uptime: N/A
=====
xDSL Port Details      Upstream      Downstream
Line Rate: 0.000 Mbps  0.000 Mbps
Actual Net Data Rate: 0.000 Mbps  0.000 Mbps
Trellis Coding: N/A    N/A
SNR Margin: 0.0 dB    0.0 dB
Actual Delay: 0 ms    0 ms
Transmit Power: 0.0 dBm  0.0 dBm
Receive Power: 0.0 dBm  0.0 dBm
Actual INP: 0.0 symbols  0.0 symbols
Attainable Net Data Rate: 0.000 Mbps  0.000 Mbps
=====
xDSL Counters
Downstream      Upstream
Since Link time = 0 sec
FEC: 0          0
CRC: 0          0
ES: 0          0
SES: 0          0
UAS: 101467    0
LOS: 0          0
LOF: 0          0
LOM: 0          0
Retr: 0
FastRetr: 0
FailedRetr: 0
FailedFastRetr: 0
```



The following table describes the labels in this screen.

Table 104 Status &gt; xDSL Statistics

LABEL	DESCRIPTION
Refresh Interval	Select the time interval for refreshing statistics.
Line	Select which DSL line's statistics you want to display.
xDSL Training Status	This displays the current state of setting up the DSL connection.
Mode	This displays the ITU standard used for this connection.
Traffic Type	This displays the type of traffic the DSL port is sending and receiving. <b>Inactive</b> displays if the DSL port is not currently sending or receiving traffic.
Link Uptime	This displays how long the port has been running (or connected) since the last time it was started.
xDSL Port Details	
Upstream	These are the statistics for the traffic direction going out from the port to the service provider.
Downstream	These are the statistics for the traffic direction coming into the port from the service provider.
Line Rate	These are the data transfer rates at which the port is sending and receiving data.
Actual Net Data Rate	These are the rates at which the port is sending and receiving the payload data without transport layer protocol headers and traffic.
Trellis Coding	This displays whether or not the port is using Trellis coding for traffic it is sending and receiving. Trellis coding helps to reduce the noise in ADSL transmissions. Trellis may reduce throughput but it makes the connection more stable.
SNR Margin	This is the upstream and downstream Signal-to-Noise Ratio margin (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the system still being able to meet its transmission targets.
Actual Delay	This is the upstream and downstream interleave delay. It is the wait (in milliseconds) that determines the size of a single block of data to be interleaved (assembled) and then transmitted. Interleave delay is used when transmission error correction (Reed-Solomon) is necessary due to a less than ideal telephone line. The bigger the delay, the bigger the data block size, allowing better error correction to be performed.
Transmit Power	This is the upstream and downstream far end actual aggregate transmit power (in dBm). Upstream is how much power the port is using to transmit to the service provider. Downstream is how much power the service provider is using to transmit to the port.
Receive Power	Upstream is how much power the service provider is receiving from the port. Downstream is how much power the port is receiving from the service provider.
Actual INP	Sudden spikes in the line's level of external noise (impulse noise) can cause errors and result in lost packets. This could especially impact the quality of multimedia traffic such as voice or video. Impulse noise protection (INP) provides a buffer to allow for correction of errors caused by error correction to deal with this. The number of DMT (Discrete Multi-Tone) symbols shows the level of impulse noise protection for the upstream and downstream traffic. A higher symbol value provides higher error correction capability, but it causes overhead and higher delay which may increase error rates in received multimedia data.
Attainable Net Data Rate	These are the highest theoretically possible transfer rates at which the port could send and receive payload data without transport layer protocol headers and traffic.
xDSL Counters	
Downstream	These are the statistics for the traffic direction coming into the port from the service provider.
Upstream	These are the statistics for the traffic direction going out from the port to the service provider.
FEC	This is the number of Far End Corrected blocks.
CRC	This is the number of Cyclic Redundancy Checks.

Table 104 Status &gt; xDSL Statistics (continued)

<b>LABEL</b>	<b>DESCRIPTION</b>
ES	This is the number of Errored Seconds meaning the number of seconds containing at least one errored block or at least one defect.
SES	This is the number of Severely Errored Seconds meaning the number of seconds containing 30% or more errored blocks or at least one defect. This is a subset of ES.
UAS	This is the number of UnAvailable Seconds.
LOS	This is the number of Loss Of Signal seconds.
LOF	This is the number of Loss Of Frame seconds.
LOM	This is the number of Loss of Margin seconds.
Retr	This is the number of DSL retraining count in BRCM DSL driver.
