

CHAPTER 12

Dynamic DNS Setup

12.1 DNS Overview

DNS

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

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

Dynamic DNS

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

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

12.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes ([Section 12.2 on page 197](#)).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Zyxel Device ([Section 12.3 on page 198](#)).

12.1.2 What You Need To Know

DYNDNS Wildcard

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

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

12.2 DNS Entry

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

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

Figure 110 Network Setting > DNS > DNS Entry

Domain Name System(DNS) translates hostnames into IP addresses for the purpose of locating and addressing these devices worldwide. You can start by adding a new DNS entry.

+ Add New DNS Entry

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

The following table describes the fields in this screen.

Table 70 Network Setting > DNS > DNS Entry

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

12.2.1 Add/Edit DNS Entry

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

Figure 111 DNS Entry: Add/Edit

The following table describes the labels in this screen.

Table 71 DNS Entry: Add/Edit

LABEL	DESCRIPTION
Host Name	Enter the host name of the DNS entry.
IP Address	Enter the IP address of the DNS entry.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

12.3 Dynamic DNS

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

Figure 112 Network Setting > DNS > Dynamic DNS

The following table describes the fields in this screen.

Table 72 Network Setting > DNS > > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select Enable to use dynamic DNS.
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Host Name	Type the domain name assigned to your Zyxel Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Username	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable Off Line Option (Only applies to custom DNS)	Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Dynamic DNS Status	
User Authentication Result	This shows Success if the account is correctly set up with the Dynamic DNS provider account.
Last Updated Time	This shows the last time the IP address the Dynamic DNS provider has associated with the hostname was updated.
Current Dynamic IP	This shows the IP address your Dynamic DNS provider has currently associated with the hostname.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

CHAPTER 13

IGMP/MLD

13.1 IGMP/MLD Overview

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

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

13.1.1 What You Need To Know

Multicast and IGMP

See [Multicast on page 87](#) for more information.

Multicast Listener Discovery (MLD)

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

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

IGMP Fast Leave

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

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

13.2 IGMP/MLD Settings

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

Figure 113 Network Setting > IGMP/MLD

IGMP/MLD

Enter IGMP/MLD protocol configuration fields if you want modify default values shown below.

IGMP Configuration

Default Version	3
Query Interval	125
Query Response Interval	10
Last Member Query Interval	10
Robustness Value	2
Maximum Multicast Groups	25
Maximum Multicast Data Sources(for IGMPv3)	10
Maximum Multicast Groups Members	25
Fast Leave Enable	☒
LAN to LAN (Intra LAN) Multicast Enable	☒
Membership Join Immediate (IPTV)	☒

MLD Configuration

Default Version	2
Query Interval	125
Query Response Interval	10
Last Member Query Interval	10
Robustness Value	2
Maximum Multicast Groups	10
Maximum Multicast Data Sources(for mldv2)	10
Maximum Multicast Groups Members	10
Fast Leave Enable	☒
LAN to LAN (Intra LAN) Multicast Enable	☒

The following table describes the labels in this screen.

Table 73 Network Setting > IGMP/MLD

LABEL	DESCRIPTION
IGMP/MLD Configuration	
Default Version	Enter the version of IGMP (1~3) and MLD (1~2) that you want the Zyxel Device to use on the WAN.

Table 73 Network Setting > IGMP/MLD (continued)

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

CHAPTER 14

VLAN Group

14.1 Overview

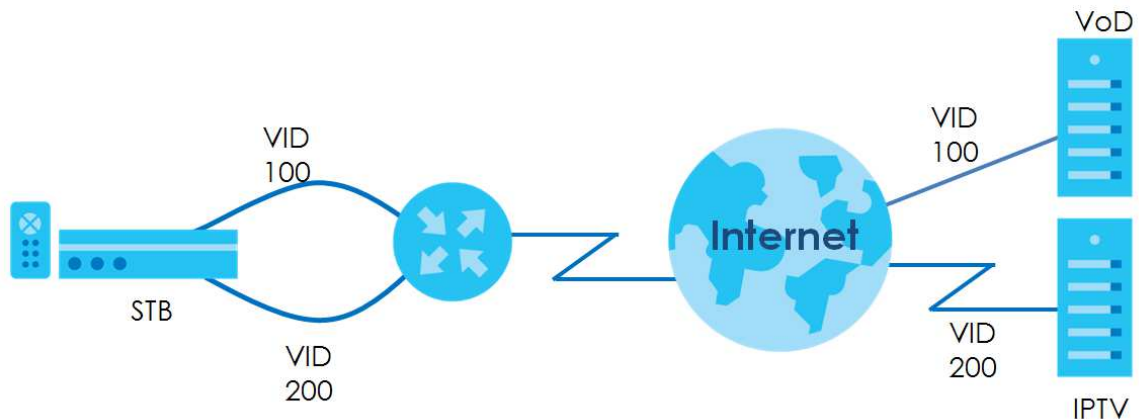
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

Ports in the same VLAN group share the same frame broadcast domain thus increase network performance through reduced broadcast traffic. Shared resources such as a server can be used by all ports in the same VLAN as the server. Ports can belong to other VLAN groups too. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network.

In the following example, VLAN IDs (VIDs) 100 and 200 are added to identify Video-on-Demand and IPTV traffic respectively coming from the VoD and IPTV multicast servers. The Zyxel Device can also tag outgoing requests to these servers with the VLAN IDs.

Figure 114 VLAN Group Example



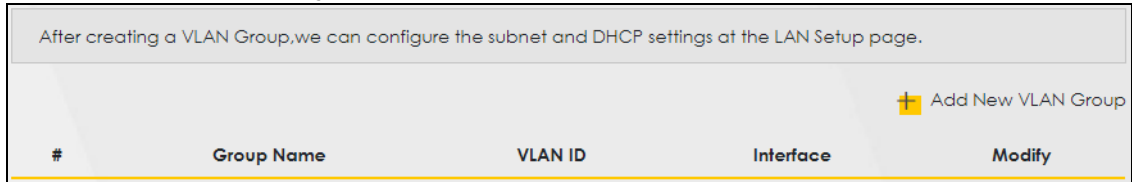
14.1.1 What You Can Do in this Chapter

Use these screens to group separate VLAN groups together to be treated as one VLAN group.

