

PLA-450

Homeplug AV to WLAN AP/Bridge

User's Guide

Version 3.60
6/2007
Edition 1

DEFAULT LOGIN

IP Address <http://192.168.1.2>

Password 1234

ZyXEL
www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator.

Related Documentation

- Quick Start Guide
The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help
Embedded web help for descriptions of individual screens and supplementary information.



It is recommended you use the web configurator to configure the ZyXEL Device.

- Supporting Disk
Refer to the included CD for support documents.
- ZyXEL Web Site
Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.



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











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

Syntax Conventions

- The PLA-450 may be referred to as the “ZyXEL Device”, the “device”, the “product” or the “system” in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the “enter” or “return” key on your keyboard.
- “Enter” means for you to type one or more characters and then press the [ENTER] key. “Select” or “choose” means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the “metric” value or the “scientific” value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

ZyXEL Device 	Computer 	Notebook computer 
Server 	Switch 	Router 
Modem 	HomePlug AV powerline adaptor 	

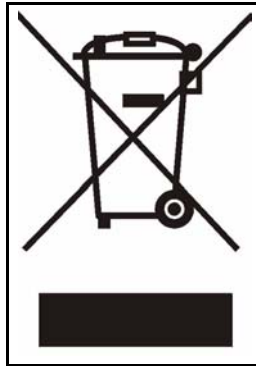
Safety Warnings



For your safety, be sure to read and follow all warning notices and instructions.

- 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 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 device or unit. 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.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- 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.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. 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.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

This product is recyclable. Dispose of it properly.



Contents Overview

Introduction	21
Getting to Know Your ZyXEL Device	23
Wireless Tutorial	27
Introducing the Web Configurator	35
Network	45
Wireless LAN	47
LAN	67
HomePlug AV	71
Maintenance and Troubleshooting	79
System	81
Logs	85
Tools	89
Configuration Mode	95
Troubleshooting	97
Appendices and Index	103

Table of Contents

About This User's Guide	3
Document Conventions.....	4
Safety Warnings.....	6
Contents Overview	9
Table of Contents.....	11
List of Figures	15
List of Tables.....	19
Part I: Introduction.....	21
Chapter 1	
Getting to Know Your ZyXEL Device	23
1.1 Overview	23
1.1.1 Wireless LAN Application	23
1.1.2 HomePlug AV	23
1.2 Ways to Manage the ZyXEL Device	24
1.3 Good Habits for Managing the ZyXEL Device	24
1.4 LEDs	25
Chapter 2	
Wireless Tutorial	27
2.1 Example Parameters	27
2.2 Configuring the ZyXEL Device	27
2.3 Configuring the Wireless Client	29
2.3.1 Connecting to a Wireless LAN	29
2.3.2 Creating and Using a Profile	31
Chapter 3	
Introducing the Web Configurator	35
3.1 Web Configurator Overview	35
3.2 Accessing the Web Configurator	35
3.3 Resetting the ZyXEL Device	37
3.3.1 Procedure to Use the Reset Button	37

3.4 Navigating the Web Configurator	37
3.4.1 The Status Screen	37
3.4.2 Navigation Panel	40
3.4.3 Summary: Packet Statistics	41
3.4.4 Summary: Wireless Station Status	42
3.4.5 Summary: My HomePlug Network Status	42
Part II: Network.....	45
Chapter 4	
Wireless LAN.....	47
4.1 Wireless Network Overview	47
4.2 Wireless Security Overview	49
4.2.1 SSID	49
4.2.2 MAC Address Filter	49
4.2.3 User Authentication	49
4.2.4 Encryption	50
4.3 Roaming	51
4.3.1 Requirements for Roaming	52
4.4 Quality of Service	52
4.4.1 WMM QoS	53
4.5 General Wireless LAN Screen	53
4.5.1 No Security	54
4.5.2 WEP Encryption	55
4.5.3 WPA-PSK/WPA2-PSK	57
4.5.4 WPA/WPA2	58
4.6 MAC Filter	60
4.7 Wireless LAN Advanced Screen	61
4.8 Quality of Service (QoS) Screen	62
4.8.1 Application Priority Configuration	64
Chapter 5	
LAN.....	67
5.1 LAN Overview	67
5.1.1 Factory LAN Defaults	67
5.1.2 IP Address	67
5.1.3 IP Address and Subnet Mask	68
5.2 LAN IP Screen	68
Chapter 6	
HomePlug AV	71

6.1 Overview	71
6.2 Privacy and Powerline Adapters	72
6.2.1 Setting Up a Private Powerline Network	72
6.2.2 Setting Up Multiple Powerline Networks.	73
6.3 Configuring Your HomePlug AV Devices	74
Part III: Maintenance and Troubleshooting	79
Chapter 7	
System	81
7.1 System General Screen	81
7.2 Time Setting Screen	82
Chapter 8	
Logs	85
8.1 View Log	85
8.2 Log Settings	86
Chapter 9	
Tools.....	89
9.1 Firmware Upload Screen	89
9.2 Configuration Screen	91
9.2.1 Backup Configuration	91
9.2.2 Restore Configuration	91
9.2.3 Back to Factory Defaults	92
9.3 Restart Screen	93
Chapter 10	
Configuration Mode	95
Chapter 11	
Troubleshooting.....	97
11.1 Power, Hardware Connections, and LEDs	97
11.2 ZyXEL Device Access and Login	98
11.3 Internet Access	99
11.4 Resetting the ZyXEL Device to Its Factory Defaults	100
11.5 Wireless Troubleshooting	101
11.6 HomePlug AV Troubleshooting	101
11.7 Advanced Features	102
Part IV: Appendices and Index	103

Appendix A Product Specifications and Wall-Mounting Instructions 105

Appendix B Pop-up Windows, JavaScripts and Java Permissions 109

Appendix C IP Addresses and Subnetting 115

Appendix D Setting up Your Computer's IP Address 123

 11.7.1 Verifying Settings 138

Appendix E Wireless LANs 139

Appendix F Common Services 153

Appendix G Legal Information 157

Appendix H 161

Appendix H Customer Support 161

Index 167

List of Figures

Figure 1 WLAN Application Example	23
Figure 2 HomePlug AV Internet Connection Example	24
Figure 3 Front Panel LEDs	25
Figure 4 Network > Wireless LAN > General	28
Figure 5 Status: Wireless Settings Example	28
Figure 6 AP: Status: WLAN Station Status	29
Figure 7 Connecting to a Wireless LAN	29
Figure 8 ZyXEL Utility: Security Settings	30
Figure 9 ZyXEL Utility: Confirm Save	31
Figure 10 ZyXEL Utility: Link Info	31
Figure 11 ZyXEL Utility: Profile	32
Figure 12 ZyXEL Utility: Add New Profile	32
Figure 13 ZyXEL Utility: Profile Security	32
Figure 14 ZyXEL Utility: Profile Encryption	33
Figure 15 Profile: Wireless Protocol Settings.	33
Figure 16 Profile: Confirm Save	33
Figure 17 Profile: Activate	34
Figure 18 Change Password Screen	36
Figure 19 Choose Basic or Advanced Screen	36
Figure 20 Web Configurator Status Screen	38
Figure 21 Summary: Packet Statistics	41
Figure 22 Summary: Wireless Association List	42
Figure 23 Summary: My Homeplug Network.	42
Figure 24 Example of a Wireless Network	47
Figure 25 Roaming Example	52
Figure 26 Network > Wireless LAN > General	54
Figure 27 Network > Wireless LAN > General: No Security	55
Figure 28 Network > Wireless LAN > General: Static WEP	56
Figure 29 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK	57
Figure 30 Network > Wireless LAN > General: WPA/WPA2	58
Figure 31 Network > Wireless LAN > MAC Filter	60
Figure 32 Network > Wireless LAN > Advanced	61
Figure 33 Network > Wireless LAN > QoS	63
Figure 34 Network > Wireless LAN > QoS: Application Priority Configuration	64
Figure 35 Network > LAN > IP	68
Figure 36 Expand Your Network	71
Figure 37 Powerline Network Scenario	73
Figure 38 Two Private Powerline Networks on One Circuit	74

Figure 39 Network > HomePlug > Network Settings	75
Figure 40 Network > HomePlug > Edit	76
Figure 41 Maintenance > System > General	81
Figure 42 Maintenance > System > Time Setting	82
Figure 43 Maintenance > Logs > View Log	85
Figure 44 Maintenance > Logs > Log Settings	87
Figure 45 Maintenance > Tools > Firmware	89
Figure 46 Upload Warning	90
Figure 47 Network Temporarily Disconnected	90
Figure 48 Upload Error Message	90
Figure 49 Maintenance > Tools > Configuration	91
Figure 50 Configuration Restore Successful	92
Figure 51 Temporarily Disconnected	92
Figure 52 Configuration Restore Error	92
Figure 53 Maintenance > Tools > Restart	93
Figure 54 Maintenance > Config Mode > General	95
Figure 55 Wall-mounting Example	108
Figure 56 Pop-up Blocker	109
Figure 57 Internet Options: Privacy	110
Figure 58 Internet Options: Privacy	111
Figure 59 Pop-up Blocker Settings	111
Figure 60 Internet Options: Security	112
Figure 61 Security Settings - Java Scripting	113
Figure 62 Security Settings - Java	113
Figure 63 Java (Sun)	114
Figure 64 Network Number and Host ID	116
Figure 65 Subnetting Example: Before Subnetting	118
Figure 66 Subnetting Example: After Subnetting	119
Figure 67 WInDows 95/98/Me: Network: Configuration	124
Figure 68 Windows 95/98/Me: TCP/IP Properties: IP Address	125
Figure 69 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	126
Figure 70 Windows XP: Start Menu	127
Figure 71 Windows XP: Control Panel	127
Figure 72 Windows XP: Control Panel: Network Connections: Properties	128
Figure 73 Windows XP: Local Area Connection Properties	128
Figure 74 Windows XP: Internet Protocol (TCP/IP) Properties	129
Figure 75 Windows XP: Advanced TCP/IP Properties	130
Figure 76 Windows XP: Internet Protocol (TCP/IP) Properties	131
Figure 77 Macintosh OS 8/9: Apple Menu	132
Figure 78 Macintosh OS 8/9: TCP/IP	132
Figure 79 Macintosh OS X: Apple Menu	133
Figure 80 Macintosh OS X: Network	134
Figure 81 Red Hat 9.0: KDE: Network Configuration: Devices	135

