

User's Guide

VMG4005-B50A/B60A

VDSL2 17a Bonding and 35b Single Line Bridge

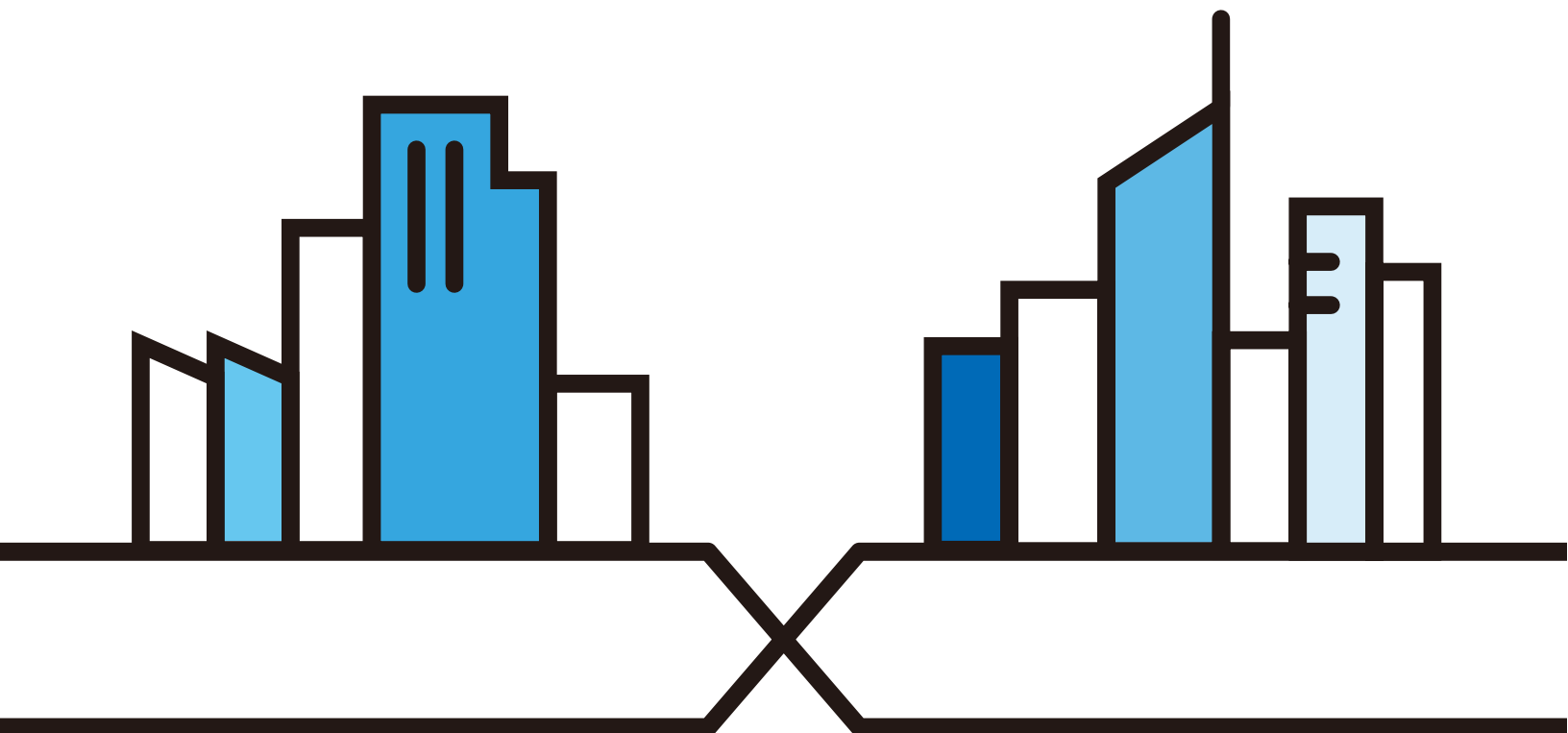
DM4200-B0

VDSL2 35b Bonding Bridge

Default Login Details

LAN IP Address	http://192.168.1.1
Login	admin
Password	See the device label

Version 5.17 Ed 1, 5/2023



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from what you see due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

The Quick Start Guide shows how to connect the Zyxel Device.

- More Information

Go to <https://service-provider.zyxel.com/global/en/tech-support> to find other information on Zyxel Device.



Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this guide.

Warnings tell you about things that could harm you or your device.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The VMG4005-B50A/B60A and DM4200-B0 may be referred to as the “Zyxel Device” in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **System Monitor > Traffic Status > LAN** means you first click **System Monitor** in the navigation panel, then the **Traffic Status** sub menu and finally the **LAN** tab to get to that screen.

Icons Used in Figures

Figures in this user guide may use the following generic icons. The Zyxel Device icon is not an exact representation of your device.










Zyxel Device 	Generic Router 	Laptop Computer 
Switch 	Firewall 	Server 
Internet 	User 	Wireless Device 

Table of Contents

Document Conventions	3
Table of Contents	4
Part I: User's Guide.....	10
Chapter 1	
Introducing the Zyxel Device	11
1.1 Overview	11
1.2 Example Applications	11
1.2.1 Internet Access	12
1.3 Manage the Zyxel Device	14
1.4 Good Habits for Managing the Zyxel Device	14
1.5 Hardware	14
1.5.1 LED Indicators	15
1.5.2 Ports Panel	16
1.5.3 RESET Button	16
Chapter 2	
The Web Configurator.....	18
2.1 Overview	18
2.1.1 Accessing the Web Configurator	18
2.2 Web Configurator Layout	21
2.2.1 Menu Icon	21
Chapter 3	
Quick Start Wizard.....	26
3.1 Overview	26
3.2 Quick Start Wizard Setup	26
3.2.1 Time Zone	26
3.2.2 Internet	27
Part II: Technical Reference.....	29
Chapter 4	
Status.....	30

4.1 Status Overview	30
4.1.1 Management Service	30
4.1.2 System Info	30
4.1.3 Ethernet UNI	32
Chapter 5	
Broadband.....	33
5.1 Broadband Overview	33
5.1.1 What You Can Do in this Chapter	33
5.1.2 What You Need to Know	34
5.1.3 Before You Begin	37
5.2 The Broadband Screen	37
5.2.1 Add/Edit Internet Connection	38
5.3 The Broadband Advanced Screen	45
5.4 Technical Reference	49
Chapter 6	
Home Networking.....	55
6.1 Home Networking Overview	55
6.1.1 What You Can Do in this Chapter	55
6.1.2 What You Need To Know	55
6.1.3 Before You Begin	56
6.2 LAN Setup	56
6.3 Static DHCP	62
6.3.1 Before You Begin	62
6.4 Ethernet UNI	63
6.5 Technical Reference	65
6.5.1 DHCP Setup	65
6.5.2 DNS Server Addresses	65
6.5.3 LAN TCP/IP	66
6.6 Web Configurator Easy Access in Windows 10	67
Chapter 7	
Routing.....	69
7.1 Routing Overview	69
7.2 Configure Static Route	69
7.2.1 Add or Edit Static Route	70
Chapter 8	
Quality of Service (QoS).....	75
8.1 QoS Overview	75
8.1.1 What You Can Do in this Chapter	75
8.2 What You Need to Know	75

8.3 Quality of Service General Settings	77
8.4 Queue Setup	79
8.4.1 Add a QoS Queue	80
8.5 QoS Classification Setup	81
8.5.1 Add or Edit QoS Class	82
8.6 QoS Shaper Setup	86
8.6.1 Add or Edit a QoS Shaper	87
8.7 QoS Policer Setup	88
8.7.1 Add or Edit a QoS Policer	88
8.8 Technical Reference	91
 Chapter 9	
VLAN Group.....	96
9.1 VLAN Group Overview	96
9.1.1 What You Can Do in this Chapter	96
9.2 VLAN Group Settings	97
9.2.1 Add or Edit a VLAN Group	97
 Chapter 10	
Interface Grouping	99
10.1 Interface Grouping Overview	99
10.1.1 What You Can Do in this Chapter	99
10.2 Interface Grouping	99
10.2.1 Interface Group Configuration	100
10.2.2 Interface Grouping Criteria	102
 Chapter 11	
Firewall	104
11.1 Firewall Overview	104
11.1.1 What You Need to Know About Firewall	104
11.2 Firewall	105
11.2.1 What You Can Do in this Chapter	106
11.3 Firewall General Settings	106
11.4 Protocol (Customized Services)	107
11.4.1 Add New Protocol Entry	108
11.5 Access Control (Rules)	109
11.5.1 Add New ACL Rule	109
11.6 DoS	111
11.7 Firewall Technical Reference	112
11.7.1 Firewall Rules Overview	112
11.7.2 Guidelines For Security Enhancement With Your Firewall	113
11.7.3 Security Considerations	114

Chapter 12	
MAC Filter	115
12.1 MAC Filter Overview	115
12.2 MAC Filter	115
12.2.1 Add New Rule	116
Chapter 13	
Scheduler Rule	118
13.1 Scheduler Rule Overview	118
13.2 Scheduler Rule Settings	118
13.2.1 Add or Edit a Schedule Rule	119
Chapter 14	
Certificates	120
14.1 Certificates Overview	120
14.1.1 What You Can Do in this Chapter	120
14.2 What You Need to Know	120
14.3 Local Certificates	120
14.3.1 Create Certificate Request	122
14.3.2 View Certificate Request	122
14.4 Trusted CA	124
14.5 Import Trusted CA Certificate	125
14.6 View Trusted CA Certificate	126
14.7 Certificates Technical Reference	126
14.7.1 Verify a Certificate	127
Chapter 15	
Log	129
15.1 Log Overview	129
15.1.1 What You Can Do in this Chapter	129
15.1.2 What You Need To Know	129
15.2 System Log	130
15.3 Security Log	130
Chapter 16	
Traffic Status	132
16.1 Traffic Status Overview	132
16.1.1 What You Can Do in this Chapter	132
16.2 WAN Status	132
16.3 LAN Status	133
Chapter 17	
ARP Table	135

17.1 ARP Table Overview	135
17.1.1 How ARP Works	135
17.2 ARP Table Settings	136
Chapter 18	
Routing Table.....	137
18.1 Routing Table Overview	137
18.2 Routing Table	137
Chapter 19	
MAC Address Table	140
19.1 MAC Address Table Overview	140
19.2 MAC Address Table Settings	140
Chapter 20	
xDSL Statistics	141
20.1 xDSL Statistics Overview	141
Chapter 21	
System.....	144
21.1 System Overview	144
21.2 System Settings	144
Chapter 22	
User Account.....	145
22.1 User Account Overview	145
22.2 User Account Settings	145
22.2.1 User Account Add/Edit	146
Chapter 23	
Remote Management.....	148
23.1 Remote Management Overview	148
23.1.1 What You Can Do in this Chapter	148
23.2 MGMT Services	148
23.3 Trust Domain	149
23.3.1 Add Trust Domain	150
Chapter 24	
Time Settings.....	151
24.1 Time Settings Overview	151
24.2 Time Setup	151
Chapter 25	
Log Setting	155

25.1 Logs Setting Overview	155
25.2 Log Setup	155
Chapter 26	
Firmware Upgrade	158
26.1 Firmware Upgrade Overview	158
26.2 Firmware Settings	158
Chapter 27	
Backup/Restore	160
27.1 Backup/Restore Overview	160
27.2 Backup/Restore Settings	160
27.3 Reboot	163
Chapter 28	
Diagnostic.....	164
28.1 Diagnostic Overview	164
28.1.1 What You Can Do in this Chapter	164
28.2 What You Need to Know	164
28.3 Ping & TraceRoute & Nslookup	165
28.4 802.1ag (CFM)	166
28.5 802.3ah (OAM)	167
28.6 OAM Ping	168
 Part III: Troubleshooting and Appendices.....	 171
Chapter 29	
Troubleshooting.....	172
29.1 Power, Hardware Connections, and LEDs	172
29.2 Zyxel Device Access and Login	173
29.3 Internet Access	174
29.4 IP Address Setup	175
Appendix A IPv6	179
Appendix B Customer Support	185
Appendix C Legal Information	190
Index	194

PART I

User's Guide

CHAPTER 1

Introducing the Zyxel Device

1.1 Overview

The following table describes the feature differences of the Zyxel Device by model.

Table 1 Zyxel Device Comparison Table

	VMG4005-B50A	VMG4005-B60A	DM4200-B0	DESCRIPTION
Annex A (ADSL over POTS)	YES	NO	YES	The telephone line carries voice and ADSL. If you have standard analog lines (POTS) and your ADSL is coming over POTS, use Annex A.
Annex B (ADSL over ISDN, can be used on normal POTS lines as well)	NO	YES	NO	Voice, ISDN (Integrated Services Digital Network) and ADSL are on the same line. If you have ISDN line or telephone and your ADSL is coming over ISDN, use Annex B.
Supported VDSL2 Single-Line / Bonding Transmission Vectoring Profiles	35b / 17a	35b / 17a	35b / 35b	Vectoring is a technique used to reduce signal interference (crosstalk) and improve the transmission data rate. Signal interference happens between DSL cables when more than one DSL cable is transmitting signals. Transmission data rates differ by the supported vectoring profile. You should use the same profile as what the ISP uses.
Latest Supported Firmware Version	5.17	5.17	5.17	See Section 26.2 on page 158 for more information.

The Zyxel Device is a VDSL modem, which provides fast Internet access over a plain telephone wire. After you set up the connections and turn it on, the Zyxel Device automatically access the Internet. Refer to [Section 29.3 on page 174](#) if you cannot access the Internet.

It also supports VDSL bonding that allows the combining of DSL connections for even faster speeds. Universal Plug and Play (UPnP) where UPnP devices can dynamically join the Zyxel Device network is also supported.

You can use the Web Configurator to view traffic statistics, upload firmware and allow external management of the Zyxel Device.

1.2 Example Applications

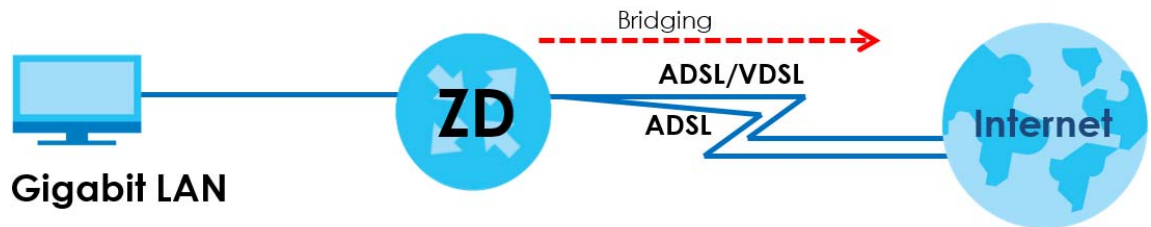
This section shows a few examples of using the Zyxel Device in various network environments. Note that the Zyxel Device in the figure is just an example Zyxel Device and not your actual Zyxel Device.

1.2.1 Internet Access

Your Zyxel Device provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. You can have multiple WAN services over one ADSL or VDSL. The Zyxel Device cannot work in ADSL and VDSL mode at the same time.

A computer, gateway, or router can connect to the Zyxel Device's LAN port.

Figure 1 Zyxel Device's Internet Access Application



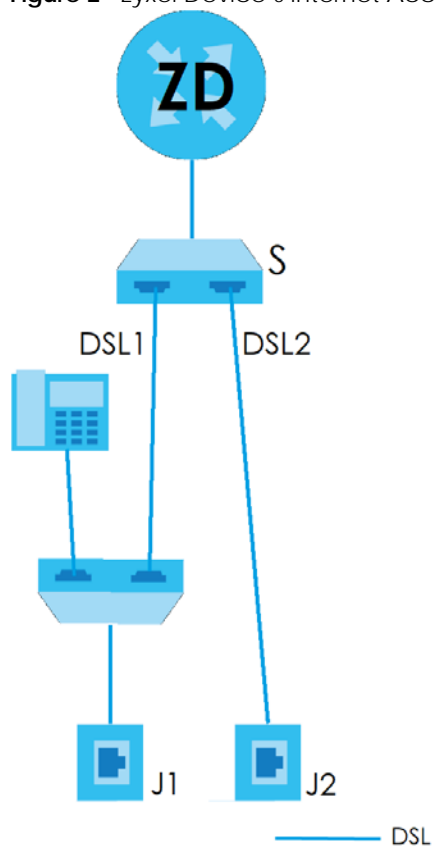
DSL Bonding

DSL bonding allows the Zyxel Device to aggregate two DSL lines into a virtual connection. The Zyxel Device will have higher bandwidth and faster transmission speed at longer distances. Note that the two DSL lines must come from the same ISP, and they both need to support DSL bonding. Also, only DSL 1 supports telephone service.

To set up your network for DSL bonding:

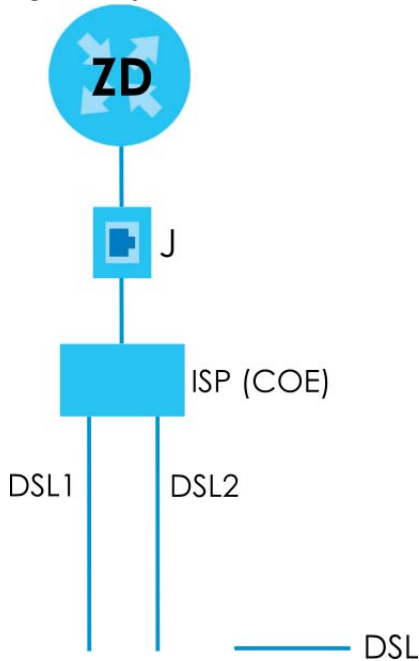
Example 1

- 1 Connect a two-line splitter to the Zyxel Device (**ZD** in the figure).
- 2 Connect two DSL lines (**DSL1** and **DSL2**) to the two-line splitter (**S**).
- 3 Connect the two DSL lines to two separate telephone jacks (**J1**, **J2**) on the wall.

Figure 2 Zyxel Device's Internet Access Application: DSL Bonding (Example 1)**Example 2**

Connect the DSL port on the Zyxel Device (**DSL** in the figure) to a telephone jack (**J**).

The **ISP** will split the DSL connection at their end for **DSL 1** and **DSL 2** bonding.

Figure 3 Zyxel Device's Internet Access Application: DSL Bonding (Example 2)

1.3 Manage the Zyxel Device

Use the Web Configurator for management of the Zyxel Device using a (supported) web browser.

1.4 Good Habits for Managing the Zyxel Device

Do the following things regularly to make the Zyxel Device more secure and to manage the Zyxel Device more effectively.

- Change the Web Configurator password. Use a password that is not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the Zyxel Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Zyxel Device. You could simply restore your last configuration.

1.5 Hardware

This section describes the LEDs and ports panel for each model. Refer to the Zyxel Device's Quick Start Guides to see the product drawings and how to make the hardware connections.

1.5.1 LED Indicators

Use the LEDs to determine if the Zyxel Device is behaving normally or if there are problems on your network.


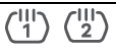

Note: None of the LEDs are on if the Zyxel Device is not receiving power.

Figure 4 Front Panel






The following are the LED descriptions of your VMG4005-B50A/B60A.

Table 2 VMG4005-B50A/B60A LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
 Power	Green	On	The Zyxel Device is receiving power and ready for use.
		Blinking	The Zyxel Device is booting up and getting ready for use.
	Red	On	The Zyxel Device has detected an error while self-testing, or there is a device malfunction.
		Blinking	The Zyxel Device is upgrading firmware.
		Off	The Zyxel Device is not receiving power.
 DSL1 DSL2	Green	On	The ADSL/VDSL link is up.
		Blinking	The Zyxel Device is initializing the ADSL/VDSL link.
		Off	The ADSL/VDSL link is down.
 Ethernet LAN	Green	On	The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The Zyxel Device is sending or receiving data to/from the LAN at 10/100/1000 Mbps.
		Off	There is no Ethernet connection on the LAN.

The following are the LED descriptions of your DM4200-B0.

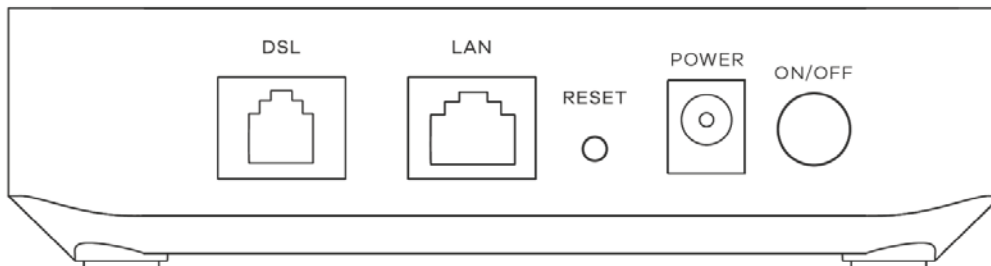
Table 3 DM4200-B0 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
 Power	Green	On	The Zyxel Device is receiving power and ready for use.
		Blinking	The Zyxel Device is booting up and getting ready for use.
	Red	On	The Zyxel Device has detected an error while self-testing, or there is a device malfunction.
		Blinking	The Zyxel Device is upgrading firmware.
		Off	The Zyxel Device is not receiving power.
 DSL1 DSL2	Green	On	The ADSL/VDSL link is up.
		Slow Blinking	The Zyxel Device detects carrier signals on the DSL line and is performing link negotiation before initializing the ADSL/VDSL link.
		Fast Blinking	The Zyxel Device is initializing the ADSL/VDSL link.
		Off	The ADSL/VDSL link is down.
 Ethernet LAN	Green	On	The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The Zyxel Device is sending or receiving data to/from the LAN at 10/100/1000 Mbps.
		Off	There is no Ethernet connection on the LAN.

1.5.2 Ports Panel

The connection ports are located on the ports panel.

Figure 5 Ports Panel



The following table describes the items on the ports panel.

Table 4 Ports Panel

LABEL	DESCRIPTION
DSL	Connect a RJ-45 cable to the DSL port for Internet access.
LAN	Connect a router/gateway to the Ethernet port for Internet access.
RESET	Press the button to return the Zyxel Device to the factory defaults.
POWER	Connect the power adapter and then can press the ON/OFF button to start the Zyxel Device.

1.5.3 RESET Button

If you forget your password or cannot access the Web Configurator, you will need to use the **RESET** button to reload the factory-default configuration file. This means that you will lose all configurations

that you had previously. The password will be reset to the factory default (see the device label), and the LAN IP address will be "192.168.1.1".

- 1** Make sure the **POWER** LED is on (not blinking).
- 2** To set the device back to the factory default settings, press the **RESET** button for more than 5 seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

CHAPTER 2

The Web Configurator

2.1 Overview

This section introduces the configuration and functions of the Web Configurator.

The Web Configurator is an HTML-based management interface that allows easy Zyxel Device setup and management through Internet browser. Use a browser that supports HTML5, such as Microsoft Edge, Mozilla Firefox, or Google Chrome. The recommended minimum screen resolution is 1024 by 768 pixels. The recommended screen resolution is 1024 by 768 pixels.

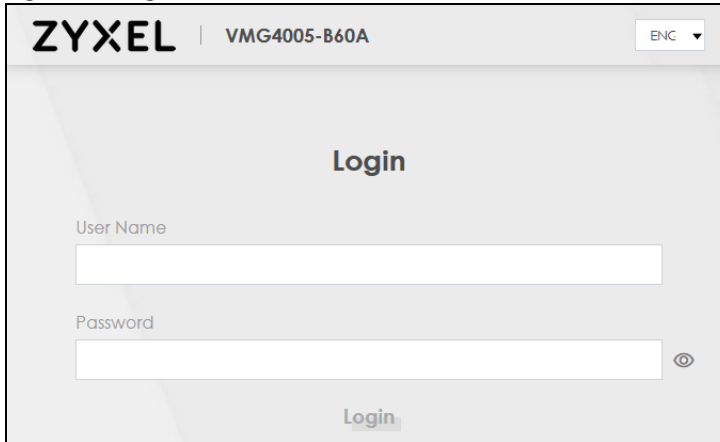
In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your Zyxel Device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

2.1.1 Accessing the Web Configurator

- 1 Make sure your Zyxel Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Make sure your computer has an IP address in the same subnet as the Zyxel Device. Your computer should have an IP address from 192.168.1.2 to 192.168.1.254. See [Section 29.4 on page 175](#) for details.
- 3 Launch your web browser. If the Zyxel Device does not automatically re-direct you to the login screen, go to <http://192.168.1.1>.
- 4 A login screen displays. Select a language you prefer.
- 5 To access the administrative Web Configurator and manage the Zyxel Device, type the default username **admin** and the randomly assigned default password (see the device label) in the login screen and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 6 Login Screen

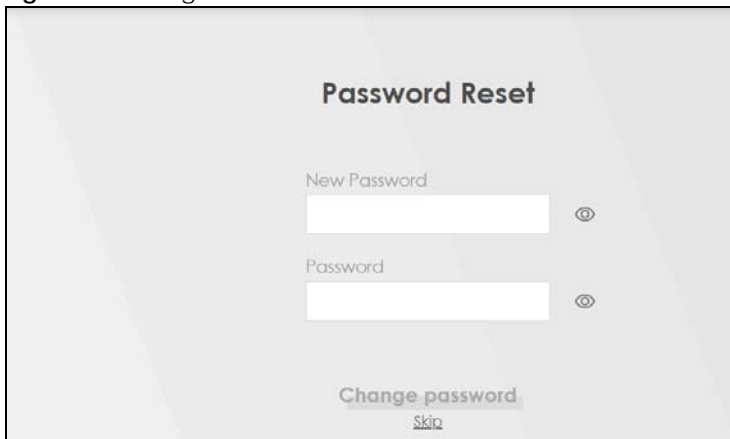


The login screen for the ZYXEL VMG4005-B60A device. At the top, the ZYXEL logo is on the left, the model number VMG4005-B60A is in the center, and a language dropdown menu set to 'ENG' is on the right. The main heading is 'Login'. Below it are two input fields: 'User Name' and 'Password'. The 'Password' field has a toggle icon (an eye) to its right. At the bottom center is a 'Login' button.

Note: The default allowable times that you can enter the **Password** is 3. If you entered the wrong password for the fourth time, by default the Web Configurator will lock itself for 5 minutes before you can try entering the correct **Password** again. You can change these settings in **Maintenance > User Account > Add New / Edit Account** (see [Section 22.2.1 on page 146](#)).

- 6 The following screen may display when you log into the Web Configurator for the first time. Enter a new password, retype it to confirm, and click **Change password**. If you prefer to use the default password, click **Skip**.

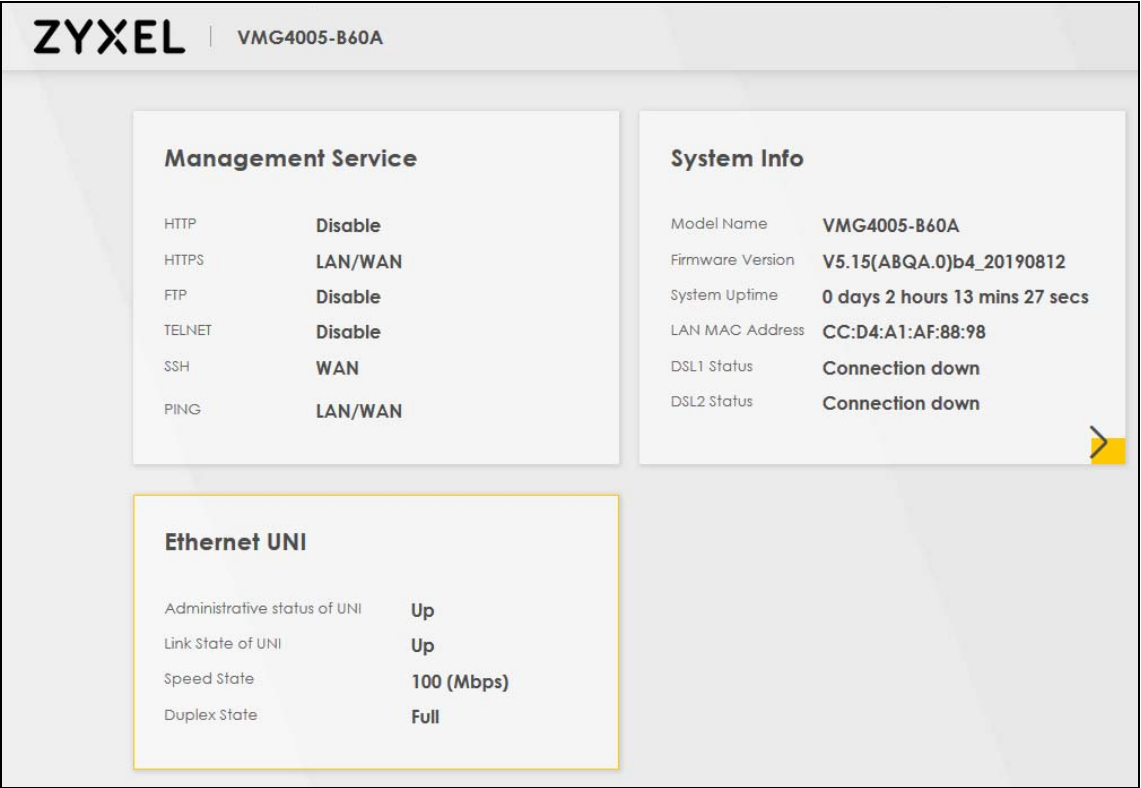
Figure 7 Change Password Screen



The 'Password Reset' screen. It features the heading 'Password Reset'. Below it are two input fields: 'New Password' and 'Password'. Both fields have toggle icons (eyes) to their right. At the bottom are two buttons: 'Change password' and 'Skip'.