14.2 VLAN Group Settings

Add a VLAN group and/or change their basic settings in the Vlan Group screen. The subnet and DHCP settings of each group can be configured at the **LAN Setup page**. Click **Network Setting > Vlan Group** to open the following screen.

Figure 115 Network Setting > Vlan Group



The following table describes the fields in this screen.

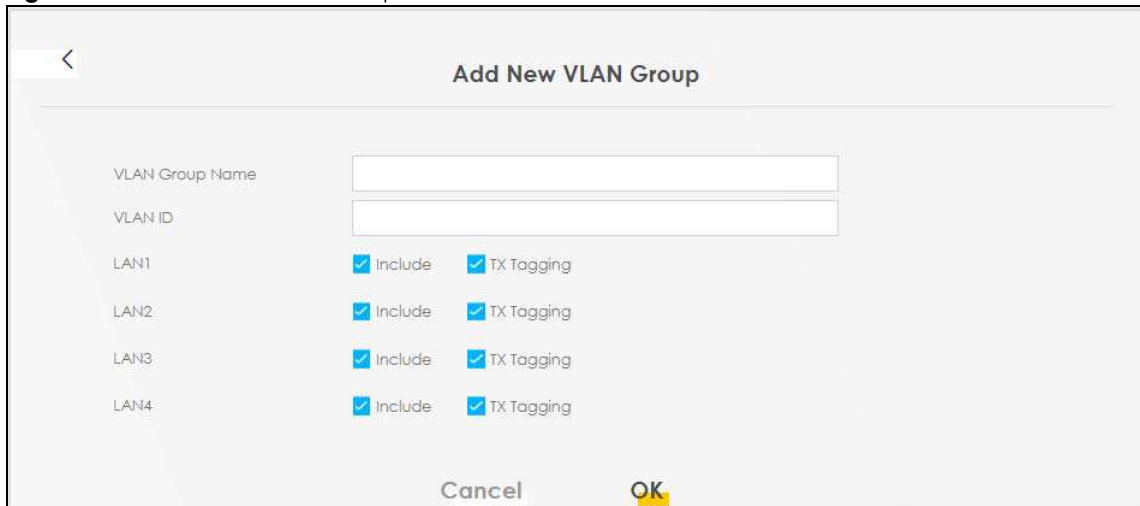
Table 74 Network Setting > Vlan Group

LABEL	DESCRIPTION
Add New VLAN Group	Click this button to create a new VLAN group.
#	This is the index number of the VLAN group.
Group Name	This shows the descriptive name of the VLAN group.
VLAN ID	This shows the unique ID number that identifies the VLAN group.
Interface	This shows the LAN ports included in the VLAN group and if traffic leaving the port will be tagged with the VLAN ID.
Modify	Click the Edit icon to change an existing VLAN group setting or click the Delete icon to remove the VLAN group.

14.2.1 Add/Edit a VLAN Group

Click the **Add New VLAN Group** button in the **Vlan Group** screen to open the following screen. Use this screen to create a new VLAN group.

Figure 116 Add/Edit VLAN Group



The following table describes the fields in this screen.

Table 75 Add/Edit VLAN Group

LABEL	DESCRIPTION
VLAN Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
VLAN ID	Enter a unique ID number, from 1 to 4,094, to identify this VLAN group. Outgoing traffic is tagged with this ID if TX Tagging is selected below.
LAN	Select Include to add the associated LAN interface to this VLAN group. Note: Select TX Tagging to tag outgoing traffic from the associated LAN port with the VLAN ID number entered above.
Apply	Click Apply to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

CHAPTER 15

Interface Grouping

15.1 Interface Grouping Overview

By default, all LAN and WAN interfaces on the Zyxel Device are in the same group and can communicate with each other. Create interface groups to have the Zyxel Device assign IP addresses in different domains to different groups. Each group acts as an independent network on the Zyxel Device. [Devices in different groups cannot communicate with each other directly.](#)

15.1.1 What You Can Do in this Chapter

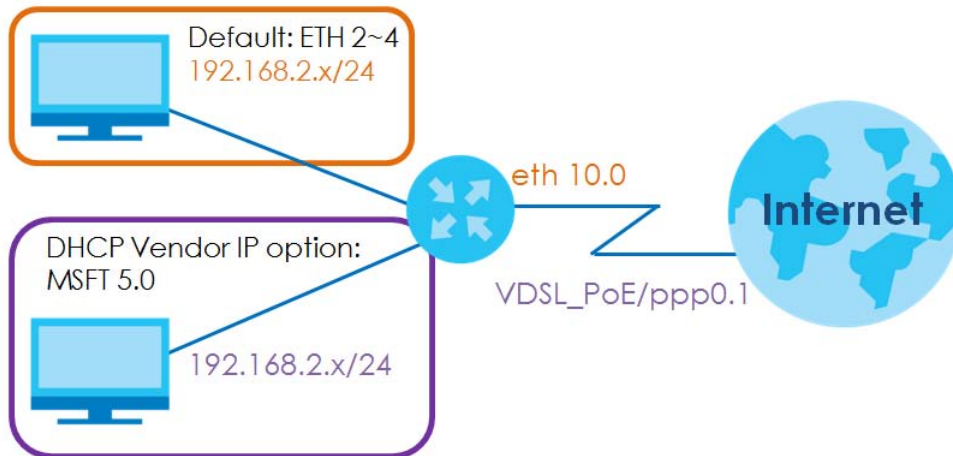
The **Interface Grouping** screens let you [map a port to a PVC or bridge group](#) on the Zyxel Device ([Section 15.2 on page 206](#)).

15.2 Interface Grouping Setup

You can manually add a LAN interface to a new group. Alternatively, you can have the Zyxel Device automatically add the incoming traffic and the LAN interface on which traffic is received to an interface group when its DHCP Vendor ID option information matches one listed for the interface group.

Use the **LAN** screen to configure the private IP addresses the DHCP server on the Zyxel Device assigns to the clients in the default and/or user-defined groups. If you set the Zyxel Device to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See [Chapter 8 on page 131](#) for more information.

In the following example, the client that sends packets with the DHCP Vendor ID option set to MSFT 5.0 (meaning it is a Windows 2000 DHCP client) is assigned the IP address 192.168.2.2 and uses the WAN VDSL_PoE/ppp0.1 interface.