HostInitRetr	This is the number of the retraining counts the host initiated.
FailedRetr	This is the number of failed retraining counts.

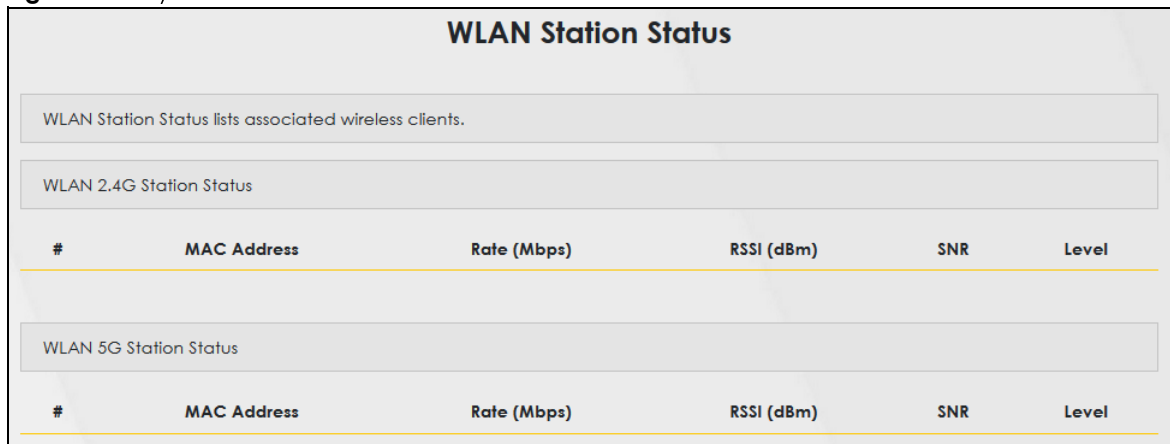
# CHAPTER 26

## WLAN Station Status

### 26.1 WLAN Station Status Overview

Click **System Monitor > WLAN Station Status** to open the following screen. View the wireless stations that are currently associated to the Zyxel Device. Being associated means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel, and security settings.

**Figure 147** 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'.

The following table describes the labels in this screen.

Table 105 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 the WiFi traffic between an associated wireless station and an AP.
RSSI (dBm)	This field displays the strength of the WiFi signal between an associated wireless station and an AP.  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 105 System Monitor &gt; 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. 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. The Zyxel Device uses the RSSI and SNR values to determine the strength of the WiFi signal.</p> <p><b>5</b> means the Zyxel Device is receiving an excellent WiFi signal.</p> <p><b>4</b> means the Zyxel Device is receiving a very good WiFi signal.</p> <p><b>3</b> means the Zyxel Device is receiving a weak WiFi signal,</p> <p><b>2</b> means the Zyxel Device is receiving a very weak WiFi signal.</p> <p><b>1</b> means the Zyxel Device is not receiving a WiFi signal.</p>

# CHAPTER 27

## Cellular Statistics

### 27.1 Cellular Statistics Overview

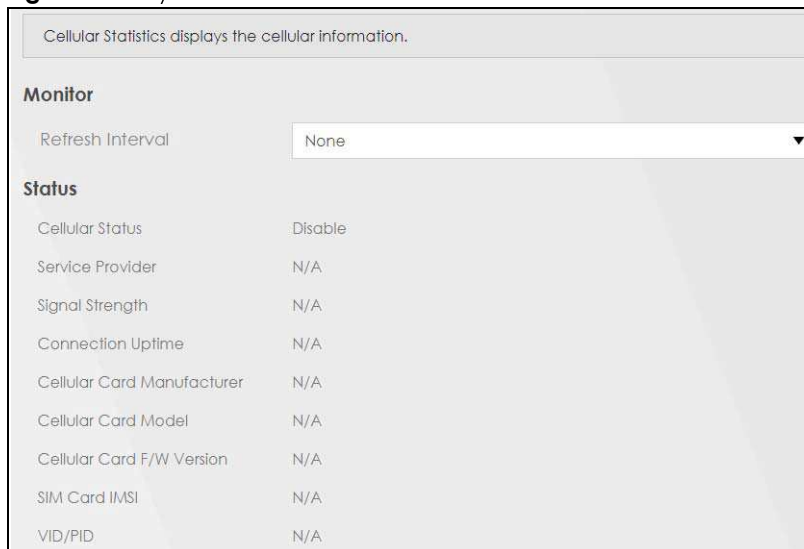
Use the **Cellular Statistics** screens to look at cellular Internet connection status. By default, a cellular WAN connection is used as a backup for the wired DSL/Ethernet WAN connections.