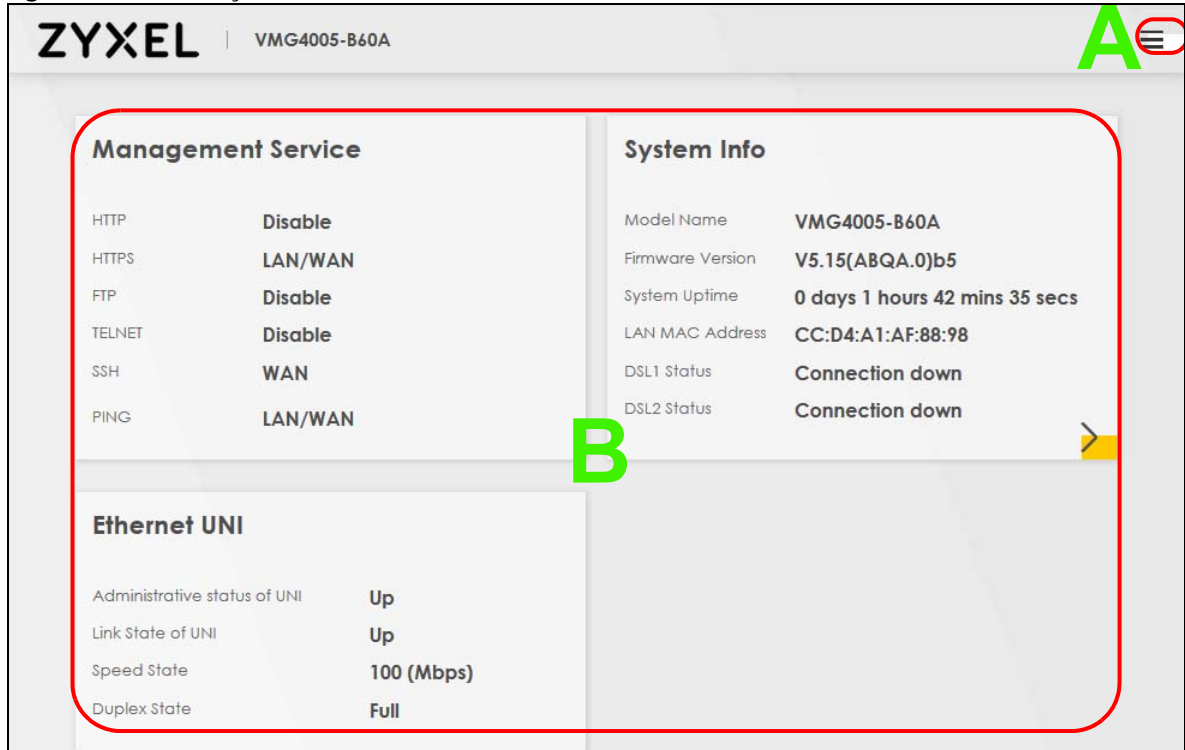
- 7 The **Connection Status** page appears. See [Chapter 4 on page 30](#) for details.

Figure 8 Connection Status



2.2 Web Configurator Layout

Figure 9 Screen Layout



As illustrated above, the main screen is divided into these parts:

- **A** - Menu Icon (Navigation Panel)
- **B** - Main Window

2.2.1 Menu Icon

Click this icon (☰) to display the navigation panel that contains configuration menus and quick links.



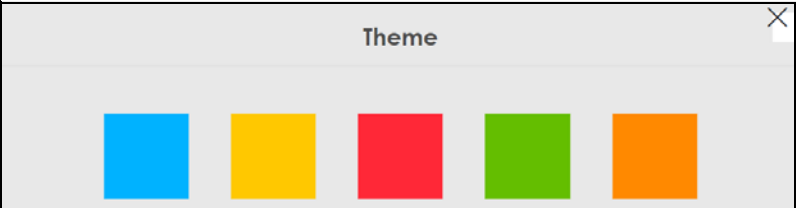



2.2.1.1 Quick Links

The quick links provides some icons on the right hand side.



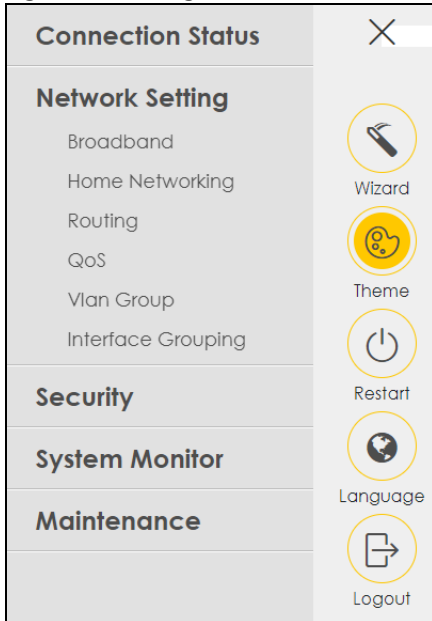
The icons provide the following functions.

Table 5 Quick Link Icons

ICON	DESCRIPTION
 Wizard	Wizard: Click this icon to open screens where you can configure the Zyxel Device's time zone Internet access, and wireless settings. See Chapter 3 on page 26 for more information about the Wizard screens.
 Theme	Theme: Click this icon to select a color that you prefer and apply it to the Web Configurator. 
 Language	Language: Select the language you prefer.
 Restart	Restart: Click this icon to reboot the Zyxel Device without turning the power off.
 Logout	Logout: Click this icon to log out of the Web Configurator.

2.2.1.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure Zyxel Device features. The following tables describe each menu item.

Figure 10 Navigation Panel

Note: The menu items on the navigation panel vary among the models. See [Section 1.1 on page 11](#) for more information about the feature differences of the ZyXel Device.

Table 6 Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		Use this screen to view the network status of the ZyXel Device and computers/devices connected to it.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the ZyXel Device. You can export or email the logs.
	Security Log	Use this screen to view all security related events. You can select level and category of the security events in their proper drop-down list window.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the ZyXel Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the ZyXel Device.
ARP Table	ARP Table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.
MAC Address Table	MAC Address Table	Use this screen to view the MAC address table. It displays the MAC address of each client device and the VLAN group of each associated wired client.
xDSL Statistics	xDSL Statistics	Use this screen to view the ZyXel Device's xDSL traffic statistics.
Maintenance		
System	System	Use this screen to set ZyXel Device name and Domain name.
User Account	User Account	Use this screen to change user password on the ZyXel Device.
Remote Management	MGMT Services	Use this screen to enable specific traffic directions for network services.
	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.

Table 6 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Time	Time	Use this screen to change your Zyxel Device's time and date.
Log Settings	Log Setting	Use this screen to change your Zyxel Device's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your Zyxel Device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your Zyxel Device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the Zyxel Device without turning the power off.
Diagnostic	Ping&Traceroute &Nslookup	Use this screen to identify problems with the Zyxel Device. You can use Ping, TraceRoute, or Nslookup to help you identify problems.
	802.1ag	Use this screen to configure CFM (Connectivity Fault Management) MD (maintenance domain) and MA (maintenance association), perform connectivity tests and view test reports.
	802.3ah	Use this screen to configure link OAM port parameters,
	OAM Ping	Use this screen to view information to help you identify problems with the DSL connection.

Table 7 DM4200-B0 Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		Use this screen to view the network status of the Zyxel Device and computers/devices connected to it.
Network Setting		
Broadband	Broadband	Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections.
	Advanced	Use this screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	Ethernet UNI	Use the Ethernet UNI screen to set the link speed and duplex mode for the Zyxel Device Ethernet LAN port.
Routing	Routing	Use this screen to view and set up static routes on the Zyxel Device.
QoS	General	Use this screen to enable QoS and traffic prioritizing. You can also configure the QoS rules and actions.
	Queue Setup	Use this screen to configure QoS queues.
	Classification Setup	Use this screen to define a classifier.
	Shaper Setup	Use this screen to limit outgoing traffic rate on the selected interface.
	Policer Setup	Use this screen to configure QoS policers.
VLAN Group	VLAN Group	Use this screen to group and tag VLAN IDs to outgoing traffic from the specified interface.
Interface Grouping	Interface Grouping	Use this screen to map a port to create multiple networks on the Zyxel Device.
Security		

Table 7 DM4200-B0 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the Zyxel Device.
Scheduler Rule	Scheduler Rule	Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced.
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the Zyxel Device. You can export or email the logs.
	Security Log	Use this screen to view all security related events. You can select level and category of the security events in their proper drop-down list window.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Zyxel Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Zyxel Device.
ARP Table	ARP Table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.
Routing Table	Routing Table	Use this screen to view the routing table on the Zyxel Device.
xDSL Statistics	xDSL Statistics	Use this screen to view the Zyxel Device's xDSL traffic statistics.
Maintenance		
System	System	Use this screen to set Zyxel Device name and Domain name.
User Account	User Account	Use this screen to change user password on the Zyxel Device.
Remote Management	MGMT Services	Use this screen to enable specific traffic directions for network services.
	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.
Time	Time	Use this screen to change your Zyxel Device's time and date.
Log Settings	Log Setting	Use this screen to change your Zyxel Device's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your Zyxel Device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your Zyxel Device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the Zyxel Device without turning the power off.
Diagnostic	Ping&Traceroute &Nslookup	Use this screen to identify problems with the Zyxel Device. You can use Ping, TraceRoute, or Nslookup to help you identify problems.
	802.1ag	Use this screen to configure CFM (Connectivity Fault Management) MD (maintenance domain) and MA (maintenance association), perform connectivity tests and view test reports.
	802.3ah	Use this screen to configure link OAM port parameters,

CHAPTER 3

Quick Start Wizard

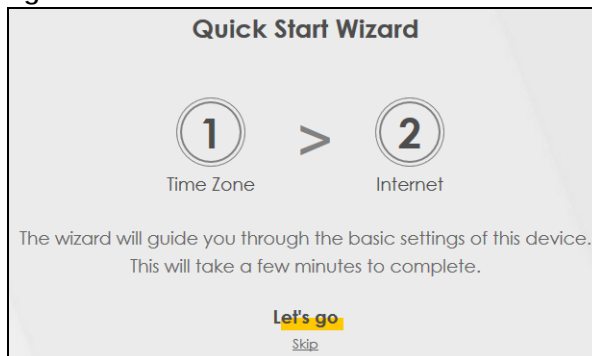
3.1 Overview

Use the **Wizard** screens to configure the Zyxel Device's time zone and check Internet access.

3.2 Quick Start Wizard Setup

You can click the **Wizard** icon in the navigation panel to open the **Wizard** screens. See [Section 2.2.1.1 on page 22](#) for more information about the navigation panel. After you click the **Wizard** icon, the following screen appears. Click **Let's go** to proceed with settings on time zone, basic Internet access, and wireless networks. It will take you a few minutes to complete the settings on the **Wizard** screens. You can also click **Skip** to leave the **Wizard** screens.

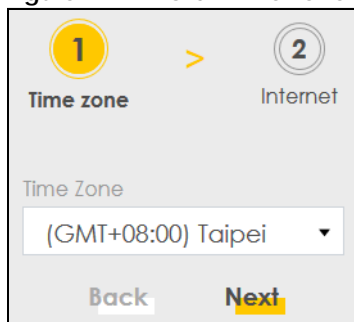
Figure 11 Wizard - Home



3.2.1 Time Zone

Select the time zone of your location. Click **Next**.

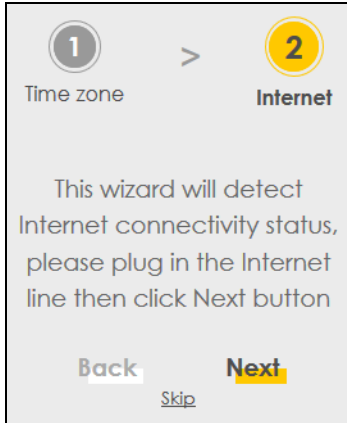
Figure 12 Wizard - Time Zone



3.2.2 Internet

The Zyxel Device will check the Internet status automatically. Click **Next** to proceed. You can also click **Skip** to pass checking of Internet connectivity in the **Wizard**.

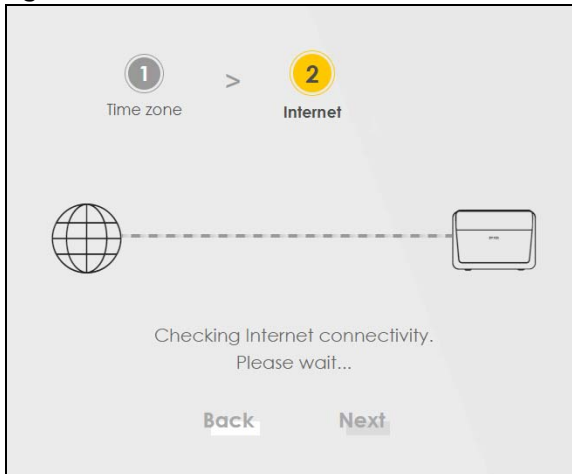
Figure 13 Wizard - Internet



Internet Status

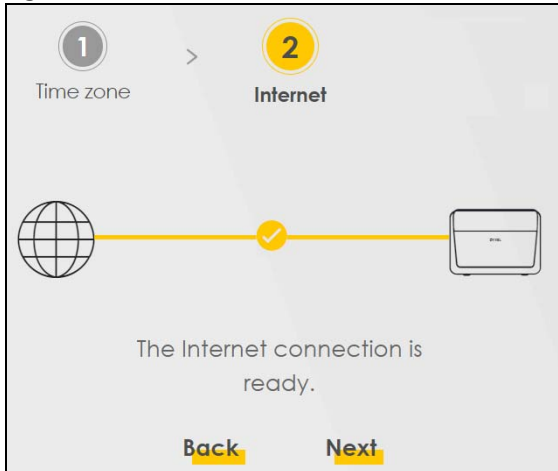
The Zyxel Device is checking the Internet status.

Figure 14 Wizard - Internet Check

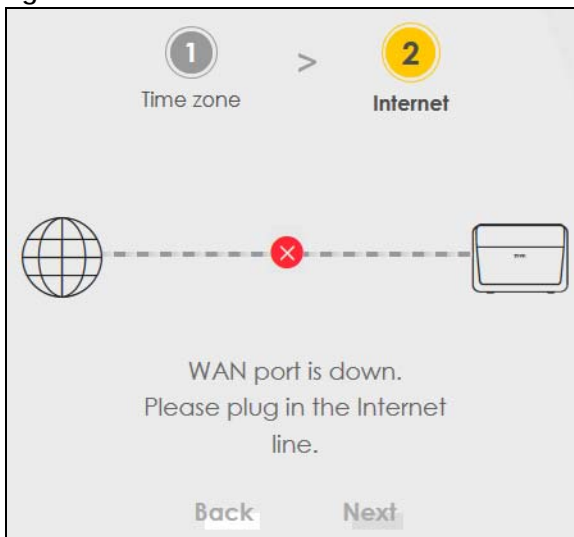


Internet Connection

The Zyxel Device has Internet access. Click **Next** to return to the **Status** screen.

Figure 15 Wizard - Successful WAN Connection

If the Zyxel Device did not detect a WAN connection, connect a DSL cable for Internet access if you have not connected any.

Figure 16 Wizard - WAN Connection is Down

PART II

Technical Reference

CHAPTER 4

Status

4.1 Status Overview

After you log into the Web Configurator, the **Status** screen appears. It shows the **Management Service**, **System Info**, and **Ethernet UNI** of the Zyxel Device.

4.1.1 Management Service

Use this panel to check if a control service (such as HTTP or Telnet) is allowed on the interfaces (LAN/WAN/Trust Domain). You can configure the services settings in the **Maintenance > Remote Management > MGMT Services** screen.

Figure 17 Management Service

Management Service	
HTTP	LAN/WAN
HTTPS	LAN/Trust Domain
FTP	LAN/WAN
TELNET	Disable
SSH	LAN/WAN
PING	LAN/WAN

4.1.2 System Info

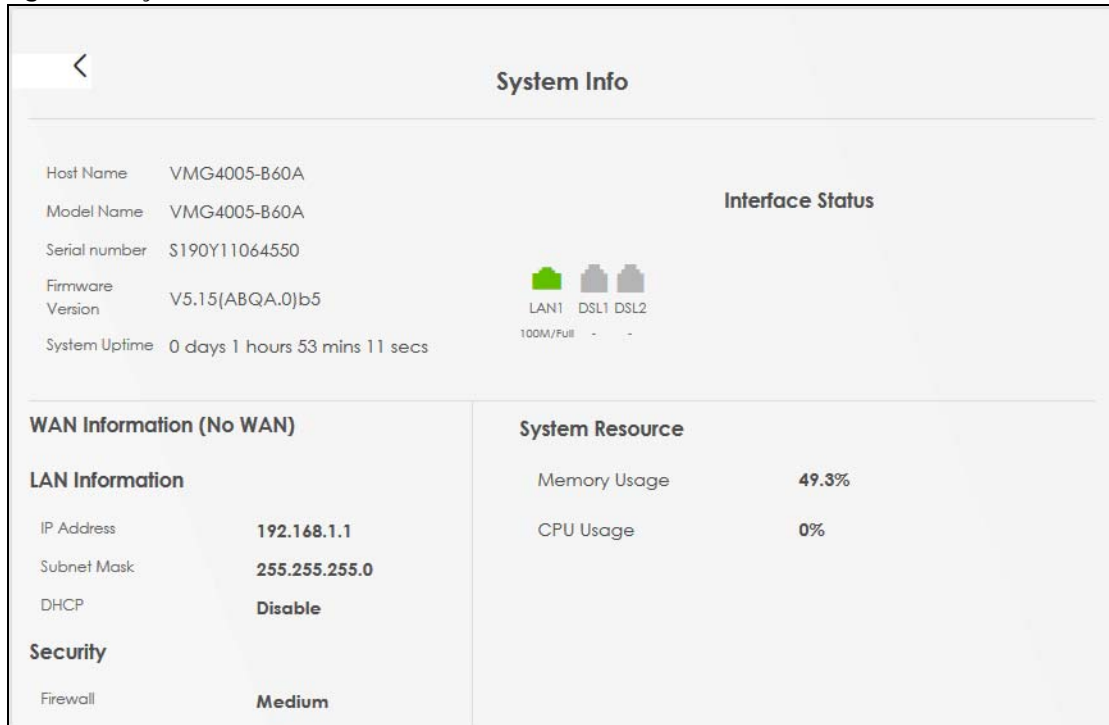
Use this screen to view the basic system information of the Zyxel Device.

Figure 18 System Info

System Info	
Model Name	VMG4005-B60A
Firmware Version	V5.15(ABQA.0)b5
System Uptime	0 days 1 hours 42 mins 35 secs
LAN MAC Address	CC:D4:A1:AF:88:98
DSL1 Status	Connection down
DSL2 Status	Connection down

Click the Arrow icon (➔) to open the following screen. Use this screen to view more system information, WAN/LAN/Firewall information, interface status (LAN and DSL), and usage of system resource.

Figure 19 System Info: Detailed Information



Each field is described in the following table.

Table 8 System Info: Detailed Information

LABEL	DESCRIPTION
Host Name	This field displays the Zyxel Device system name. It is used for identification.
Model Name	This shows the model number of your Zyxel Device.
Serial Number	This field displays the serial number of the Zyxel Device.
Firmware Version	This is the current version of the firmware on the Zyxel Device.
System Up Time	This field displays how long the Zyxel Device has been running since it last started up. The Zyxel Device starts up when you plug it in, when you restart it (Maintenance > Reboot), or when you reset it.
Interface Status	
Virtual ports are shown here. You can see whether the ports are in use and their transmission rate.	
WAN Information (These fields display when you have an Internet connection.)	
Encapsulation	This field displays the current encapsulation method.
IP Address	This field displays the current IPv4 address of the Zyxel Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
IPv6 Address	This field displays the current IPv6 address of the Zyxel Device in the WAN.
MAC Address	This shows the WAN Ethernet adapter MAC (Media Access Control) address of your Zyxel Device.
Primary DNS server	This field displays the first DNS server address assigned by the ISP.

Table 8 System Info: Detailed Information (continued)

LABEL	DESCRIPTION
Secondary DNS server	This field displays the second DNS server address assigned by the ISP.
Primary DNSv6 server	This field displays the first DNS server IPv6 address assigned by the ISP.
Secondary DNSv6 server	This field displays the second DNS server IPv6 address assigned by the ISP.
LAN Information (These fields display information about the LAN port.)	
IP Address	This is the current IPv4 address of the Zyxel Device.
Subnet Mask	This is the current subnet mask.
DHCP	<p>This field displays what DHCP services the Zyxel Device is providing to the LAN. The possible values are:</p> <p>Server - The Zyxel Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.</p> <p>Relay - The Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.</p> <p>None - The Zyxel Device is not providing any DHCP services to the LAN.</p>
Security	
Firewall	This displays the firewall's current security level.
System Resource	
Memory Usage	This field displays what percentage of the Zyxel Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the Zyxel Device is probably becoming unstable, and you should restart the device.
CPU Usage	This field displays what percentage of the Zyxel Device's processing ability is currently used. When this percentage is close to 100%, the Zyxel Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS).

4.1.3 Ethernet UNI

Use this panel to check the link state of the LAN connection. You can configure the link settings in the **Network Setting > Home Networking > Ethernet UNI** screen. The **Administrative status of UNI** displays if the LAN interface is enabled (**Up**) or not (**Down**) in the **Network Setting > Home Networking > Ethernet UNI** screen. The **Link State of UNI** displays the current link state of the LAN interface.

Figure 20 Ethernet UNI

Ethernet UNI	
Administrative status of UNI	Up
Link State of UNI	Up
Speed State	1000 (Mbps)
Duplex State	Full

CHAPTER 5

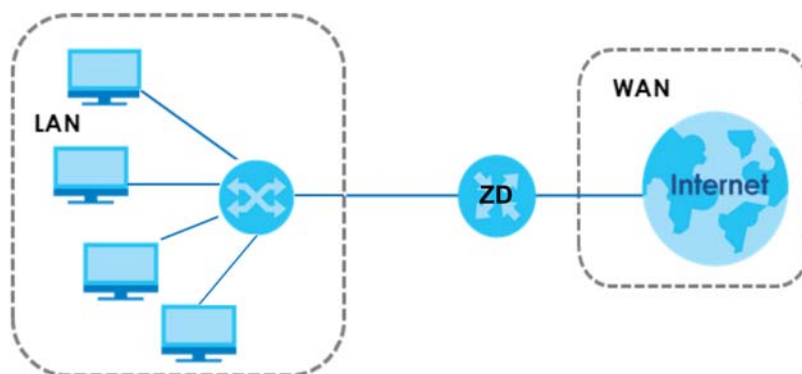
Broadband

5.1 Broadband Overview

This chapter discusses the Zyxel Device's **Broadband** screens. Use these screens to configure your Zyxel Device for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 21 LAN and WAN



5.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view, remove or add a WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access ([Section 5.2 on page 37](#)).
- Use the **Advanced** screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions ([Section 5.3 on page 45](#)).

Table 9 WAN Setup Overview

LAYER-2 INTERFACE		INTERNET CONNECTION		
CONNECTION	DSL LINK TYPE	MODE	ENCAPSULATION	CONNECTION SETTINGS
VDSL over PTM	N/A	Routing	PPPoE	PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
			IPoE	IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		Bridge	N/A	VLAN and QoS

Table 9 WAN Setup Overview (continued)

LAYER-2 INTERFACE		INTERNET CONNECTION		
CONNECTION	DSL LINK TYPE	MODE	ENCAPSULATION	CONNECTION SETTINGS
ADSL over ATM	EoA	Routing	PPPoE/PPPoA	ATM PVC configuration, PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
			IPoE/IPoA	ATM PVC configuration, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		Bridge	N/A	ATM PVC configuration, and QoS

5.1.2 What You Need to Know

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

WAN IP Address

The WAN IP address is an IP address for the Zyxel Device, which makes it accessible from an outside network. It is used by the Zyxel Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the Zyxel Device tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es).

ATM

Asynchronous Transfer Mode (ATM) is a WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC).

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

IPv6 Introduction

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses. The Zyxel Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

IPv6 Prefix and Prefix Length

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

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

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

IPv6 Subnet Masking

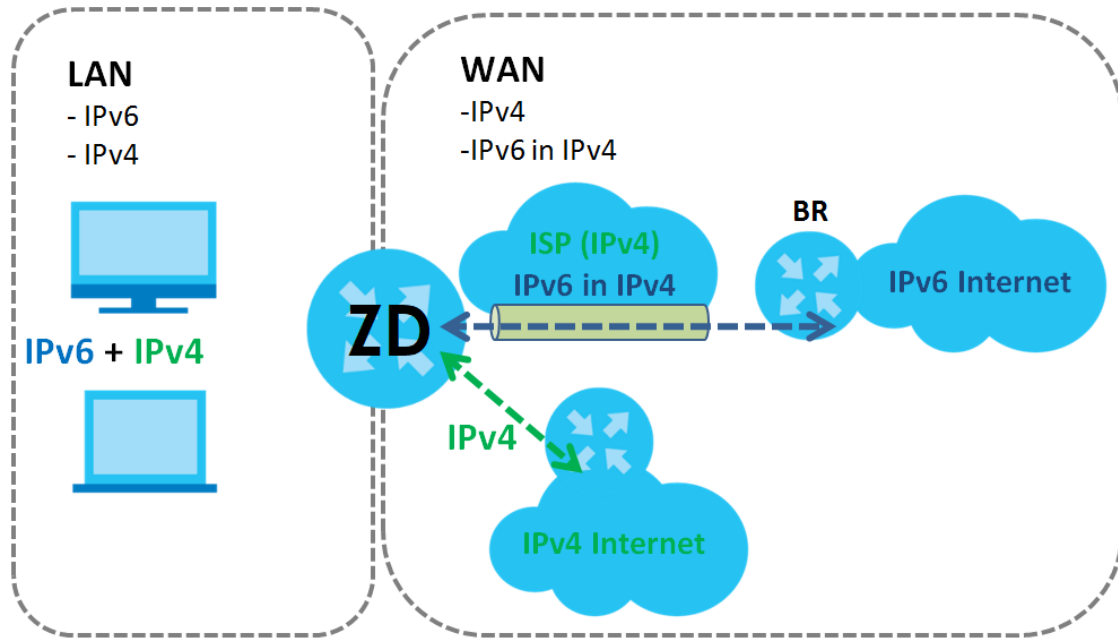
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example,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

IPv6 Rapid Deployment

Use IPv6 Rapid Deployment (6rd) when the local network uses IPv6 and the ISP has an IPv4 network. When the Zyxel Device has an IPv4 WAN address and you set **IPv6/IPv4 Mode** to **IPv4 Only**, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.

The Zyxel Device generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router (BR in the figure) to connect to the native IPv6 Internet. The local network can also use IPv4 services. The Zyxel Device uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 22 IPv6 Rapid Deployment

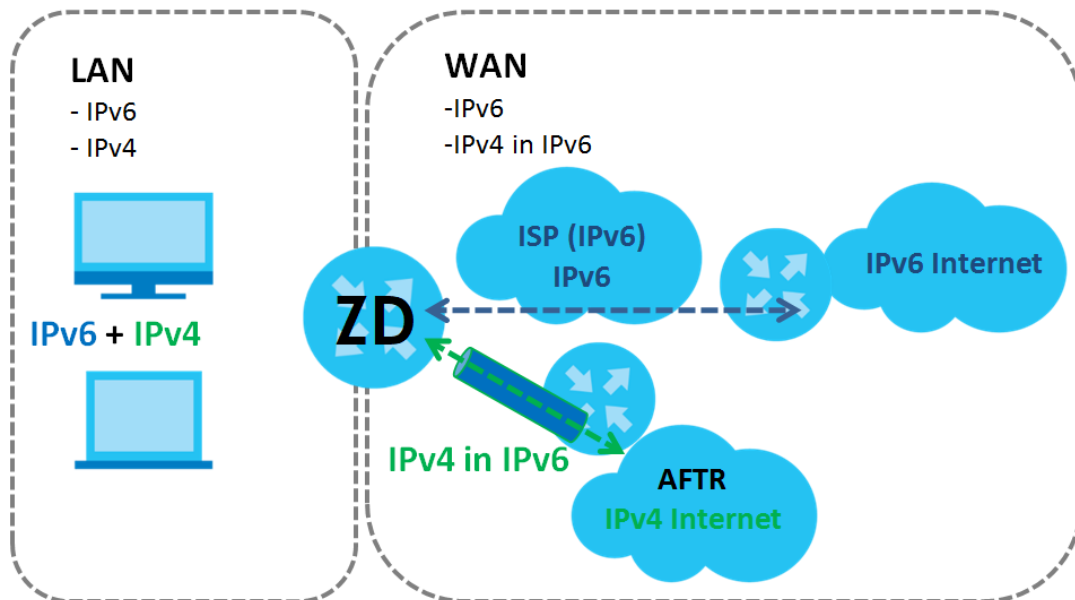


Dual Stack Lite

Use Dual Stack Lite when local network computers use IPv4 and the ISP has an IPv6 network. When the Zyxel Device has an IPv6 WAN address and you set **IPv6/IPv4 Mode** to **IPv6 Only**, you can enable Dual Stack Lite to use IPv4 computers and services.