Figure 82 Red Hat 9.0: KDE: Ethernet Device: General	136
Figure 83 Red Hat 9.0: KDE: Network Configuration: DNS	136
Figure 84 Red Hat 9.0: KDE: Network Configuration: Activate	137
Figure 85 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0	137
Figure 86 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0	137
Figure 87 Red Hat 9.0: DNS Settings in resolv.conf	138
Figure 88 Red Hat 9.0: Restart Ethernet Card	138
Figure 89 Red Hat 9.0: Checking TCP/IP Properties	138
Figure 90 Peer-to-Peer Communication in an Ad-hoc Network	139
Figure 91 Basic Service Set	140
Figure 92 Infrastructure WLAN	141
Figure 93 RTS/CTS	142
Figure 94 WPA(2) with RADIUS Application Example	149
Figure 95 WPA(2)-PSK Authentication	150

List of Tables

Table 1 Front Panel LEDs	25
Table 2 Status Screen Icon Key	38
Table 3 Web Configurator Status Screen	39
Table 4 Screens Summary	40
Table 5 Summary: Packet Statistics	41
Table 6 Summary: Wireless Association List	42
Table 7 Summary: My Homeplug Network	43
Table 8 Types of Encryption for Each Type of Authentication	50
Table 9 WMM QoS Priorities	53
Table 10 Network > Wireless LAN > General	54
Table 11 Wireless No Security	55
Table 12 Network > Wireless LAN > General: Static WEP	56
Table 13 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK	57
Table 14 Network > Wireless LAN > General: WPA/WPA2	59
Table 15 Network > Wireless LAN > MAC Filter	60
Table 16 Network > Wireless LAN > Advanced	61
Table 17 Network > Wireless LAN > QoS	63
Table 18 Network > Wireless LAN > QoS: Application Priority Configuration	64
Table 19 Private IP Address Ranges	67
Table 20 Network > LAN > IP	68
Table 21 Network > HomePlug > Network Settings	75
Table 22 Network > HomePlug > Edit	76
Table 23 Maintenance > System > General	81
Table 24 Maintenance > System > Time Setting	83
Table 25 Maintenance > Logs > View Log	86
Table 26 Maintenance > Logs > Log Settings	87
Table 27 Maintenance > Tools > Firmware	89
Table 28 Maintenance Restore Configuration	91
Table 29 Maintenance > Config Mode > General	95
Table 30 Advanced Configuration Options	95
Table 31 Hardware Features	105
Table 32 Firmware Features	105
Table 33 Standards Supported	106
Table 34 Subnet Mask - Identifying Network Number	116
Table 35 Subnet Masks	117
Table 36 Maximum Host Numbers	117
Table 37 Alternative Subnet Mask Notation	117
Table 38 Subnet 1	119

Table 39 Subnet 2	120
Table 40 Subnet 3	120
Table 41 Subnet 4	120
Table 42 Eight Subnets	120
Table 43 24-bit Network Number Subnet Planning	121
Table 44 16-bit Network Number Subnet Planning	121
Table 45 IEEE 802.11g	143
Table 46 Wireless Security Levels	144
Table 47 Comparison of EAP Authentication Types	147
Table 48 Wireless Security Relational Matrix	150
Table 49 Commonly Used Services	153

PART I

Introduction

Getting to Know Your ZyXEL Device (23)

Wireless Tutorial (27)

Introducing the Web Configurator (35)

Getting to Know Your ZyXEL Device

This chapter introduces the main features and applications of the ZyXEL Device.

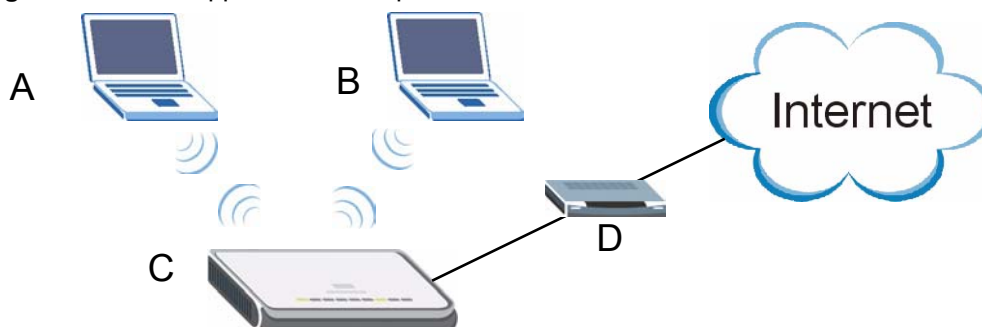
1.1 Overview

The ZyXEL Device is the ideal device for connecting a HomePlug AV powerline network (which uses your electrical wiring) to your wireless and wired (Ethernet) LAN.

1.1.1 Wireless LAN Application

The ZyXEL Device Wireless LAN feature allows IEEE 802.11b or IEEE 802.11g compatible wireless clients to access the Internet or the local network as well as to communicate with each other. Wireless stations can move freely anywhere in the coverage area and use resources on the wired network. The Super G function allows compatible clients to connect to the ZyXEL Device at up to 108 Mbps. In the following figure, wireless clients **A** and **B** connect to ZyXEL Device **C** wirelessly to access the Internet through broadband modem **D**.

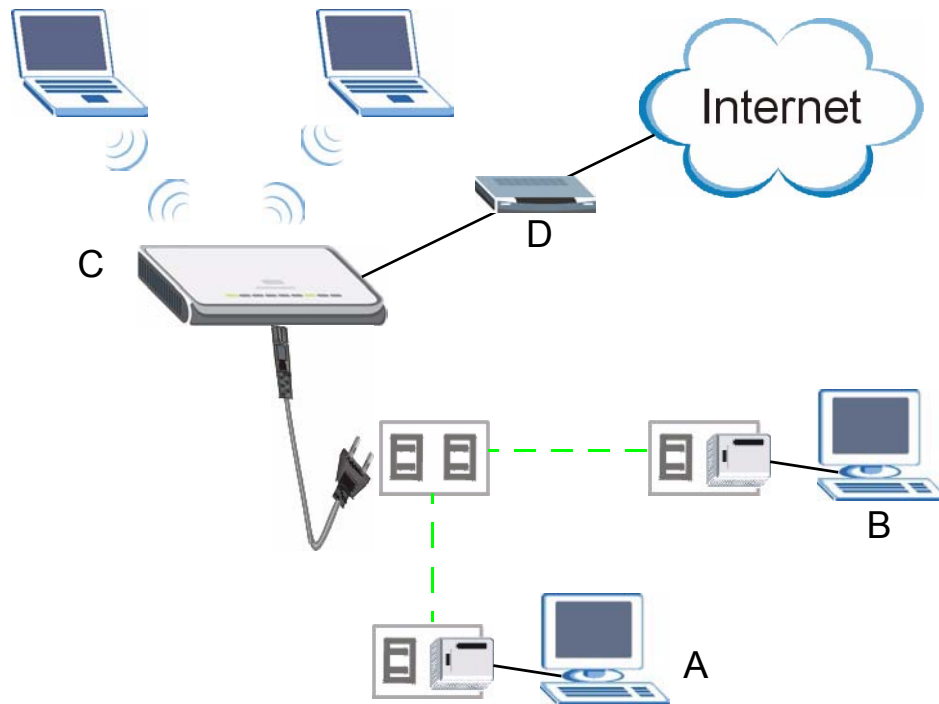
Figure 1 WLAN Application Example



1.1.2 HomePlug AV

Connect to other HomePlug AV compatible devices through your home electrical wiring. A HomePlug AV network is capable of up to 200Mbps data transfer without the need for network cables. In the following figure, computers **A** and **B** use HomePlug AV powerline adapters and the building's electrical wiring to connect to the ZyXEL Device **C** and access the Internet through broadband modem **D**.

Figure 2 HomePlug AV Internet Connection Example



1.2 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/restore.

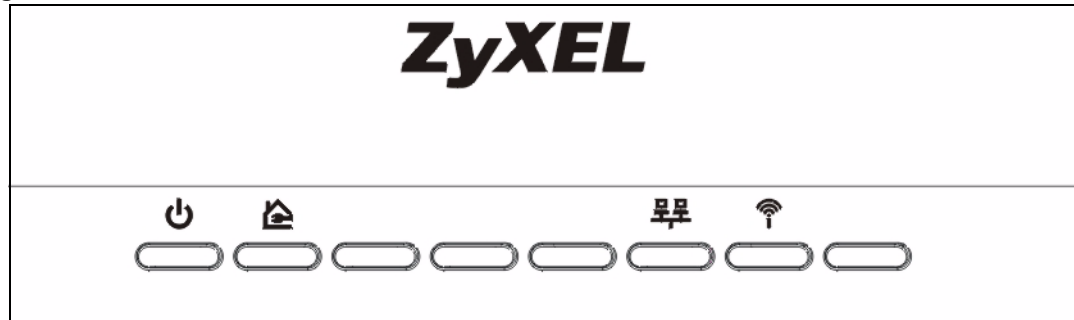
1.3 Good Habits for Managing the ZyXEL Device

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

- Change the password. Use a password that's 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.





1.4 LEDs

Figure 3 Front Panel LEDs



The following table describes the LEDs.

Table 1 Front Panel LEDs

LED	ICON	COLOR	STATUS	DESCRIPTION
POWER		Green	On	The ZyXEL Device is receiving power and functioning properly.
			Off	The ZyXEL Device is not receiving power.
HomePlug		Green	On	The ZyXEL Device has a successful HomePlug AV connection.
			Blinking	The ZyXEL Device is sending/receiving data.
			Off	The HomePlug AV connection is not ready, or failed.
LAN		Green	On	The ZyXEL Device has a successful Ethernet connection.
			Blinking	The ZyXEL Device is sending/receiving data.
			Off	The LAN is not connected.
WLAN		Green	On	The ZyXEL Device is ready, but is not sending/receiving data through the wireless LAN.
			Blinking	The ZyXEL Device is sending/receiving data through the wireless LAN.
		None	Off	The wireless LAN is not ready or has failed.

Wireless Tutorial

This chapter gives you examples of how to set up the ZyXEL Device and wireless client for wireless communication using the following parameters. The wireless clients can access the Internet through the ZyXEL Device wirelessly. See [Chapter 4 on page 47](#) for more on the ZyXEL Device's wireless LAN configuration.