Note: This function is not available at the time of writing.

### 27.2 The Cellular Statistics Screen

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 148** System Monitor > Cellular Statistics



The following table describes the labels in this screen.

Table 106 System Monitor &gt; Cellular Statistics

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen. Select <b>No Refresh</b> to stop refreshing.
Cellular Status	This field displays the status of the cellular Internet connection. This field can display: <b>GSM</b> - Global System for Mobile Communications, 2G <b>GPRS</b> - General Packet Radio Service, 2.5G <b>EDGE</b> - Enhanced Data rates for GSM Evolution, 2.75G <b>WCDMA</b> - Wideband Code Division Multiple Access, 3G <b>HSDPA</b> - High-Speed Downlink Packet Access, 3.5G <b>HSUPA</b> - High-Speed Uplink Packet Access, 3.75G <b>HSPA</b> - 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 28

## System

### 28.1 System Overview

Use this screen to name your Zyxel Device and give it an associated domain name. The domain name is used to reach the Zyxel Device network from Internet, and the host name is used to reach a computer behind the Zyxel Device.

### 28.2 System Settings

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

**Figure 149** Maintenance > System

**System**

You can assign a unique name to this modem so it can be recognized easily on your network.

Host Name

Domain Name

**Cancel**      **Apply**

The following table describes the labels in this screen.

Table 107 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 host Zyxel Device.
Cancel	Click <b>Cancel</b> to abandon this screen without saving.
Apply	Click <b>Apply</b> to save your changes.

# CHAPTER 29

## User Account

### 29.1 User Account Overview

Use this screen to view, edit and manage the settings of the **admin** and other user accounts that you used to log into the Zyxel Device.

### 29.2 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 150** Maintenance > User Account

#	Active	User Name	Retry Times	Idle Timeout	Lock Period	Group	Modify
1	<input checked="" type="checkbox"/>	admin	3	60	5	Administrator	
2	<input type="checkbox"/>	Zyxel	3	5	5	User	

The following table describes the labels in this screen.

Table 108 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account.
#	This is the index number.
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.



Table 108 Maintenance &gt; User Account (continued)

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

## 29.2.1 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 151 Maintenance &gt; User Account &gt; Add/Edit

The following table describes the labels in this screen.

Table 109 Maintenance &gt; User Account &gt; Add/Edit

LABEL	DESCRIPTION
Active	Select <b>Enable</b> or <b>Disable</b> to activate or deactivate the user account.
User Name	<u>Enter a new name for the account. (The <b>User Name</b> must contain 1 to 15 characters, including 0 to 9, a to z, or !@#%*()- +=~.,{}[]?;\. Spaces are not allowed.)</u>
Password	Type your new system password. <u>The <b>Password</b> must contain 1 to 64 characters, including 0 to 9, a to z, or !@#%*()- +=~.,{}[]?;\.</u> 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.

Table 109 Maintenance &gt; User Account &gt; Add/Edit (continued) (continued)

LABEL	DESCRIPTION
Verify New Password	Type the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	Enter the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in <b>Retry Times</b> .
Group	<p>Specify whether this user will have <b>Administrator</b> or <b>User</b> privileges.</p> <p><u>Administrator additional privileges:</u></p> <ul style="list-style-type: none"> <li>• <u>System screens</u></li> <li>• <u>Network Settings screens</u></li> <li>• <u>Security screens</u></li> <li>• <u>Create User and Administrator accounts</u></li> </ul>
Cancel	Click <b>Cancel</b> to restore your previously saved settings.
OK	Click <b>OK</b> to save your changes.

# CHAPTER 30

## Remote Management

### 30.1 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.

### 30.2 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 152** Maintenance > Remote Management > MGMT Services

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	

The following table describes the fields in this screen.

Table 110 Maintenance > Remote Management > MGMT Services

LABEL	DESCRIPTION
WAN Interface used for services	Select <b>Any_WAN</b> to have the Zyxel Device automatically activate the remote management service when any WAN connection is up.  Select <b>Multi_WAN</b> 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.  <a href="#">For other field options, see Appendix C on page 305</a>
Service	This is the service you may use to access the Zyxel Device.  <a href="#">For the field options, see Appendix C on page 305.</a>
LAN/WLAN	Select the <b>Enable</b> check box for the corresponding services that you want to allow access to the Zyxel Device from the LAN/WLAN.