Figure 117 Interface Grouping Application

You can use this screen to create new user-defined interface groups or modify existing ones. Interfaces that do not belong to any user-defined group always belong to the default group.

Click **Network Setting > Interface Grouping** to open the following screen.

Figure 118 Network Setting > Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.				
+ Add New Interface Group				
Group Name	WAN Interface	LAN Interface	Criteria	Modify
Default	Any WAN	LAN1,LAN2,LAN3,LAN4 .ZyxeL_9DE5,ZyxeL_9DE5 _guest1,ZyxeL_9DE5_gu est2,ZyxeL_9DE5_guest 3,ZyxeL_9DE5,ZyxeL_9DE 5_guest1,ZyxeL_9DE5_g uest2_5G,ZyxeL_9DE5_ guest3_5G,Zyx31@198 9816,7dd02bef35ce02 6db42a26095282ec38_		

The following table describes the fields in this screen.

Table 76 Network Setting > Interface Grouping

LABEL	DESCRIPTION
Add New Interface Group	Click this button to create a new interface group.
Group Name	This shows the descriptive name of the group.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN interfaces in the group.
Criteria	This shows the filtering criteria for the group.

Table 76 Network Setting > Interface Grouping (continued)

LABEL	DESCRIPTION
Modify	Click the Edit icon to modify an existing Interface group setting or click the Delete icon to remove the Interface group.
Add	Click this button to create a new group.

15.2.1 Interface Group Configuration

Click the **Add New Interface Group** button in the **Interface Grouping** screen to open the following screen. Use this screen to create a new interface group. If you want to automatically add LAN clients to a WAN interface in the new group, add a DHCP vendor ID string. By configuring this, any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

Note: An interface can belong to only one group at a time.

Note: After configuring a vendor ID, reboot the client device attached to the Zyxel Device to obtain an appropriate IP address.

Note: You can have up to 15 filter criteria.

Figure 119 Interface Group Configuration

Add New Interface Group

1. Enter a unique Group name.

2. If you like to automatically add LAN clients to a WAN Interface in the new group, add the DHCP vendor ID string. By configuring a DHCP vendor ID string, any DHCP client request with the specified Vendor ID (DHCP option 60), will be denied an IP address from the local DHCP server.

Group Name

WAN Interfaces used in the grouping

PTM type-

None

ATM type-

None

ETH type-

None

WWAN type-

None

Available LAN Interfaces

☐ LAN1

☐ LAN2

☐ LAN3

☐ LAN4

☐ LAN5

Selected LAN Interfaces

Automatically Add Clients With the following DHCP Vendor IDs

#

Filter Criteria

Wildcard Support

Modify

Add

Note

(1) If a Vendor ID Is configured for a specific client device, please REBOOT the client device attached to the router, to allow the client device to obtain an appropriate IP address.

(2) Total criteria rules can not add over than 15.

Cancel

OK

The following table describes the fields in this screen.

Table 77 Interface Group Configuration

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
WAN Interfaces used in the grouping	Select the WAN interface this group uses. The group can have up to one ETH interface. Select None to not add a WAN interface to this group.
Selected LAN Interfaces Available LAN Interfaces	Select one or more LAN interfaces (Ethernet LAN, HPNA or wireless LAN) in the Available LAN Interfaces list and use the left arrow to move them to the Selected LAN Interfaces list to add the interfaces to this group. To remove a LAN or wireless LAN interface from the Selected LAN Interfaces , use the right-facing arrow.
Automatically Add Clients With the following DHCP Vendor IDs	Click Add to identify LAN hosts to add to the interface group by criteria such as the type of the hardware or firmware. See Section 15.2.2 on page 210 for more information.
#	This shows the index number of the rule.
Filter Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.
Wildcard Support	This shows if wildcard on DHCP option 60 is enabled.
Modify	Click the Edit icon to change the group setting. Click the Delete icon to delete this group from the Zyxel Device.
Apply	Click Apply to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

15.2.2 Interface Grouping Criteria

Click the **Add** button in the **Interface Grouping Configuration** screen to open the following screen. Use this screen to automatically add clients to an interface group based on specified criteria. You can choose to define a group based on a MAC address, a vendor ID (DHCP option 60), an Identity Association Identifier (DHCP option 61), vendor specific information (DHCP option 125), or a VLAN group.

Figure 120 Interface Grouping Criteria

Add new criteria

Criteria

☐ Source MAC address

☐ DHCP option 60

☐ DHCP option 61

☒ DHCP option 125

☐ VLAN Group

Enterprise Number

Manufacture OUI

Serial Number

Product Class

Cancel OK

The following table describes the fields in this screen.

Table 78 Interface Grouping Criteria

LABEL	DESCRIPTION
Source MAC Address	Enter the source MAC address of the packet.
DHCP Option 60	Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
Enable wildcard	Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60.
DHCP Option 61	Select this and enter the device identity of the matched traffic.
	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.
Enterprise Number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address.
Serial Number	Enter the serial number of the device.
Product Class	Enter the product class of the device.
VLAN Group	Select this and the VLAN group of the matched traffic from the drop-down list box. A VLAN group can be configured in Network Setting > Vlan Group .
Apply	Click Apply to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

CHAPTER 16

Firewall

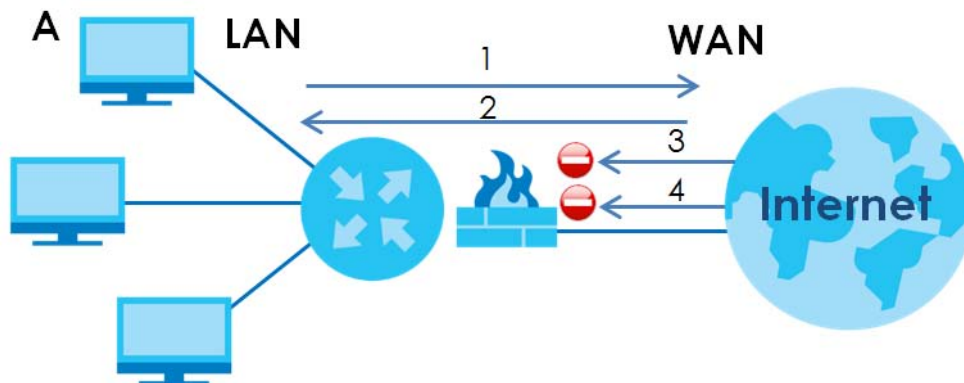
16.1 Firewall Overview

This chapter shows you how to enable and configure the Zyxel Device's security settings. Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

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

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

Figure 121 Default Firewall Action



16.1.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the Zyxel Device ([Section 16.2 on page 214](#)).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules ([Section 16.3 on page 215](#)).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules ([Section 16.4 on page 217](#)).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks ([Section 16.5 on page 220](#)).