2.1 Example Parameters

SSID	SSID_Example3
Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)
802.11 mode	IEEE 802.11b/g

In this chapter, the ZyXEL Device is also referred to as an access point (AP). A computer with a wireless network card or USB/PCI adapter is referred to here as a “wireless client”.

This chapter uses the M-302 utility screens as an example for the wireless client. The screens may vary for different models.

2.2 Configuring the ZyXEL Device

Follow the steps below to configure the wireless settings on your ZyXEL Device.

- 1 Open the **Network > Wireless LAN > General** screen in the web configurator.

Figure 4 Network > Wireless LAN > General

Wireless Setup

Enable Wireless LAN

Name(SSID)

Hide SSID

Channel Selection

Operating Channel

Security

Security Mode

Pre-Shared Key

ReAuthentication Timer (In Seconds)

Idle Timeout (In Seconds)

Group Key Update Timer (In Seconds)

- 2 Make sure the **Enable Wireless LAN** check box is selected.
- 3 Enter **SSID_Example3** as the SSID and select a channel.
- 4 Set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.
- 5 Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Figure 5 Status: Wireless Settings Example

Device Information

System Name: PLA-450
 Firmware Version: V3.60(AAJ.0)b2 | 04/16/2007

LAN Information:

- MAC Address: 00:19:cb:00:aa:a1
- IP Address: 192.168.1.2
- IP Subnet Mask: 255.255.255.0
- DHCP: None

WLAN Information:

- MAC Address: 00:19:cb:00:aa:a1
- Name(SSID): SSID_Example3
- Channel: 6
- Operating Channel: 6
- Security Mode: WPA-PSK
- 802.11 Mode: 802.11b/g
- Super G Mode: Disabled

HomePlug Information

- MAC Address: 00:13:49:D1:CB:88

System Status

System Up Time: 1:17:51
 Current Date/Time: 2000-1-1/1:17:48

System Resource:

- CPU Usage:
- Memory Usage:

System Setting:

- Configuration Mode: Advanced

Interface Status

Interface	Status	Rate
LAN	Up	100M/Full
WLAN	Up	54M
HomePlug AV	Up	200M

Summary

Packet Statistics (Details...)

WLAN Station Status (Details...)

My HomePlug network (Details...)

- 6 Click the **WLAN Station Status** hyperlink in the AP's **Status** screen. You can see if any wireless client has connected to the AP.

Figure 6 AP: Status: WLAN Station Status

Association List		
#	MAC Address	Association Time
001	00:13:49:63:3f:5e	00:18:23 2000/01/01

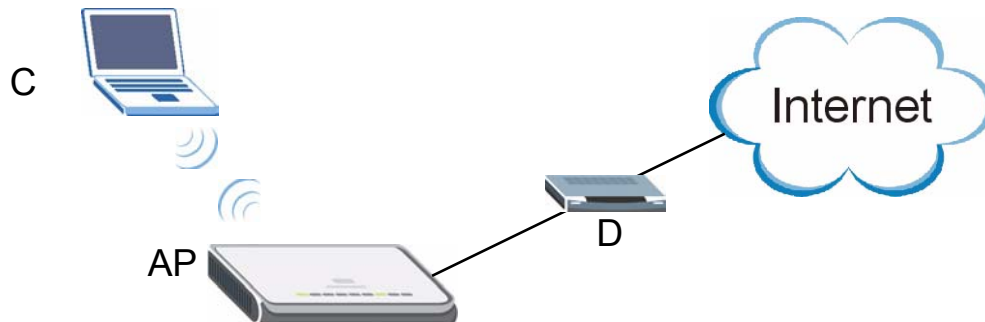
Refresh

2.3 Configuring the Wireless Client

This section describes how to connect the wireless client to a network.

2.3.1 Connecting to a Wireless LAN

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labelled **C** and the access point (ZyXEL Device) is labelled **AP**. **D** is the broadband modem.

Figure 7 Connecting to a Wireless LAN

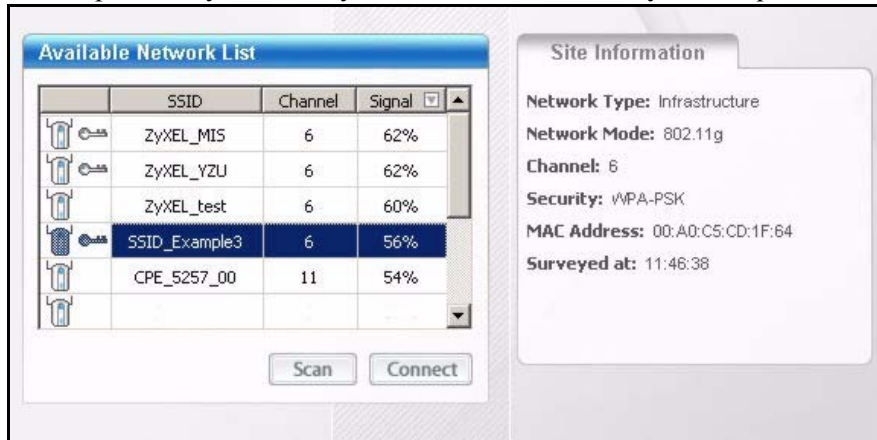
There are three ways to connect the client to an access point.

- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is “SSID_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey”.

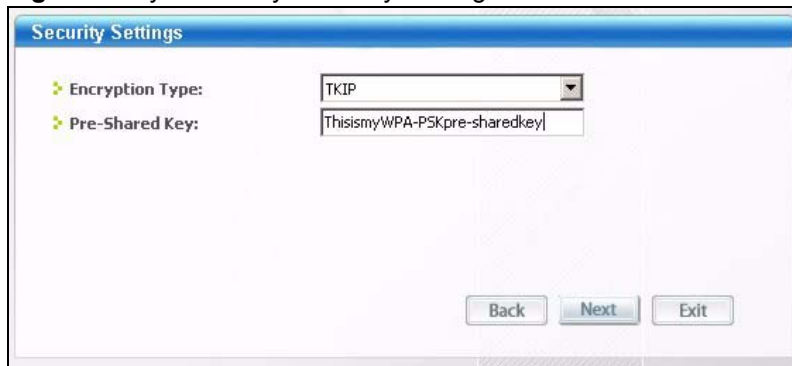
After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

- 1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

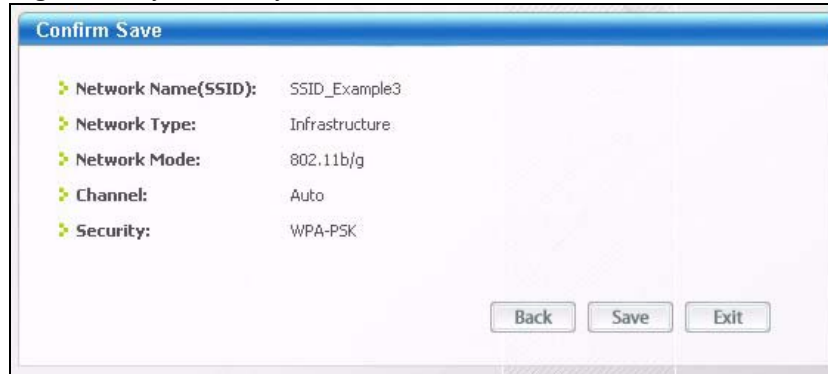


- 2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the wireless client closer to the AP or peer computer.
- 3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.
 Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

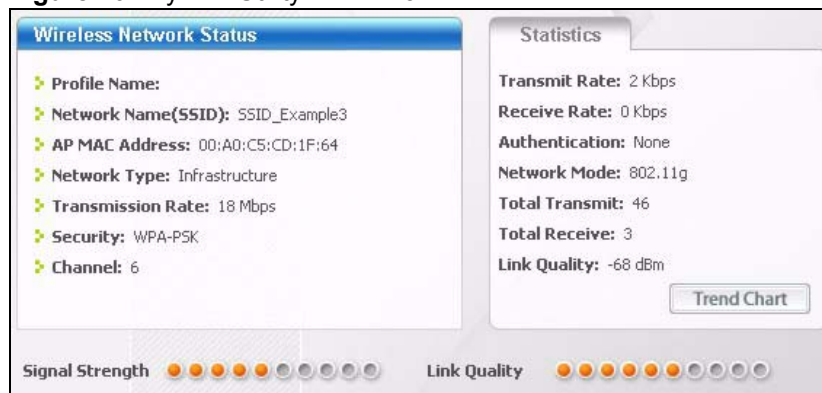
Figure 8 ZyXEL Utility: Security Settings



- 4 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 9 ZyXEL Utility: Confirm Save

- 5 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.

Figure 10 ZyXEL Utility: Link Info

- 6 Open your Internet browser and enter <http://www.zyxel.com> or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.
- If you cannot access the web site, try changing the encryption type in the **Security Settings** screen, check the Troubleshooting section of this User's Guide or contact your network administrator.

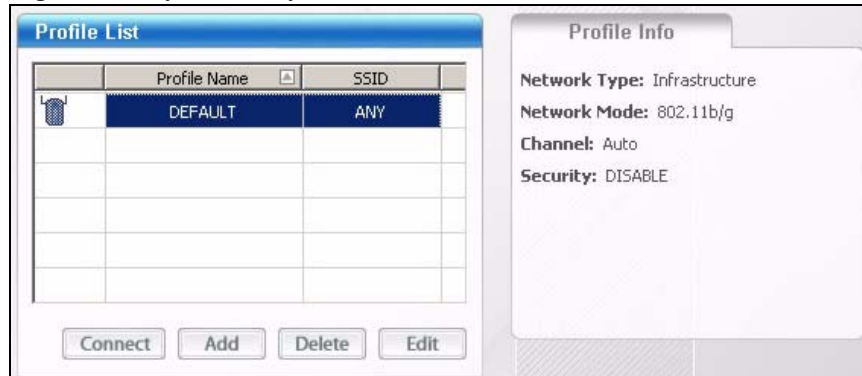
2.3.2 Creating and Using a Profile

A profile lets you automatically connect to the same wireless network every time you use the wireless client. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the SSID is “SSID_Example3”, the profile name is “PN_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey”. You have chosen the profile name “PN_Example3”.