The Zyxel Device tunnels IPv4 packets inside IPv6 encapsulation packets to the ISP's Address Family Transition Router (AFTR in the graphic) to connect to the IPv4 Internet. The local network can also use IPv6 services. The Zyxel Device uses its configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

Figure 23 Dual Stack Lite



5.1.3 Before You Begin






You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

5.2 The Broadband Screen

Use this screen to change your Zyxel Device's Internet access settings. The summary table shows you the configured WAN services (connections) on the Zyxel Device. Use information provided by your ISP to configure WAN settings.

Click **Network Setting** > **Broadband** to access this screen.

Figure 24 Network Setting > Broadband

Broadband Advanced										
Use this screen to change your Zyxel Device's Internet access settings. The summary table shows you the configured WAN services (connections) on the Zyxel Device. Use information provided by your ISP to configure WAN settings.										
										 Add New WAN Interface
#	Name	Type	Mode	Encapsulation	802.1p	802.1q	NAT	Default Gateway	IPv6	Modify
1	Bridge_ATM	ATM	Bridge	Bridge	N/A	N/A	N	N	N	 
2	Bridge_PTM	PTM	Bridge	Bridge	N/A	N/A	N	N	N	 

The following table describes the labels in this screen.

Table 10 Network Setting > Broadband

LABEL	DESCRIPTION
Add New WAN Interface	Click this button to create a new connection.
#	This is the index number of the entry.
Name	This is the service name of the connection.
Type	This shows whether it is an ATM, Ethernet or a PTM connection.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.
802.1p	This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays N/A when there is no priority level assigned.
802.1q	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays N/A when there is no VLAN ID number assigned.
NAT	This shows whether NAT is activated or not for this connection.
Default Gateway	This shows whether the Zyxel Device use the WAN interface of this connection as the system default gateway.
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service.
Modify	Click the Edit icon to configure the WAN connection. Click the Delete icon to remove the WAN connection.

5.2.1 Add/Edit Internet Connection

Click **Add New WAN Interface** in the Broadband screen or the **Edit** icon next to an existing WAN interface to open the following screen. Use this screen to configure a WAN connection. The screen varies depending on the interface type, mode, encapsulation, and IPv6/IPv4 mode you select.

5.2.1.1 The Routing Mode

Use **Routing** mode if your ISP give you one IP address only and you want multiple computers to share an Internet account.

The following example screen displays when you select the **VDSL over PTM** connection type, **Routing** mode, and **PPPoE** encapsulation. The screen varies when you select other interface type, encapsulation, and IPv6/IPv4 mode.

Figure 25 Network Setting > Broadband > Add/Edit New WAN Interface (Routing Mode)

Add New WAN Interface

General ☒

Name:

Type: **VDSL over PTM**

Mode: **Routing**

Encapsulation: **PPPoE**

IPv4/IPv6 Mode: **IPv4 IPv6 DualStack**

PPP Information

PPP User Name:

PPP Password:

PPP Connection Trigger: ☒ Auto Connect ☐ On Demand

PPPoE Passthrough: ☐

VLAN ☐

802.1p:

802.1q: (0~4094)

MTU

MTU:

IP Address

☒ Obtain an IP Address Automatically

☐ Static IP Address

DNS Server

☒ Obtain DNS Info Automatically

☐ Use Following Static DNS Address

Routing Feature

NAT: ☒ **Apply as Default Gateway** ☐

Fullcone NAT: ☐

IPv6 Address

☒ Obtain an IPv6 Address Automatically

☐ Static IPv6 Address

IPv6 DNS Server

☒ Obtain IPv6 DNS Info Automatically

☐ Use Following Static IPv6 DNS Address

IPv6 Routing Feature

Apply as Default Gateway ☐

Cancel **Apply**

The following table describes the labels in this screen.

Table 11 Network Setting > Broadband > Add/Edit New WAN Interface (Routing Mode)

LABEL	DESCRIPTION
General	
Click the switch to the right to enable this WAN interface. Otherwise, click the switch to the left to disable.	
Name	Specify a descriptive name for this connection. Up to 15 printable ASCII characters are allowed except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;].
Type	Select whether it is an VDSL over PTM or ADSL over ATM connection.
Mode	Select Routing if your ISP give you one IP address only and you want multiple computers to share an Internet account. Otherwise, select Bridge .
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select Routing in the Mode field. The choices depend on the connection type you selected. If your connection type is VDSL over PTM , the choices are PPPoE and IPoE . If your connection type is ADSL over ATM , the choices are PPPoE , PPPoA , IPoE and IPoA .
IPv4/IPv6 Mode	Select IPv4 Only if you want the Zyxel Device to run IPv4 only. Select IPv4 IPv6 DualStack to allow the Zyxel Device to run IPv4 and IPv6 at the same time. Select IPv6 Only if you want the Zyxel Device to run IPv6 only.
PPP Information (This is available only when you select PPPoE or PPPoA in the Mode field.)	
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above. Select password unmask to show your entered password in plain text.
PPP Connection Trigger	Select when to have the Zyxel Device establish the PPP connection. Auto Connect - select this to not let the connection time out. On Demand - select this to automatically bring up the connection when the Zyxel Device receives packets destined for the Internet.
Idle Timeout	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server. This field is not available if you select Auto Connect in the PPP Connection Trigger field.
PPPoE Passthrough	This field is available when you select PPPoE encapsulation. In addition to the Zyxel Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Zyxel Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
ATM PVC Configuration (These fields appear when the Type is set to ADSL over ATM .)	
VPI [0-255]	The valid range for the VPI is 0 to 255. Type the VPI assigned to you.
VCI [32-65535]	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.

Table 11 Network Setting > Broadband > Add/Edit New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
Encapsulation	<p>Select the method of multiplexing used by your ISP from the drop-down list box. Choices are:</p> <ul style="list-style-type: none"> • LLC/SNAP-BRIDGING: In LLC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. • VC/MUX: In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the Zyxel Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.
Service Category	<p>Select UBR Without PCR for applications that are non-time sensitive, such as email.</p> <p>Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.</p> <p>Select Non Realtime VBR (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.</p> <p>Select Realtime VBR (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.</p>
Peak Cell Rate [cells/s]	<p>This field appears when you set the Service Category to CBR, Non Realtime VBR, or Realtime VBR.</p> <p>Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.</p>
Sustainable Cell Rate	<p>This field appears when you set the Service Category to Non Realtime VBR or Realtime VBR.</p> <p>The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.</p>
Maximum Burst Size [cells]	<p>This field appears when you set the Service Category to Non Realtime VBR or Realtime VBR.</p> <p>Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.</p>
VLAN Click the switch to the right to enable VLAN on this WAN interface. Otherwise, click the switch to the left to disable.	
802.1p	<p>IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.</p> <p>Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.</p>
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
MTU	
MTU	Enter the Maximum Transfer Unit (MTU) size for this traffic.
IP Address (This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Static IP Address	Select this option if the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the gateway IP address provided by your ISP.
DNS Server (This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
Obtain DNS Info Automatically	Select this if you want the Zyxel Device to use the DNS server addresses assigned by your ISP.
Use Following Static DNS Address	Select this if you want the Zyxel Device to use the DNS server addresses you configure manually.

Table 11 Network Setting > Broadband > Add/Edit New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
Routing Feature (This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
NAT	Click the switch to the right to enable NAT on this connection. Otherwise, click the switch to the left to disable.
Apply as Default Gateway	Click this switch to the right to have the Zyxel Device use the WAN interface of this connection as the system default gateway. Otherwise, click the switch to the left.
Fullcone NAT	Click this switch to the right to enable full cone NAT on this connection. Otherwise, click the switch to the left to disable. This field is available only when you activate NAT . In full cone NAT, the Zyxel Device maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The Zyxel Device also maps packets coming to that external IP address and port to the internal IP address and port.
6RD The 6RD (IPv6 rapid deployment) fields display when you set the IPv6/IPv4 Mode field to IPv4 Only . See IPv6 Rapid Deployment on page 35 for more information. Click this switch to the right to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.	
Automatically configured by DHCP	This option is configurable only when you set the method of encapsulation to IPoE . Select this to have the Zyxel Device detect the relay server automatically through DHCP.
Manually Configured	Select this if you have the IPv4 address of the relay server.
Service Provider IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet.
IPv4 Mask Length	Enter the subnet mask number (1~32) for the IPv4 network.
Border Relay IPv4 Address	When you select Manually Configured , specify the relay server's IPv4 address in this field.
DHCP Options (This is available only when you set Encapsulation to IPoE and select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
Request Options	Select Option 43 to have the Zyxel Device get vendor specific information from DHCP packets sent from the DHCP server. Select Option 121 to have the Zyxel Device get static route information from DHCP packets sent from the DHCP server.
Sent Options	
option 60	Select this and enter the device identity you want the Zyxel Device to add in the DHCP discovery packets that go to the DHCP server.
Vendor ID	Enter the Vendor Class Identifier, such as the type of the hardware or firmware.
option 61	Select this and enter any string that identifies the device.
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DUID	Enter the hardware type, a time value and the MAC address of the device.
option 125	Select this to have the Zyxel Device automatically generate and add vendor specific parameters in the DHCP discovery packets that go to the DHCP server.
IPv6 Address (This is available only when you select IPv4 IPv6 DualStack or IPv6 Only in the IPv4/IPv6 Mode field.)	

Table 11 Network Setting > Broadband > Add/Edit New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
Obtain an IPv6 Address Automatically	Select this if you want to have the Zyxel Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Static IPv6 Address	Select this if you have a fixed IPv6 address assigned by your ISP. When you select this, the following fields appear.
IPv6 Address	Enter an IPv6 IP address that your ISP gave to you for this WAN interface.
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
IPv6 Default Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your Zyxel Device's interface(s). The gateway helps forward packets to their destinations.
IPv6 DNS Server (This is available only when you select IPv4 IPv6 DualStack or IPv6 Only in the IPv4/IPv6 Mode field. Configure the IPv6 DNS server in the following section.)	
Obtain IPv6 DNS Info Automatically	Select this to have the Zyxel Device get the IPv6 DNS server addresses from the ISP automatically.
Use Following Static IPv6 DNS Address	Select this to have the Zyxel Device use the IPv6 DNS server addresses you configure manually.
Primary DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.
IPv6 Routing Feature (This is available only when you select IPv4 IPv6 DualStack or IPv6 Only in the IPv4/IPv6 Mode field. You can enable IPv6 routing features in the following section.)	
Apply as Default Gateway	Select this option to have the Zyxel Device use the WAN interface of this connection as the system default gateway.
DS-Lite	<p>This is available only when you select IPv6 Only in the IPv4/IPv6 Mode field. Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network. See Dual Stack Lite on page 36 for more information.</p> <p>Click the switch to the right to let local computers use IPv4 through an ISP's IPv6 network. Otherwise, click the switch to the left to disable DS-Lite.</p>
DS-Lite Relay Server IP	Specify the transition router's IPv6 address.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

5.2.1.2 The Bridge Mode

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **Bridge** as the encapsulation mode. The screen varies depending on the interface type you select.

The following example screen displays when you select the **ADSL over ATM** connection type, **Bridge** mode

Figure 26 Network Setting > Broadband > Add/Edit New WAN Interface (Bridge Mode)

Add New WAN Interface

General ☒

Name

Type **ADSL over ATM** ▼

Mode **Bridge** ▼

ATM PVC Configuration

VPI [0-255]

VCI [32-65535]

Encapsulation **LLC/SNAP-BRIDGIN** ▼

Service Category **UBR Without PCR** ▼

VLAN ☐

802.1p

802.1q (0~4094)

MTU

MTU

Cancel **Apply**

The following table describes the fields in this screen.

Table 12 Network Setting > Broadband > Add/Edit New WAN Interface (Bridge Mode)


LABEL	DESCRIPTION
General	Click this switch to enable or disable the interface. When the switch goes to the right  , the function is enabled. Otherwise, it's not.
Name	Enter a service name of the connection.
Type	Select whether it is an VDSL over PTM or ADSL over ATM connection. Select ADSL over ATM to have the Zyxel Device uses the ADSL technology for data transmission over the DSL port. Select VDSL over PTM to have the Zyxel Device uses the VDSL technology for data transmission over the DSL port.
Mode	Select Routing if your ISP give you one IP address only and you want multiple computers to share an Internet account. Otherwise, select Bridge .
ATM PVC Configuration (These fields appear when the Type is set to ADSL over ATM .)	
VPI [0-255]	The valid range for the VPI is 0 to 255. Type the VPI assigned to you.
VCI [32-65535]	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.

Table 12 Network Setting > Broadband > Add/Edit New WAN Interface (Bridge Mode) (continued)

LABEL	DESCRIPTION
Encapsulation	<p>Select the method of multiplexing used by your ISP from the drop-down list box. Choices are:</p> <ul style="list-style-type: none"> • LLC/SNAP-BRIDGING: In LLC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. • VC/MUX: In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the Zyxel Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.
Service Category	<p>Select UBR Without PCR for applications that are non-time sensitive, such as email.</p> <p>Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.</p> <p>Select Non Realtime VBR (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.</p> <p>Select Realtime VBR (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.</p>
Peak Cell Rate [cells/s]	<p>This field appears when you set the Service Category to CBR, Non Realtime VBR, or Realtime VBR.</p> <p>Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.</p>
Sustainable Cell Rate	<p>This field appears when you set the Service Category to Non Realtime VBR or Realtime VBR.</p> <p>The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.</p>
Maximum Burst Size [cells]	<p>This field appears when you set the Service Category to Non Realtime VBR or Realtime VBR.</p> <p>Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.</p>
<p>VLAN</p> <p>Slide the switch to the right to enable VLAN on this WAN interface. Otherwise, slide the switch to the left to disable.</p>	
802.1p	<p>IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.</p> <p>Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.</p>
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
MTU	
MTU	Enter the MTU (Maximum Transfer Unit) size for this traffic.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

5.3 The Broadband Advanced Screen

Use the **Advanced** screen to enable or disable ADSL over PTM, Annex M, DSL PhyR, and SRA (Seamless Rate Adaptation) functions. The Zyxel Device supports the PhyR retransmission scheme. PhyR is a retransmission scheme designed to provide protection against noise on the DSL line. It improves voice, video and data transmission resilience by utilizing a retransmission buffer. It also lists ITU-T G.993.2 standard VDSL profiles you can comply with.

ITU-T G.993.2 standard defines a wide range of settings for various parameters, some of which are encompassed in profiles as shown in the next table.

Note: If the settings in the screen are changed, the Zyxel Device will re-establish the DSL connection(s).

Table 13 VDSL Profiles

PROFILE	BANDWIDTH (MHZ)	NUMBER OF DOWNSTREAM CARRIERS	CARRIER BANDWIDTH (KHZ)	POWER (DBM)	MAX. DOWNSTREAM THROUGHPUT (MBIT/S)
8a	8.832	2048	4.3125	17.5	50
8b	8.832	2048	4.3125	20.5	50
8c	8.5	1972	4.3125	11.5	50
8d	8.832	2048	4.3125	14.5	50
12a	12	2783	4.3125	14.5	68
12b	12	2783	4.3125	14.5	68
17a	17.664	4096	4.3125	14.5	100
35b	35.328	8192	4.3125	17.0	300

Click **Network Setting** > **Broadband** > **Advanced** to display the following screen.

Figure 27 Network Setting > Broadband > Advanced

Broadband

Advanced

Use the **Advanced** screen to enable or disable PTM over ADSL, Annex M, DSL PhyR, and SRA (Seamless Rate Adaptation) functions. The Zyxel Device supports the PhyR retransmission scheme. PhyR is a retransmission scheme designed to provide protection against noise on the DSL line. It improves voice, video and data transmission resilience by utilizing a retransmission buffer. It also lists ITU-T G.993.2 standard VDSL profiles you can comply with.

DSL Capabilities

PhyR US

☐

PhyR DS

☐

Bitswap

☒

SRA

☒

DSL Modulation

PTM over ADSL

☒

G.dmt

☒

G.lite

☒

T1.413

☒

ADSL2

☒

Annex L

☒

ADSL2+

☒

Annex M/J

☒

VDSL2

☒

VDSL Profile

8a Enable

☒

8b Enable

☒

8c Enable

☒

8d Enable

☒

12a Enable

☒

12b Enable

☒

17a Enable

☒

30a Enable

☒

35b Enable

☒

US0

☒

Cancel

Apply

The following table describes the labels in this screen.

Table 14 Network Setting > Broadband > Advanced

LABEL	DESCRIPTION
DSL Capabilities	
PhyR US	Enable or disable PhyR US (upstream) for upstream transmission to the WAN. PhyR US should be enabled if data being transmitted upstream is sensitive to noise. However, enabling PhyR US can decrease the US line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled.
PhyR DS	Enable or disable PhyR DS (downstream) for downstream transmission from the WAN. PhyR DS should be enabled if data being transmitted downstream is sensitive to noise. However, enabling PhyR DS can decrease the DS line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled.
Bitswap	Select Enable to allow the Zyxel Device to adapt to line changes when you are using G.dmt. Bit-swapping is a way of keeping the line more stable by constantly monitoring and redistributing bits between channels.
SRA	Enable or disable Seamless Rate Adaption (SRA). Select Enable to have the Zyxel Device automatically adjust the connection's data rate according to line conditions without interrupting service.
DSL Modulation	
PTM over ADSL	Select Enable to use PTM over ADSL. Since PTM has less overhead than ATM, some ISPs use this for better performance.
G.dmt	ITU G.992.1 (better known as G.dmt) is an ITU standard for ADSL using discrete multitone modulation. G.dmt full-rate ADSL expands the usable bandwidth of existing copper telephone lines, delivering high-speed data communications at rates up to 8 Mbit/s downstream and 1.3 Mbit/s upstream.
G.lite	ITU G.992.2 (better known as G.lite) is an ITU standard for ADSL using discrete multitone modulation. G.lite does not strictly require the use of DSL filters, but like all variants of ADSL generally functions better with splitters.
T1.413	ANSI T1.413 is a technical standard that defines the requirements for the single asymmetric digital subscriber line (ADSL) for the interface between the telecommunications network and the customer installation in terms of their interaction and electrical characteristics.
ADSL2	It optionally extends the capability of basic ADSL in data rates to 12 Mbit/s downstream and, depending on Annex version, up to 3.5 Mbit/s upstream (with a mandatory capability of ADSL2 transceivers of 8 Mbit/s downstream and 800 kbit/s upstream).
Annex L	Annex L is a specification in the ITU-T ADSL2 recommendation G.992.3 titled Specific requirements for a Reach Extended ADSL2 (READSL2) system operating in the frequency band above POTS, therefore it is often referred to as Reach Extended ADSL2 or READSL2. The main difference between this specification and commonly deployed Annex A is the maximum distance that can be used. The power of the lower frequencies used for transmitting data is boosted up to increase the reach of this signal up to 7 kilometers (23,000 ft).
ADSL2+	ADSL2+ extends the capability of basic ADSL by doubling the number of downstream channels. The data rates can be as high as 24 Mbit/s downstream and up to 1.4 Mbit/s upstream depending on the distance from the DSLAM to the customer's premises.

Table 14 Network Setting > Broadband > Advanced (continued)

LABEL	DESCRIPTION
Annex M/J	<p>Annex M and Annex J are specified in ITU-T recommendations G.992.3 (ADSL2) and G.992.5 (ADSL2+). Annex M and Annex J enhance the capabilities of Annex A and Annex B by increasing the upstream transmission data rate, but slightly reduce the downstream data rates as a trade-off. Annex M supports data rates of up to 12 Mbit/s downstream and 3.5 Mbit/s upstream for ADSL2, and up to 24 Mbit/s downstream and 2.5 Mbit/s upstream for ADSL2+. Annex J supports data rates of up to 12 Mbit/s downstream and 3.5 Mbit/s upstream for ADSL2, and up to 24 Mbit/s downstream and 3.5 Mbit/s upstream for ADSL2+. However, the actual downstream/upstream data rates depend on the distance from the ISP DSLAM to the Zyxel Device and the quality of your telephone line.</p> <p>Click the switch to enable the Zyxel Device to use Annex M for Zyxel Device models that use POTS WAN connection, and use Annex J for Zyxel Device models that use ISDN WAN connection. Check Section 1.1 on page 11 to see whether your Zyxel Device model uses POTS or ISDN WAN.</p>
VDSL2	VDSL2 (Very High Speed Digital Subscriber Line 2) is the second generation of the VDSL standard (which is currently denoted VDSL1). VDSL2 is defined in G.993.2.
VDSL Profile VDSL2 profiles differ in the width of the frequency band used to transmit the broadband signal. Profiles that use a wider frequency band can deliver higher maximum speeds.	
8a, 8b, 8c, 8d, 12a, 12b, 17a, 30a, 35b US0	<p>The G.993.2 VDSL standard defines a wide range of profiles that can be used in different VDSL deployment settings, such as in a central office, a street cabinet or a building.</p> <p>The Zyxel Device must comply with at least one profile specified in G.993.2. but compliance with more than one profile is allowed.</p>
Cancel	Click Cancel to return to the previous configuration.
Apply	Click Apply to save your changes back to the Zyxel Device.

5.4 Technical Reference

The following section contains additional technical information about the Zyxel Device features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The Zyxel Device can work in bridge mode or routing mode. When the Zyxel Device is in routing mode, it supports the following methods.

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

PPP over ATM (PPPoA)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The Zyxel Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's

(ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

PPP over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the Zyxel Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Zyxel Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

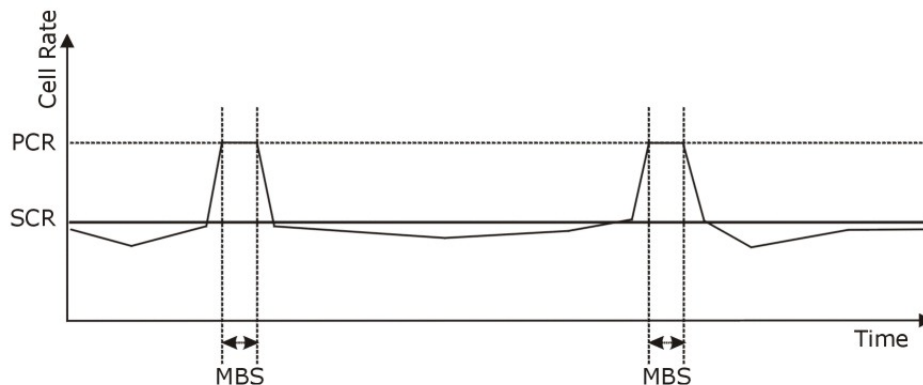
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 28 Example of Traffic Shaping



ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However, the encapsulation method assigned influences your choices for IP address and default gateway.

Introduction to VLANs

A Virtual Local Area Network (VLAN) 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.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network.

A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

Multicast

IP packets are transmitted in either one of two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

At start up, the Zyxel Device queries all directly connected networks to gather group membership. After that, the Zyxel Device periodically updates this information.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The Zyxel Device can get the DNS server addresses in the following ways.

- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- 2 If your ISP dynamically assigns the DNS server IP addresses (along with the Zyxel Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

IPv6 Prefix and Prefix Length

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

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

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

CHAPTER 6

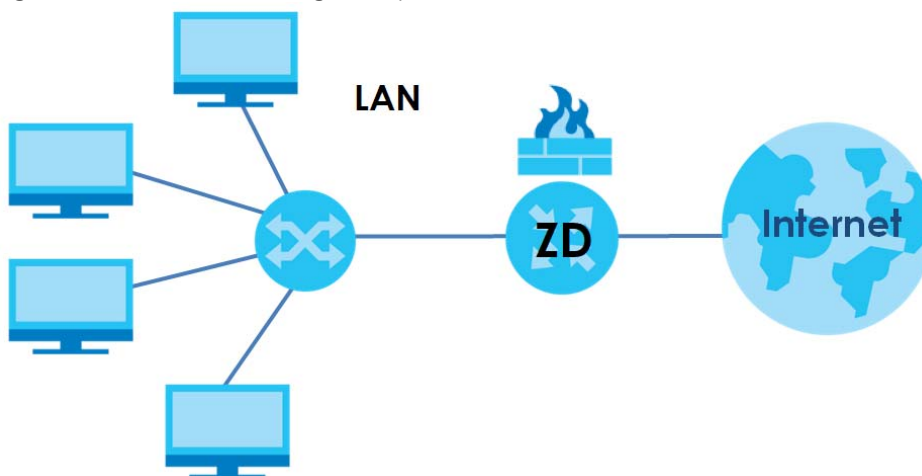
Home Networking

6.1 Home Networking Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually located in one immediate area such as a building or floor of a building.

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

Figure 29 Home Networking Example



6.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings ([Section 6.2 on page 56](#)).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC addresses ([Section 6.3 on page 62](#)).
- Use the **Ethernet UNI** screen to set the link speed and duplex mode for the Zyxel Device Ethernet LAN port ([Section 6.4 on page 63](#)).

6.1.2 What You Need To Know

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

6.1.2.1 About LAN

IP Address

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number. This is known as an Internet Protocol address.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your Zyxel Device will compute the subnet mask automatically based on the IP address that you entered. You do not need to change the subnet mask computed by the Zyxel Device unless you are instructed to do otherwise.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server. This Zyxel Device has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DNS

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

RADVD (Router Advertisement Daemon)

When an IPv6 host sends a Router Solicitation (RS) request to discover the available routers, RADVD with Router Advertisement (RA) messages in response to the request. It specifies the minimum and maximum intervals of RA broadcasts. RA messages containing the address prefix. IPv6 hosts can be generated with the IPv6 prefix an IPv6 address.

6.1.3 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

6.2 LAN Setup

A LAN IP address is the IP address of a networking device in the LAN. You can use the Zyxel Device's LAN IP address to access its Web Configurator from the LAN. The DHCP server settings define the rules on assigning IP addresses to LAN clients on your network.

Use this screen to set the Local Area Network IP address and subnet mask of your Zyxel Device. Configure DHCP settings to have the Zyxel Device or a DHCP server assign IP addresses to devices. Click **Network Setting > Home Networking** to open the **LAN Setup** screen.

Follow these steps to configure your LAN settings.

- 1 Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your Zyxel Device.
- 2 Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.

- 3 Click **Apply** to save your settings.

Figure 30 Network Setting > Home Networking > LAN Setup

The screenshot shows the 'LAN Setup' configuration page. At the top, there are three tabs: 'LAN Setup' (selected), 'Static DHCP', and 'Ethernet UNI'. Below the tabs is a descriptive text box: 'Use this screen to set the Local Area Network IP address and subnet mask of your Zyxel Device. Configure DHCP settings to have the Zyxel Device or a DHCP server assign IP addresses to devices.'

The configuration is organized into several sections:

- Interface Group:** A dropdown menu for 'Group Name' is set to 'Default'.
- LAN IP Setup:** Two rows of input fields. The first row is for 'IP Address' with values 192, 168, 1, and 123. The second row is for 'Subnet Mask' with values 255, 255, 255, and 0.
- DHCP Server State:** A section with the label 'DHCP' and three radio buttons: 'Enable' (selected), 'Disable', and 'DHCP Relay'.
- IP Addressing Values:** Two rows of input fields. The first row is for 'Beginning IP Address' with values 192, 168, 1, and 2. The second row is for 'Ending IP Address' with values 192, 168, 1, and 254. Below these is a toggle switch for 'Auto reserve IP for the same host', which is currently turned off.
- DHCP Server Lease Time:** A section with three input fields and labels: '1' days, '0' hours, and '0' minutes.
- DNS Values:** A section with the label 'DNS' and three radio buttons: 'DNS Proxy' (selected), 'Static', and 'From ISP'.

Figure 31 Network Setting > Home Networking > LAN Setup (Continued)

LAN IPv6 Mode Setup

IPv6 Active ☒

Link Local Address Type

☒ EUI64

☐ Manual

LAN Global Identifier Type

☒ EUI64

☐ Manual

LAN IPv6 Prefix Setup

☒ Delegate prefix from WAN

☐ Static

LAN IPv6 Address Assign Setup

LAN IPv6 DNS Assign Setup

DHCPv6 Configuration

DHCPv6 Active ☒ DHCPv6 Server

IPv6 Router Advertisement State

RADVD Active ☒ Enable

IPv6 DNS Values

IPv6 DNS Server 1

IPv6 DNS Server 2

IPv6 DNS Server 3

DNS Query Scenario

The following table describes the fields in this screen.

Table 15 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select an interface group to configure its LAN settings. Otherwise, select Default to configure the LAN settings of the default interface group. You can configure interface groups in Network Setting > Interface Grouping .