16.1.2 What You Need to Know

SYN Attack

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

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The Zyxel Device is pre-configured to automatically detect and thwart all known DoS attacks.

DDoS

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

LAND Attack

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

Ping of Death

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

SPI

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

16.2 Firewall Settings

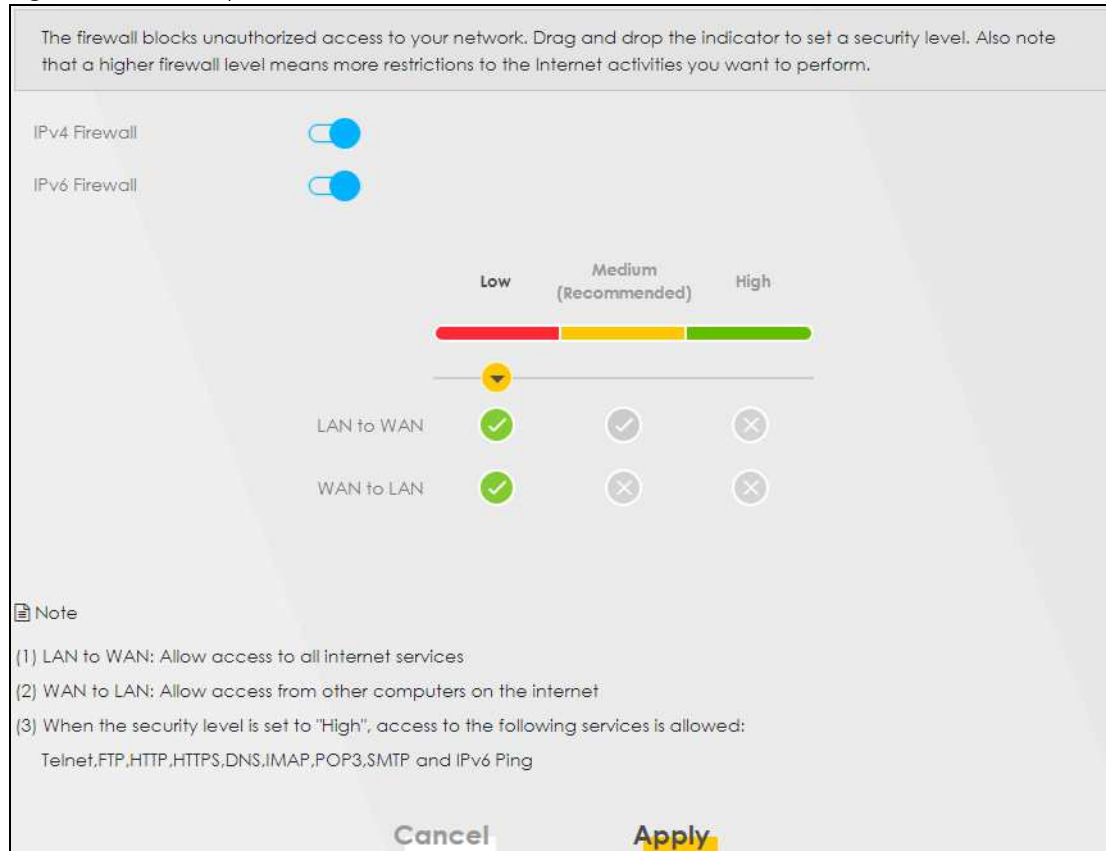
Use this screen to set the security level of the firewall on the Zyxel Device. Firewall rules are grouped based on the direction of travel of packets to which they apply. A higher firewall level means more restrictions on the Internet activities you can perform.

Note: LAN to WAN is your access to all Internet services. WAN to LAN is the access of other computers on the Internet to devices behind the Zyxel Device.

Note: When the security level is set to **High**, access to Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and IPv6 Ping are still allowed from the LAN.

Click **Security > Firewall** to display the **General** screen.

Figure 122 Security > Firewall > General



The following table describes the labels in this screen.

Table 79 Security > Firewall > General

LABEL	DESCRIPTION
Firewall	Select Enable to activate the firewall feature on the Zyxel Device.
Low	Select Low to allow LAN to WAN and WAN to LAN packet directions.
Medium	Select Medium to allow LAN to WAN but deny WAN to LAN packet directions.
High	Select High to deny LAN to WAN and WAN to LAN packet directions.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

16.3 Protocol Settings

You can configure customized services and port numbers in the **Protocol** screen. Each set of protocol rules listed in the table are reusable objects to be used in conjunction with ACL rules in the Access

Control screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See [Appendix C on page 305](#) for some examples.

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

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

Figure 123 Security > Firewall > Protocol

Each entry in the following table represents a protocol rule or a set of custom protocol rules. It is a re-usable object and should be used in conjunction with ACL Rules in Access Control.			
			 Add New Protocol Entry
Name	Description	Ports/Protocol Number	Modify
Note If a protocol rule is removed, related ACL rules will also be removed.			

The following table describes the labels in this screen.

Table 80 Security > Firewall > Protocol

LABEL	DESCRIPTION
Add New Protocol Entry	Click this to add a new service.
Name	This is the name of your customized service.
Description	This is the description of your customized service.
Ports/Protocol Number	This shows the IP protocol (TCP , UDP , ICMP , or TCP/UDP) and the port number or range of ports that defines your customized service. Other and the protocol number displays if the service uses another IP protocol.
Modify	Click the Edit icon to edit the entry. Click the Delete icon to remove this entry.

16.3.1 Add New/Edit Protocol Entry

Use this screen to add a customized service rule that you can use in the firewall's ACL rule configuration. Click **Add New Protocol Entry** or the **Edit** icon next to an existing service in the **Protocol** screen to display the following screen.