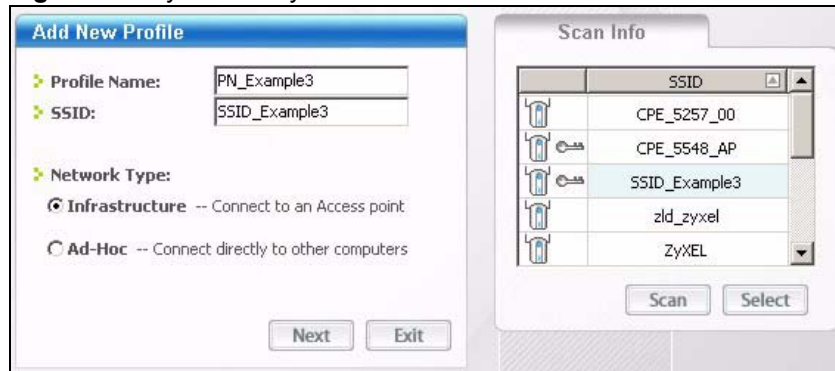
- 1 Open the ZyXEL utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.

Figure 11 ZyXEL Utility: Profile



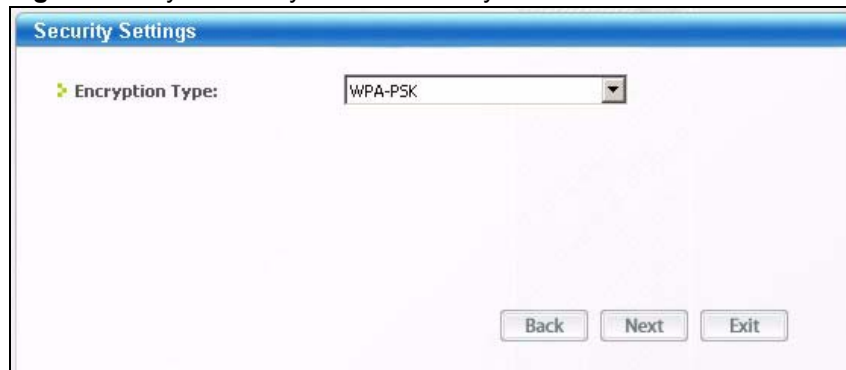
- 2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. Click on **Scan** if you want to search again. You can also configure your profile for a wireless network that is not in the list.

Figure 12 ZyXEL Utility: Add New Profile



- 3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.
- 4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

Figure 13 ZyXEL Utility: Profile Security



- 5 This screen varies depending on the encryption method you selected in the previous screen. Enter the pre-shared key and leave the encryption type at the default setting.

Figure 14 ZyXEL Utility: Profile Encryption

The screenshot shows a window titled "Security Settings". It contains two fields: "Encryption Type" with a dropdown menu set to "TKIP", and "Pre-Shared Key" with a text input field containing "ThisismyWPA-PSKpre-sharedkey". At the bottom, there are three buttons: "Back", "Next", and "Exit".

- 6 In the next screen, leave both boxes checked.

Figure 15 Profile: Wireless Protocol Settings.

The screenshot shows a window titled "Wireless Protocol Settings". It contains two checkboxes: "802.11b" and "802.11g", both of which are checked. At the bottom, there are three buttons: "Back", "Next", and "Exit".

- 7 Verify the profile settings in the read-only screen. Click **Save** to save and go to the next screen.

Figure 16 Profile: Confirm Save

The screenshot shows a window titled "Confirm Save". It displays a summary of the profile settings: "Network Name(SSID): SSID_Example3", "Network Type: Infrastructure", "Network Mode: 802.11b/g", "Channel: Auto", and "Security: WPA-PSK". At the bottom, there are three buttons: "Back", "Save", and "Exit".

- 8 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button.

If you clicked **Activate Later**, you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.



Only one profile can be activated and used at any given time.

Figure 17 Profile: Activate



- 9** When you activate the new profile, the ZyXEL utility returns to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.
- 10** Open your Internet browser, enter <http://www.zyxel.com> or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.
- 11** If you cannot access the Internet go back to the **Profile** screen, select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

Introducing the Web Configurator

This chapter describes how to access the ZyXEL Device web configurator and provides an overview of its screens.

3.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy setup and management of the ZyXEL Device via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. 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 device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter to see how to make sure these functions are allowed in Internet Explorer.

3.2 Accessing the Web Configurator

- 1 Make sure your ZyXEL Device hardware is properly connected and prepare your computer or computer network to connect to the ZyXEL Device (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "http://192.168.1.2" as the URL.
- 4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
- 5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 18 Change Password Screen



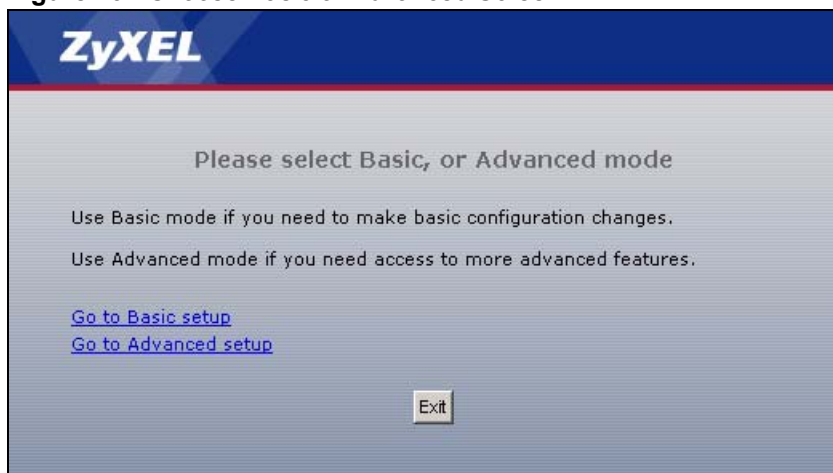
The screenshot shows the ZyXEL web configurator's 'Change Password' screen. At the top is the ZyXEL logo. Below it, the text reads 'Please enter a new password'. A paragraph explains that the router is currently using the default password and suggests changing it for security, recommending a combination of text and numbers. A note specifies that the administrator password must be between 1 and 30 characters. There are two input fields: 'New Password:' with a masked password '****' and 'Retype to Confirm:'. At the bottom are 'Apply' and 'Ignore' buttons.



The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the ZyXEL Device if this happens.

- 6 Select the setup mode you want to use.
 - Click **Go to Basic Setup** if you want to view and configure basic settings. Not all Web Configurator screens are available in this mode.
 - Click **Go to Advanced Setup** to view and configure all the ZyXEL Device's settings.

Figure 19 Choose Basic or Advanced Screen



The screenshot shows the ZyXEL web configurator's 'Choose Basic or Advanced Screen'. At the top is the ZyXEL logo. Below it, the text reads 'Please select Basic, or Advanced mode'. Two paragraphs explain the modes: 'Use Basic mode if you need to make basic configuration changes.' and 'Use Advanced mode if you need access to more advanced features.'. There are two blue hyperlinks: 'Go to Basic setup' and 'Go to Advanced setup'. At the bottom is an 'Exit' button.

3.3 Resetting the ZyXEL Device

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the ZyXEL Device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, and the password will be reset to “1234”.

3.3.1 Procedure to Use the Reset Button

- 1 Make sure the **PWR** LED is on.
- 2 Press the **RESET** button for ten seconds or until the **PWR** LED begins to blink and then release it. When the **PWR** LED begins to blink, the defaults have been restored and the ZyXEL Device restarts.

3.4 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **Status** screen.

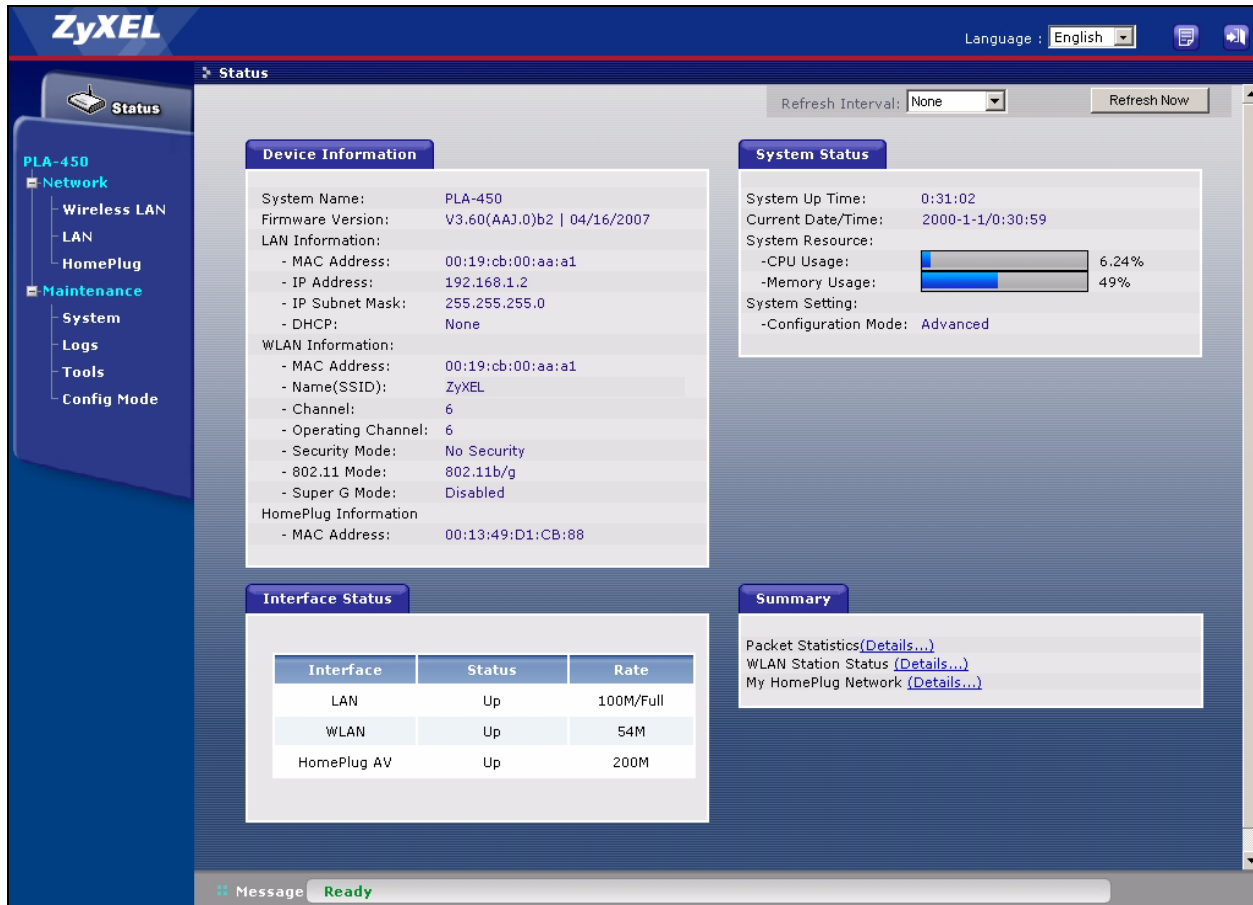
3.4.1 The Status Screen

The following screen displays when you log into the ZyXEL Device.