Table 15 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
DHCP Server State	
DHCP	<p>Select Enable to have your Zyxel Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients.</p> <p>If you select Disable, you need to manually configure the IP addresses of the computers and other devices on your LAN.</p> <p>If you select DHCP Relay, the Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.</p> <p>When DHCP is used, the following fields need to be set:</p>
DHCP Relay Server Address	
This field is only available when you select DHCP Relay in the DHCP field.	
IP Address	Enter the IPv4 IP address of the actual remote DHCP server in this field.
IP Addressing Values	
The IP Addressing Values fields appear only when you select Enable in the DHCP field.	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Enable this if you want to reserve the IP address for the same host.
DHCP Server Lease Time	
<p>This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are “recycled” and made available for future reassignment to other systems.</p> <p>This field is only available when you select Enable in the DHCP field.</p>	
Days/Hours/Minutes	DHCP server leases an address to a new client device for a period of time, called the DHCP lease time. When the lease expires, the DHCP server might assign the IP address to a different client device.
DNS Values	
This field appears only when you select Enable in the DHCP field.	

Table 15 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION						
DNS	<p>The Zyxel Device supports DNS proxy by default. The Zyxel Device sends out its own LAN IP address to the DHCP clients as the first DNS server address. DHCP clients use this first DNS server to send domain-name queries to the Zyxel Device. The Zyxel Device sends a response directly if it has a record of the domain-name to IP address mapping. If it does not, the Zyxel Device queries an outside DNS server and relays the response to the DHCP client.</p> <p>Select DNS Proxy to have the DHCP clients use the Zyxel Device's own LAN IP address. The Zyxel Device works as a DNS relay.</p> <p>Select Static if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.</p> <p>Select From ISP if your ISP dynamically assigns DNS server information (and the Zyxel Device's WAN IP address).</p>						
LAN IPv6 Mode Setup							
IPv6 Active	<p>Use this to enable or disable IPv6 activation on the Zyxel Device.</p> <p>When IPv6 activation is used, the following fields need to be set.</p>						
Link Local Address Type	<p>A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv6. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows. Select EUI64 to allow the Zyxel Device to generate an interface ID for the LAN interface's link-local address using the EUI-64 format. Otherwise, enter an interface ID for the LAN interface's link-local address if you select Manual.</p> <p>Link-local Unicast Address Format</p> <table><tr><td>1111 1110 10</td><td>0</td><td>Interface ID</td></tr><tr><td>10 bits</td><td>54 bits</td><td>64 bits</td></tr></table>	1111 1110 10	0	Interface ID	10 bits	54 bits	64 bits
1111 1110 10	0	Interface ID					
10 bits	54 bits	64 bits					
EUI64	Select this to have the Zyxel Device generate an interface ID for the LAN interface's link-local address using the EUI-64 format.						
Manual	Select this to manually enter an interface ID for the LAN interface's link-local address.						
LAN Global Identifier Type	Select EUI64 to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address. Select Manual to manually enter an interface ID for the LAN interface's global IPv6 address.						
EUI64	Select this to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address.						
Manual	Select this to manually enter an interface ID for the LAN interface's global IPv6 address.						
LAN IPv6 Prefix Setup	Select Delegate prefix from WAN to automatically obtain an IPv6 network prefix from the service provider or an uplink router. Select Static to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.						
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.						
Static	Select this option to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.						
LAN IPv6 Address Assign Setup	<p>Select how you want to obtain an IPv6 address:</p> <p>Stateless: The Zyxel Device uses IPv6 stateless auto-configuration. RADVD (Router Advertisement Daemon) is enabled to have the Zyxel Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled.</p> <p>Stateful: The Zyxel Device uses IPv6 stateful auto-configuration. The DHCPv6 server is enabled to have the Zyxel Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.</p>						

Table 15 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
LAN IPv6 DNS Assign Setup	<p>Select how the Zyxel Device provide DNS server and domain name information to the clients:</p> <p>From RA & DHCPv6 Server: The Zyxel Device provides DNS information through both router advertisements and DHCPv6.</p> <p>From DHCPv6 Server: The Zyxel Device provides DNS information through DHCPv6.</p> <p>From Router Advertisement: The Zyxel Device provides DNS information through router advertisements.</p>
DHCPv6 Configuration	
DHCPv6 Active	This shows the status of the DHCPv6. DHCP Server displays if you configured the Zyxel Device to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients.
IPv6 Router Advertisement State	
RADVD Active	This shows whether RADVD is enabled or not.
IPv6 Address Values	
The IPv6 Address Values settings appear when you select Stateful in the LAN IPv6 Address Assign Setup field.	
IPv6 Start Address	This field specifies the first of the contiguous addresses in the IPv6 address pool.
IPv6 End Address	This field specifies the last of the contiguous addresses in the IPv6 address pool.
IPv6 Domain Name	The field specifies the domain name of the IPv6 address.
IPv6 DNS Values	
IPv6 DNS Server 1 – 3	<p>Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses.</p> <p>User Defined – Select this if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the Zyxel Device passes to the DHCP clients.</p> <p>From ISP – Select this if your ISP dynamically assigns IPv6 DNS server information.</p> <p>Proxy – Select this if the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay.</p> <p>Otherwise, select None if you do not want to configure IPv6 DNS servers.</p>
DNS Query Scenario	<p>Select how the Zyxel Device handles clients' DNS information requests.</p> <p>IPv4/IPv6 DNS Server: The Zyxel Device forwards the requests to both the IPv4 and IPv6 DNS servers and sends clients the first DNS information it receives.</p> <p>IPv6 DNS Server Only: The Zyxel Device forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives.</p> <p>IPv4 DNS Server Only: The Zyxel Device forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives.</p> <p>IPv6 DNS Server First: The Zyxel Device forwards the requests to the IPv6 DNS server first and then the IPv4 DNS server. Then it sends clients the first DNS information it receives.</p> <p>IPv4 DNS Server First: The Zyxel Device forwards the requests to the IPv4 DNS server first and then the IPv6 DNS server. Then it sends clients the first DNS information it receives.</p>
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

6.3 Static DHCP

When any of the LAN clients in your network want an assigned fixed IP address, add a static lease for each LAN client. Knowing the LAN client's MAC addresses is necessary. This table allows you to assign IP addresses on the LAN to individual computers based on their MAC addresses.

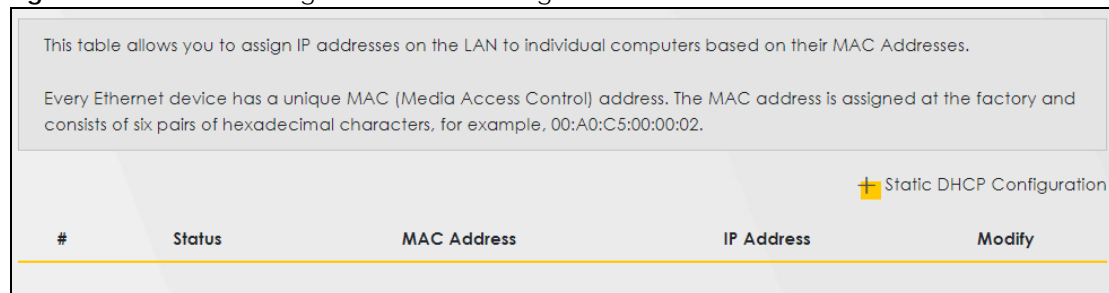
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

6.3.1 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the **Static DHCP** screen.

Use this screen to change your Zyxel Device's static DHCP settings. Click **Network Setting > Home Networking > Static DHCP** to open the following screen.

Figure 32 Network Setting > Home Networking > Static DHCP



The following table describes the labels in this screen.

Table 16 Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Static DHCP Configuration	Click this to add a new static DHCP entry.
#	This is the index number of the entry.
Status	This field displays whether the client is connected to the Zyxel Device.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address relative to the # field listed above.
Modify	Click the Edit icon to configure the connection. Click the Delete icon to remove the connection.

If you click **Static DHCP Configuration** in the **Static DHCP** screen, the following screen displays. Using a static DHCP means a LAN client will always have the same IP address assigned to it by the DHCP server. Assign a fixed IP address to a client device by selecting the interface group of this client device and its IP address type and selecting the device/computer from a list or manually entering its MAC address and assigned IP address.

Figure 33 Network Setting > Home Networking > Static DHCP: Static DHCP Configuration

The following table describes the labels in this screen.

Table 17 Network Setting > Home Networking > Static DHCP: Static DHCP Configuration

LABEL	DESCRIPTION
Active	Select Enable to activate static DHCP in your Zyxel Device.
Group Name	The Group Name is normally Default .
IP Type	The IP Type is normally IPv4 (non-configurable).
Select Device Info	Select between Manual Input which allows you to enter the next two fields (MAC Address and IP Address); or select an existing LAN device to show its MAC address and IP address.
MAC Address	Enter the MAC address of a computer on your LAN if you select Manual Input in the previous field.
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify if you select Manual Input in the previous field.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

6.4 Ethernet UNI

Ethernet User-Network Interface (UNI), is a standard interface between your LAN network and the ISP network in order to provide Ethernet services such as point-to-point Ethernet connections, Ethernet VPNs, and Ethernet access to the Internet. This is not the WAN connection. The WAN connection is through the DSL port.

Configure media type, speed and duplex mode as required by the ISP.

If you disable Ethernet UNI, WAN connections through the DSL port still work, but you will not be able to receive Ethernet services from the ISP, nor access the web configurator through the LAN port. You will have to restart the Zyxel Device to enable Ethernet UNI.

Click **Network Setting > Home Networking > Ethernet UNI** to access this screen.

Figure 34 Network Setting > Home Networking > Ethernet UNI

LAN Setup Static DHCP **Ethernet UNI**

Ethernet UNI(User Network Interface) allow the configuration of one from all possible modes of UNI operation.(e.g. auto-negotiation, 1000Mbps/FD or 100Mbps/FD.)

Ethernet UNI Setup

Interface	Enable	Media Type	Speed and Duplex State
LAN1	<input checked="" type="checkbox"/>	Auto	1000FD

Cancel Apply

The following table describes the labels in this screen.

Table 18 Network Settings > Home Networking > Ethernet UNI

LABEL	DESCRIPTION
Ethernet UNI Setup	
Interface	This displays the name of this Ethernet interface entry.
Enable	Slide the switch to the right to activate this Ethernet interface. Otherwise, slide to the left to deactivate this Ethernet interface. Connection on this interface will be down.
Media Type	Select the link speed and duplex mode of this connection. The available link speeds are 10/100/1000 Mbps. The available duplex modes are FD (Full Duplex) and HD (Half Duplex). Full-duplex mode allows data transmission in both directions at the same time. Half-duplex mode only allows data transmission in one direction at a time. Select Auto to enable auto-negotiation on this Ethernet interface. The Ethernet interface will negotiate with the peer port automatically to determine the optimum link speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Zyxel Device determines the connection speed and duplex mode by detecting the signal on the cable. Note: If you do not select Auto -negotiation, make sure the peer port uses the same duplex mode as you configured here in order to connect. If the peer port does not support the link speed you set, the Zyxel Device will automatically choose the optimum link speed available. Note: Use a Cat 5e or higher standard cable to achieve an1000 Mbps connection speed.
Speed and Duplex State	This field displays the current link speed and duplex mode of this connection. This displays - if the connection is down.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

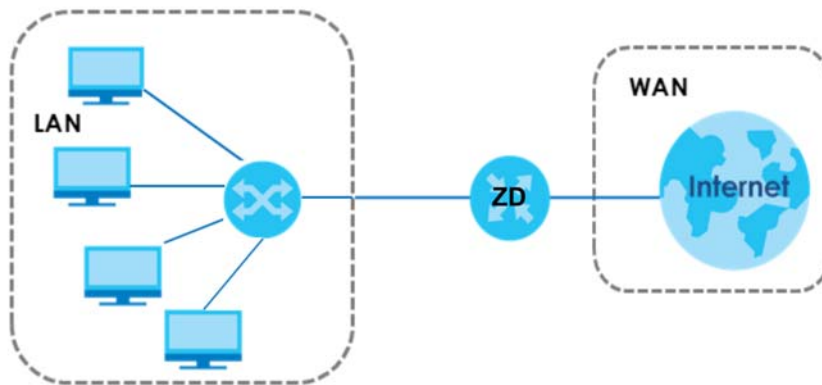
6.5 Technical Reference

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

LANs, WANs and the Zyxel Device

The actual physical connection determines whether the Zyxel Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 35 LAN and WAN IP Addresses



6.5.1 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Zyxel Device as a DHCP server or disable it. When configured as a server, the Zyxel Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The Zyxel Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

6.5.2 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.

- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The Zyxel Device supports the IPCP DNS server extensions through the DNS proxy feature.

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

6.5.3 LAN TCP/IP

The Zyxel Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the Zyxel Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Zyxel Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Zyxel Device will compute the subnet mask automatically based on the IP address that you entered. You do not need to change the subnet mask computed by the Zyxel Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

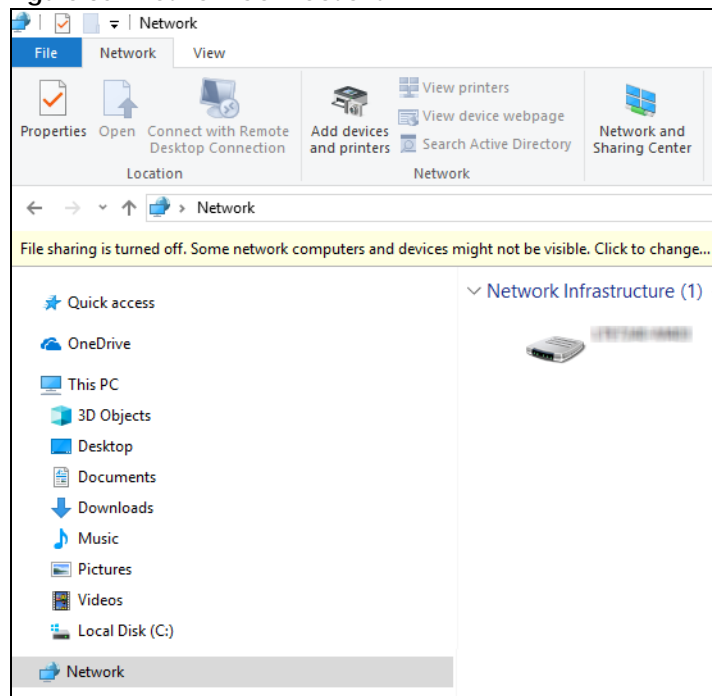
Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space".

6.6 Web Configurator Easy Access in Windows 10

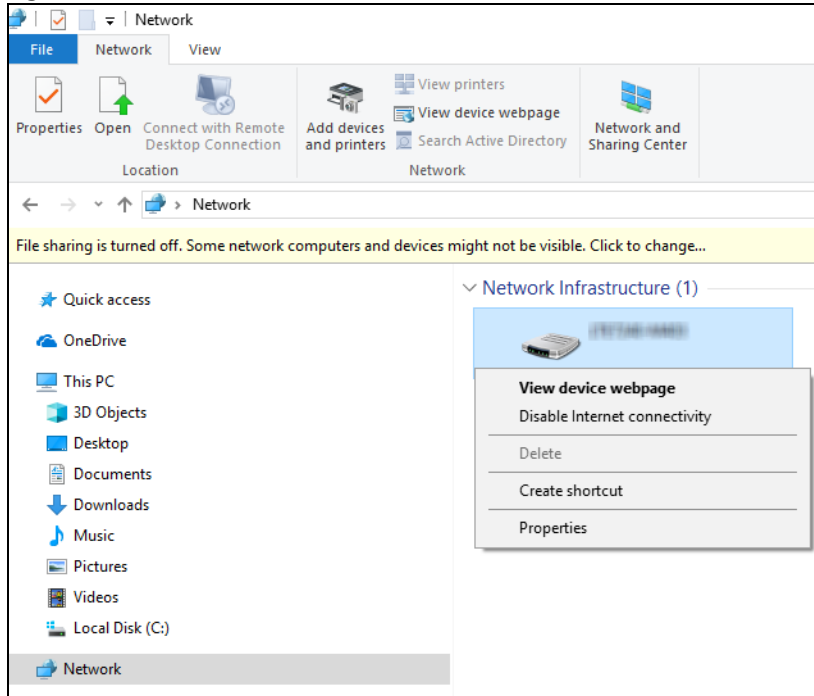
Follow the steps below to access the Web Configurator.

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

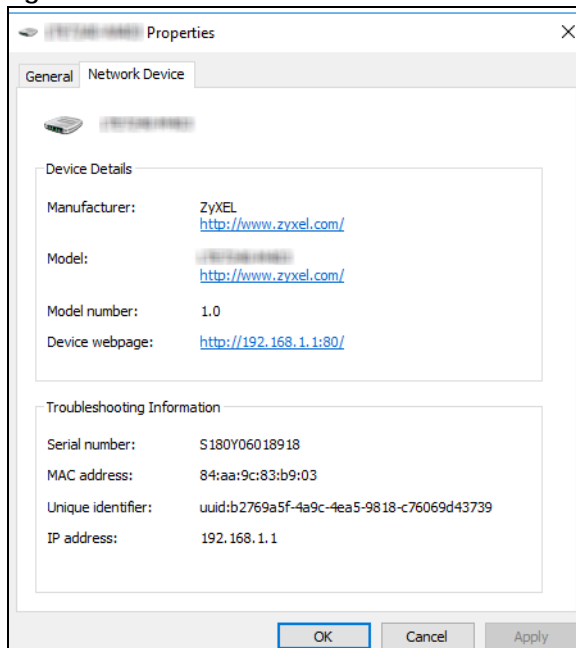
Figure 36 Network Connections



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

Figure 37 Network Connections: Network Infrastructure

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

Figure 38 Network Connections: Network Infrastructure: Properties: Example

CHAPTER 7

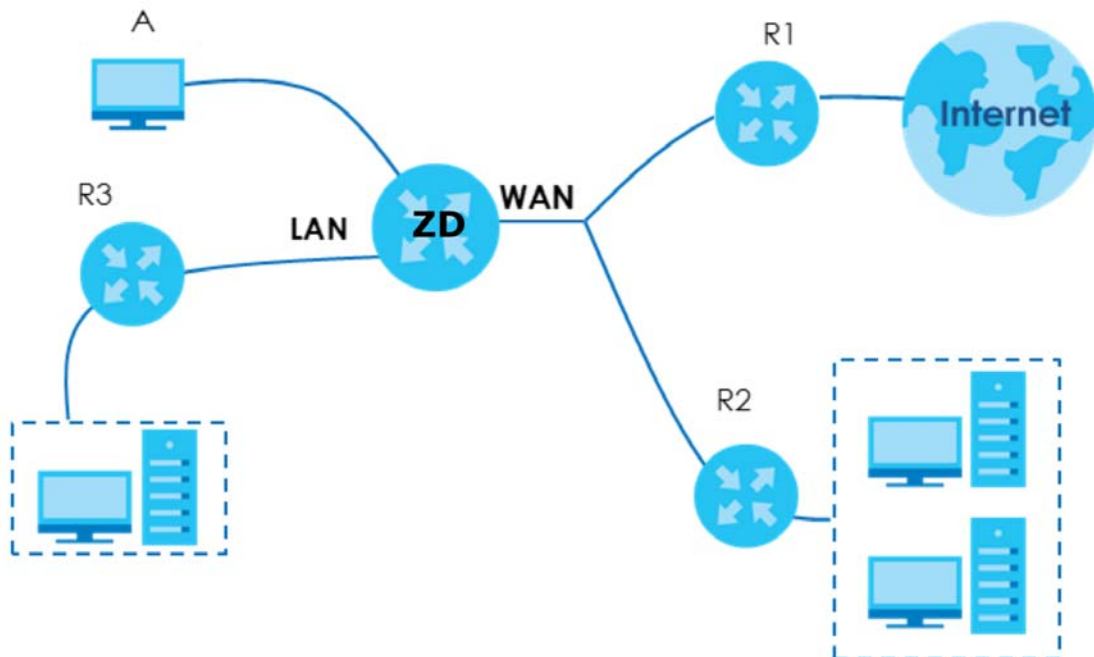
Routing

7.1 Routing Overview

The Zyxel Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Zyxel Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the Zyxel Device's LAN interface. The Zyxel Device routes most traffic from **A** to the Internet through the Zyxel Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 39 Example of Static Routing Topology




7.2 Configure Static Route

Use this screen to view and configure static route rules on the Zyxel Device. A static route is used to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets, especially when there are more than two Internet connections in your home or office network. Click **Network Setting > Routing** to access this screen.

Figure 40 Network Setting > Routing

Use this screen to view and configure the static route rules on the Zyxel Device. A static route is used to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets, especially when there are more than two Internet connections available in your home or office network.

 Add New Static Route

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

The following table describes the labels in this screen.

Table 19 Network Setting > Routing

LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the Zyxel Device.
#	This is the number of an individual static route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Name	This is the name of the static route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask/Prefix Length	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the Zyxel Device. Click the Delete icon to remove a static route from the Zyxel Device.

7.2.1 Add or Edit Static Route

Use this screen to add or edit a static route. Click **Add New Static Route** in the **Static Route** screen, the following screen appears. Configure the required information for a static route.

Note: The **Gateway IP Address** must be within the range of the selected interface in **Use Interface**.

Figure 41 Network Setting > Routing > Add New Static Route

Add New Static Route

Active ☒

Route Name

IP Type IPv4 ▼

Destination IP Address

Subnet Mask

Use Gateway IP Address ☒

Gateway IP Address

Use Interface Default ▼

Note
The **Gateway IP Address** must be within the range of the selected interface in **Use Interface**.

Cancel OK

The following table describes the labels in this screen.

Table 20 Network Setting > Routing > Add New Static Route

LABEL	DESCRIPTION
Active	Slide the switch button to the right to activate static route. Otherwise, click to disable.
Route Name	Assign a name for your static route. Up to 15 printable ASCII characters are allowed except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;].
IP Type	Select between IPv4 or IPv6 . Compared to IPv4 , IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10 ³⁸ IP addresses. The Zyxel Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Subnet Mask	If you are using IPv4 and need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. Enter the IP subnet mask here.
Use Gateway IP Address	The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. Click this switch to enable or disable the gateway IP address. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Gateway IP Address	Enter the IP address of the gateway.
Use Interface	Select the WAN interface you want to use for this static route.

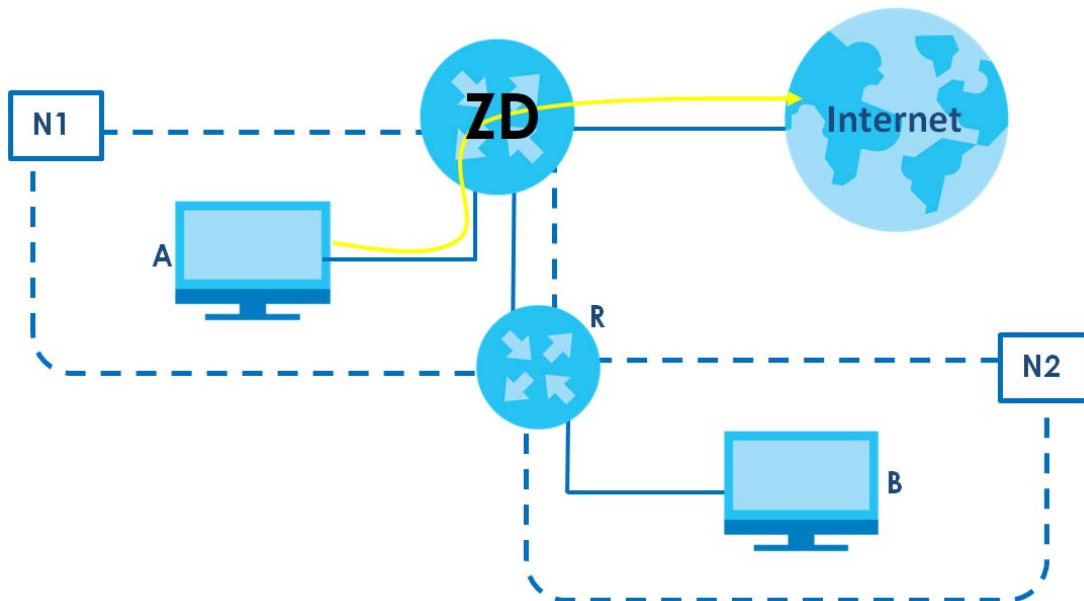
Table 20 Network Setting > Routing > Add New Static Route (continued)

LABEL	DESCRIPTION
User Interface	You can decide if you want to forward packets to a gateway IP address (Default) or a bound interface (Cellular WAN). If you want to configure bound interface, choose an interface through which the traffic is sent. You must have the WAN interfaces already configured in the Broadband screen.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

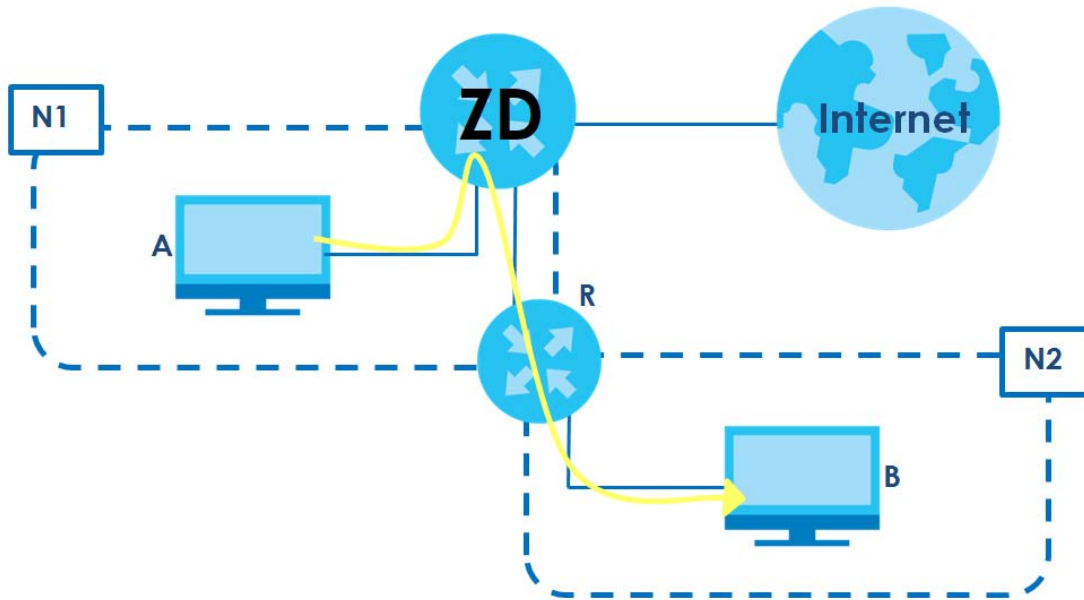
7.2.1.1 An Example of Adding a Static Route

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the Zyxel Device's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the Zyxel Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the Zyxel Device's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the Zyxel Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the Zyxel Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

Table 21 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The Zyxel Device's WAN	172.16.1.1
The Zyxel Device's LAN	192.168.1.1
IP Type	IPv4
Use Interface	VDSL
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

- 1 Log into the Zyxel Device's Web Configurator.
- 2 Click **Network Setting > Routing**.
- 3 Click **Add new Static Route** in the **Static Route** screen.

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

[Add New Static Route](#)

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

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

- 4a** Click the **Active** button to enable this static route. When the switch goes to the right, the function is enabled. Enter the **Route Name** as **R**.
- 4b** Set **IP Type** to **IPv4**.
- 4c** Enter the **Destination IP Address** **192.168.10.0** and **IP Subnet Mask** **255.255.255.0** for the destination, **N2**.
- 4d** Click the **Use Gateway IP Address** button to enable this function. When the switch goes to the right, the function is enabled. Enter **192.168.1.253** (**R**'s **N1** address) in the **Gateway IP Address** field.
- 4e** Select **VDSL** as the **Use Interface**.
- 4f** Click **OK**.

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.

Add New Static Route

Active ☒

Route Name

IP Type

Destination IP Address

Subnet Mask

Use Gateway IP Address ☒

Gateway IP Address

Use Interface

Note
The input range of the Gateway IP Address must be in the same range of the Use Interface.

Cancel **OK**

CHAPTER 8

Quality of Service (QoS)

8.1 QoS Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as video-on-demand.

Configure QoS on the Zyxel Device to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

- 1 Configure classifiers to sort traffic into different flows.
- 2 Assign priority and define actions to be performed for a classified traffic flow.

The Zyxel Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video. There are eight priority levels, with 1 having the highest priority.

This chapter contains information about configuring QoS and editing classifiers.

8.1.1 What You Can Do in this Chapter

- The **QoS** screen lets you enable or disable QoS and set the upstream bandwidth ([Section 8.3 on page 77](#)).
- The **General** screen lets you enable or disable QoS and set the upstream bandwidth ([Section 8.3 on page 77](#)).
- The **Queue Setup** screen lets you configure QoS queue assignment ([Section 8.4 on page 79](#)).
- The **Classification Setup** screen lets you add, edit or delete QoS classifiers ([Section 8.5 on page 81](#)).
- The **Shaper Setup** screen limits outgoing traffic transmission rate on the selected interface ([Section 8.6 on page 86](#)).
- The **Policer Setup** screen lets you control incoming traffic transmission rate and bursts ([Section 8.7 on page 88](#)).