Figure 124 Protocol Entry: Add New/Edit

The following table describes the labels in this screen.

Table 81 Security > Firewall > Protocol: Add/Edit

LABEL	DESCRIPTION
Service Name	Enter a unique name (up to 32 printable English keyboard characters, including spaces) for your customized port.
Description	Enter a description for your customized port.
Protocol	Choose the IP protocol (TCP , UDP , ICMP , ICMPv6 , or Other) that defines your customized port from the drop-down list box. Select Other to be able to enter a protocol number.
Protocol Number	This field is displayed if you select Other as the protocol. Enter the protocol number of your customized port.
Source Port	This field is displayed if you select either the TCP or UDP protocol. You may set it to Any , Single , or Range and enter the Port Number or range of Port Numbers for your source port.
Destination Port	This field is displayed if you select either the TCP or UDP protocol. You may set it to Any , Single , or Range and enter the Port Number or range of Port Numbers for your destination port.
ICMPv6type	This field is displayed if you select the ICMPv6 protocol. From the drop-down menu, select which type value you would like to use.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

16.4 Access Control

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

Figure 125 Security > Firewall > Access Control

An ACL rule is a manually defined rule to accept, reject, or drop the incoming or outgoing data of your network. You may need to create at least one Protocol entry in order to add an ACL rule.

Rules Storage Space Usage %

 Add New ACL Rule

#	Name	Src IP	Dest IP	Service	Action	Modify
---	------	--------	---------	---------	--------	--------

The following table describes the labels in this screen.

Table 82 Security > Firewall > Access Control

LABEL	DESCRIPTION
Add New ACL Rule	Click this to add a filter rule for incoming or outgoing IP traffic.
#	This is the index number of the entry.
Name	This displays the name of the rule.
Src IP	This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to Any .
Dst IP	This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to Any .
Service	This displays the transport layer protocol that defines the service and the direction of traffic to which this rule applies.
Action	This field displays whether the rule silently discards packets (DROP), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (REJECT) or allows the passage of packets (ACCEPT).
Modify	Click the Edit icon to edit the rule. Click the Delete icon to delete an existing rule. Note that subsequent rules move up by one when you take this action. Click the Move To icon to change the order of the rule. Enter the number in the # field.

16.4.1 Add/Edit an ACL Rule

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

Figure 126 Access Control: Add/Edit

The following table describes the labels in this screen.

Table 83 Access Control: Add/Edit

LABEL	DESCRIPTION
Filter Name	Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes. You must enter the filter name to add an ACL rule. This field is read-only if you are editing the ACL rule.
Order	Select the order of the ACL rule.
Select Source IP Address	Select the source device to which the ACL rule applies. If you select Specific IP Address , enter the source IP address in the field below.
Source IP Address	Enter the source IP address.
Select Destination Device	Select the destination device to which the ACL rule applies. If you select Specific IP Address , enter the destination IP address in the field below.

Table 83 Access Control: Add/Edit (continued)

LABEL	DESCRIPTION
Destination IP Address	Enter the destination IP address.
IP Type	Select whether your IP type is IPv4 or IPv6 .
Select Service	Select the transport layer protocol that defines your customized port from the drop-down list box. The specific protocol rule sets you add in the Security > Firewall > Protocol > Add screen display in this list. If you want to configure a customized protocol, select Specific Service .
Protocol	This field is displayed only when you select Specific Protocol in Select Service . Choose the IP port (TCP/UDP , TCP , UDP , ICMP , or ICMPv6) that defines your customized port from the drop-down list box.
Custom Source Port	This field is displayed only when you select Specific Protocol in Select Service and have either TCP or UDP in the Protocol field. Enter a single port number or the range of port numbers of the source.
Custom Destination Port	This field is displayed only when you select Specific Protocol in Select Service and have either TCP or UDP in the Protocol field. Enter a single port number or the range of port numbers of the destination.
TCP flag	This field is displayed only when you select Specific Protocol in Select Service and have TCP in the Protocol field. Select one of the following TCP flags: SYN (Synchronize), ACK (Acknowledge), URG (Urgent), PSH (Push), RST (Reset), or FIN (Finished).
Type	This field is displayed only when you select Specific Protocol in Select Service and ICMPv6 in the protocol field. From the drop-down list box, select which ICMPv6 type you would like to use.
Policy	Use the drop-down list box to select whether to discard (DROP), deny and send an ICMP destination-unreachable message to the sender of (REJECT) or allow the passage of (ACCEPT) packets that match this rule.
Direction	Use the drop-down list box to select the direction of traffic to which this rule applies.
Enable Rate Limit	Select this check box to set a limit on the upstream/downstream transmission rate for the specified protocol. Specify how many packets per minute or second the transmission rate is.
Scheduler Rules	Select a schedule rule for this ACL rule form the drop-down list box. You can configure a new schedule rule by click Add New Rule . This will bring you to the Security > Scheduler Rules screen.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

16.5 DoS Settings

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

Use the **DoS** screen to activate protection against DoS attacks. Click **Security > Firewall > DoS** to display the following screen.

Figure 127 Security > Firewall > DoS

The following table describes the labels in this screen.

Table 84 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Select Enable to enable protection against DoS attacks.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

CHAPTER 17

MAC Filter

17.1 MAC Filter Overview

You can configure the Zyxel Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the LAN client to configure this screen.

17.2 MAC Filter Settings

Enable **MAC Address Filter** and add the host name and MAC address of a LAN client to the table if you wish to allow or deny them access to your network. Click **Security > MAC Filter**. The screen appears as shown.

Figure 128 Security > MAC Filter

Enable MAC filters and add the MAC addresses of LAN client in your home or office network to the following table, if you wish to allow or deny them to access your network. Sometimes, MAC Filter is considered a method to increase the security of your network.

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

MAC Restrict Mode ☒ Allow ☐ Deny

+ Add New Rule

Set	Active	Host Name	MAC Address	Delete
-----	--------	-----------	-------------	--------

Note
Only devices listed here are granted access to the network;

Cancel Apply

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

Figure 129 Enabling individual MAC Filters

Set	Active	Host Name	MAC Address	Delete
1	☐	test	BC - 22 - 33 - 44 - 55 - AA	
2	☒	Test	BC - 88 - 99 - 00 - 11 - 22	

The following table describes the labels in this screen.