Not all screens are available when you select **Basic** mode ([Table 30 on page 95](#) lists which screens are only available in **Advanced** mode). See the **Configuration Mode** field in the **System Status** box to check whether you are in **Basic** or **Advanced** mode. Use the **Config Mode > General** screen to change between modes.

Figure 20 Web Configurator Status Screen



The following table describes the icons shown in the **Status** screen.

Table 2 Status Screen Icon Key

ICON	DESCRIPTION
	Select a language from the drop-down list box to have the web configurator display in that language.
	Click this icon to open a web help page relevant to the screen you are currently configuring.
	Click this icon to view copyright and a link for related product information.
	Click this icon at any time to exit the web configurator.
	Select a number of seconds or None from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
	Click this button to refresh the status screen statistics.

The following table describes the labels shown in the **Status** screen.

Table 3 Web Configurator Status Screen

LABEL	DESCRIPTION
Device Information	
System Name	This is the System Name you enter in the Maintenance > System > General screen. It is for identification purposes.
Firmware Version	This is the ZyNOS firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - Server or None .
WLAN Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Name (SSID)	This shows a descriptive name used to identify the ZyXEL Device in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the ZyXEL Device is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the ZyXEL Device is using.
- 802.11 Mode	This shows the wireless standard.
- Super G Mode	This shows whether SuperG is enabled or not.
HomePlug Information	
- MAC Address	This shows the MAC Address of your device.
System Status	
System Uptime	This is the total time the ZyXEL Device has been on.
Current Date/Time	This field displays your ZyXEL Device's present date and time.
System Resource	
- CPU Usage	This 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.
- Memory Usage	This shows what percentage of the heap memory the ZyXEL Device is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running the ZyXEL Device's processes.
System Setting	
- Configuration Mode	This shows whether the advanced screens of each feature are turned on (Advanced) or not (Basic).
Interface Status	
Interface	This displays the ZyXEL Device port types. The port types are: LAN , HomePlug AV and WLAN .

Table 3 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
Status	For the LAN port, this field displays Down (line is down) or Up (line is up or connected). For the WLAN, it displays Up when the WLAN is enabled or Down when the WLAN is disabled. For the HomePlug AV port it displays Up when the power cord is connected.
Rate	For the LAN port, this displays the port speed and duplex setting or N/A when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and N/A when the WLAN is disabled. For the HomePlug AV port it displays the maximum transmission rate when the HomePlug AV is enabled.
Summary	
Packet Statistics	Click Details to view port status and packet specific statistics.
WLAN Station Status	Click Details to view the wireless stations that are currently associated to the ZyXEL Device.
My HomePlug Network	Click Details to view information on the stations connected to your Home Plug network.

3.4.2 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure ZyXEL Device features.

The following table describes the sub-menus.

Table 4 Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the ZyXEL Device's general device, system and interface status information. Use this screen to access the summary statistics tables.
Network		
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the ZyXEL Device to block access to devices or block the devices from accessing the ZyXEL Device.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
HomePlug	Network Settings	Use this screen to configure HomePlug AV devices and set up a power line network.
Maintenance		
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Time Setting	Use this screen to change your ZyXEL Device's time and date.

Table 4 Screens Summary

LINK	TAB	FUNCTION
Logs	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your ZyXEL Device's log settings.
Tools	Firmware	Use this screen to upload firmware to your ZyXEL Device.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your ZyXEL Device.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.
Config Mode	General	This screen allows you to display or hide the advanced screens or features.

3.4.3 Summary: Packet Statistics

Click the **Packet Statistics (Details...)** hyperlink in the **Status** screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Figure 21 Summary: Packet Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
LAN	100M/Full	1158	7396	0	0	0	1:48:19
WLAN	54M	7054	0	0	0	0	1:48:19

System Up Time : 1:48:25

Poll Interval(s) : sec

The following table describes the labels in this screen.

Table 5 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the ZyXEL Device's port type.
Status	For the LAN ports, this displays the port speed and duplex setting or Down when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and Down when the WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.

Table 5 Summary: Packet Statistics

LABEL	DESCRIPTION
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the ZyXEL Device has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the Poll Interval(s) field.
Stop	Click Stop to stop refreshing statistics, click Stop .

3.4.4 Summary: Wireless Station Status

Click the **WLAN Station Status (Details...)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the ZyXEL Device in the **Association List** screen.

Figure 22 Summary: Wireless Association List

#	MAC Address	Association Time
001	00:0e:35:96:6d:6a	01:38:47 2000/01/01

Refresh

The following table describes the labels in this screen.

Table 6 Summary: Wireless Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the ZyXEL Device.
Refresh	Click Refresh to reload the list.

3.4.5 Summary: My HomePlug Network Status

Click the **My HomePlug Network (Details...)** hyperlink in the **Status** screen. View the powerline stations that are currently associated to the ZyXEL Device in the **My Homeplug Network** screen.

Figure 23 Summary: My Homeplug Network.

Site	MAC Address
Local	00:13:49:D1:CB:88
Remote	00:13:49:EA:F0:BE

Refresh

The following table describes the labels in this screen.

Table 7 Summary: My Homeplug Network

LABEL	DESCRIPTION
Site	This ZyXEL Device is the Local device. All other devices on your network will be Remote .
MAC Address	This field displays the MAC address of a HomePlug AV device detected by your ZyXEL Device.
Refresh	Click Refresh to reload the list.

PART II

Network

Wireless LAN (47)

LAN (67)

HomePlug AV (71)

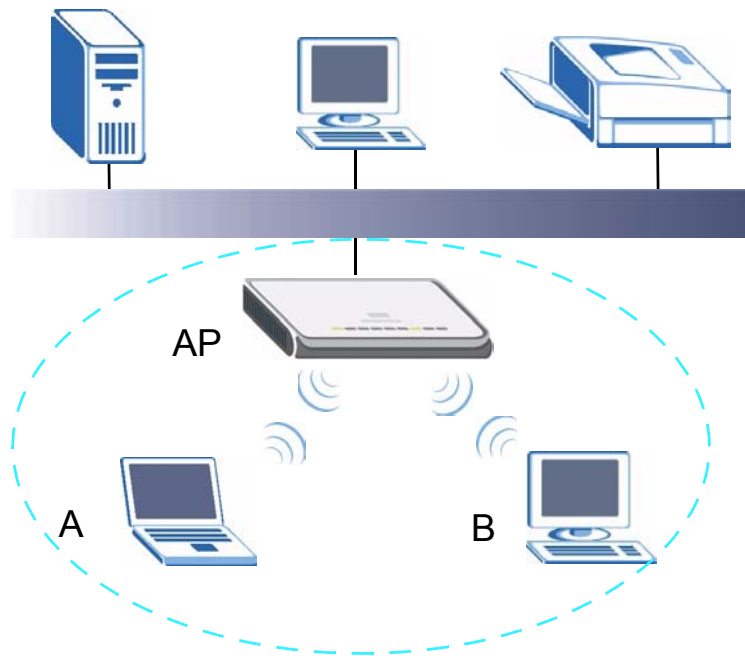
Wireless LAN

This chapter discusses how to configure the wireless network settings in your ZyXEL Device. See the appendices for more detailed information about wireless networks.

4.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 24 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your ZyXEL Device is the AP.

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID. The SSID is the name of the wireless network. It stands for Service Set Identity.
- If two wireless networks overlap, they should use different channels.

Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every wireless client in the same wireless network must use security compatible with the AP.

Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Requirements

To add a wireless LAN to your existing network, make sure you have the following:

- 1 an access point (AP) or a router with the wireless feature
- 2 at least one wireless network card/adaptor which varies according to your computer.
 - If you have a desktop, use either a wireless USB adapter or a wireless PCI adapter.
 - If you have a laptop, use either a wireless USB adapter or a wireless CardBus card.
- 3 a RADIUS server only if you want to use WPA or WPA2

To have two or more computers communicate with each other wirelessly without an AP or wireless router, make sure you have the following:

- 1 two or more wireless network cards/adaptors which vary according to your computers.
 - If you have a desktop, use either a wireless USB adapter or a wireless PCI adapter.
 - If you have a laptop, use either a wireless USB adapter or a wireless CardBus card.

Setup Information

To set up your wireless network using an AP or wireless router, make sure your AP or wireless router and wireless network card(s)/adapter(s) use the same following settings:

- SSID: _____
- Channel: _____
- Network type of a wireless network card/adaptor: Infrastructure
- wireless standard: IEEE 802.11b, g, or b/g
- Security:
 - () None
 - () WEP (64 bit or 128 bit key) (ASCII or Hex): _____
 - () WPA-PSK (TKIP): _____
 - () WPA (TKIP)
 - () WPA2-PSK (AES): _____
 - () WPA2 (AES)
- Preamble type (if available): auto, short or long

To set up your wireless network without an AP or wireless router, make sure wireless network cards/adaptors use the same following settings:

- Network type: Ad-Hoc
- SSID: _____
- Channel: _____
- wireless standard: IEEE 802.11b, g, or b/g

- Security:
 - () None
 - () WEP (64 bit or 128 bit key) (ASCII or Hex): _____

4.2 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

4.2.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

4.2.2 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

4.2.3 User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support the authentication method to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.


Local user databases also have an additional limitation that is explained in the next section.

4.2.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of user authentication. (See [Section 4.2.3 on page 49](#) for information about this.)

Table 8 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest  Strongest	No Security	WPA
	Static WEP	
	WPA-PSK	
	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.