8.2 What You Need to Know

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

QoS versus CoS

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

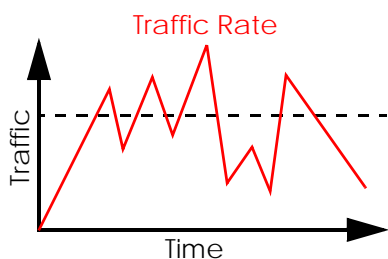
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of 3 bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

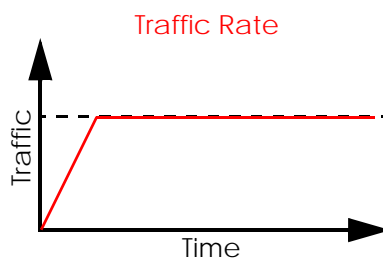
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or queues). Your Zyxel Device uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



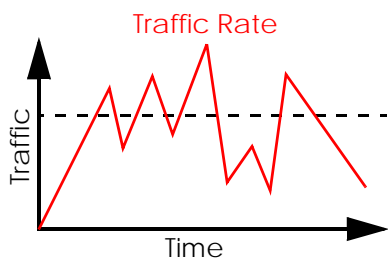
(Before Traffic Shaping)



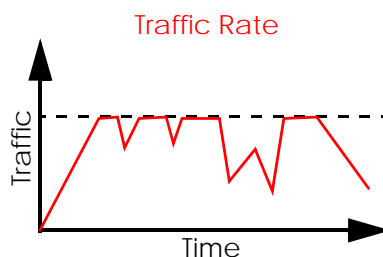
(After Traffic Shaping)

Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.



(Before Traffic Policing)



(After Traffic Policing)

The Zyxel Device supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Marker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See [Section 8.8 on page 91](#) for more information on each metering algorithm.

Strictly Priority

Strictly Priority (SP) services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.

Weighted Round Robin Schedule (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

8.3 Quality of Service General Settings

Use this screen to enable or disable QoS and set the upstream bandwidth or assign traffic priority. See [Section 8.1 on page 75](#) for more information.

When one of the following situations happens, the current WAN linkup rate will be used instead:

- 1 **WAN Managed Upstream Bandwidth** is set to 0
- 2 **WAN Managed Upstream Bandwidth** is empty
- 3 **WAN Managed Upstream Bandwidth** is higher than the current WAN interface linkup rate

Note: Manually defined QoS is ignored when **Upstream Traffic Priority** is selected.

Note: **Upstream Traffic Priority** automatically assigns a traffic priority level based on the selected criteria.

Note: To have your QoS settings configured in other **QoS** screens take effect, select **None** in the **Upstream Traffic Priority Assigned by** field.

Click **Network Setting > QoS > General** to open the screen as shown next.

Figure 42 Network Setting > QoS > General

Use this screen to enable or disable QoS and set the upstream bandwidth or assign traffic priority.

When one of the following situations happens, the current WAN linkup rate will be used instead:

1. **WAN Managed Upstream Bandwidth** is set to 0
2. **WAN Managed Upstream Bandwidth** is empty
3. **WAN Managed Upstream Bandwidth** is higher than the current WAN interface linkup rate

QoS ☐

WAN Managed Upstream Bandwidth (kbps)

Upstream Traffic Priority Assigned by

Note

(1) Manually defined QoS is ignored when **Upstream Traffic Priority** is selected.

(2) **Upstream Traffic Priority** automatically assigns a traffic priority level based on the selected criteria.

(3) To have your QoS settings configured in other **QoS** screens take effect, select **None** in the **Upstream Traffic Priority Assigned by** field.

Cancel **Apply**

The following table describes the labels in this screen.

Table 22 Network Setting > QoS > General

LABEL	DESCRIPTION
QoS	Select the switch to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	<p>Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS.</p> <p>The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps.</p> <p>You can also set this number lower than the interfaces' actual transmission speed. This will cause the Zyxel Device to not use some of the interfaces' available bandwidth.</p> <p>If you leave this field blank, the Zyxel Device automatically sets this number to be 95% of the WAN interfaces' actual upstream transmission speed.</p>
Upstream traffic priority Assigned by	<p>Select how the Zyxel Device assigns priorities to various upstream traffic flows.</p> <ul style="list-style-type: none"> • None: Disables auto priority mapping and has the Zyxel Device put packets into the queues according to your classification rules. Traffic which does not match any of the classification rules is mapped into the default queue with the lowest priority. • Ethernet Priority: Automatically assign priority based on the IEEE 802.1p priority level. • IP Precedence: Automatically assign priority based on the first three bits of the TOS field in the IP header. • Packet Length: Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, Internet gaming, or other real-time packets are usually small while larger packets are usually best effort data packets like file transfers.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

8.4 Queue Setup

Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

Use this screen to configure QoS queue assignment to decide the priority on WAN or LAN interfaces. Traffic with higher priority gets through faster than those with lower priority. Low-priority traffic is dropped first when the network is congested.

Note: Configure the priority level for a QoS queue from 1 to 8. The smaller the number in the **Priority** column, the higher the priority.


Note: The corresponding classifiers will be removed automatically if a queue is deleted.

Note: Rate limit 0 means there is no rate limit on a queue.

Figure 43 Network Setting > QoS > Queue Setup

Use this screen to configure QoS queue assignment to decide the priority on WAN/LAN interfaces. Traffic with higher priority gets through faster than those with lower priority. Low-priority traffic is dropped first when the network is congested.

+ Add New Queue

#	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit	Modify
1		default queue	WAN	8	1	DT		

Note

- (1) Apart from the default entry that cannot be edited, you can add up to 7 extra entries.
- (2) Configure the priority level for a QoS queue from 1 to 8. The smaller the number in the **Priority** column, the higher the priority.
- (3) Rate limit 0 means there's no rate limit on a queue.
- (4) The corresponding classifier(s) will be removed automatically if a queue is deleted.

The following table describes the labels in this screen.

Table 23 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add New Queue	Click this button to create a new queue entry.
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the Zyxel Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue. The lower the number, the higher the priority level.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used for this queue. Queue management algorithms determine how the Zyxel Device should handle packets when it receives too many (network congestion).

Table 23 Network Setting > QoS > Queue Setup (continued)

LABEL	DESCRIPTION
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the Edit icon to edit the queue. Click the Delete icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

8.4.1 Add a QoS Queue

Click **Add New Queue** or the **Edit** icon in the **Queue Setup** screen to configure a queue.

Figure 44 Network Setting > QoS > Queue Setup > Add New Queue/Edit

The following table describes the labels in this screen.

Table 24 Network Setting > QoS > Queue Setup > Add New Queue/Edit

LABEL	DESCRIPTION
Active	Slide the switch button to the right to enable this queue. Otherwise, slide the switch to the left to disable.
Name	Enter the descriptive name of this queue. Up to 32 printable ASCII characters are allowed except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;].
Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 8) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the Zyxel Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.

Table 24 Network Setting > QoS > Queue Setup > Add New Queue/Edit (continued)

LABEL	DESCRIPTION
Buffer Management	This field displays Drop Tail (DT) . Drop Tail (DT) is a simple queue management algorithm that allows the Zyxel Device buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it).
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue. If you enter 0 here, this means there's no rate limit on this queue.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

8.5 QoS Classification Setup

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the Zyxel Device forwards through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting > QoS > Classification Setup** to open the following screen.

Figure 45 Network Setting > QoS > Classification Setup

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the Zyxel Device forwards through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

+ Add New Classification

Order	Status	Class Name	Classification Criteria	DSCP Mark	802.1P Mark	VLAN ID Tag	To Queue	Modify
-------	--------	------------	-------------------------	-----------	-------------	-------------	----------	--------

The following table describes the labels in this screen.

Table 25 Network Setting > QoS > Classification Setup

LABEL	DESCRIPTION
Add New Classification	Click this to create a new classifier.
Order	This is the index number of the entry. The classifiers are applied in order of their numbering.
Status	This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.

Table 25 Network Setting > QoS > Classification Setup (continued)

LABEL	DESCRIPTION
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the Edit icon to edit the classifier. Click the Delete icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

8.5.1 Add or Edit QoS Class

Click **Add New Classification** in the **Classification Setup** screen or the **Edit** icon next to a classifier to open the following screen.

Figure 46 Network Setting > QoS > Classification Setup > Add New Classification/Edit

Add New Classification

Please follow the guidance through step 1~5 to configure a QoS rule

Step1: Class Configuration

Active ☒

Class Name

Classification Order Last

Step2: Criteria Configuration

Use the configurations below to specify the characteristics of a data flow needed to be managed by this QoS rule

Basic

From Interface LAN

Ether Type NA

Source

☒ Address Subnet Mask ☐ Exclude

☒ Port Range ~ ☐ Exclude

☐ MAC - - - - - MAC Mask ☐ Exclude

Destination

☒ Address Subnet Mask ☐ Exclude

☒ Port Range ~ ☐ Exclude

☐ MAC - - - - - MAC Mask ☐ Exclude

Others

☒ Service RTSP Server ☐ Exclude

☒ IP protocol TCP ☐ Exclude

☒ DHCP ☐ Exclude

☒ IP Packet Length ~ ☐ Exclude

☒ DSCP (0~63) ☐ Exclude

☒ 802.1P 0 BE ☐ Exclude

☒ VLAN ID (1~4094) ☐ Exclude

☒ TCP ACK ☐ Exclude

Step3: Packet Modification

The content of the packet can be modified by applying the following settings

DSCP Mark Unchange (0~63)

VLAN ID Tag Unchange 0 (1~4094)

802.1P Mark 0 BE

Step4: Class Routing

This module can route a packet to a certain interface according to the class setting

Forward To Interface Unchange

Step5: Outgoing Queue Selection

Outgoing queue decides the priority of the traffic and how traffic should be shaped in the WAN interface.

To Queue Index default queue

Cancel OK

The following table describes the labels in this screen.

Table 26 Network Setting > QoS > Classification Setup > Add New Classification/Edit

LABEL	DESCRIPTION
Step1: Class Configuration	
Active	Slide the switch to the right to enable the classifier. Otherwise, slide the switch to the left to disable.
Class Name	Enter a descriptive name for this class. Up to 32 printable ASCII characters are allowed except [], [`], ['], [<], [>], [^], [\$], [], [&], or [;].
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking Apply . Select Last to put this rule in the back of the classifier list.
Step2: Criteria Configuration	
Basic	
From Interface	If you want to classify the traffic by an ingress interface, select an interface from the From Interface drop-down list box. Local identifies the local traffic coming from the Zyxel Device itself. LAN identifies all traffic from the Zyxel Device LAN.
Target Interface	This appears only when you select Local in the From Interface field. Select a WAN interface to classify the Zyxel Device local traffic by an egress WAN interface.
Ether Type	Select a predefined application to configure a class for the matched traffic. Traffic will be classified with the Ether Type of Ethernet frames. Ether Type is a field in an Ethernet frame used to identify the protocol encapsulated in the frame. Select NA to specify traffic that does not belong to any Ether type. If you select IP , you also need to configure source or destination, IP address, DHCP options, DSCP value or the protocol type. If you select IPv6 , you also need to configure source or destination, IPv6 address, DSCP value or the protocol type. If you select 802.1Q , you can configure an 802.1p priority level.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Mask	This field is available only when you select IP in the Ether Type field. Enter the source subnet mask.
Prefix Length	This field is available only when you select IPv6 in the Ether Type field. Enter the source prefix length.
Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port numbers of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	

Table 26 Network Setting > QoS > Classification Setup > Add New Classification/Edit (continued)

LABEL	DESCRIPTION
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Mask	This field is available only when you select IP in the Ether Type field. Enter the source subnet mask.
Prefix Length	This field is available only when you select IPv6 in the Ether Type field. Enter the source prefix length. See IPv6 on page 179 for more IPv6 information.
Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port numbers of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
Service	This field is available only when you select IP or IPv6 in the Ether Type field. This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields.
IP Protocol	This field is available only when you select IP or IPv6 in the Ether Type field. Select this option and select the protocol (service type) from TCP , UDP , ICMP or IGMP . If you select User defined , enter the protocol (service type) number.
DHCP	This field is available only when you select IP in the Ether Type field. Select this option and select a DHCP option. If you select Vendor Class ID (DHCP Option 60) , enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware. If you select Client ID (DHCP Option 61) , enter the Identity Association Identifier (IAD Option 61) of the matched traffic, such as the MAC address of the device. If you select User Class ID (DHCP Option 77) , enter a string that identifies the user's category or application type in the matched DHCP packets. If you select Vendor Specific Info (DHCP Option 125) , enter the vendor specific information of the matched traffic, such as the product class, model name, and serial number of the device.
IP Packet Length	This field is available only when you select IP in the Ether Type field. Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.
DSCP	This field is available only when you select IP or IPv6 in the Ether Type field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
802.1P	This field is available only when you select 802.1Q in the Ether Type field. Select this option and select a priority level (between 0 and 7) from the drop-down list box. "0" is the lowest priority level and "7" is the highest.

Table 26 Network Setting > QoS > Classification Setup > Add New Classification/Edit (continued)

LABEL	DESCRIPTION
VLAN ID	This field is available only when you select 802.1Q in the Ether Type field. Select this option and specify a VLAN ID number.
TCP ACK	This field is available only when you select IP in the Ether Type field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Step3: Packet Modification	
DSCP Mark	If you select Remark , enter a DSCP value with which the Zyxel Device replaces the DSCP field in the packets. If you select Unchange , the Zyxel Device keep the DSCP field in the packets.
VLAN ID Tag	If you select Remark , enter a VLAN ID number with which the Zyxel Device replaces the VLAN ID of the frames. If you select Remove , the Zyxel Device deletes the VLAN ID of the frames before forwarding them out. If you select Add , the Zyxel Device treat all matched traffic untagged and add a second VLAN ID. If you select Unchange , the Zyxel Device keep the VLAN ID in the packets.
802.1P Mark	Select a priority level with which the Zyxel Device replaces the IEEE 802.1p priority field in the packets. If you select Unchange , the Zyxel Device keep the 802.1p priority field in the packets.
Step4: Class Routing	
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select Unchange , the Zyxel Device forward traffic of this class according to the default routing table.
Step5: Outgoing Queue Selection	
To Queue Index	Select a queue that applies to this class. You should have already configured a queue in the Queue Setup screen.
Cancel	Click Cancel to exit this screen without saving any changes.
OK	Click OK to save your changes.

8.6 QoS Shaper Setup

This screen lets you use the token bucket algorithm to allow a certain amount of large bursts of traffic while keeping most outgoing traffic at the average rate. Click **Network Setting > QoS > Shaper Setup**. The screen appears as shown.

Figure 47 Network Setting > QoS > Shaper Setup

This screen lets you use the token bucket algorithm to allow a certain amount of large bursts of traffic while keeping most outgoing traffic at the average rate.

+ Add New Shaper

#	Status	Interface	Rate Limit	Modify

The following table describes the labels in this screen.

Table 27 Network Setting > QoS > Shaper Setup

LABEL	DESCRIPTION
Add New Shaper	Click this to create a new entry.
#	This is the index number of the entry.
Status	This field displays whether the shaper is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this shaper is not active.
Interface	This shows the name of the Zyxel Device's interface through which traffic in this shaper applies.
Rate Limit	This shows the average rate limit of traffic bursts for this shaper.
Modify	Click the Edit icon to edit the shaper. Click the Delete icon to delete an existing shaper. Note that subsequent rules move up by one when you take this action.

8.6.1 Add or Edit a QoS Shaper

Click **Add New Shaper** in the **Shaper Setup** screen or the **Edit** icon next to a shaper to show the following screen.

Figure 48 Network Setting > QoS > Shaper Setup > Add New Shaper/Edit

The following table describes the labels in this screen.

Table 28 Network Setting > QoS > Shaper Setup > Add New Shaper/Edit

LABEL	DESCRIPTION
Active	Slide the switch to the right to enable the shaper. Otherwise, slide the switch to the left to disable.
Interface	Select a Zyxel Device's interface through which traffic in this shaper applies.
Rate Limit	Enter the average rate limit of traffic bursts for this shaper.
Cancel	Click Cancel to exit this screen without saving any changes.
OK	Click OK to save your changes.

8.7 QoS Policer Setup

Use this screen to view QoS policers that allow you to limit the transmission rate of incoming traffic and apply actions, such as drop, pass, or modify, to the DSCP value of matched traffic. Click **Network Setting** > **QoS** > **Policer Setup**. The screen appears as shown.

Figure 49 Network Setting > QoS > Policer Setup

Use this screen to view QoS policers that allow you to limit the transmission rate of incoming traffic and apply actions, such as drop, pass, or modify, to the DSCP value of matched traffic.

+ Add New Policer

#	Status	Name	Regulated Classes	Meter Type	Rule	Action	Modify
---	--------	------	-------------------	------------	------	--------	--------

The following table describes the labels in this screen.

Table 29 Network Setting > QoS > Policer Setup

LABEL	DESCRIPTION
Add new Policer	Click this to create a new entry.
#	This is the index number of the entry.
Status	This field displays whether the policer is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this policer is not active.
Name	This field displays the descriptive name of this policer.
Regulated Classes	This field displays the name of a QoS classifier
Meter Type	This field displays the type of QoS metering algorithm used in this policer.
Rule	These are the rates and burst sizes against which the policer checks the traffic of the member QoS classes.
Action	This shows how the policer has the Zyxel Device treat different types of traffic belonging to the policer's member QoS classes.
Modify	Click the Edit icon to edit the policer. Click the Delete icon to delete an existing policer. Note that subsequent rules move up by one when you take this action.

8.7.1 Add or Edit a QoS Policer

Click **Add New Policer** in the **Policer Setup** screen or the **Edit** icon next to a policer to show the following screen.

Figure 50 Network Setting > QoS > Policer Setup > Add New Policer/Edit

QoS Policer Configuration

Active ☐

Name

Meter Type Simple Token Bucket ▼

Committed Rate (kbps)

Committed Burst Size (kbytes)

Conforming Action Pass ▼

Non-Conforming Action Drop ▼

Regulated Classes Member Setting

Available Class **Selected Class**

➤ ➤

➤ ➤

➤ ➤

Cancel **OK**

The following table describes the labels in this screen.

Table 30 Network Setting > QoS > Policer Setup > Add New Policer/Edit

LABEL	DESCRIPTION
Active	Slide the switch to the right to enable the policer. Otherwise, slide the switch to the left to disable.
Name	Enter a descriptive name of this policer. Up to 16 printable ASCII characters are allowed except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;].

Table 30 Network Setting > QoS > Policer Setup > Add New Policer/Edit (continued)

LABEL	DESCRIPTION
Meter Type	<p>This shows the traffic metering algorithm used in this policer.</p> <p>The Simple Token Bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to <i>b</i> bytes which is also the bucket size.</p> <p>The Single Rate Three Color Marker (srTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR), the Committed Burst Size (CBS) and the Excess Burst Size (EBS).</p> <p>The Two Rate Three Color Marker (trTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR) and the Peak Information Rate (PIR).</p>
Committed Rate	Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic.
Committed Burst Size	<p>Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured.</p> <p>This is the maximum size of the (first) token bucket in a traffic metering algorithm.</p>
Excess Burst Size	<p>Specify the additional amount of bytes that are admitted at the committed rate besides the committed burst size.</p> <p>This is the maximum size of the second token bucket in the srTCM.</p> <p>This field is only available when you select Single Rate Three Color in the Meter Type field.</p>
Peak Rate	<p>Specify the maximum rate at which packets are admitted to the network.</p> <p>The peak rate should be greater than or equal to the committed rate. This is to specify how many bytes of tokens are added to the second bucket every second in the trTCM.</p> <p>This field is only available when you select Two Rate Three Color in the Meter Type field.</p>
Peak Burst Size	<p>Specify the maximum amount of bytes that are admitted at the committed rate.</p> <p>This is the maximum size of the second token bucket in the trTCM.</p> <p>This field is only available when you select Two Rate Three Color in the Meter Type field.</p>
Conforming Action	<p>Specify what the Zyxel Device does for packets within the committed rate and burst size (green-marked packets).</p> <ul style="list-style-type: none"> • Pass: Send the packets without modification. • DSCP Mark: Change the DSCP mark value of the packets. Enter the DSCP mark value to use.
Partial Conforming Action	<p>Specify the action that the Zyxel Device takes on yellow-marked packets.</p> <p>Select Pass to forward the packets.</p> <p>Select Drop to discard the packets.</p> <p>Select DSCP Mark to assign a specified DSCP number (between 0 and 63) to the packets and forward them. The packets are dropped if there is congestion on the network.</p> <p>This field is only available when you select Single/Two Rate Three Color in the Meter Type field.</p>
Non-Conforming Action	<p>Specify what the Zyxel Device does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets).</p> <ul style="list-style-type: none"> • Drop: Discard the packets. • DSCP Mark: Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network.
Regulated Classes Member Setting	

Table 30 Network Setting > QoS > Policer Setup > Add New Policer/Edit (continued)

LABEL	DESCRIPTION
Available Class	Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier.
Selected Class	Highlight a QoS classifier in the Available Class box and use the > button to move it to the Selected Class box. To remove a QoS classifier from the Selected Class box, select it and use the < button.
Cancel	Click Cancel to exit this screen without saving any changes.
OK	Click OK to save your changes.

8.8 Technical Reference

The following section contains additional technical information about the Zyxel Device features described in this chapter.

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 31 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the

packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new Differentiated Services (DS) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)
---------------	-----------------

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

Automatic Priority Queue Assignment

If you enable QoS on the Zyxel Device, the Zyxel Device can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the Zyxel Device. On the Zyxel Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 32 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250 – 1100

Table 32 Internal Layer2 and Layer3 QoS Mapping (continued)

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to b bytes which is also the bucket size, so the bucket can hold up to b tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.
- If there are no tokens in the bucket, the Zyxel Device stops transmitting until enough tokens are generated.
- If not enough tokens are available, the Zyxel Device treats the packet in either one of the following ways:

In traffic shaping:

- Holds it in the queue until enough tokens are available in the bucket.

In traffic policing:

- Drops it.
- Transmits it but adds a DSCP mark. The Zyxel Device may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface's capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

Single Rate Three Color Marker

The Single Rate Three Color Marker (srTCM, defined in RFC 2697) is a type of traffic policing that identifies packets by comparing them to one user-defined rate, the Committed Information Rate (CIR), and two burst sizes: the Committed Burst Size (CBS) and Excess Burst Size (EBS).

The srTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The srTCM is based on the token bucket filter and has two token buckets (CBS and EBS). Tokens are generated and added into the bucket at a constant rate, called Committed Information Rate (CIR). When the first bucket (CBS) is full, new tokens overflow into the second bucket (EBS).

All packets are evaluated against the CBS. If a packet does not exceed the CBS it is marked green. Otherwise it is evaluated against the EBS. If it is below the EBS then it is marked yellow. If it exceeds the EBS then it is marked red.

The following shows how tokens work with incoming packets in srTCM:

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.
- If there are not enough tokens in the CBS bucket, the Zyxel Device checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

Two Rate Three Color Marker

The Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

The trTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

The following shows how tokens work with incoming packets in trTCM:

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.
- If the PBS bucket has enough tokens, the Zyxel Device checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

CHAPTER 9

VLAN Group

9.1 VLAN Group Overview

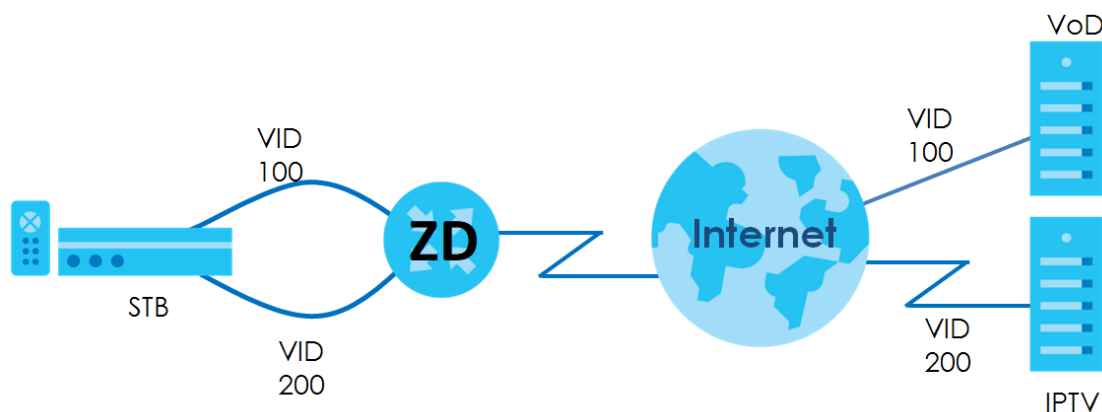
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same groups; 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 the 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 the servers with these VLAN IDs.

Figure 51 VLAN Group Example



9.1.1 What You Can Do in this Chapter

Use these screens to manage VLAN groups on the Zyxel Device.

9.2 VLAN Group Settings

This screen shows the VLAN groups created on the Zyxel Device. Click **Network Setting > VLAN Group** to open the following screen.

Figure 52 Network Setting > VLAN Group

#	Group Name	VLAN ID	Interface	Modify
---	------------	---------	-----------	--------

The following table describes the fields in this screen.

Table 33 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.

9.2.1 Add or 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 53 Network Setting > VLAN Group > Add New VLAN Group/Edit

The following table describes the fields in this screen.

Table 34 Network Setting > VLAN Group > Add New VLAN Group/Edit

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 VLAN ID number, from 1 to 4,094, to identify this VLAN group.
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 you set.
Cancel	Click Cancel to exit this screen without saving any changes.
OK	Click OK to save your changes.

CHAPTER 10

Interface Grouping

10.1 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. This lets devices connected to an interface group's LAN interfaces communicate through the interface group's WAN or LAN interfaces but not other WAN or LAN interfaces.

10.1.1 What You Can Do in this Chapter

The **Interface Grouping** screen lets you create multiple networks on the Zyxel Device ([Section 10.2 on page 99](#)).

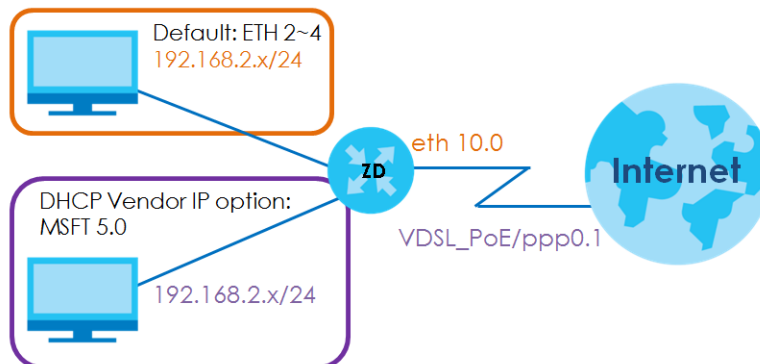
10.2 Interface Grouping

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 Setup** 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 6 on page 55](#) 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 54 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 55 Network Setting > Interface Grouping

Interface Grouping

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.

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.

 Add New Interface Group

Group Name	WAN Interface	LAN Interface	Criteria	Modify
Default	Any WAN	LAN1		

The following table describes the fields in this screen.

Table 35 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.
Modify	Click the Edit icon to modify an existing Interface group setting or click the Delete icon to remove the Interface group.

10.2.1 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 new group, use filtering criteria.

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 56 Network Setting > Interface Grouping > Add New Interface Group/Edit

The following table describes the fields in this screen.

Table 36 Network Setting > Interface Grouping > Add New Interface Group/Edit

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. Up to 32 printable ASCII characters are allowed except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;].
WAN Interfaces used in the grouping	Select the WAN interface this group uses. The group can have up to one PTM interface, up to one ATM interface. Select None to not add a WAN interface to this group.
Available LAN Interfaces Selected LAN Interfaces	Select one or more interfaces (Ethernet LAN, 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 10.2.2 on page 102 for more information.
#	This shows the index number of the rule.

Table 36 Network Setting > Interface Grouping > Add New Interface Group/Edit (continued)

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

10.2.2 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 57 Network Setting > Interface Grouping > Interface Group Configuration: Add

The following table describes the fields in this screen.

Table 37 Network Setting > Interface Grouping > Interface Group Configuration: Add

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.

Table 37 Network Setting > Interface Grouping > Interface Group Configuration: Add (continued)

LABEL	DESCRIPTION
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 3 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 .
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

CHAPTER 11

Firewall

11.1 Firewall Overview

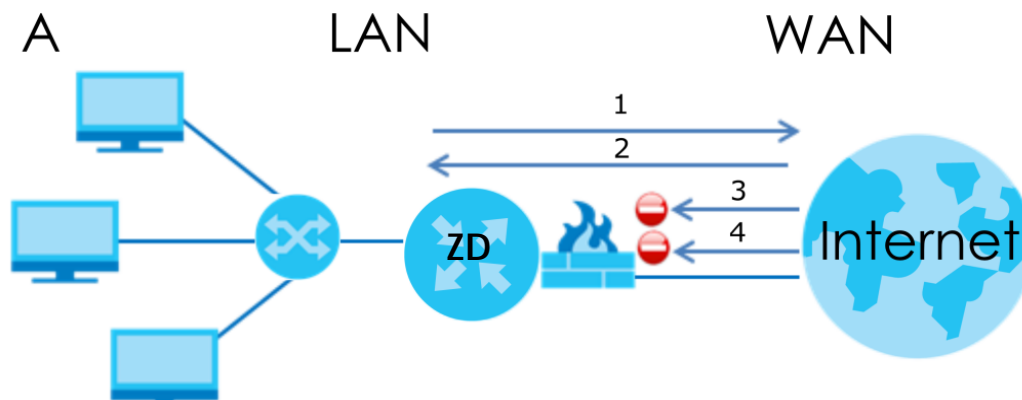
This chapter shows you how to enable the Zyxel Device firewall. Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. The firewall:

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

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

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

Figure 58 Default Firewall Action



11.1.1 What You Need to Know About Firewall

SYN Attack

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

DoS

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

DoS Thresholds

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

DDoS

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

ICMP

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

LAND Attack

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

Ping of Death

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

SPI

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

11.2 Firewall

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

11.2.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the Zyxel Device ([Section 11.3 on page 106](#)).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules ([Section 11.4 on page 107](#)).
- Use the **Access Control** screen to view and configure incoming or outgoing filtering rules ([Section 11.5 on page 109](#)).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks ([Section 11.6 on page 111](#)).