WAN	Select the <b>Enable</b> check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the <b>Enable</b> check box for the corresponding services that you want to allow access to the Zyxel Device from the trusted hosts configured in the <b>Maintenance &gt; Remote MGMT &gt; Trust Domain</b> screen.  If you only want certain WAN connections to have access to the Zyxel Device using the corresponding services, then clear <b>WAN</b> , select <b>Trust Domain</b> and configure the allowed IP address(es) in the <b>Trust Domain</b> 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 <b>Cancel</b> to restore your previously saved settings.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.

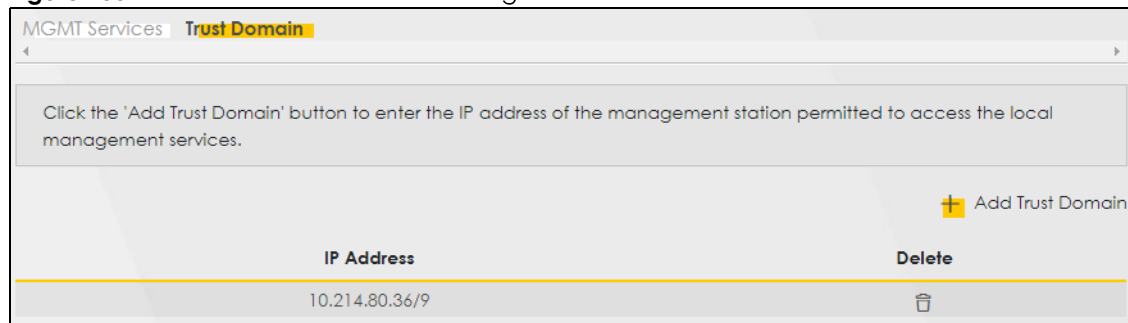
## 30.3 Trust Domain

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 this list is empty, all public IP addresses can access the Zyxel Device from the WAN through the specified services.

Figure 153 Maintenance > Remote Management > Trust Domain



The following table describes the fields in this screen.

Table 111 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 <b>Delete</b> icon to remove the trust IP address.

## 30.4 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 154 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 112 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.
OK	Click <b>OK</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

# CHAPTER 31

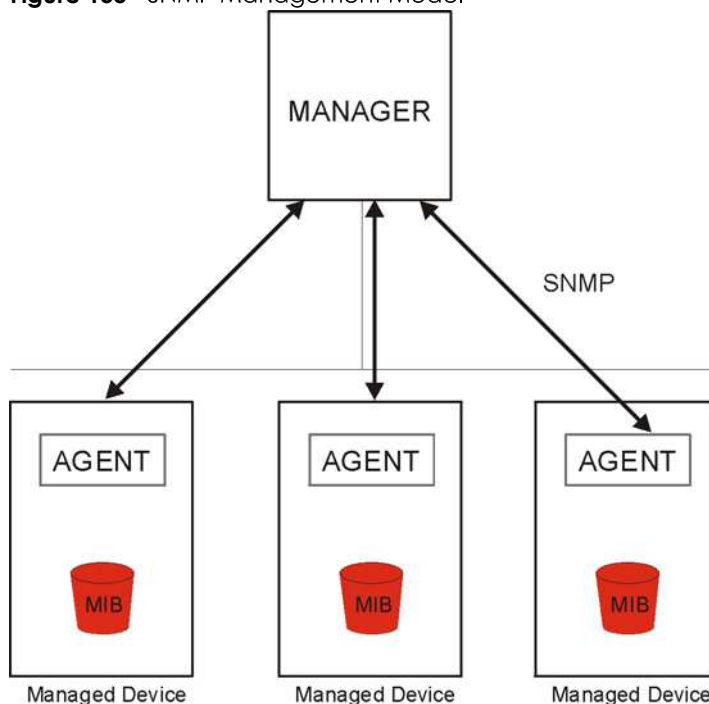
# SNMP

## 31.1 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 155** 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.

## 31.2 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 156** Maintenance > SNMP


**SNMP**

The modem supports SNMP and can be managed and monitored on a computer network, by a Network Management System (NMS). The settings below, displays the access information about how this device modem information via SNMP to the NMS.

SNMP Agent	<input checked="" type="checkbox"/>
Get Community	<input type="text" value="public"/>
Set Community	<input type="text" value="private"/>
Trap Community	<input type="text" value="public"/>
System Name	<input type="text" value="DX5510-B0"/>
System Location	<input type="text" value="Taiwan"/>
System Contact	<input type="text"/>
Trap Destination	<input type="text"/>

The following table describes the fields in this screen.