It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. WEP encryption is better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

When you select **WPA2** or **WPA2-PSK** in your ZyXEL Device, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA Compatible** option in the ZyXEL Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

4.3 Roaming

A wireless station is a device with an IEEE 802.11a/b/g compliant wireless interface. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

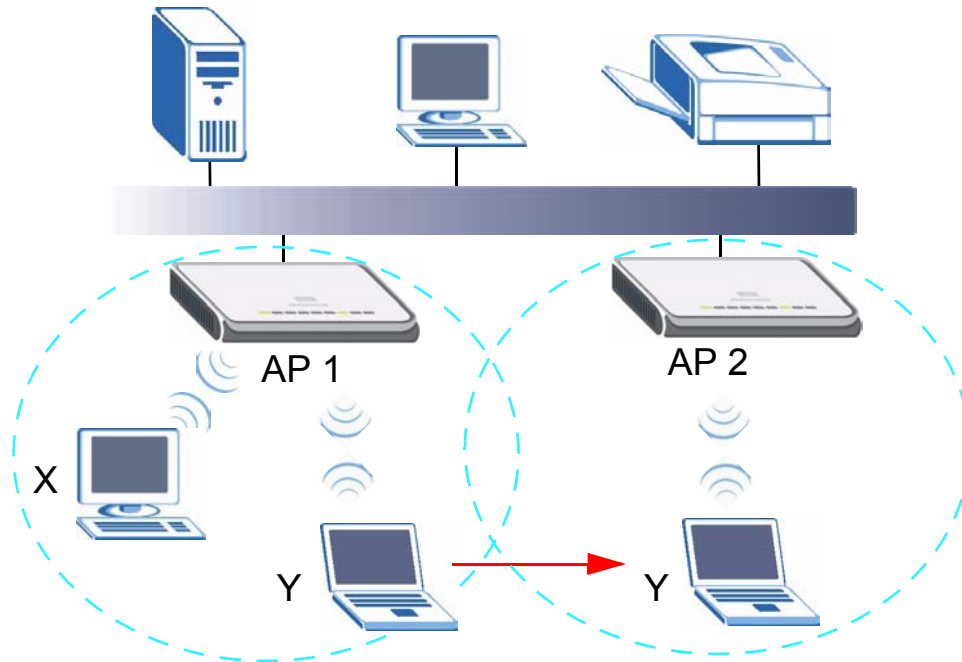
In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is known as roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the other access points on the LAN about the change. An example is shown in [Figure 25 on page 52](#).

With roaming, a wireless LAN mobile user enjoys a continuous connection to the wired network through an access point while moving around the wireless LAN.

Enable roaming to exchange the latest bridge information of all wireless stations between APs when a wireless station moves between coverage areas. Wireless stations can still associate with other APs even if you disable roaming. Enabling roaming ensures correct traffic forwarding (bridge tables are updated) and maximum AP efficiency. The AP deletes records of wireless stations that associate with other APs (Non-ZyXEL APs may not be able to perform this).

Figure 25 Roaming Example



The steps below describe the roaming process.

- 1 Wireless station **Y** moves from the coverage area of access point **AP 1** to that of access point **AP 2**.
- 2 Wireless station **Y** scans and detects the signal of access point **AP 2**.
- 3 Wireless station **Y** sends an association request to access point **AP 2**.
- 4 Access point **AP 2** acknowledges the presence of wireless station **Y** and relays this information to access point **AP 1** through the wired LAN.
- 5 Access point **AP 1** updates the new position of wireless station **Y**.

4.3.1 Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

- 1 All the access points must be on the same subnet and configured with the same ESSID.
- 2 The adjacent access points should use different radio channels when their coverage areas overlap.
- 3 All access points must use the same port number to relay roaming information.
- 4 The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

4.4 Quality of Service

This section discusses the Quality of Service (QoS) features available on the ZyXEL Device.

4.4.1 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) ensures quality of service in wireless networks. It controls WLAN transmission priority on packets to be transmitted over the wireless network.

WMM QoS prioritizes wireless traffic according to delivery requirements. WMM QoS is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.

On APs without WMM QoS, all traffic streams are given the same access priority to the wireless network. If the introduction of another traffic stream creates a data transmission demand that exceeds the current network capacity, then the new traffic stream reduces the throughput of the other traffic streams.

The ZyXEL Device uses WMM QoS to prioritize traffic streams according to the IEEE 802.1q tag or DSCP information in each packet's header. The ZyXEL Device automatically determines the priority to use for an individual traffic stream. This prevents reductions in data transmission for applications that are sensitive to latency (delay) and jitter (variations in delay).

4.4.1.1 WMM QoS Priorities

The following table describes the WMM QoS priority levels that the ZyXEL Device uses.

Table 9 WMM QoS Priorities

PRIORITY LEVEL	DESCRIPTION
voice (WMM_VOICE)	Typically used for traffic that is especially sensitive to jitter. Use this priority to reduce latency for improved voice quality.
video (WMM_VIDEO)	Typically used for traffic which has some tolerance for jitter but needs to be prioritized over other data traffic.
best effort (WMM_BEST_EFFORT)	Typically used for traffic from applications or devices that lack QoS capabilities. Use best effort priority for traffic that is less sensitive to latency, but is affected by long delays, such as Internet surfing.
background (WMM_BACKGROUND)	This is typically used for non-critical traffic such as bulk transfers and print jobs that are allowed but that should not affect other applications and users. Use background priority for applications that do not have strict latency and throughput requirements.

4.5 General Wireless LAN Screen



If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.

Click **Network > Wireless LAN** to open the **General** screen.

Figure 26 Network > Wireless LAN > General

The following table describes the general wireless LAN labels in this screen.

Table 10 Network > Wireless LAN > General

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate wireless LAN.
Name(SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the IEEE 802.11 mode you are using and the country you are in. Refer to Appendix E on page 139 for more information on channels.
Operating Channel	This displays the channel the ZyXEL Device is currently using.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to reload the previous configuration for this screen.

See the rest of this chapter for information on the other labels in this screen.

4.5.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption.



If you do not enable any wireless security on your ZyXEL Device, your network is accessible to any wireless networking device that is within range.

Figure 27 Network > Wireless LAN > General: No Security

The screenshot shows the 'General' configuration page for the Wireless LAN. It has four tabs: 'General' (selected), 'MAC Filter', 'Advanced', and 'QoS'. Under the 'Wireless Setup' section, there are four items: 'Enable Wireless LAN' (checked), 'Name(SSID)' (text box with 'ZyXEL'), 'Hide SSID' (unchecked), and 'Channel Selection' (dropdown menu with 'Channel-06 2437MHz'). Below this is the 'Operating Channel' (text box with 'Channel-006'). Under the 'Security' section, there is one item: 'Security Mode' (dropdown menu with 'No Security'). At the bottom right, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 11 Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose No Security from the drop-down list box.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to reload the previous configuration for this screen.

4.5.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your ZyXEL Device allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption; click **Network > Wireless LAN** to display the **General** screen. Select **Static WEP** from the **Security Mode** list.

Figure 28 Network > Wireless LAN > General: Static WEP

The following table describes the wireless LAN security labels in this screen.

Table 12 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Passphrase	Enter a passphrase (password phrase) of up to 32 printable characters and click Generate . The ZyXEL Device automatically generates four different WEP keys and displays them in the Key fields below.
WEP Encryption	Select 64-bit WEP or 128-bit WEP to enable data encryption.
Authentication Method	This field is activated when you select 64-bit WEP or 128-bit WEP in the WEP Encryption field. Select Auto , Open System or Shared Key from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. If you chose 64-bit WEP , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bit WEP , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to reload the previous configuration for this screen.

4.5.3 WPA-PSK/WPA2-PSK

Click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 29 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

The following table describes the labels in this screen.

Table 13 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select WPA2-PSK or WPA2 in the Security Mode field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
Pre-Shared Key	The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).

Table 13 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP (if using WPA-PSK/WPA2-PSK key management) or RADIUS server (if using WPA/WPA2 key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA-PSK/WPA2-PSK mode. The default is 1800 seconds (30 minutes).
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to reload the previous configuration for this screen.

4.5.4 WPA/WPA2

Click **Network > Wireless LAN** to display the **General** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Figure 30 Network > Wireless LAN > General: WPA/WPA2

The screenshot shows the configuration interface for Wireless LAN. The 'General' tab is selected. Under 'Wireless Setup', the 'Enable Wireless LAN' checkbox is checked. The 'Name(SSID)' field contains 'ZyXEL'. The 'Channel Selection' dropdown is set to 'Channel-06 2437MHz'. Under the 'Security' section, 'Security Mode' is set to 'WPA2'. The 'Group Key Update Timer' is set to 1800 seconds. There are also fields for 'Authentication Server' (IP: 0.0.0.0, Port: 1812) and 'Accounting Server' (IP: 0.0.0.0, Port: 1813). 'Apply' and 'Reset' buttons are at the bottom.

The following table describes the labels in this screen.

Table 14 Network > Wireless LAN > General: WPA/WPA2

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select WPA2-PSK or WPA2 in the Security Mode field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP (if using WPA-PSK/WPA2-PSK key management) or RADIUS server (if using WPA/WPA2 key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA-PSK/WPA2-PSK mode. The ZyXEL Device default is 1800 seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812 . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
Accounting Server	
Active	Select Yes from the drop down list box to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is 1813 . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to reload the previous configuration for this screen.

4.6 MAC Filter

The MAC filter screen allows you to configure the ZyXEL Device to give exclusive access to up to 32 devices (Allow) or exclude up to 32 devices from accessing the ZyXEL Device (Deny). 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 address of the devices to configure this screen.

To change your ZyXEL Device's MAC filter settings, click **Network > Wireless LAN > MAC Filter**. The screen appears as shown.

Figure 31 Network > Wireless LAN > MAC Filter

Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
6	00:00:00:00:00:00	22	00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

The following table describes the labels in this menu.

Table 15 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Active	Select Yes from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the MAC Address table. Select Deny to block access to the ZyXEL Device, MAC addresses not listed will be allowed to access the ZyXEL Device Select Allow to permit access to the ZyXEL Device, MAC addresses not listed will be denied access to the ZyXEL Device.

Table 15 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied 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.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to reload the previous configuration for this screen.

4.7 Wireless LAN Advanced Screen

Click **Network > Wireless LAN > Advanced**. The screen appears as shown.