Table 85 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select Enable to activate the MAC filter function.
MAC Restrict Mode	Select Allow to only permit the listed MAC addresses access to the Zyxel Device. Select Deny to permit anyone access to the Zyxel Device except the listed MAC addresses.
Add New Rule	Click this button to create a new entry.
Set	This is the index number of the MAC address.
Active	Select Active to enable the MAC filter rule. The rule will not be applied if Allow is not selected.
Host Name	Enter the host name of the wireless or LAN clients that are allowed access to the Zyxel Device.
MAC Address	Enter the MAC addresses of the wireless or LAN clients that are allowed access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Delete	Click the Delete icon to delete an existing rule.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

CHAPTER 18

Scheduler Rule

18.1 Scheduler Rule Overview

A Scheduler Rule allows you to define time periods and days during which the Zyxel Device allows certain actions.

18.2 Scheduler Rule Settings

Use this screen to view, add, or edit time schedule rules. A scheduler rule is a reusable object that is applied to other features, such as Firewall Access Control.

Click **Security > Scheduler Rule** to open the following screen.

Figure 130 Security > Scheduler Rule

#	Rule Name	Day	Time	Description	Modify
1	Barton_1	M T W T F S S	07:00-23:59	ParentalControl	

The following table describes the fields in this screen.

Table 86 Security > Scheduler Rule

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Rule Name	This shows the name of the rule.
Day	This shows the day(s) on which this rule is enabled.
Time	This shows the period of time on which this rule is enabled.
Description	This shows the description of this rule.
Modify	Click the Edit icon to edit the schedule. Click the Delete icon to delete a scheduler rule. Note: You cannot delete a scheduler rule once it is applied to a certain feature.

18.2.1 Add/Edit a Schedule Rule

Click the **Add New Rule** button in the **Scheduler Rule** screen or click the **Edit** icon next to a schedule rule to open the following screen. Use this screen to configure a restricted access schedule.

Figure 131 Scheduler Rule: Add/Edit

The screenshot shows a window titled "Add New Schedule Rule". It contains the following fields and controls:

- Rule Name:** A text input field.
- Day:** Seven circular buttons labeled Mon, Tue, Wed, Thu, Fri, Sat, and Sun.
- Time of Day Range:** Two text input fields labeled "From" and "To", followed by a "(hh:mm)" placeholder.
- Description:** A text input field.
- Buttons:** "Cancel" and "OK" buttons at the bottom.

The following table describes the fields in this screen.

Table 87 Scheduler Rule: Add/Edit

LABEL	DESCRIPTION
Rule Name	Enter a name (up to 31 printable English keyboard characters, not including spaces) for this schedule.
Day	Select check boxes for the days that you want the Zyxel Device to perform this scheduler rule.
Time of Day Range	Enter the time period of each day, in 24-hour format, during which the rule will be enforced.
Description	Enter a description for this scheduler rule.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

CHAPTER 19

Certificates

19.1 Certificates Overview

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

19.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the Zyxel Device's CA-signed certificates ([Section 19.4 on page 230](#)).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the Zyxel Device ([Section 19.4 on page 230](#)).

19.2 What You Need to Know

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

Certification Authority

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

19.3 Local Certificates

Click **Security > Certificates** to open the **Local Certificates** screen. Use this screen to view the Zyxel Device's summary list of certificates, generate certification requests, and import the signed certificates.

Figure 132 Security > Certificates > Local Certificates

Certificate (also known as digital IDs) can authenticate, you can generate certification requests and import the signed certificates. Maximum of 4 certificates can be stored.

Replace PrivateKey/Certificate file in PEM format

☒ Private Key is protected by password

No file selected.

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

The following table describes the labels in this screen.

Table 88 Security > Certificates > Local Certificates

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

19.3.1 Create Certificate Request

Click **Security > Certificates > Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the Zyxel Device generate a certification request. To create a certificate signing request, you need to enter a common name, organization name, state/province name, and the two-letter country code for the certificate.

Figure 133 Create Certificate Request

The following table describes the labels in this screen.

Table 89 Create Certificate Request

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

19.3.2 View Certificate Request

Click the **View** icon in the **Local Certificates** screen to open the following screen. Use this screen to view in-depth information about the certificate request. The **Certificate** is used to verify the authenticity of the certification authority. The **Private Key** serves as your digital signature for authentication and must be safely stored.

Figure 134 Certificate Request: View

The screenshot shows a window titled "View Certificate" with a close button in the top right corner. Below the title bar is a section labeled "Certificate Details". This section contains a table with the following information:

Name	Test
Type	none
Subject	/CN=588BF3-1A4C0095-B50D-S172V48000015/O=Zyxel/ST=Hsinchu/C=TW

Below the details table are three large text areas for viewing the certificate data:

- Certificate:** A large empty box for the certificate content.
- Private Key:** A text area containing a long string of alphanumeric characters, including "hGEzXjrkPkeJHmKBehzvdv", "KGLNbx22N1C0qtl++BwFFzOK8xTshyNxGW27goeOY", "1QpuD2RQy1FB+Ky9zVNCRuP", "6C1korOCNOwp2Mds4udfazEZEefm7ysyC0P2etwd7", "AbLBM49P1qUsWbGWR9snO74", "Myqhf+kCc2R801HUQvWX7XbHzTG+8RKTpV/oCkLZy", "cUBlyq0IY2f6FkWQBxp9C2H", "xteLLgB6SXDfK5vTyQTcj0spmPNdj4ZkxKhqtuLwM8E3", "bzHGdujBwvzZXnf6NxAZ", and "fAdmacECaYEA+SiZJoWxoB90BopN1JP3t//IOLPznbs".
- Signing Request:** A text area containing a long string of alphanumeric characters, including "-----BEGIN CERTIFICATE REQUEST-----", "MIICoDCCAYgCAQAwWzEqMCgGA1UEAwwhNTg4", "QkYzLVZNRzg4MjUtQjUwQjE1MTcy", "VjQ4MDAwMDE1MQ4wDAYDVQQKDAVaeXhlbDEQ", "MA4GA1UECAwHSHNpbmNodTElMAkG", "A1UEBhMCVFcwggEIMA0GCSqGSIb3DQEBAQUAA4I", "BDwAwggEKAoIBAQMCMCB3HK+Su", "PeKUpWld2QkPL4qsQsYXhL7chHWxCYAFw9QQYXP", and "NDQm4l3bS9rfwLqUMFck3F4HQ".