Table 113 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 <b>Get Community</b> , which is the password for the incoming Get and GetNext requests from the management station.
Set Community	Enter the <b>Set Community</b> , which is the password for the incoming Set requests from the management station.
Trap Community	Enter the <b>Trap Community</b> , 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.
Apply	Click <b>Apply</b> to save your changes back to the Zyxel Device.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.



# CHAPTER 32

## Time Settings

### 32.1 Time Settings Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

### 32.2 Time

To change your Zyxel Device's time and date, click **Maintenance > Time**. The screen appears as shown. Use this screen to configure the Zyxel Device's time based on your local time zone. You can add a time server address, select your time zone, and configure Daylight Savings if your location uses it.

Figure 157 Maintenance &gt; Time

## Time

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

**Current Date/Time**

Current Time: 03:13:59  
Current Date: 1970-01-04

**Time and Date Setup**

Time Protocol: SNTP (RFC-1769)

First Time Server Address: pool.ntp.org

Second Time Server Address: clock.nyc.he.net

Third Time Server Address: clock.sjc.he.net

Fourth Time Server Address: None

Fifth Time Server Address: None

**Time Zone**

Time Zone: (GMT+01:00) Amsterdam, Berlin, Bern, Rome

**Daylight Savings**

Active:

**Start Rule**

Day:  1  Last  Sunday

Month: March

Hour: 2 0

**End Rule**


Day:  1  Last  Sunday

Month: October

Hour: 3 0

The following table describes the fields in this screen.

Table 114 Maintenance &gt; 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 <b>Other</b> and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select <b>None</b> if you do not want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Active	Click this switch to enable or disable Daylight Saving Time. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Start Rule	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The <b>Time</b> 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 <b>Second, Sunday</b> , the month to <b>March</b> and the time to <b>2</b> in the <b>Hour</b> 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 <b>Last, Sunday</b> and the month to <b>March</b> . The time you select in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would select <b>2</b> in the <b>Hour</b> 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 <b>Time</b> 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 <b>First, Sunday</b> , the month to <b>November</b> and the time to <b>2</b> in the <b>Hour</b> 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 <b>Last, Sunday</b> , and the month to <b>October</b> . The time you select in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would select <b>2</b> in the <b>Hour</b> field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Cancel	Click <b>Cancel</b> to exit this screen without saving.
Apply	Click <b>Apply</b> to save your changes.

# CHAPTER 33

## E-mail Notification

### 33.1 E-mail Notification Overview

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

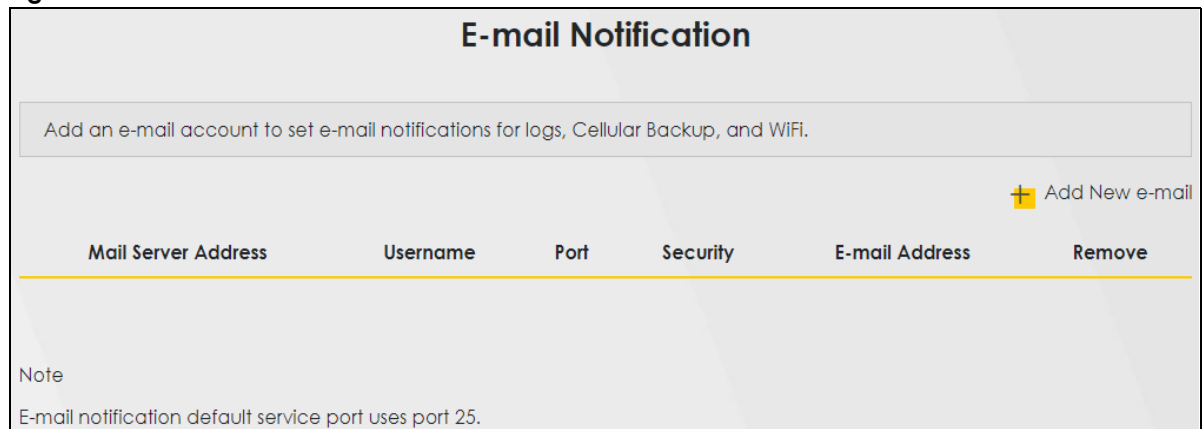
To have the Zyxel Device send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

### 33.2 E-mail Notification Settings

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

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

**Figure 158** Maintenance > E-mail Notification



The following table describes the labels in this screen.