11.3 Firewall General Settings

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

Figure 59 Security > Firewall > General

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

IPv4 Firewall ☒

IPv6 Firewall ☒

Low Medium (Recommended) High

LAN to WAN ☒ ☒ ☐

WAN to LAN ☒ ☒ ☐

Note

(1) LAN to WAN is your access to all Internet services.

(2) WAN to LAN is the access of other computers on the Internet to devices behind the Zyxel Device.

(3) 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.

Cancel Apply

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

The following table describes the labels in this screen.

Table 38 Security > Firewall > General

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

11.4 Protocol (Customized Services)

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

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

Figure 60 Security > Firewall > Protocol

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

+ Add New Protocol Entry

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

The following table describes the labels in this screen.

Table 39 Security > Firewall > Protocol

LABEL	DESCRIPTION
Add New Protocol Entry	Click this to configure a customized service.
Name	This is the name of your customized service.
Description	This is a description of your customized service.

Table 39 Security > Firewall > Protocol (continued)

LABEL	DESCRIPTION
Ports/Protocol Number	This shows the port number or range and the IP protocol (TCP or UDP) that defines your customized service.
Modify	Click this to edit a customized service.

11.4.1 Add New Protocol Entry

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

Figure 61 Security > Firewall > Protocol: Add New Protocol Entry

The following table describes the labels in this screen.

Table 40 Security > Firewall > Protocol: Add New Protocol Entry

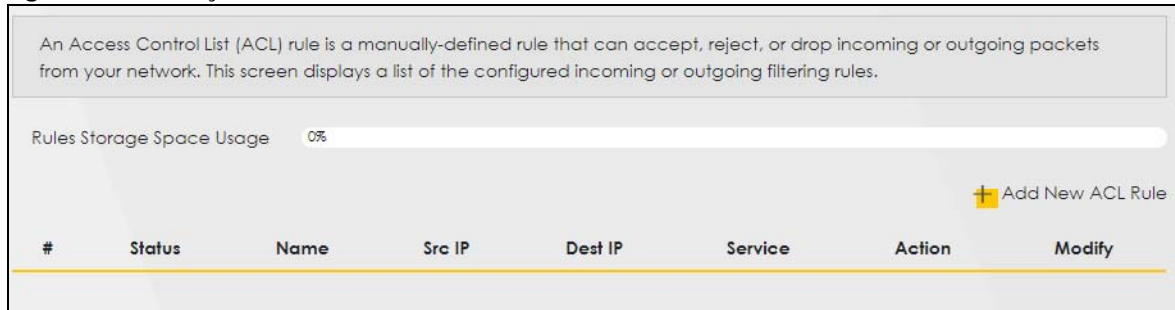
LABEL	DESCRIPTION
Service Name	Enter a unique name for your custom port. Up to 16 printable ASCII characters are allowed except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;].
Description	Enter a description for your custom port. Up to 16 printable ASCII characters are allowed except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;].
Protocol	Choose the protocol (TCP , UDP , ICMP , ICMPv6 , or Other) that defines your customized port from the drop down list box.
Protocol Number	Enter a single port number or the range of port numbers (0 – 255) that define your customized service.
Source Port	This field is displayed if you select either the TCP or UDP protocol. You may set it to Any , Single , or Range and enter the Port Number or range of Port Numbers for your source port.
Destination Port	This field is displayed if you select either the TCP or UDP protocol. You may set it to Any , Single , or Range and enter the Port Number or range of Port Numbers for your destination port.
ICMPv6type	This field is displayed if you select the ICMPv6 protocol. From the drop-down menu, select which type value you would like to use.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

11.5 Access Control (Rules)

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

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

Figure 62 Security > Firewall > Access Control



The following table describes the labels in this screen.

Table 41 Security > Firewall > Access Control

LABEL	DESCRIPTION
Rules Storage Space Usage	This read-only bar shows how much of the Zyxel Device's memory is in use for recording firewall rules. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Add New ACL Rule	Select an index number and click Add New ACL Rule to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
#	This field displays the rule index number. The ordering of your rules is important as rules are applied in turn.
Status	This field displays the status of the ACL rule. A yellow bulb signifies that this ACL rule is active, while a gray bulb signifies that this ACL rule is not active.
Name	This field displays the rule name.
Src IP	This field displays the source IP addresses to which this rule applies.
Dest IP	This field displays the destination IP addresses to which this rule applies.
Service	This field displays the protocol (All, TCP, UDP, TCP/UDP, ICMP, ICMPv6, or any) used to transport the packets for which you want to apply the rule.
Action	Displays whether the firewall silently discards packets (Drop), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (Reject), or allow the passage of (Accept) packets that match this rule.
Modify	Click the Edit icon to edit the firewall rule. Click the Delete icon to delete an existing firewall rule.

11.5.1 Add New ACL Rule

Click **Add new ACL rule** or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays. Use this screen to accept, reject, or drop packets based on specified parameters, such as source and destination IP address, IP Type, service, and direction. You can also

specify a limit as to how many packets this rule applies to at a certain period of time or specify a schedule for this rule.

Figure 63 Security > Firewall > Access Control > Add New ACL Rule

The following table describes the labels in this screen.

Table 42 Security > Firewall > Access Control > Add New ACL Rule

LABEL	DESCRIPTION
Active	Slide the switch to the right to enable this ACL rule. Otherwise, slide the switch to the left to disable.
Filter Name	Enter a unique name for your filter rule. Up to 16 printable ASCII characters are allowed except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;].
Order	Assign the order of your rules as rules are applied in turn.
Select Source IP Address	If you want the source to come from a particular (single) IP, select Specific IP Address . If not, select from a detected device.
Source IP Address	If you selected Specific IP Address in the previous item, enter the source device's IP address here. Otherwise this field will be hidden if you select the detected device.
Select Destination Device	If you want your rule to apply to packets with a particular (single) IP, select Specific IP Address . If not, select a detected device.

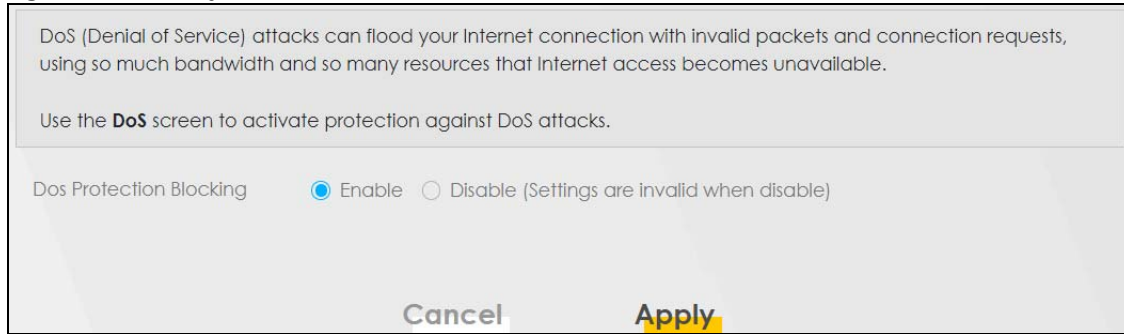
Table 42 Security > Firewall > Access Control > Add New ACL Rule (continued)

LABEL	DESCRIPTION
Destination IP Address	If you selected Specific IP Address in the previous item, enter the destination device's IP address here. Otherwise this field will be hidden if you select the detected device.
MAC Address	Enter the MAC addresses of the WiFi or wired LAN clients that are allowed access to the 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.
IP Type	Select between IPv4 or IPv6 . Compared to IPv4 , IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses. The Zyxel Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).
Select Service	Select a service from the Select Service List.
Protocol	Select the protocol (ALL , TCP/UDP , TCP , UDP , ICMP , or ICMPv6) used to transport the packets for which you want to apply the rule.
Custom Source Port	This is a single port number or the starting port number of a range that defines your rule.
Custom Destination Port	This is a single port number or the ending port number of a range that defines your rule.
TCP Flag	Select the TCP Flag (SYN, ACK, URG, PSH, RST, FIN). This appears when you select TCP/UDP or TCP in the Protocol field.
Type	This field is displayed only when you set Protocol to ICMPv6 . From the drop-down list box, select which ICMPv6 type you would like to use.
Policy	Use the drop-down list box to select whether to discard (DROP), deny and send an ICMP destination-unreachable message to the sender (REJECT), or allow the passage of (ACCEPT) packets that match this rule.
Direction	Select WAN to LAN to apply the rule to traffic from WAN to LAN. Select LAN to WAN to apply the rule to traffic from LAN to WAN. Select WAN to Router to apply the rule to traffic from WAN to router. Select LAN to Router to apply the rule to traffic from LAN to router.
Enable Rate Limit	Slide the switch to the right to enable the setting of maximum number of packets per maximum number of minute or second to limit the throughput of traffic that matches this rule. Otherwise, , the next item will be disabled.
packet(s) per (1-512)	Enter the maximum number of packets (1 – 512) per minute or second.
Scheduler Rules	Select a schedule rule for this ACL rule from the drop-down list box. You can configure a new schedule rule by clicking Add New Rule . This will bring you to the Security > Scheduler Rules screen.
Add New Rule	Select a schedule rule for this ACL rule from the drop-down list box. You can configure a new schedule rule by clicking Add New Rule .
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

11.6 DoS

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

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

Figure 64 Security > Firewall > DoS


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

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

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

Cancel Apply

The following table describes the labels in this screen.

Table 43 Security > Firewall > DoS

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

11.7 Firewall Technical Reference

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

11.7.1 Firewall Rules Overview

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

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

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

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

- LAN to Router

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

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

- LAN to WAN

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

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

- WAN to LAN

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

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

- WAN to Router

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

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

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

For example, you may create rules to:

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

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

11.7.2 Guidelines For Security Enhancement With Your Firewall

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

- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

11.7.3 Security Considerations

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

Consider these security ramifications before creating a rule:

- 1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC (Internet Relay Chat) is blocked, are there users that require this service?
- 2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- 3 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- 4 Does this rule conflict with any existing rules?

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

CHAPTER 12

MAC Filter

12.1 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 connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of wired LAN client to configure this screen.

12.2 MAC Filter

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

Figure 65 Security > MAC Filter

MAC Filter

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

Enable **MAC Address Filter** and add the host name and MAC address of a LAN client to the table if you wish to allow or deny them access to your network. You can choose to enable or disable the filters per entry; make sure that the check box under **Active** is selected if you want to use a filter.

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

MAC Restrict Mode ☒ Allow ☐ Deny

Add New Rule **Add**

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

Cancel **Apply**

The following table describes the labels in this screen.

Table 44 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	Select an existing wired LAN client from the list to add as a new entry. Select Custom if you want to manually enter the Host Name and MAC Address . Click the Add button to create a new entry.
Set	This is the index number of the MAC address.
Active	Select Active to enable the MAC filter rule. The rule will not be applied if Allow is not selected under MAC Restrict Mode .
Host Name	Enter the host name of the wired LAN clients that are allowed access to the Zyxel Device. Up to 17 printable ASCII characters are allowed except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;].
MAC Address	Enter the MAC addresses of the or wired 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.

12.2.1 Add New Rule

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. Select **Security > MAC Filter > Add New Rule**. The screen appears as shown.

Figure 66 Security > MAC Filter > Add New Rule

Set	Active	Host Name	MAC Address	Delete
1	<input checked="" type="checkbox"/>	test	BC - 22 - 33 - 11 - 66 - AA	
2	<input checked="" type="checkbox"/>	Test	BC - 88 - 99 - 00 - 11 - 22	

The following table describes the labels in this screen.

Table 45 Security > MAC Filter > Add New Rule

LABEL	DESCRIPTION
Set	This is the index number of the MAC address.
Active	Select Active to enable the MAC filter rule. The rule will not be applied if Allow is not selected under MAC Restrict Mode .
Host Name	Enter the host name of the or wired LAN clients that are allowed access to the Zyxel Device.
MAC Address	Enter the MAC addresses of the or wired 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.

Table 45 Security > MAC Filter > Add New Rule

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

CHAPTER 13

Scheduler Rule

13.1 Scheduler Rule Overview

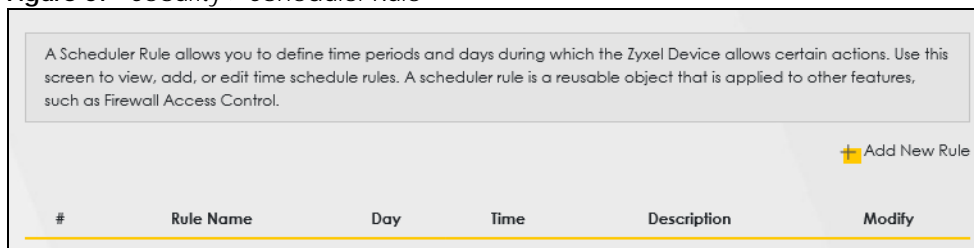
A Scheduler Rule allows you to define time periods and days during which the Zyxel Device allows certain actions.

13.2 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 67 Security > Scheduler Rule



The following table describes the fields in this screen.

Table 46 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 days 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.

13.2.1 Add or 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 68 Security > Scheduler Rule: Add or Edit

The following table describes the fields in this screen.

Table 47 Security > Scheduler Rule: Add or Edit

LABEL	DESCRIPTION
Rule Name	Enter a name for this schedule. Up to 31 printable ASCII characters are allowed except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;].
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. Up to 63 printable ASCII characters are allowed except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;].
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

CHAPTER 14

Certificates

14.1 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.

14.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to view and import the Zyxel Device's CA-signed (Certification Authority) certificates ([Section 14.3 on page 120](#)).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the Zyxel Device. You can also export the certificates to a computer ([Section 14.4 on page 124](#)).

14.2 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.

14.3 Local Certificates

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

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

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

Figure 69 Security > Certificates > Local Certificates

Local Certificates Trusted CA

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

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

Replace PrivateKey/Certificate file in PEM format

☐ Private Key is protected by password

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

The following table describes the labels in this screen.

Table 48 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Replace Private Key/Certificate file in PEM format	
Private Key is protected by 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).
Choose File/Browse	Click this button to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the 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 a unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the View icon to open a screen with an in-depth list of information about the certificate. For a certification request, click Load Signed to import the signed certificate. Click the Remove icon to remove the certificate (or certification request). A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.

14.3.1 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 or province name, and the default US two-letter country code (The US country code is by default and not changeable when sold in the U.S.) for the certificate.

Figure 70 Security > Certificates > Local Certificates: Create Certificate Request

The following table describes the labels in this screen.

Table 49 Security > Certificates > Local Certificates: 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 email address in the field provided. The domain name or email address can be up to 63 ASCII characters. The domain name or email address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the 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.

14.3.2 View Certificate Request

Use this screen to view in-depth information about the certificate request. The **Certificate** is used to verify the authenticity of the certification authority. The **Private Key** serves as your digital signature for

authentication and must be safely stored. The **Signing Request** contains the certificate signing request value that you will copy upon submitting the certificate request to the CA (certificate authority).

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

Figure 71 Security > Certificates > Local Certificates: View Certificate

The screenshot shows a window titled "View Certificate" with a close button (X) in the top right corner. The window contains the following sections:

- Certificate Details** (header):
 - Name: Test
 - Type: none
 - Subject: /CN=588BF3-VMG8825-B50B-S172V48000015/O=Zyxel/ST=Hsinchu/C=TW
- Certificate**: A large empty box for the certificate image.
- Private Key**: A text area containing a long alphanumeric string:


```
hGEzXjrKpkeJHmKBehzvdv
KGLNbx22N1C0qtl++BwFFzOK8xTshyNxGW27goeOY
1QpuD2RQy1FB+Ky9zVNCRuP
6C1korOCNOwp2Mds4udfazEZefm7ysyC0P2etwd7
AbLBM49P1qUsWbGWR9snO74
Myqhf+kCc2R801HUQvWX7XbHzTG+8RKTpV/oCkLZy
cUBlyq0IY2f6FkWQBxp9C2H
xteLLgB6SXDfK5vTyQTcj0spmPndj4ZkxKhqtuLwM8E3
bzHGdujBwvzZXnf6NxAZ
fAdmacECaYEA+SIZJoWxoB90BopN1JP3t//IOLPznbs
```
- Signing Request**: A text area containing a long alphanumeric string:


```
-----BEGIN CERTIFICATE REQUEST-----
MIICoDCCAYgCAQAwWzEqMCgGA1UEAwwhNTg4
QkYzLVZNRzg4MjU0fQJlUwQl1TMTcy
VjQ4MDAwMDE1MQ4wDAYDVQQKDAVaeXhibDEQ
MA4GA1UECAwHSHNpbnNodTElMAkG
A1UEBhMCVFcwggEIMA0GCSqGSIb3DQEBAAQUAAI
BDwAwggEKAoIBAQMCMCB3HK+Su
PeKUpWld2QkPL4qsQsYXhL7chHWxCYAFw9QQYXP
NDQm4l3bS9fWlqUMFck3F4HQ
```

At the bottom center of the window is a yellow **Back** button.

The following table describes the fields in this screen.

Table 50 Security > Certificates > Local Certificates: View Certificates

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 50 Security > Certificates > Local Certificates: View Certificates (continued)

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

14.4 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, which means you do not need to import any certificate that is signed by one of these certification authorities.

Note: A maximum of ten certificates can be added.

Figure 72 Security > Certificates > Trusted CA

The following table describes the labels in this screen.

Table 51 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 a unique subject information.

Table 51 Security > Certificates > Trusted CA (continued)

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

14.5 Import Trusted CA Certificate

Click **Import Certificate** in the **Trusted CA** screen to open the **Import Certificate** 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.

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

Figure 73 Security > Certificates > Trusted CA > Import Certificate

The following table describes the labels in this screen.

Table 52 Security > Certificates > Trusted CA > Import Certificate

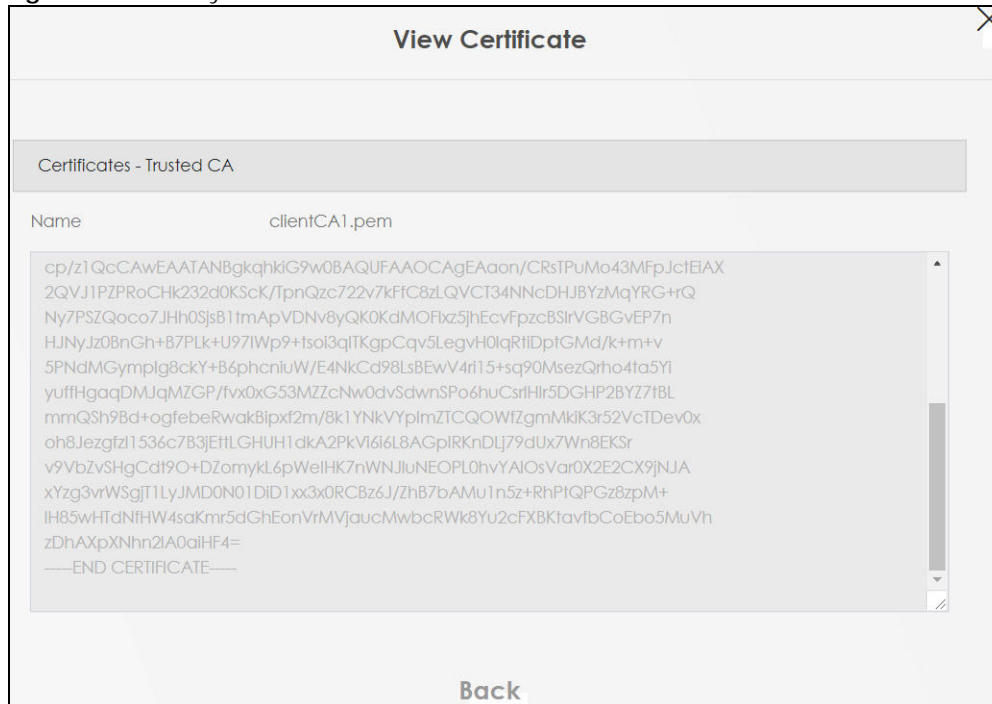
LABEL	DESCRIPTION
Certificate File Path	Type in the location of the file you want to upload in this field or click Choose File/Browse to find it.
Choose File/Browse	Click this button to find the certificate file you want to upload.
OK	Click this to save the certificate on the Zyxel Device.
Cancel	Click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

14.6 View Trusted CA Certificate

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

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

Figure 74 Security > Certificates > Trusted CA > View Certificate



The following table describes the labels in this screen.

Table 53 Security > Certificates > Trusted CA > View Certificate

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

14.7 Certificates Technical Reference

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

Certification Authorities

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

Public and Private Keys

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

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

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

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

Advantages of Certificates

Certificates offer the following benefits.

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

Certificate File Format

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

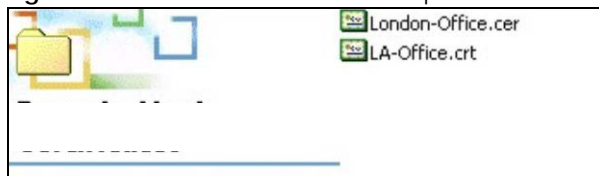
14.7.1 Verify a Certificate

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

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

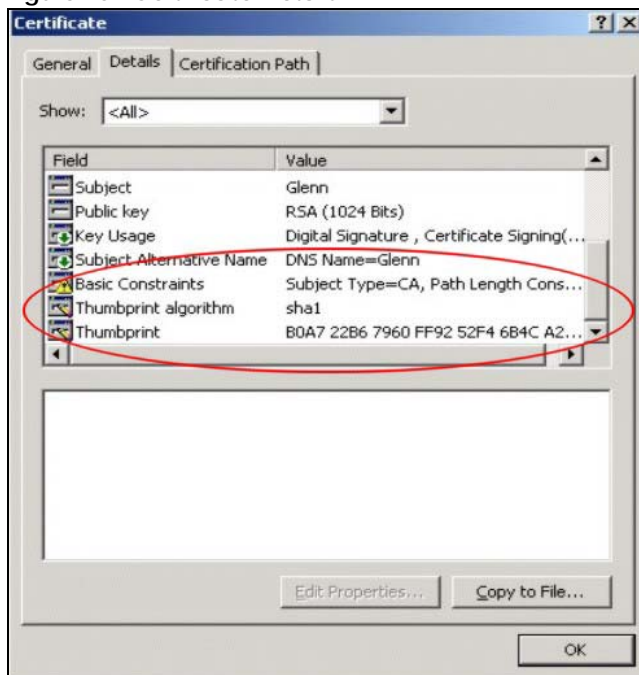
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 75 Certificates on Your Computer



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

Figure 76 Certificate Details



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

CHAPTER 15

Log

15.1 Log Overview

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

15.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs ([Section 15.2 on page 130](#)).
- Use the **Security Log** screen to see the security-related logs for the categories that you select ([Section 15.3 on page 130](#)).

15.1.2 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 54 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 54 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.

15.2 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 77 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](#)

#	Time	Facility	Level	Category	Messages
---	------	----------	-------	----------	----------

The following table describes the fields in this screen.

Table 55 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).
#	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.

15.3 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 78 System Monitor > Log > Security Log

All security 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](#)

#	Time	Facility	Level	Category	Messages
---	------	----------	-------	----------	----------

The following table describes the fields in this screen.

Table 56 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).
#	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 16

Traffic Status

16.1 Traffic Status Overview

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

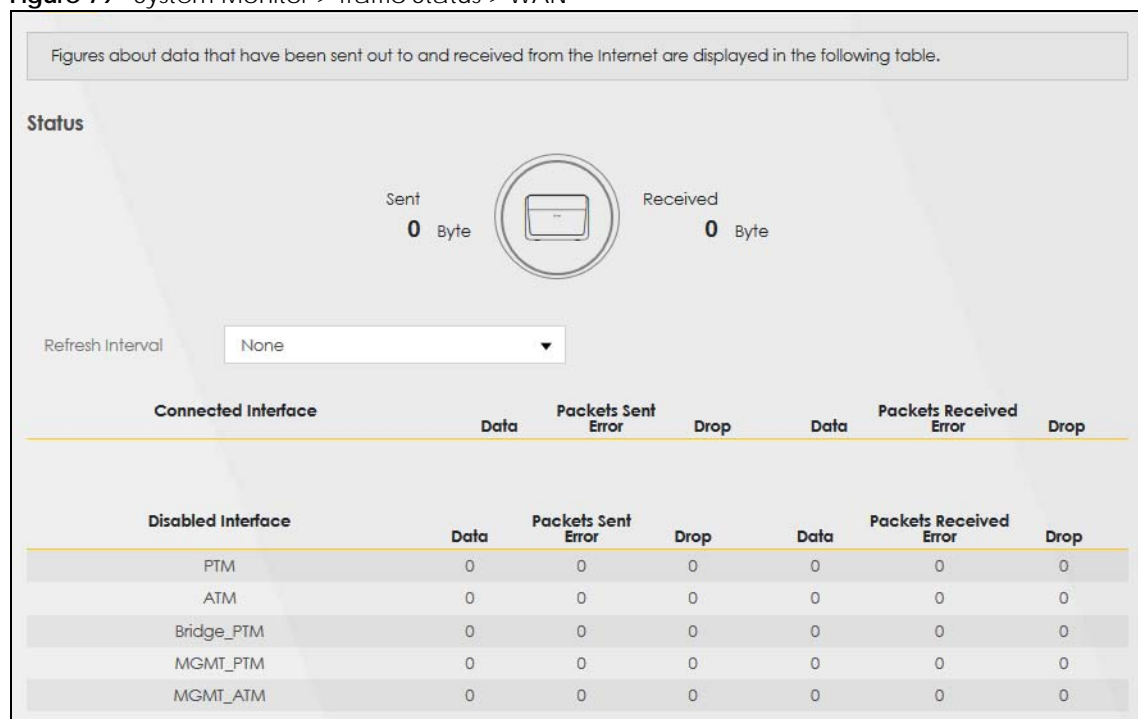
16.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the DSL traffic statistics ([Section 16.2 on page 132](#)).
- Use the **LAN** screen to view the LAN traffic statistics ([Section 16.3 on page 133](#)).

16.2 WAN Status

Click **System Monitor > Traffic Status** to open the **WAN** screen. The figures in this screen show the number of bytes received and sent through the Zyxel Device. Detailed information about each interface are listed in the tables below.

Figure 79 System Monitor > Traffic Status > WAN



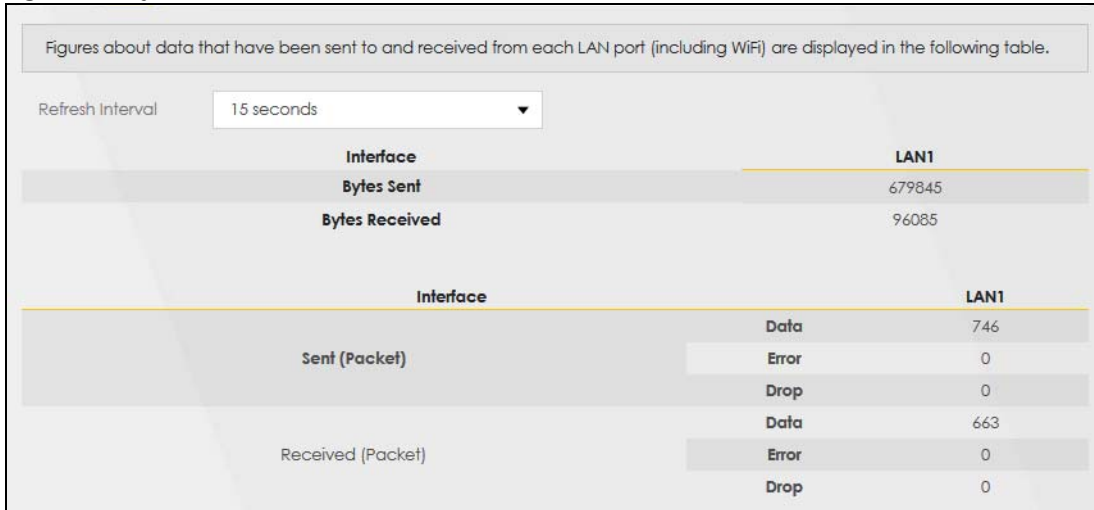
The following table describes the fields in this screen.

Table 57 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.

16.3 LAN Status

Click **System Monitor > Traffic Status > LAN** to open the following screen. The figures in this screen show the number of bytes received and sent from each LAN port and wireless network.

Figure 80 System Monitor > Traffic Status > LAN

The following table describes the fields in this screen.