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

The following table describes the fields in this screen.

Table 90 Certificate Request: View

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

Table 90 Certificate Request: View (continued)

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

19.4 Trusted CA

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

Note: You can have a maximum of 4 trusted certificates.

Figure 135 Security > Certificates > Trusted CA

Certification Authority(CA) issues certificates and guarantees the identity of each certificate owner.In Trusted CA,you can save certificates of trusted CAs.

+ Import Certificate

#	Name	Subject	Type	Modify
---	------	---------	------	--------

Note
Maximum of 4 certificates

The following table describes the fields in this screen.

Table 91 Security > Certificates > Trusted CA

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

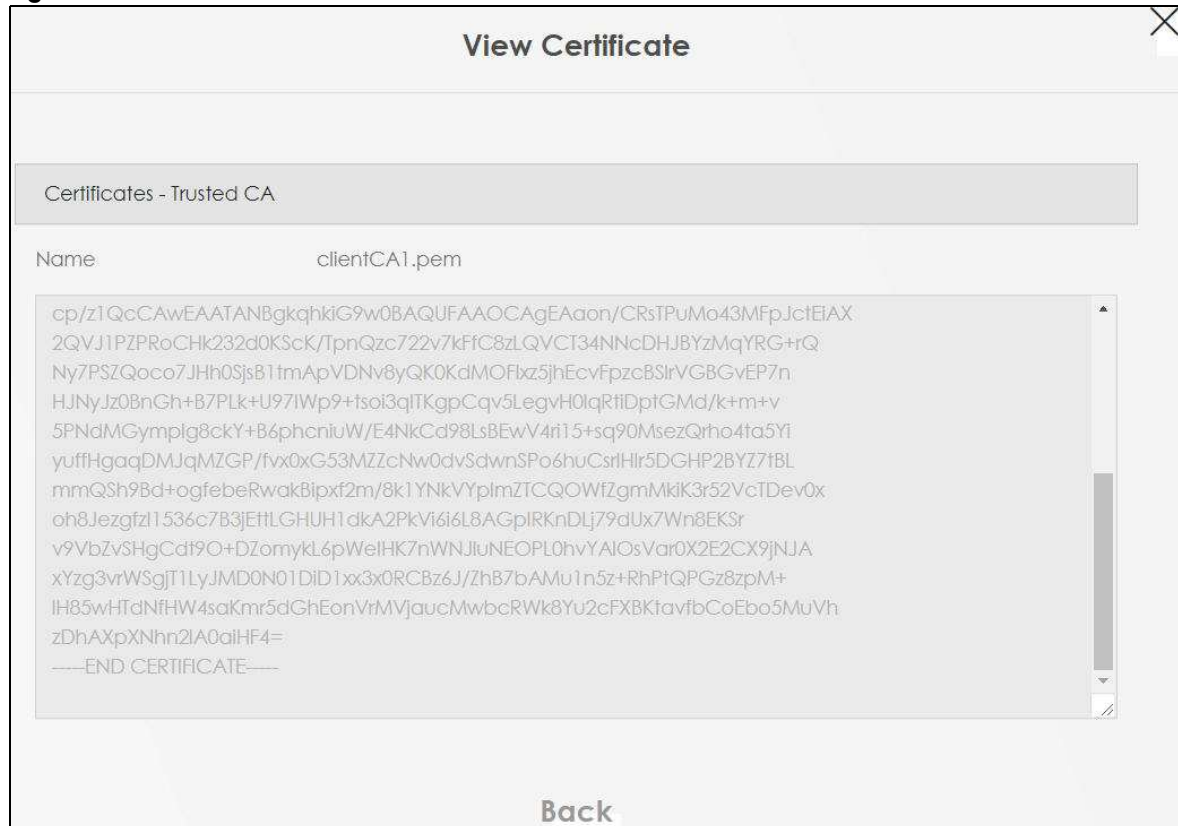
Table 91 Security > Certificates > Trusted CA (continued)

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

19.4.1 View Trusted CA Certificate

Click the **View** icon in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate. The certificate text box is read-only and can be distributed to others.

Figure 136 Trusted CA: View



The following table describes the fields in this screen.

Table 92 Trusted CA: View

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

19.4.2 Import Trusted CA Certificate

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

Figure 137 Trusted CA: Import Certificate

Import Certificate

The certificates is in one of the following formats:

- Binary X.509
- PEM (base-64) encoded
- Binary PKCS#7
- PEM(base-64) encoded PKCS#7

Certificate File Path No file selected.

Cancel **OK**

The following table describes the fields in this screen.

Table 93 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate File Path	Click Browse and select the certificate you want to upload.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

CHAPTER 20

Log

20.1 Log Overview

These screens allow you to determine the categories of events and/or alerts that the Zyxel Device logs and then display these logs or have the Zyxel Device send them to an administrator (through e-mail) or to a syslog server.

20.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs ([Section 20.2 on page 234](#)).
- Use the **Security Log** screen to see the security-related logs for the categories that you select ([Section 20.3 on page 235](#)).

20.1.2 What You Need To Know

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

Alerts and Logs

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

Syslog Overview

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

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

Table 94 Syslog Severity Levels

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

Table 94 Syslog Severity Levels

CODE	SEVERITY
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

20.2 System Log

Use the **System Log** screen to see the system logs. You can filter the entries by clicking on the **Level** and/or **Category** drop-down list boxes. Click **System Monitor > Log** to open the **System Log** screen.

Figure 138 System Monitor > Log > System Log

All system events will be logged and displayed in the following table. Select a level from the pull-down menu to show filtered results.

Level: Category: [Clear Log](#) [Refresh](#) [Export Log](#) [E-mail Log Now](#)

#	Time	Facility	Level	Category	Messages
1	Jan 1 00:00:50	user	notice	system	esmd: System: System init finished
2	Jan 1 00:00:36	daemon	err	dhcpcd	dnsmasq-dhcp: failed to read /etc/ethers: No such file or directory
3	Jan 1 00:00:36	daemon	info	dhcpcd	dnsmasq-dhcp: DHCP, IP range 192.168.1.2 -- 192.168.1.254, lease time 1d

The following table describes the fields in this screen.