Table 115 Maintenance > E-mail Notification

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

Table 115 Maintenance &gt; E-mail Notification (continued)

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

### 33.2.1 E-mail Notification Edit

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

Figure 159 E-mail Notification &gt; Add

The following table describes the labels in this screen.

Table 116 E-mail Notification &gt; Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the <b>Account e-mail Address</b> field.  If this field is left blank, reports, logs or notifications will not be sent via e-mail.
Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication User name	Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the <b>Account e-mail Address</b> field.
Authentication Password	Enter the password associated with the user name above.
Account e-mail Address	Enter the e-mail address that you want to be in the from/sender line of the e-mail notification that the Zyxel Device sends.  If you activate SSL/TLS authentication, the e-mail address must be able to be authenticated by the mail server as well.
Connection Security	Select <b>SSL</b> 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 <b>STARTTLS</b> to upgrade a plain text connection to a secure connection using SSL/TLS.

Table 116 E-mail Notification > Add (continued)

<b>LABEL</b>	<b>DESCRIPTION</b>
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 34

## Log Setting

### 34.1 Logs Setting Overview

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

### 34.2 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 160 Maintenance &gt; 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 117 Maintenance &gt; 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 <b>Remote</b> , the log(s) will be sent to a remote syslog server. If you select <b>Local File</b> , 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 <b>Local File and Remote</b> .
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.



Table 117 Maintenance &gt; Log Setting (continued)

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

### 34.2.1 Example E-mail Log

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

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

**Figure 161** E-mail 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 35

## Firmware Upgrade

### 35.1 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](http://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.**

### 35.2 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 162** 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

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.

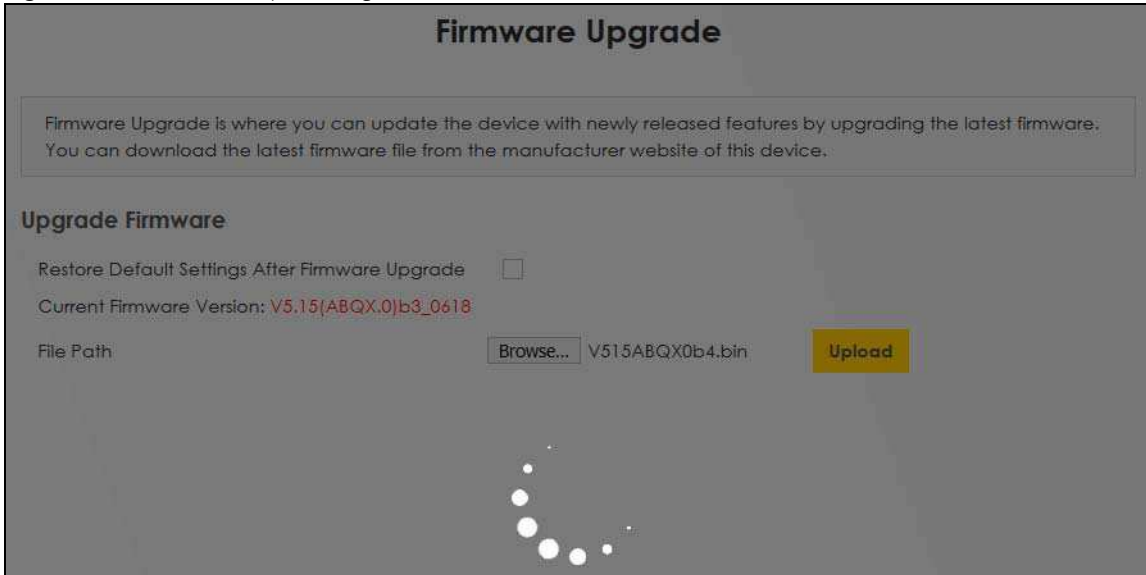
**Table 118** Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Select the check box to have the Zyxel Device automatically reset itself after the new firmware is uploaded.

Table 118 Maintenance &gt; Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type the location of the file you want to upload in this field or click <b>Browse</b> 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.