Figure 32 Network > Wireless LAN > Advanced

The following table describes the labels in this screen.

Table 16 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Roaming Configuration	
Enable Roaming	Select this option if your network environment has multiple APs and you want your wireless device to be able to access the network as you move between wireless networks.
Wireless Advanced Setup	
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. If the RTS/CTS value is greater than the Fragmentation Threshold value, then the RTS/CTS handshake will never occur as data frames will be fragmented before they reach RTS/CTS size. Enter a value between 256 and 2346.

Table 16 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Fragmentation Threshold	It is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Enable Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client A and B can still access the wired network but cannot communicate with each other.
Output Power	Set the output power of the ZyXEL Device in this field. If there is a high density of APs within an area, decrease the output power of the ZyXEL Device to reduce interference with other APs.
802.11 Mode	Select 802.11b to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select 802.11g to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select 802.11b/g to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Super G Mode	Use this field to enable or disable the Super G function. Super G mode is available only if you select 802.11g or 802.11b/g in the 802.11 Mode field. Super G provides higher data transmission rates than 802.11g. Select Disabled if your wireless clients do not support Super G. Select Super G with Dynamic Turbo if some or all of your wireless clients support Super G with Dynamic Turbo. Dynamic Turbo uses two channels bonded together to achieve higher transmission rates than 802.11g or Super G without Dynamic Turbo. Dynamic turbo is on only when all wireless devices on the network support it. The wireless channel is automatically fixed at 6 if you select this mode. Select Super G without Turbo if the wireless clients on your network support Super G but do not support Dynamic Turbo.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to reload the previous configuration for this screen.

4.8 Quality of Service (QoS) Screen

The QoS screen allows you to automatically give a service (such as e-mail, VoIP or FTP) a priority level.

Click **Network > Wireless LAN > QoS**. The following screen appears.

Figure 33 Network > Wireless LAN > QoS

QoS Setup

Enable WMM QoS

WMM QoS Policy Application Priority

#	Name	Service	Dest Port	Priority	Modify
1	-	-	0	-	
2	-	-	0	-	
3	-	-	0	-	
4	-	-	0	-	
5	-	-	0	-	
6	-	-	0	-	
7	-	-	0	-	
8	-	-	0	-	
9	-	-	0	-	
10	-	-	0	-	
11	-	-	0	-	
12	-	-	0	-	
13	-	-	0	-	
14	-	-	0	-	
15	-	-	0	-	
16	-	-	0	-	

Apply

The following table describes the labels in this screen.

Table 17 Network > Wireless LAN > QoS

LABEL	DESCRIPTION
Enable WMM QoS	Use WMM QoS (Wifi MultiMedia Quality of Service) to give different types of traffic different priorities. The ZyXEL Device assigns priority to packets based on the 802.1q or DSCP information in their headers. If a packet has no WMM information in its header, it is assigned the default priority. See Section 4.4.1 on page 53 for more information.
WMM QoS Policy	Select Default to have the ZyXEL Device automatically give voice and video traffic priority so their services operate more smoothly. The ZyXEL Device gives a service a priority level according to the ToS value in the IP header of packets it sends. Select Application Priority from the drop-down list box to display a table of application names, services, ports and priorities to which you want to apply WMM QoS.
	The table appears only if you select Application Priority in WMM QoS Policy .
#	This is the number of an individual application entry.
Name	This field displays a description given to an application entry.
Service	This field displays either FTP , WWW , E-mail or a User Defined service to which you want to apply WMM QoS.
Dest Port	This field displays the destination port number to which the application sends traffic.

Table 17 Network > Wireless LAN > QoS (continued)

LABEL	DESCRIPTION
Priority	This field displays the priority of the application.
Modify	Click the Edit icon to open the Application Priority Configuration screen. Modify an existing application entry or create a application entry in the Application Priority Configuration screen. Click the Remove icon to delete an application entry.
Apply	Click Apply to save your changes to the ZyXEL Device.

4.8.1 Application Priority Configuration

Use this screen to edit a WMM QoS application entry. Click the edit icon under **Modify**. The following screen displays.

Figure 34 Network > Wireless LAN > QoS: Application Priority Configuration

See [Appendix F on page 153](#) for a list of commonly-used services and destination ports. The following table describes the fields in this screen.

Table 18 Network > Wireless LAN > QoS: Application Priority Configuration

LABEL	DESCRIPTION
Application Priority Configuration	
Name	Type a description of the application priority.

Table 18 Network > Wireless LAN > QoS: Application Priority Configuration (continued)

LABEL	DESCRIPTION
Service	<p>The following is a description of the applications you can prioritize with WMM QoS. Select a service from the drop-down list box.</p> <ul style="list-style-type: none"> • E-Mail Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80 • FTP File Transfer Protocol enables fast transfer of files, including large files that it may not be possible to send via e-mail. FTP uses port number 21. • WWW The World Wide Web is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser. • User-Defined User-defined services are user specific services configured using known ports and applications.
Dest Port	This displays the port the selected service uses. Type a port number in the field provided if you want to use a different port to the default port.
Priority	<p>Select a priority from the drop-down list box.</p> <p>Highest - Typically used for voice.</p> <p>High - Typically used for video.</p> <p>Mid - Typically used for applications that do not fit into another priority. For example, Internet surfing.</p> <p>Low - Typically used for non-critical "background" applications, such as large file transfers and print jobs that should not affect other applications.</p>
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previous screen.

This chapter describes how to configure LAN settings.

5.1 LAN Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. Use the LAN screen to configure the ZyXEL Device's IP address to be on your network.

5.1.1 Factory LAN Defaults

The LAN parameters of the ZyXEL Device are preset in the factory with the following values:

- IP address of 192.168.1.2
- subnet mask of 255.255.255.0 (24 bits)

5.1.2 IP Address

Every computer on your network must have a unique IP address. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 19 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

The ZyXEL Device's IP address can be assigned manually (a static or 'fixed' IP address) or by a DHCP server on your network.



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.

5.1.3 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. 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 don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

5.2 LAN IP Screen

Use this screen to change your ZyXEL Device's IP address. Click **Network > LAN**.

Figure 35 Network > LAN > IP

The following table describes the labels in this screen.

Table 20 Network > LAN > IP

LABEL	DESCRIPTION
LAN TCP/IP	
Get from DHCP Server	Select this option if you have a DHCP server on your network. If you have a router, it likely includes a DHCP server function.

Table 20 Network > LAN > IP

LABEL	DESCRIPTION
User Defined LAN IP	Select this option to use a specific (fixed) IP address.
IP Address	Enter the ZyXEL Device's IP address in dotted decimal notation. 192.168.1.2 is the factory default.
IP Subnet Mask	Enter the IP subnet mask in this field if you have a specific for the ZyXEL Device to use. The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
Gateway IP Address	Enter a gateway IP address in this field if you have a specific for the ZyXEL Device to use.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

HomePlug AV

This chapter introduces the main applications and management of the powerline feature.

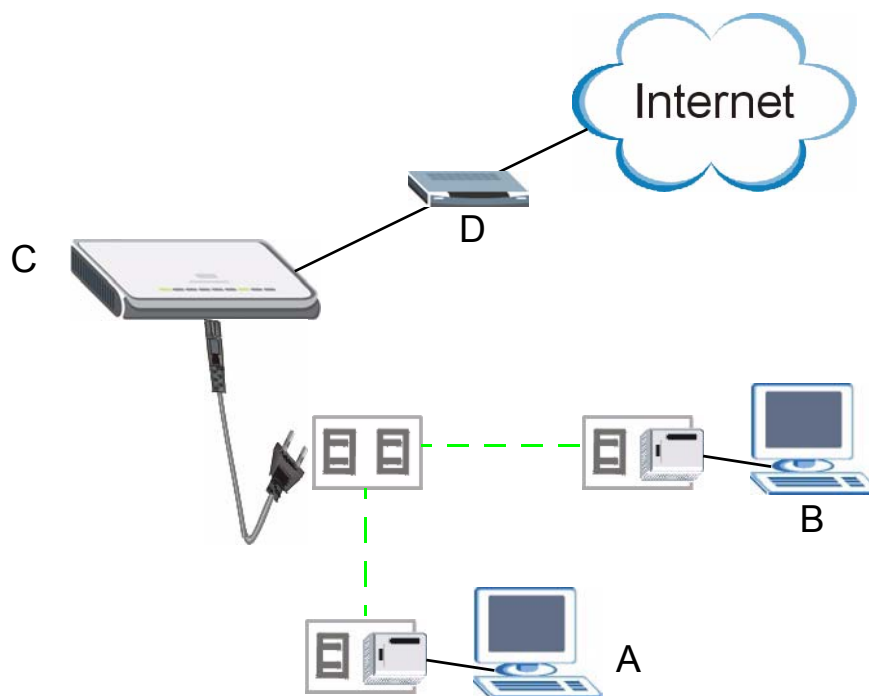
6.1 Overview

The ZyXEL Device is a HomePlug AV compliant powerline Ethernet adapter. The ZyXEL Device and other HomePlug AV powerline adapters in your network communicate with each other by sending and receiving information over your home's electrical wiring.

The ZyXEL Device plugs into an ordinary outlet to create a new network which can extend to any other electrical outlet in any room of a house.

The following section shows you a typical application. Computers **A** and **B** use HomePlug AV powerline adapters and the building's electrical wiring to connect to the ZyXEL Device **C** and access the Internet through broadband modem **D**.

Figure 36 Expand Your Network



To set up your powerline network do the following.

- 1 Connect your ZyXEL Device to the Internet.

- 2 Then plug your ZyXEL Device into a power outlet.

The ZyXEL Device is ready for connection on a powerline network.

- 3 Connect another HomePlug AV compatible adapter to a computer and then plug it in on the same home or office wiring.

After configuring the settings on all adapters (see [Section 6.3 on page 74](#)) your computer can now connect to the powerline network and to the Internet. Your powerline network can be further expanded by plugging additional powerline adapters into other outlets in your home and connecting other computers or network devices (for example, a printer) to them.

In this User's Guide the electrical wiring network may be referred to as the "powerline network".

6.2 Privacy and Powerline Adapters

When the ZyXEL Device communicates with each other HomePlug AV compliant powerline adapters, they use encryption to scramble the information that is sent in the powerline network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message. The HomePlug AV standard uses 128-bit AES (Advanced Encryption Standard) to safely transmit data between powerline adapters.