Table 58 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 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 interface.
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.

CHAPTER 17

ARP Table

17.1 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.

17.1.1 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.

17.2 ARP Table Settings

Use the ARP table to view the IPv4-to-MAC address mapping(s) for the LAN. The neighbor table shows the IPv6-to-MAC address mapping(s) of each neighbor. To open this screen, click **System Monitor > ARP Table**.

Figure 81 System Monitor > ARP Table

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	192.168.1.13	dc:4a:3e:40:ec:5f	br0
IPv6 Neighbour Table			
#	IPv6 Address	MAC Address	Device
1	fe80::ecad:ab45:c530:cc3f	dc:4a:3e:40:ec:5f	br0

The following table describes the labels in this screen.

Table 59 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.

CHAPTER 18

Routing Table

18.1 Routing Table Overview

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

18.2 Routing Table

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

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

Figure 82 System Monitor > Routing Table

Routing Table					
<p>Routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet.</p> <p>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.</p> <p>Destination: This indicates the destination IPv4 address or IPv6 address and prefix of this route.</p> <p>Gateway: This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.</p> <p>Subnet Mask: This indicates the destination subnet mask of the IPv4 route.</p> <p>Flag: This indicates the route status.</p> <p>U-Up: The route is up.</p> <p>I-Reject: The route is blocked and will force a route lookup to fail.</p> <p>G-Gateway: The route uses a gateway to forward traffic.</p> <p>H-Host: The target of the route is a host.</p> <p>R-Reinstated: The route is reinstated for dynamic routing.</p> <p>D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect.</p> <p>M-Modified (redirect): The route is modified from a routing daemon or redirect.</p> <p>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".</p> <p>Interface: This indicates the name of the interface through which the route is forwarded.</p>					
IPv4 Routing Table					
Destination	Gateway	Subnet Mask	Flag	Metric	Interface
192.168.1.0/24	0.0.0.0	255.255.0.0	U	0	lo
192.168.1.0/24	0.0.0.0	255.255.255.0	U	0	br0
192.168.1.0/24	0.0.0.0	255.0.0.0	U	0	br0
IPv6 Routing Table					
Destination	Gateway	Flag	Metric	Interface	
fe80::/64	::	U	256	eth0	
fe80::/64	::	U	256	eth0.1	
fe80::/64	::	U	256	eth0.2	
fe80::/64	::	U	256	eth0.3	
fe80::/64	::	U	256	eth0.4	
fe80::/64	::	U	256	nas10	
fe80::/64	::	U	256	br0	
fe80::/64	::	U	256	ra0	
fe80::/64	::	U	256	ra1	
fe80::/64	::	U	256	ra2	
fe80::/64	::	U	256	ra3	
fe80::/64	::	U	256	rai0	
fe80::/64	::	U	256	rai1	
fe80::/64	::	U	256	rai2	
fe80::/64	::	U	256	rai3	
fe80::/64	::	U	256	rai5	
::1/128	::	U	0	lo	

The following table describes the labels in this screen.

Table 60 System Monitor > Routing Table

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

Table 60 System Monitor > Routing Table (continued)

LABEL	DESCRIPTION
Flag	<p>This indicates the route status.</p> <p>U-Up: The route is up.</p> <p>!-Reject: The route is blocked and will force a route lookup to fail.</p> <p>G-Gateway: The route uses a gateway to forward traffic.</p> <p>H-Host: The target of the route is a host.</p> <p>R-Reinstate: The route is reinstated for dynamic routing.</p> <p>D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect.</p> <p>M-Modified (redirect): The route is modified from a routing daemon or redirect.</p>
Metric	<p>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."</p>
Interface	<p>This indicates the name of the interface through which the route is forwarded.</p> <ul style="list-style-type: none"> • br0 indicates the LAN interface. • ptm0 indicates a VDSL (including G.fast) WAN interface using IPoE or in bridge mode. • atm0 indicates an ADSL WAN interface using IPoE or in bridge mode. • ppp0 indicates a WAN interface using PPPoE.

CHAPTER 19

MAC Address Table

19.1 MAC Address Table Overview

The MAC address (media access control address) of a device is a unique identifier assigned to a network interface controller for communications at the data link layer of a network segment. This table lists the MAC address of each client device. VLAN information also shows when this device belongs to a VLAN group.

Note: The MAC address of the Zyxel Device can be found in the **System Info** of the **Status** screen (see [Section 4.1.2 on page 30](#) for details).

19.2 MAC Address Table Settings

Aside from the MAC address, the VLAN information of the associated wired clients are also listed in the table. If the wired client does not tag with VLAN, the VLAN entry for this client is **0**.

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

Figure 83 System Monitor > MAC Address Table

MAC Address Table			
This table lists the MAC address of each client device and the VLAN group of each associated wired client. If the client device is not in the VLAN group it displays 0.			
MAC Address Table Interface: br0 WAN and LAN MAC included			
#	VLAN	MAC Address	Device
1	0	dc:4a:3e:40:ec:5f	eth1.0

The following table describes the labels in this screen.

Table 61 System Monitor > MAC Address Table

LABEL	DESCRIPTION
#	This is the MAC address table entry number.
VLAN	This is the VLAN information of the associated wired clients. This displays 0 when the wired client does not tag with VLAN.
MAC Address	This is the MAC address of the wired client's device.
Device	This is the type of interface used by the wired client's device.

CHAPTER 20

xDSL Statistics

20.1 xDSL Statistics Overview

Use this screen to view detailed DSL information. It allows you to see the DSL status, check port details, and see DSL counters. Click **System Monitor > xDSL Statistics** to open the following screen.

Figure 84 System Monitor > xDSL Statistics

xDSL Statistics

xDSL Statistics displays the DSL information.

Monitor

Type: Stats

Refresh Interval: No Refresh

Line: Line 0

Status

```
=====
=====
xDSL Training Status: Idle
      Mode: G.DMT
      G.Vector: Disable
      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
=====
```

The following table describes the labels in this screen.

Table 62 System > xDSL Statistics

LABEL	DESCRIPTION
Monitor	
Type	Select Stats to display the various DSL status, downstream/upstream counters and port details in the Status window. Select Profile to display the DSL PHY and driver version, modulations, VDSL profiles, capability and PHY type configuration details in the Status window.
Refresh Interval	Select the time interval for refreshing statistics.
Line	Select which DSL line's statistics you want to display.
Status	

Table 62 System > xDSL Statistics (continued)

LABEL	DESCRIPTION
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. Inactive 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.
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.

Table 62 System > xDSL Statistics (continued)

LABEL	DESCRIPTION
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 the BRCM DSL driver.
FastRetr	This is the number of DSL fast retraining count.
HostInitRetr	This is the number of the retraining counts the host initiated.
FastRetr	This is the number of DSL fast retraining counts.
FailedRetr	This is the number of failed retraining attempts.
FailedFastRetr	This is the number of failed fast retraining attempts.

CHAPTER 21

System

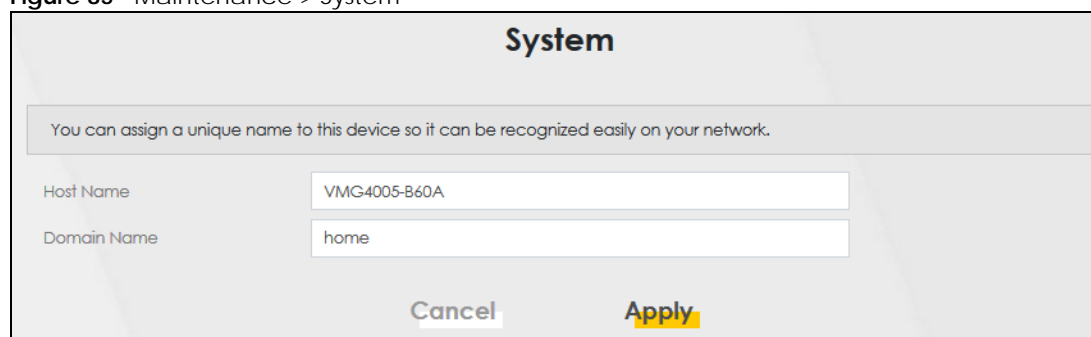
21.1 System Overview

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

21.2 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 85 Maintenance > System



System

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

Host Name VMG4005-B60A

Domain Name home

Cancel Apply

The following table describes the labels in this screen.

Table 63 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. Up to 30 printable ASCII characters are allowed except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [:].
Cancel	Click Cancel to abandon this screen without saving.
Apply	Click Apply to save your changes.

CHAPTER 22

User Account

22.1 User Account Overview

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

22.2 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 86 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	

Cancel Apply

The following table describes the labels in this screen.

Table 64 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 64 Maintenance > 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 Retry Times .
Group	This field displays whether this user has Administrator or User privileges.
Modify	Click the Edit icon to configure the entry. Click the Delete icon to remove the entry.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

22.2.1 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 87 Maintenance > User Account > Add/Edit

User Account Add

Active ☒

User Name

Password

Verify Password

Retry Times (0~5), 0 : Not limit

Idle Timeout Minute(s) (1~60)

Lock Period Minute(s) (5~90)

Group

Protocol ☒ HTTP&HTTPS ☒ SSH ☒ TELNET ☒ FTP

Note

To use Protocol control Feature for each user account under Remote Management>MGMT Services, please first enable specified service

Cancel OK

Note: When adding accounts, an **Administrator** can create new **User** or **Administrator** accounts, while a **User** can only create **User** accounts

The following table describes the labels in this screen.

Table 65 Maintenance > User Account > Add/Edit

LABEL	DESCRIPTION
Active	Select Enable or Disable to activate or deactivate the user account.
User Name	Enter a new name for the account. The User Name must contain 1 to 15 characters, including 0 to 9, a to z, and !@#%*()-_+=~.,{}[]\ . Spaces are not allowed.
Password	Enter your new system password. The Password must contain 6 to 64 characters, including 0 to 9 and a to z. 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. If you are changing your existing password, you have to first enter your Old Password then enter your New Password .
Verify Password	Enter the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	Enter the length of inactive time before the Zyxel Device will automatically log the user out of the web configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number if consecutive wrong passwords have been entered as defined in Retry Times .
Group	Specify whether this user will have Administrator or User privileges. Administrator and User privileges are mostly the same, but the System settings will only display when you log in as an Administrator .
Protocol	Select the network protocol for operating network services over an unsecured network. Only HTTP&HTTPS is available when User is selected in the Group field. Note: To use the Protocol Control feature for each user account under Remote Management > MGMT Services , please enable the specified service.
Cancel	Click Cancel to restore your previously saved settings.
OK	Click OK to save your changes.

CHAPTER 23

Remote Management

23.1 Remote Management Overview

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

23.1.1 What You Can Do in this Chapter

- Use the **MGMT Services** screen to allow various approaches to access the Zyxel Device remotely from a DSL and/or LAN connection ([Section 23.2 on page 148](#)).
- Use the **Trust Domain** screen to enable users to permit access from local management services by entering specific IP addresses ([Section 23.3 on page 149](#)).

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

23.2 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 88 Maintenance > Remote Management > MGMT Services

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

Service Control

WAN Interface used for services: ☐ Any_WAN ☒ Multi_WAN

☒ MGMT_PTM ☒ MGMT_ATM

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

The following table describes the fields in this screen.

Table 66 Maintenance > Remote Management > MGMT Services

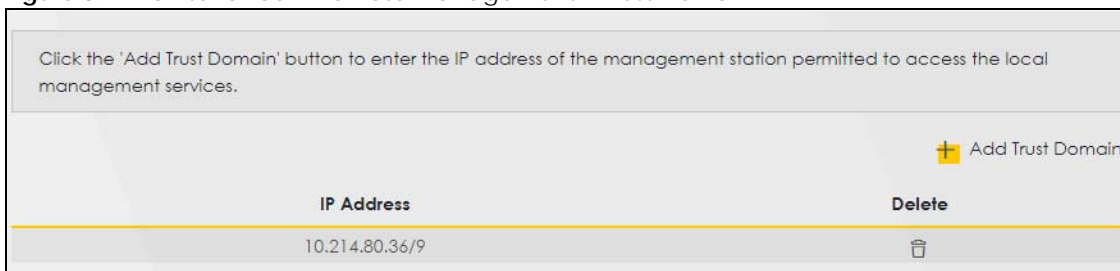
LABEL	DESCRIPTION
WAN Interface used for services	<p>Select Any_WAN to have the Zyxel Device automatically activate the remote management service when any WAN connection is up.</p> <p>Select Multi_WAN and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up.</p>
Service	<p>This is the service you may use to access the Zyxel Device.</p> <ul style="list-style-type: none"> • HTTP provides a non secured way. • HTTPS is the secured version of HTTP, it makes sure that your data cannot be read during transmission. • FTP is the most common way of communication between two devices. • TELNET provides a way to control your Zyxel Device remotely. • SSH prevents leakage of data during remote management. Additionally, it can encrypt all transmitted data. • PING is a diagnostic tool that can check if your Zyxel Device is connected to the Internet.
LAN	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from the LAN.
WAN	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	<p>Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from the trusted hosts configured in the Maintenance > Remote MGMT > Trust Domain screen.</p> <p>If you only want certain WAN connections to have access to the Zyxel Device using the corresponding services, then clear WAN, select Trust Domain and configure the allowed IP address(es) in the Trust Domain screen.</p>
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes back to the Zyxel Device.

23.3 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 cannot access the Zyxel Device from the WAN through the specified services.

Figure 89 Maintenance > Remote Management > Trust Domain


Click the 'Add Trust Domain' button to enter the IP address of the management station permitted to access the local management services.

IP Address	Delete
10.214.80.36/9	

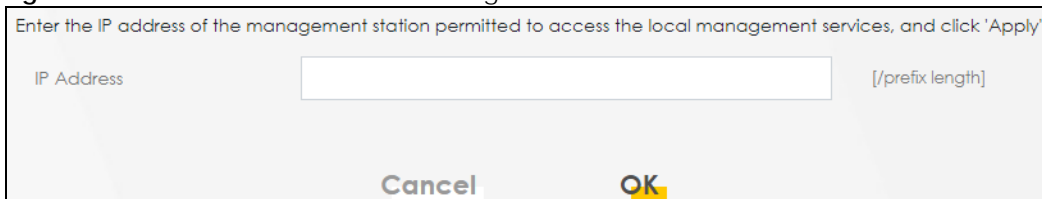
The following table describes the fields in this screen.

Table 67 Maintenance > Remote Management > Trust Domain

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

23.3.1 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 90 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 68 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 OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to restore your previously saved settings.

CHAPTER 24

Time Settings

24.1 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.

24.2 Time Setup

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 91 Maintenance > Time

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

Current Date/Time

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

Time and Date Setup

Time Protocol SNTP (RFC-1769)

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

Time Zone

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

Daylight Savings

Active ☒

Start Rule

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

End Rule

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

Cancel Apply

The following table describes the fields in this screen.

Table 69 Maintenance > Time


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

Table 69 Maintenance > Time (continued)

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

CHAPTER 25

Log Setting

25.1 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.

25.2 Log Setup

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 92 Maintenance > Log Setting

Log Setting

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

Syslog Setting

Syslog Logging ☒

Mode Local File and Remote

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

UDP Port 514 (Server Port)

Active Log

System Log

- ☒ WAN-DHCP
- ☐ DHCP Server
- ☐ PPPoE
- ☒ TR-069
- ☐ HTTP
- ☒ System
- ☒ xDSL
- ☐ ACL
- ☒ UNI

Security Log

- ☐ Account
- ☒ Attack
- ☒ Firewall
- ☐ MAC Filter

Cancel Apply

The following table describes the fields in this screen.

Table 70 Maintenance > Log Setting


LABEL	DESCRIPTION
Syslog Setting	
Syslog Logging	The Zyxel Device sends a log to an external syslog server. Click this switch to enable or disable to enable syslog logging. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Mode	Select the syslog destination from the drop-down list box. If you select Remote , the log(s) will be sent to a remote syslog server. If you select Local File , the log(s) will be saved in a local file. If you want to send the log(s) to a remote syslog server and save it in a local file, select Local File and Remote . Note: When Remote Syslog is enabled, the recipient may receive personal information of Individuals on its behalf. The types of personal information being collected includes without limitation to the following: host name, host IP address and MAC address.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
Active Log	
System Log	Select the categories of system logs that you want to record.

Table 70 Maintenance > Log Setting (continued)

LABEL	DESCRIPTION
Security Log	Select the categories of security logs that you want to record.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

CHAPTER 26

Firmware Upgrade

26.1 Firmware Upgrade Overview

This screen lets you upload new firmware to your Zyxel Device. You can download new firmware releases from the Zyxel website www.zyxel.com to upgrade your device's performance.

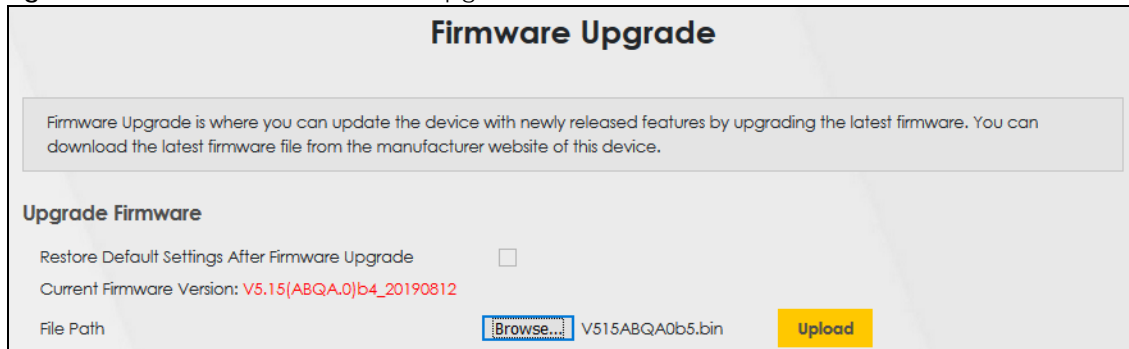
Only use firmware for your device's specific model. Refer to the label on the bottom of your Zyxel Device.

26.2 Firmware 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 93 Maintenance > Firmware Upgrade



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.

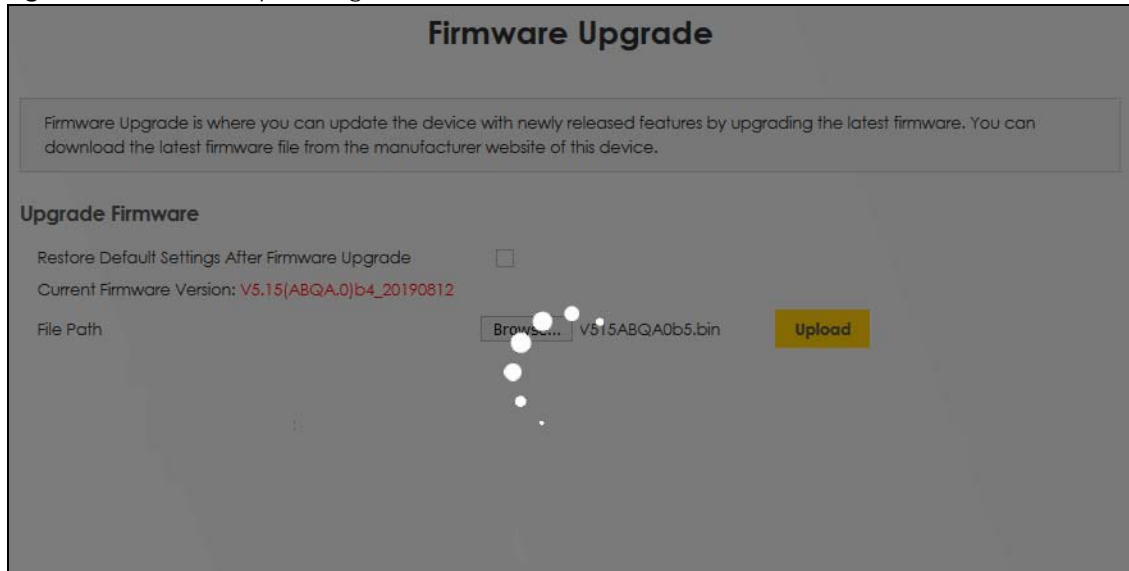
Table 71 Maintenance > Firmware Upgrade

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 71 Maintenance > Firmware Upgrade

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

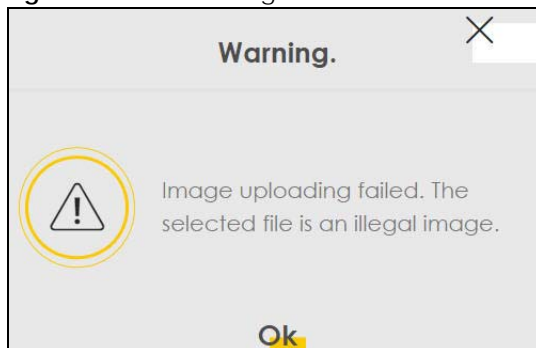
Figure 94 Firmware Uploading



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

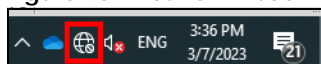
If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 95 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.

Figure 96 Network Disconnected



CHAPTER 27

Backup/Restore

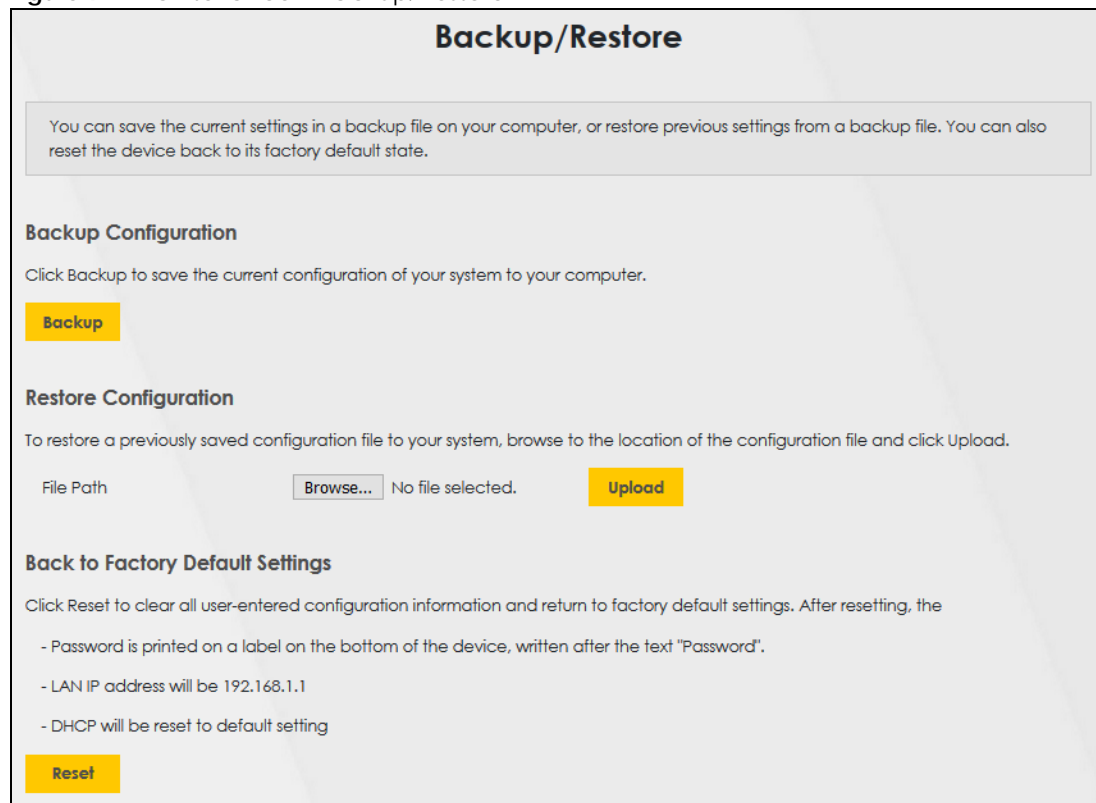
27.1 Backup/Restore Overview

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

27.2 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 97 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 72 Restore Configuration

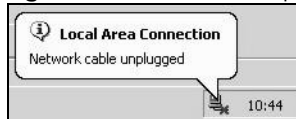
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload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

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

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

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

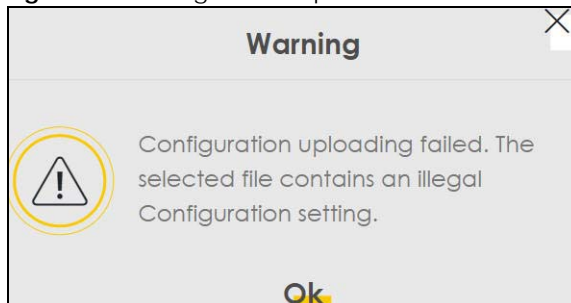
Figure 98 Network Temporarily Disconnected



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 99 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 100 Reset Warning Message

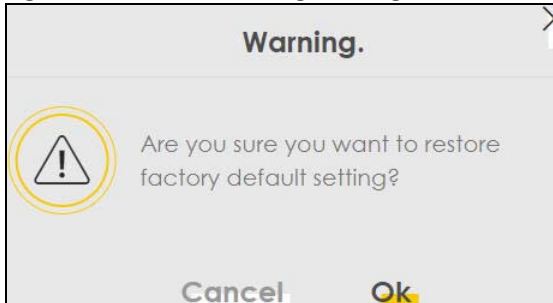
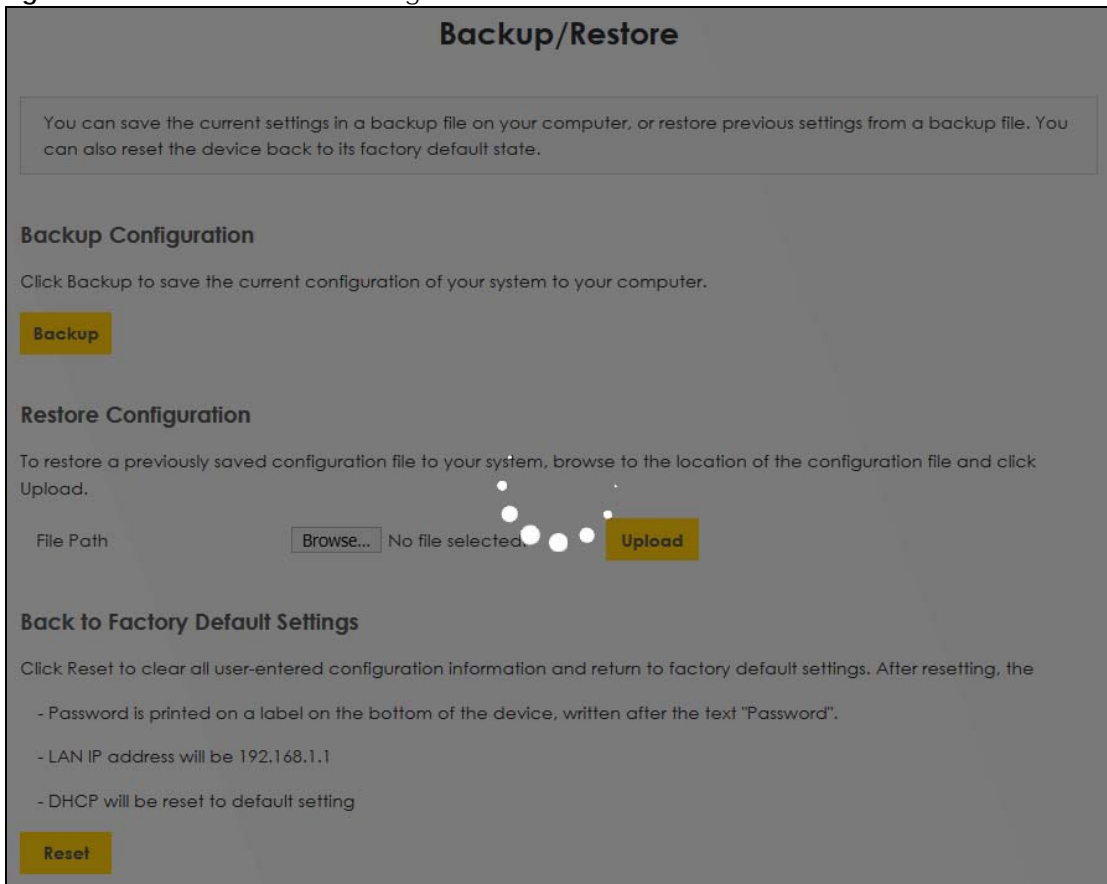


Figure 101 Reset In Process Message



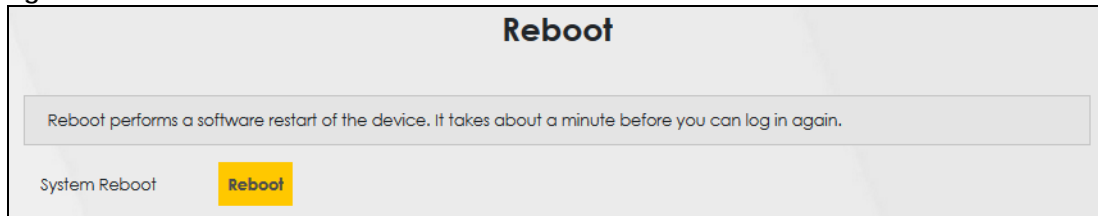
You can also press the **RESET** button on the bottom panel to reset the factory defaults of your Zyxel Device. Refer to [Section 1.5.3 on page 16](#) for more information on the **RESET** button.