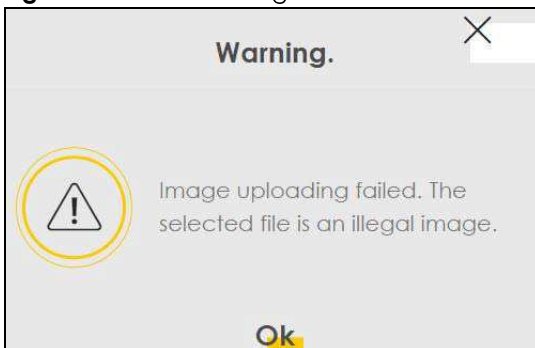
Figure 163 Firmware Uploading



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 164 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 36

## Backup/Restore

### 36.1 Backup/Restore Overview

Use this screen to backup and restore Zyxel Device configurations. You can also reset your Zyxel Device settings back to the factory defaults

### 36.2 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 165** Maintenance > Backup/Restore

**Backup/Restore**

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.

**Backup Configuration**

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

**Backup**

**Restore Configuration**

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

File Path  No file selected. **Upload**

**Back to Factory Default Settings**

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

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

**Reset**

#### 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 119 Restore Configuration

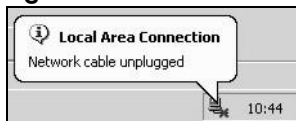
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the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

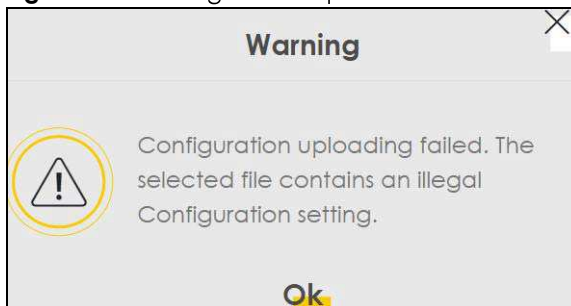
**Figure 166** Network Temporarily Disconnected



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).

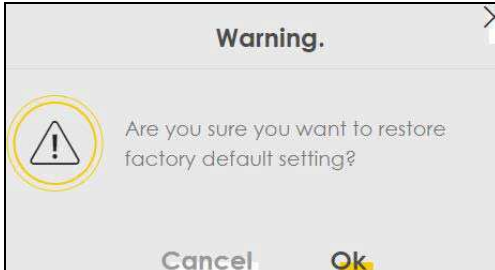
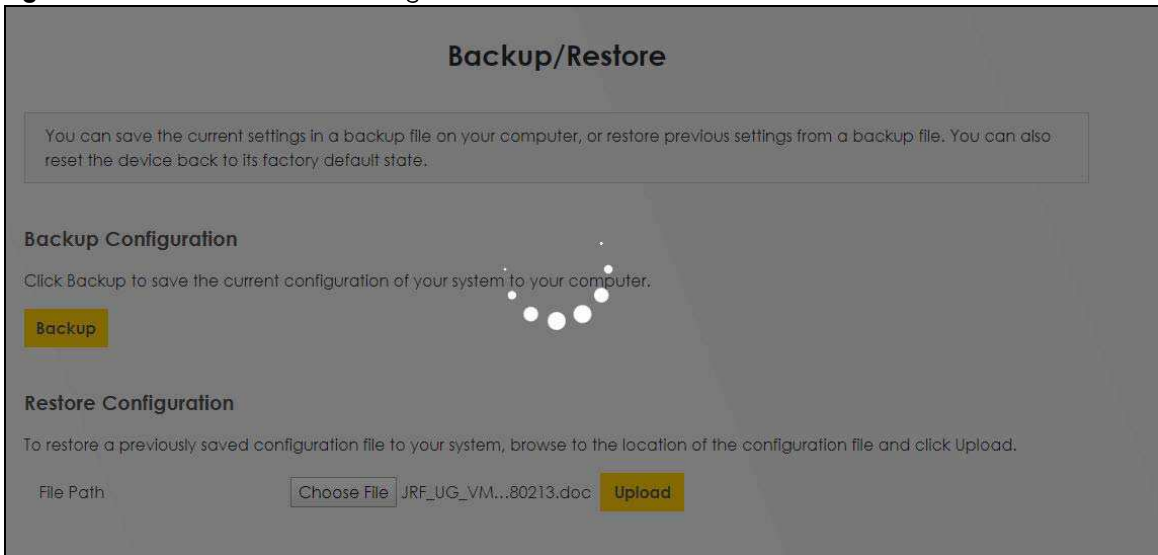
If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Configuration** screen.