Table 95 System Monitor > Log > System Log

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

20.3 Security Log

Use the **Security Log** screen to see the security-related logs for the categories that you select. You can filter the entries by clicking on the **Level** and/or **Category** drop-down list boxes. Click **System Monitor > Log > Security Log** to open the following screen.

Figure 139 System Monitor > Log > Security Log

The following table describes the fields in this screen.

Table 96 System Monitor > Log > Security Log

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

CHAPTER 21

Traffic Status

21.1 Traffic Status Overview

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

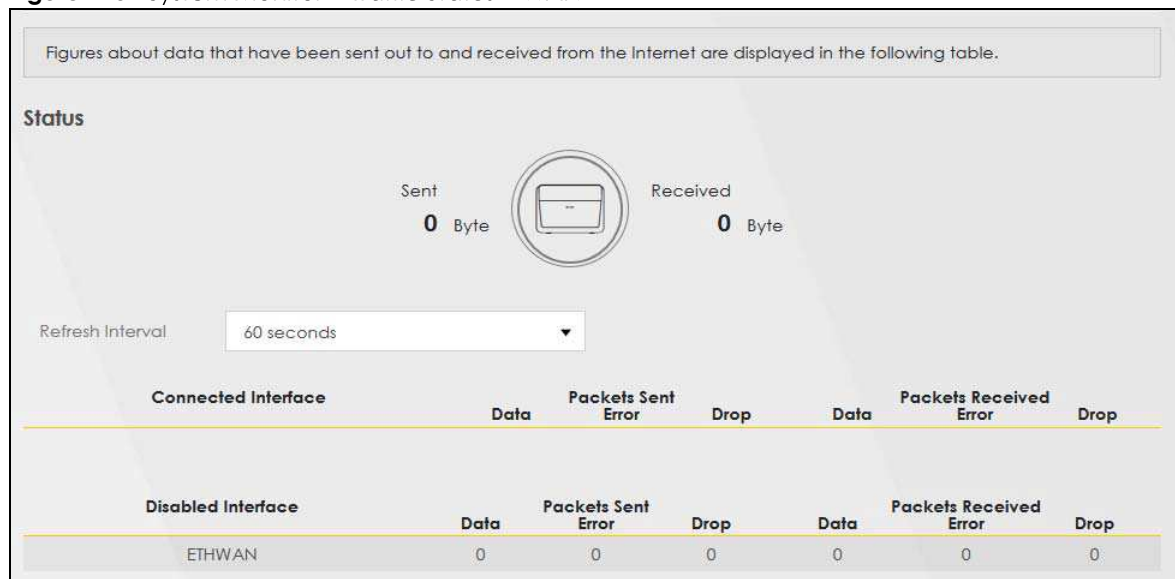
21.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics ([Section 21.2 on page 236](#)).
- Use the **LAN** screen to view the LAN traffic statistics ([Section 21.3 on page 237](#)).
- Use the **NAT** screen to view the NAT status of the Zyxel Device's client(s) ([Section 21.4 on page 239](#)).

21.2 WAN Status

Click **System Monitor > Traffic Status** to open the **WAN** screen. [Use this screen to look at network traffic status and statistics of each interfaces.](#)

Figure 140 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 97 System Monitor > Traffic Status > WAN

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

21.3 LAN Status

Click **System Monitor > Traffic Status > LAN** to open the following screen. [Use this screen to look at network traffic status and statistics of the LAN interface.](#)

System Monitor > Traffic Status > LAN

Traffic Status

WAN LAN NAT

Figures about data that have been sent to and received from each LAN port (including WIFI) are displayed in the following table.

Refresh Interval None

Interface	LAN1	LAN2	LAN3	LAN4	LAN5	2.4G WLAN	5G WLAN
Bytes Sent	0	520526	0	0	0	16463172	16483456
Bytes Received	0	264249	0	0	0	0	0

Interface		LAN1	LAN2	LAN3	LAN4	LAN5	2.4G WLAN	5G WLAN
Sent (Packet)	Data	0	2148	0	0	0	65656	65787
	Error	0	0	0	0	0	0	0
	Drop	0	0	0	0	0	0	0
Received (Packet)	Data	0	1925	0	0	0	0	0
	Error	0	0	0	0	0	17	121
	Drop	0	2	0	0	0	74	323

The following table describes the fields in this screen.

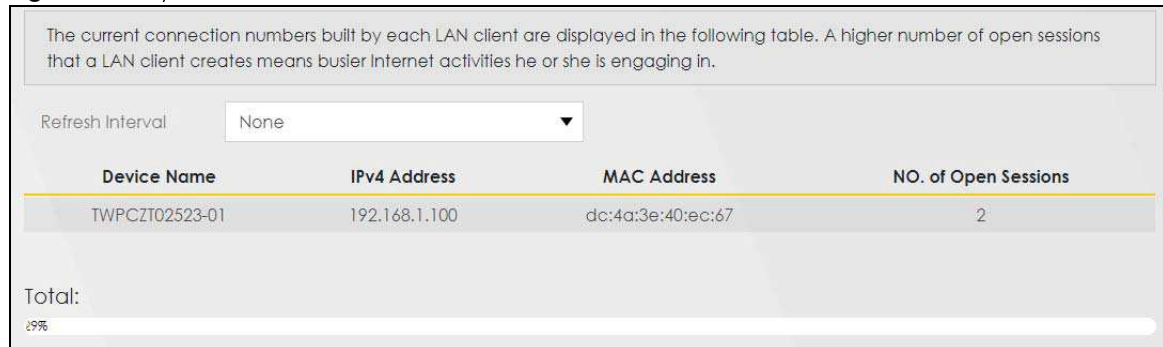
Table 98 System Monitor > Traffic Status > LAN

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

21.4 NAT Status

Click **System Monitor > Traffic Status > NAT** to open the following screen. The figures in this screen show the NAT session statistics for hosts currently connected to the Zyxel Device. A number of open sessions means there's a lot of traffic going through a host.

Figure 141 System Monitor > Traffic Status > NAT



The following table describes the fields in this screen.

Table 99 System Monitor > Traffic Status > NAT

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