27.3 Reboot

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

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

Figure 102 Maintenance > Reboot



CHAPTER 28

Diagnostic

28.1 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.

28.1.1 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 28.3 on page 165](#)).
- The **802.1ag** screen lets you perform CFM actions ([Section 28.4 on page 166](#)).
- The **802.3ah** screen lets you configure link OAM port parameters([Section 28.5 on page 167](#)).
- The **OAM Ping** screen lets you send an ATM OAM (Operation, Administration and Maintenance) packet to verify the connectivity of a specific PVC. ([Section 28.6 on page 168](#)).

28.2 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.

28.3 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 103 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 73 Maintenance > Diagnostic > Ping & TraceRoute & NsLookup

LABEL	DESCRIPTION
URL or IP 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.

28.4 802.1ag (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 104 Maintenance > Diagnostic > 802.1ag

The following table describes the fields in this screen.

Table 74 Maintenance > Diagnostic > 802.1ag



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

Table 74 Maintenance > Diagnostic > 802.1ag (continued)

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



28.5 802.3ah (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 105 Maintenance > Diagnostic > 802.3ah

The following table describes the labels in this screen.

Table 75 Maintenance > Diagnostics > 802.3ah

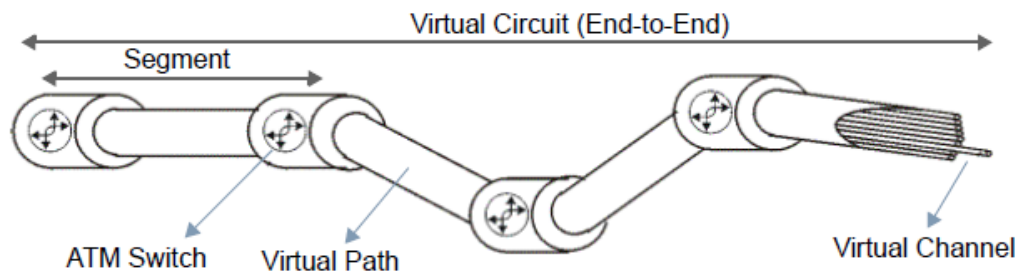
LABEL	DESCRIPTION
IEEE 802.3ah Ethernet OAM	Click this switch to enable or disable the Ethernet OAM on the specified interface. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Interface	Select the interface on which you want to enable the IEEE802.3ah.
OAM ID	Enter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

28.6 OAM Ping

Click **Maintenance > Diagnostic > OAM Ping** to open the screen shown next. Use this screen to perform an OAM (Operation, Administration and Maintenance) F4 or F5 loopback test on a PVC. The Zyxel Device sends an OAM F4 or F5 packet to the DSLAM or ATM switch and then returns it to the Zyxel Device. The test result then displays in the text box. ATM sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel (VC) Logical connections between ATM devices
- Virtual Path (VP) A bundle of virtual channels
- Virtual Circuits A series of virtual paths between circuit end points

Figure 106 Virtual Circuit Topology



Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path. A series of virtual paths make up a virtual circuit.

F4 cells operate at the virtual path (VP) level, while F5 cells operate at the virtual channel (VC) level. F4 cells use the same VPI as the user data cells on VP connections, but use different predefined VCI values. F5 cells use the same VPI and VCI as the user data cells on the VC connections, and are distinguished from data cells by a predefined Payload Type Identifier (PTI) in the cell header. Both F4 flows and F5 flows are bidirectional and have two types.

- segment F4 flows (VCI=3)
- end-to-end F4 flows (VCI=4)
- segment F5 flows (PTI=100)
- end-to-end F5 flows (PTI=101)

OAM F4 or F5 tests are used to check virtual path or virtual channel availability between two DSL devices. Segment flows are terminated at the connecting point which terminates a VP or VC segment. End-to-end flows are terminated at the end point of a VP or VC connection, where an ATM link is terminated. Segment loopback tests allow you to verify integrity of a PVC to the nearest neighboring ATM device. End-to-end loopback tests allow you to verify integrity of an end-to-end PVC.

Note: The DSLAM to which the Zyxel Device is connected must also support ATM F4 and/or F5 to use this test.

Note: This screen is available only when you configure an ATM layer-2 interface.

Figure 107 Maintenance > Diagnostic > OAM Ping

The following table describes the fields in this screen.

Table 76 Maintenance > Diagnostic > OAM Ping

LABEL	DESCRIPTION
	Select a PVC on which you want to perform the loopback test.
F4 segment	Press this to perform an OAM F4 segment loopback test.
F4 end-end	Press this to perform an OAM F4 end-to-end loopback test.

Table 76 Maintenance > Diagnostic > OAM Ping (continued)

LABEL	DESCRIPTION
F5 segment	Press this to perform an OAM F5 segment loopback test.
F5 end-end	Press this to perform an OAM F5 end-to-end loopback test.

PART III

Troubleshooting and Appendices

CHAPTER 29

Troubleshooting

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

- [Power, Hardware Connections, and LEDs](#)
- [Zyxel Device Access and Login](#)
- [Internet Access](#)
- [IP Address Setup](#)

29.1 Power, Hardware Connections, and LEDs

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

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

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

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.5.1 on page 15](#).
- 2 Check the hardware connections.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the Zyxel Device off and on.
- 5 If the problem continues, contact the vendor.

29.2 Zyxel Device Access and Login

I forgot the IP address for the Zyxel Device.

- 1 The default LAN IP address is 192.168.1.1.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the Zyxel Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Zyxel Device (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 1.5.3 on page 16](#).

I forgot the password.

- 1 See the cover page for the default login account username and password.
- 2 If you changed the username and/or password, you have to reset the device to its factory defaults. See [Section 1.5.3 on page 16](#).

I cannot see or access the **Login** screen in the Web Configurator.

- 1 Make sure you are using the correct IP address.
 - The default IP address is [192.168.1.1](#).
 - If you changed the IP address, use the new IP address. See [Section 6.2 on page 56](#).
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the Zyxel Device](#).
 - Make sure your computer has an IP address in the same subnet as the Zyxel Device. Your computer should have an IP address from 192.168.1.2 to 192.168.1.254. See [Section 29.4 on page 175](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Figure 4 on page 15](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
- 4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance > Remote Management**).
- 5 Reset the device to its factory defaults, and try to access the Zyxel Device with the default IP address. See [Section 1.5.3 on page 16](#).

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

Advanced Suggestions

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

I can see the [Login](#) screen, but I cannot log in to the Zyxel Device.

- 1 Make sure you have entered the password correctly. See the cover page for the default login names and associated passwords. The field is case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the Web Configurator while someone is using Telnet to access the Zyxel Device. Log out of the Zyxel Device in the other session, or ask the person who is logged in to log out.
- 3 Turn the Zyxel Device off and on.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 29.1 on page 172](#).

I cannot Telnet to the Zyxel Device.

See the troubleshooting suggestions for [I cannot see or access the Login screen in the Web Configurator](#). Ignore the suggestions about your browser.

29.3 Internet Access

I cannot access the Internet.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and [Figure 4 on page 15](#).
- 2 Disconnect all the cables from your device and reconnect them.
- 3 If the problem continues, contact your ISP.

I cannot access the Internet through a DSL connection.

- 1 Make sure you have the **DSL** port connected to a telephone jack (or the DSL or modem jack on a splitter if you have one).
- 2 Check the DSL LED on the Zyxel Device for DSL connection status. See [Section 1.5.1 on page 15](#).

[I cannot connect to the Internet using a second DSL connection.](#)

ADSL and VDSL connections cannot work at the same time. You can only use one type of DSL connection, either ADSL or VDSL connection at one time.

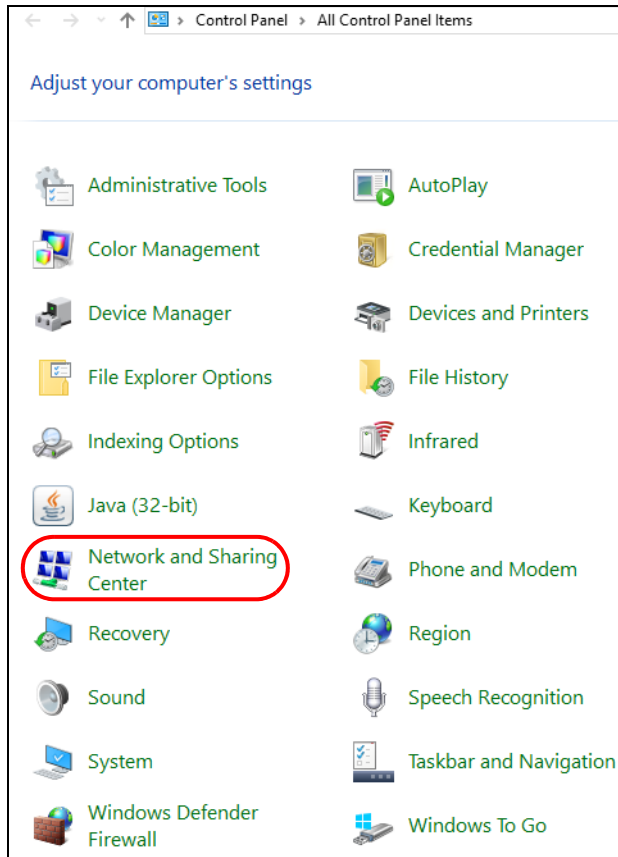
[I cannot access the Zyxel Device anymore. I had access to the Zyxel Device, but my connection is not available anymore.](#)

- 1 Your session with the Zyxel Device may have expired. Try logging into the Zyxel Device again.
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and [Figure 4 on page 15](#).
- 3 Turn the Zyxel Device off and on.
- 4 If the problem continues, contact your vendor.

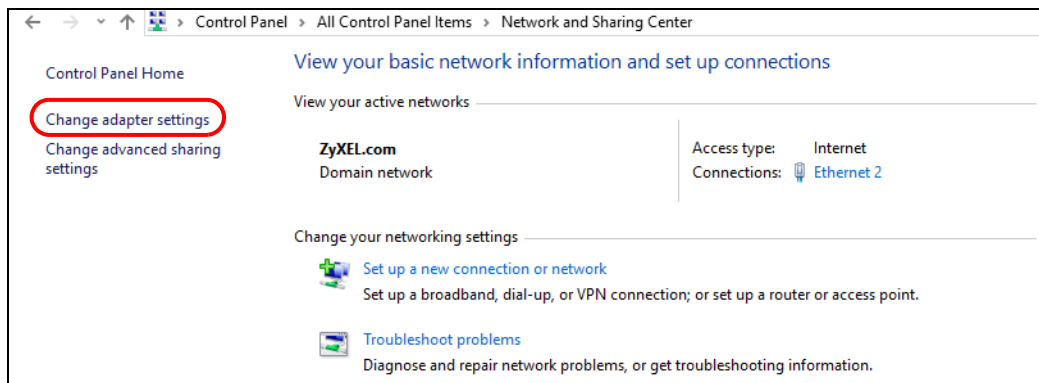
29.4 IP Address Setup

[I need to set the computer's IP address to be in the same subnet as the Zyxel Device.](#)

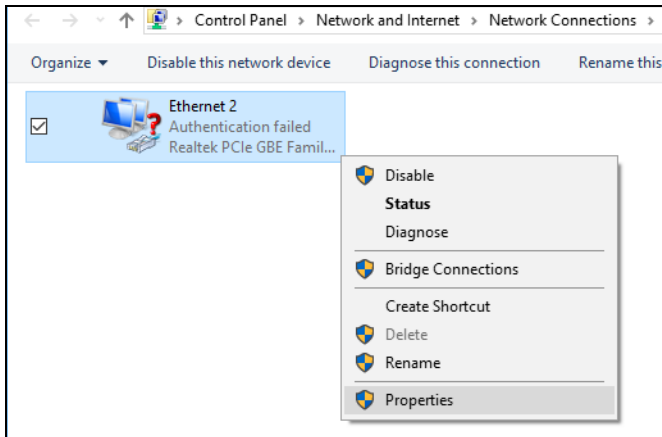
- 1 In Windows 10, open the **Control Panel**.
- 2 Click **Network and Internet** (this field may be missing in your version) > **Network and Sharing Center**.



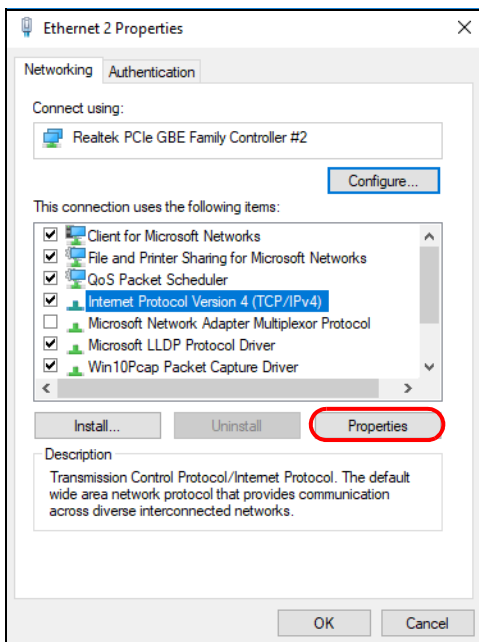
- 3 Click **Change adapter settings**.



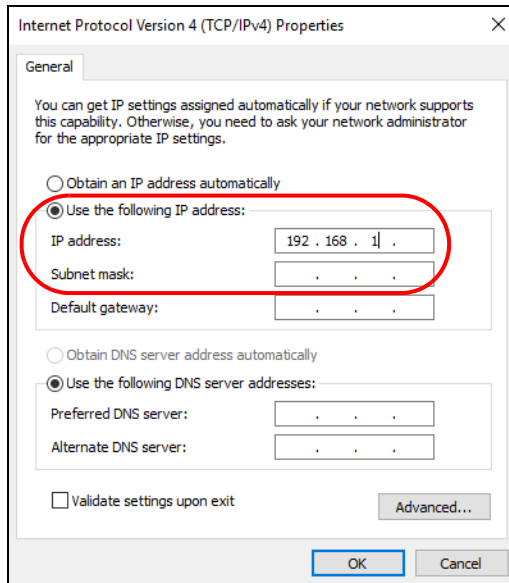
- 4 Right-click the **Ethernet** icon, and then select **Properties**



- 5 Click **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.



- 6 Select **Use the following IP address** and enter an **IP address** from **192.168.1.2** to **192.168.1.254**. The **Subnet mask** will be entered automatically.



- 7 Click **OK** when you are done and close all windows.

APPENDIX A

IPv6

Overview

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

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

Prefix and Prefix Length

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

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

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

Link-local Address

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

Table 77 Link-local Unicast Address Format

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

Global Address

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

Unspecified Address

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

Loopback Address

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

Multicast Address

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

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

Table 78 Predefined Multicast Address

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

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

Table 79 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0
FF01:0:0:0:0:0:0
FF02:0:0:0:0:0:0
FF03:0:0:0:0:0:0
FF04:0:0:0:0:0:0
FF05:0:0:0:0:0:0
FF06:0:0:0:0:0:0
FF07:0:0:0:0:0:0
FF08:0:0:0:0:0:0
FF09:0:0:0:0:0:0
FF0A:0:0:0:0:0:0
FF0B:0:0:0:0:0:0
FF0C:0:0:0:0:0:0
FF0D:0:0:0:0:0:0
FF0E:0:0:0:0:0:0
FF0F:0:0:0:0:0:0

Subnet Masking

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

Interface ID

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

EUI-64

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

Table 80

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

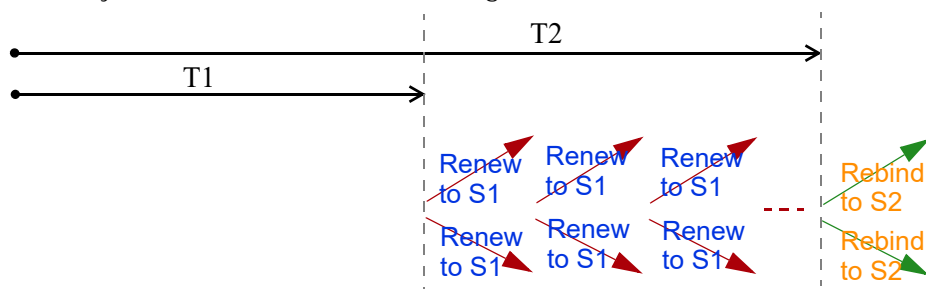
Table 81

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

Identity Association

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

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



DHCP Relay Agent

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

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

Prefix Delegation

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

ICMPv6

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

Neighbor Discovery Protocol (NDP)

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

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

IPv6 Cache

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

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

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

Multicast Listener Discovery

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

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

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

MLD filtering controls which multicast groups a port can join.

MLD Messages

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

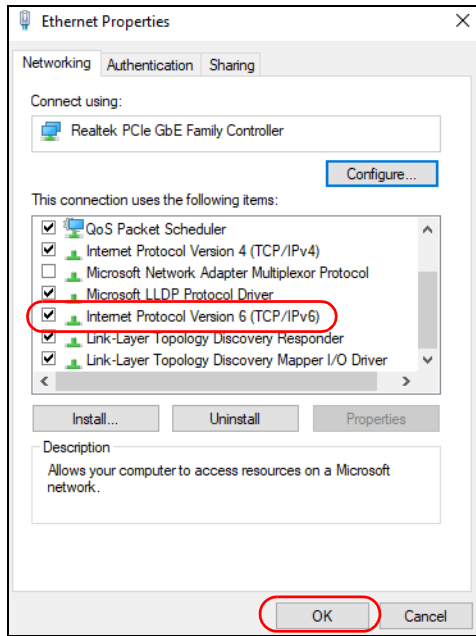
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected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

Example – Enabling IPv6 on Windows 10

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

To enable IPv6 in Windows 10:

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



- 4 Click the Search icon (🔍) and then enter "cmd" in the search box..
- 5 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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


APPENDIX B

Customer Support

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

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

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

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

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

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

Asia

China

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

India

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

Kazakhstan

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

Korea

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

Malaysia

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

Philippines

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

Singapore

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

Taiwan

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

Thailand

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

Vietnam

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

Europe

Belarus

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

Belgium (Netherlands)

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

Bulgaria

- Zyxel Bulgaria

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

Czech Republic

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

Denmark

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

Finland

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

France

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

Germany

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

Hungary

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

Italy

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

Norway

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

Poland

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

Romania

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

Russian Federation

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

Slovakia

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

Spain

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

Sweden

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

Switzerland

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

Turkey

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

UK

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

Ukraine

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

South America

Argentina

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

Brazil

- Zyxel Communications Brasil Ltda.

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

Colombia

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

Ecuador

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

South America

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

Middle East

Israel

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

North America

USA

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

APPENDIX C

Legal Information

Copyright

Copyright © 2023 by Zyxel and/or its affiliates

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

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

Disclaimer

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

Regulatory Notice and Statement

UNITED STATES of AMERICA



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

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference, and
 - (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
 - Reorient or relocate the receiving antenna
 - Increase the separation between the devices
 - Connect the equipment to an outlet other than the receiver's
 - Consult a dealer or an experienced radio/TV technician for assistance

CANADA

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

Innovation, Science and Economic Development Canada ICES Statement

CAN ICES-3 (B)/NMB-3(B)

EUROPEAN UNION and UNITED KINGDOM



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

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the Zyxel Device. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
 - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
 - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Environment Statement

ErP (Energy-related Products)

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

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

Disposal and Recycling Information

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

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

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

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

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

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



台灣

以下訊息僅適用於產品銷售至台灣地區

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。





安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸
 - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
 - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
 - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
 - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

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

Explanation of the Symbols

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

Viewing Certifications

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

Registration

Register your product online at www.zyxel.com to receive email notices of firmware upgrades and related information.

Trademarks

The trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. To request the source code covered under these licenses, please go to: <https://service-provider.zyxel.com/global/en/gpl-oss-software-notice>.

Index

A

Access Control (Rules) screen [109](#)
activation
 firewalls [106](#)
Address Resolution Protocol [135](#)
Annex A [11](#)
Annex B [11](#)
applications
 Internet access [12](#)
ARP Table [135, 137, 140](#)

B

backup
 configuration [160](#)
Broadband [33](#)
broadcast [53](#)
button
 RESET [16](#)

C

CA [127](#)
Canonical Format Indicator See CFI
CCMs [164](#)
certificate
 details [128](#)
 factory default [121](#)
 file format [127](#)
 file path [125](#)
 import [121, 124](#)
 public and private keys [127](#)
 verification [127](#)
certificate request
 create [121](#)
 view [123](#)
certificates [120](#)

 advantages [127](#)
 authentication [120](#)
 CA [120, 127](#)
 creating [122](#)
 public key [120](#)
 replacing [121](#)
 storage space [121](#)
 thumbprint algorithms [128](#)
 trusted CAs [125](#)
 verifying fingerprints [128](#)
Certification Authority [120](#)
Certification Authority, see CA
certifications [191](#)
 viewing [193](#)
CFI [53](#)
CFM [164](#)
 CCMs [164](#)
 link trace test [165](#)
 loopback test [164](#)
 MA [164](#)
 MD [164](#)
 MEP [164](#)
 MIP [164](#)
client list [62](#)
configuration
 back up [14](#)
 backup [160](#)
 firewalls [106](#)
 reset [162](#)
 restoring [161](#)
Connectivity Check Messages, see CCMs
contact information [185](#)
copyright [190](#)
CoS [91](#)
CoS technologies [76](#)
Create Certificate Request screen [122](#)
creating certificates [122](#)
customer support [185](#)
customized service [107](#)
 add [108](#)
customized services [108](#)

D

- DDoS [105](#)
- Denials of Service, see DoS
- DHCP [56, 65](#)
- DHCP Server Lease Time [59](#)
- DHCP Server State [59](#)
- Differentiated Services, see DiffServ [91](#)
- DiffServ [91](#)
 - marking rule [92](#)
- digital IDs [120](#)
- disclaimer [190](#)
- DNS [56, 65](#)
- DNS server address assignment [53](#)
- DNS Values [59](#)
- domain name system, see DNS
- Domain Name System. See DNS.
- DoS [105](#)
 - thresholds [105](#)
- DoS protection blocking
 - enable [112](#)
- DS field [92](#)
- DS, see differentiated services
- DSCP [91](#)
- DSL bonding [12](#)
 - example [13](#)
 - setup [12](#)
- DSL line [12](#)
- Dynamic Host Configuration Protocol, see DHCP

E

- Encapsulation [49](#)
 - MER [49](#)
 - PPP over Ethernet [50](#)
- encapsulation
 - RFC 1483 [50](#)
- Ether Type [84](#)

F

- factory default

- reset to [17](#)
- firewall
 - enhancing security [113](#)
 - LAND attack [105](#)
 - security considerations [114](#)
 - traffic rule direction [111](#)
- Firewall DoS screen [111](#)
- Firewall General screen [106](#)
- firewall rules
 - direction of travel [112](#)
- firewalls [104, 106](#)
 - actions [111](#)
 - configuration [106](#)
 - customized service [107](#)
 - customized services [108](#)
 - DDoS [105](#)
 - DoS [105](#)
 - thresholds [105](#)
 - ICMP [105](#)
 - Ping of Death [105](#)
 - rules [112](#)
 - security [113](#)
 - SYN attack [104](#)
- firmware [158](#)
 - version [31](#)

I

- ICMP [105](#)
- icon
 - settings [21](#)
- IEEE 802.1Q [52](#)
- IGMP [53](#)
 - version [53](#)
- Import Certificate screen [125](#)
- importing trusted CAs [125](#)
- Integrated Services Digital Network, See ISDN
- interface group [99](#)
- Internet
 - wizard setup [26](#)
- Internet access [12](#)
 - wizard setup [26](#)
- Internet Control Message Protocol, see ICMP
- Internet Protocol version 6 [34](#)
- Internet Protocol version 6, see IPv6

IP address [66](#)
 ping [165](#)
 private [66](#)
 WAN [34](#)
IP Address Assignment [52](#)
IPv4 firewall [107](#)
IPv6 [34, 179](#)
 addressing [34, 54, 179](#)
 EUI-64 [181](#)
 global address [179](#)
 interface ID [181](#)
 link-local address [179](#)
 Neighbor Discovery Protocol [179](#)
 ping [179](#)
 prefix [35, 54, 179](#)
 prefix delegation [37](#)
 prefix length [35, 54, 179](#)
 unspecified address [180](#)
IPv6 firewall [107](#)
ISDN [11](#)

J

Java permissions [18](#)
JavaScript [18](#)

L

LAN [55](#)
 client list [62](#)
 DHCP [65](#)
 DNS [65](#)
 IP address [66](#)
 MAC address [62](#)
 status [32](#)
 subnet mask [56, 66](#)
LAN IP address [59](#)
LAN IPv6 Mode Setup [60](#)
LAN Setup screen [56](#)
LAN subnet mask [59](#)
LAND attack [105](#)
language
 select [22](#)
LBR [164](#)

LEDs [15](#)
link trace [165](#)
Link Trace Message, see LTM
Link Trace Response, see LTR
Local Area Network, see LAN
Local Certificates screen [120](#)
login [18](#)
 passwords [18](#)
logs [129, 132, 155](#)
Loop Back Response, see LBR
loopback [164](#)
LTM [165](#)
LTR [165](#)

M

MA [164](#)
MAC address [62](#)
 LAN [62](#)
MAC Filter [115](#)
Maintenance Association, see MA
Maintenance Domain, see MD
Maintenance End Point, see MEP
managing the device
 good habits [14](#)
Maximum Burst Size (MBS) [51](#)
MD [164](#)
MEG [167](#)
MEP [164](#)
MTU (Multi-Tenant Unit) [52](#)
multicast [53](#)
multiplexing [50](#)
 LLC-based [50](#)
 VC-based [50](#)
multiprotocol encapsulation [50](#)

N

navigation panel [21](#)
network map [23, 24, 30](#)

P

- password
 - change [14, 19](#)
- passwords [18](#)
- Peak Cell Rate (PCR) [51](#)
- Per-Hop Behavior, see PHB [92](#)
- PHB [92](#)
- Ping of Death [105](#)
- Plain Old Telephone Service, See ISDN
- ports panel [16](#)
- PPPoE [50](#)
 - Benefits [50](#)
- prefix delegation [37](#)
- private IP address [66](#)
- product registration [193](#)
- Protocol (Customized Services) screen [107](#)
- Protocol Entry
 - add [108](#)

Q

- QoS [75, 91](#)
 - marking [76](#)
 - setup [75](#)
 - tagging [76](#)
 - versus CoS [76](#)
- Quality of Service, see QoS

R

- reboot the VMG [22](#)
- registration
 - product [193](#)
- reset [16, 162](#)
- RESET button [16](#)
- restart [163](#)
- restoring configuration [161](#)
- RFC 1483 [50](#)
- RFC 3164 [129](#)
- router features [12](#)

S

- screen resolution recommended [18](#)
- security
 - network [113](#)
- Security Log [130](#)
- Security Parameter Index, see SPI
- service access control [148](#)
- setup
 - firewalls [106](#)
- side bar [22](#)
- Single Rate Three Color Marker, see srTCM
- SPI [105](#)
- splitter [12](#)
- srTCM [94](#)
- static DHCP [62](#)
 - configuration [63](#)
- Static DHCP screen [62](#)
- static route [69](#)
- static VLAN
- status [30](#)
 - firmware version [31](#)
 - LAN [32](#)
 - WAN [31](#)
 - wireless LAN [32](#)
- subnet mask [66](#)
- Sustained Cell Rate (SCR) [51](#)
- SYN attack [104](#)
- syslog
 - protocol [129](#)
 - severity levels [129](#)
- system
 - firmware [158](#)
 - version [31](#)
 - passwords [18](#)
 - reset [16](#)
 - status [30](#)
 - LAN [32](#)
 - WAN [31](#)
 - wireless LAN [32](#)
 - time [151](#)

T

Tag Control Information See TCI
Tag Protocol Identifier See TPID
TCI
The [34](#)
thresholds
 DoS [105](#)
time [151](#)
TPID [52](#)
trademarks [193](#)
traffic shaping [51](#)
trTCM [94](#)
Trusted CA certificate
 view [126](#)
Trusted CA screen [124](#)
Two Rate Three Color Marker, see trTCM
two-line splitter [12](#)

U

unicast [53](#)
upgrading firmware [158](#)

V

VID
Virtual Circuit (VC) [50](#)
Virtual Local Area Network See VLAN
VLAN [52](#)
 Introduction [52](#)
 number of possible VIDs
 priority frame
 static
VLAN ID [52](#)
VLAN Identifier See VID
VLAN tag [52](#)
VMG
 feature difference [11](#)
 good habits for managing [14](#)
 managing [14](#)
 reboot [22](#)

W

WAN
 status [31](#)
 Wide Area Network, see WAN [33](#)
web browser
 pop-up window [18](#)
web browser version recommended [18](#)
Web Configurator
 accessing [18](#)
 layout [21](#)
 login [18](#)
 overview [18](#)
 passwords [18](#)
wireless LAN
 status [32](#)
wizard setup
 Internet [26](#)