**Figure 167** 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.

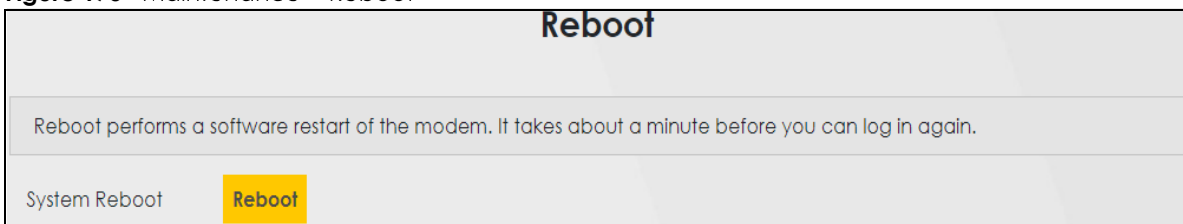
**Figure 168** Reset Warning Message**Figure 169** Reset In Process Message

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 22](#) for more information on the **RESET** button.

## 36.3 Reboot

[Use this screen to reboot the Zyxel Device remotely without turning the power off. You may need to do this if the Zyxel Device has performance issues, for example.](#)

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

**Figure 170** Maintenance > Reboot



# CHAPTER 37

# Diagnostic

## 37.1 Diagnostic Overview

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

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

### 37.1.1 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 37.3 on page 281](#)).
- The **802.1ag** screen lets you perform CFM actions ([Section 37.4 on page 281](#)).
- The **802.3ah** screen lets you configure link OAM port parameters([Section 37.5 on page 283](#)).

## 37.2 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.

## 37.3 Ping & TraceRoute & Nslookup

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

**Figure 171** 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 120 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.

## 37.4 802.1ag (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 172** Maintenance > Diagnostic > 802.1ag

IEEE 802.1ag Configuration and Link Test

### 802.1ag Connectivity Fault Management

IEEE 802.1ag CFM

Y.1731

Interface

Maintenance Domain (MD) Level

MD Name

MA ID

802.1Q VLAN ID  (1~4094); empty means no VLAN tag

Local MEP ID  (1~8191)

CCM

Remote MEP ID  (1~8191); empty means not configure Remote MEP

**Test the connection to another Maintenance End Point (MEP)**

Destination MAC Address

**Test Result**

Loopback Message (LBM)

Linktrace Message (LTM)


Apply Send Loopback Send Linktrace

The following table describes the fields in this screen.

Table 121 Maintenance &gt; Diagnostic &gt; 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 <input checked="" type="checkbox"/> , 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 <input type="checkbox"/> , 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.

Table 121 Maintenance &gt; Diagnostic &gt; 802.1ag (continued)

LABEL	DESCRIPTION
MD Name	Enter a descriptive name for the MD (Maintenance Domain). This field only appears if the <b>Y.1731</b> field is disabled.
MA ID	Enter a descriptive name to identify the Maintenance Association. This field only appears if the <b>Y.1731</b> field is disabled.
MEG ID	Enter a descriptive name to identify the Maintenance Entity Group. This field only appears if the <b>Y.1731</b> 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 <b>Enable</b> to continue sending MEP information by CCM (Connectivity Check Messages). When CCMs are received the Zyxel Device will always process it, whether <b>CCM</b> 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 <b>Pass</b> if a Loop Back Messages (LBMs) responses are received. If LBMs do not get a response it shows <b>Fail</b> .
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.

## 37.5 802.3ah (OAM)

Click **Maintenance > Diagnostic > 803.ah** to open the following screen. Link layer Ethernet OAM (Operations, Administration and Maintenance) as described in IEEE 802.3ah is a link monitoring protocol. It utilizes OAM Protocol Data Units (OAM PDU's) to transmit link status information between directly connected Ethernet devices. Both devices must support IEEE 802.3ah.

Figure 173 Maintenance &gt; Diagnostic &gt; 802.3ah

IEEE 802.3ah Configuration

IEEE 802.3ah Ethernet OAM

Interface

OAM ID



Auto Event

Features:  Variable Retrieval  Link Events  Remote Loopback  Active Mode

**Apply**

The following table describes the labels in this screen.

Table 122 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 <b>Variable Retrieval</b> so the Zyxel Device can respond to requests for information, such as requests for Ethernet counters and statistics, about link events.</p> <p>Select <b>Link Events</b> 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 <b>Remote Loopback</b> so the Zyxel Device can accept loopback control PDUs to convert Zyxel Device into loopback mode.</p> <p>Select <b>Active Mode</b> 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.