For the ZyXEL Device and powerline adapters to communicate with each other they all need to use the same Network Membership Key (NMK). Otherwise, they cannot unscramble the encrypted data sent in the powerline network.

The NMK is derived from the network name (password) you assign to the ZyXEL Device and powerline adapters. By default all HomePlug powerline adapters are configured with the network password **HomePlugAV**. This allows all HomePlug powerline adapters and the ZyXEL Device to communicate with each other without any software configuration. This also means that if you don't change the network password, any HomePlug AV powerline adapter connected to your powerline circuit can see your network data.



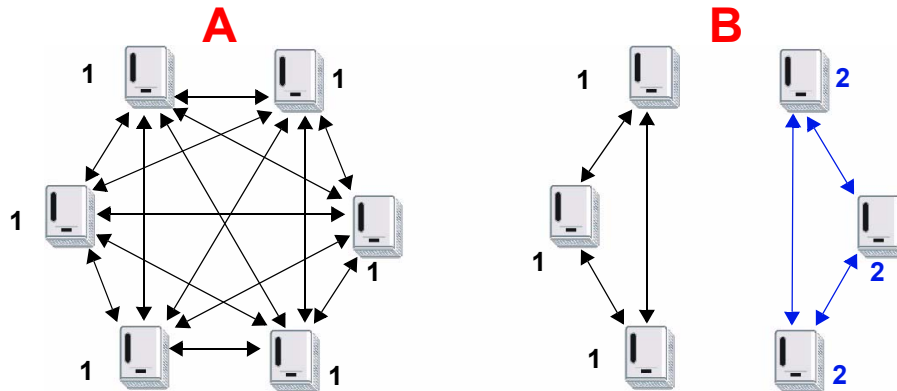
Change the network password on your powerline adapters to ensure secure data transmission on your powerline network.

6.2.1 Setting Up a Private Powerline Network

To prevent others compromising your network security, you can create a private network. Create a private network by changing the network password only on the powerline adapters you want to communicate in your network. Only the powerline adapters with the same network password can communicate in your network.

The following figure shows a scenario **A** - where all the powerline adapters have the same network password (**1**) and scenario **B** - where some adapters use password **1** and some use password **2**.

Figure 37 Powerline Network Scenario



In both cases the powerline adapters reside on the same electrical circuit. In scenario **A** all the powerline adapters can communicate with each other. In scenario **B** only the adapters with the same password can receive and unscramble communication between each other.

6.2.2 Setting Up Multiple Powerline Networks.

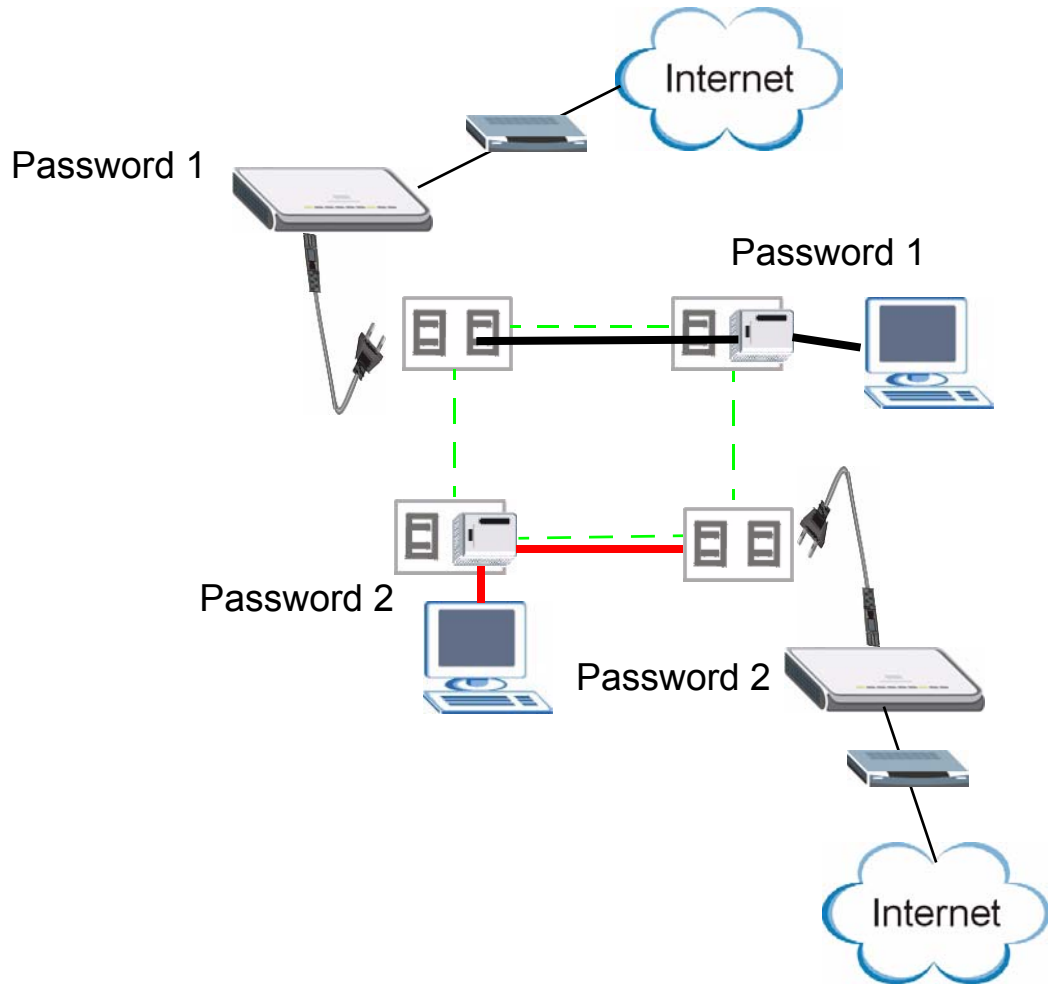
Multiple powerline networks can coexist on a single powerline circuit. You might want to implement multiple powerline networks in a small office environment where you have two separate Ethernet networks.

Connect one powerline adapter to a router or switch on the first Ethernet network and assign a network password (for example, “Password1”) to this powerline adapter. Add additional powerline adapters to your network by plugging them into your powerline outlets and assigning them the same network password, “Password1”. This completes the configuration of your first powerline network.

Connect another powerline adapter to a router or switch on the second Ethernet network and assign a different network password (for example “Password2”) to this powerline adapter. Again, add additional powerline adapters and assign them the same second network password, “Password2”.

You now have two private networks on your powerline circuit. Information is not shared between the two networks as only powerline adapters with the same password can communicate with each other. The following figure shows two private powerline networks on the same electrical circuit.

Figure 38 Two Private Powerline Networks on One Circuit



6.3 Configuring Your HomePlug AV Devices

Click on **Network > HomePlug** to see the screen below. Use this screen to set up a HomePlug AV network and to check the status of HomePlug AV devices on your electrical circuit.

Figure 39 Network > HomePlug > Network Settings

Network Settings

Network Name

Network Type

Public, Network Name is HomePlugAV

Private, Network Name is

Set

Add New Member

Device Information

Nickname

MAC Address

DAK Password

Add

Note:

1. Nickname is a friendly name for this device; name it if you like.

2. You can find your MAC Address and DAK Password on your device back label, and the password format should be "XXXX-XXXX-XXXX-XXXX".

My HomePlug Network

Nickname	MAC Address	Status	Member Action
Scan			

Note:

1. If a device is "Out of network", check its DAK password and make sure the device is powered ON.

The following table describes the labels in the screen.

Table 21 Network > HomePlug > Network Settings

LABEL	DESCRIPTION
Network Name	This section lets you set the name of your network and to make it either public or private. The Network Name performs the same function as a network password. All devices on your HomePlug network have the same Network Name . A device with a different Network Name cannot be on your network. You can add other HomePlugAV devices to your network by giving them the same Network Name .
Network Type	The network may be either public or private.
Public, Network Name is HomePlug AV	Select this option if you want to make your powerline network public with the default Network Name of "HomePlug AV". Since this is well known, it is less secure than a private network name.
Private, Network Name is	Select this option if you wish to make your powerline network more secure with a private Network Name . Type the name of your private powerline network in the field. You may enter up to 64 alphanumeric characters for the Network Name .
Set	Click Set to change the Network Name of all the devices currently in your network.
Add New Member	This section lets you add new Home Plug AV enabled devices to your powerline network. When you add the device it is given the current Network Name .
Device Information	In this section type information to identify the new powerline device you are adding on your network.
Nickname	Type a name you wish to use to identify a specific powerline adapter, for example, "Mary's room".
MAC Address	Type the MAC address of the adapter you wish to add. The MAC address of your powerline adapter can be found by looking at the label on your device. It consists of six pairs of hexadecimal characters (hexadecimal characters are "0-9" and "a-f"). In the case of the ZyXEL Device, this label is on the bottom of the device.

Table 21 Network > HomePlug > Network Settings

LABEL	DESCRIPTION
DAK Password	The DAK Password (DAK stands for Device Access Key), is used to verify that you are authorized to perform changes on a device. You can find the DAK printed on a sticker on the bottom of a HomePlug enabled device.
My Homeplug Network	This section provides information on the HomePlug AV devices in your network (or that were previously connected on it but are currently disconnected).
Nickname	This is the nickname you gave to the HomePlug AV device.
MAC Address	This is the MAC address of the HomePlug AV device.
Status	This field shows the status of the device. Active: the device is connected to your network. Out of Network: the device has been added to the network but it is not ready. Check whether it is turned on and connected. Not member: the device is not on the network. The ZyXEL Device is aware of it, but cannot manage the device. If you click Set , the device's Network Name will not change. You can add it to the network by clicking on Edit or entering its details in the Add New member section .
Member Action	This field shows the Add , Edit and Delete icons. Click Add to add a device to the network . Click Edit to edit a device's details such as the device's Nickname . Click Delete to remove the device from the network. If you want to set up a second network, remove the devices from My HomePlug Network that you want to keep in your first network before you set the new Network Name for the second network.
Scan	Click Scan to detect devices on the same electrical circuit as the ZyXEL Device.

Click **Network > HomePlug > Edit** to see the screen below. Use this screen to add a new HomePlug AV device to the network. You can also edit a device's details.

Figure 40 Network > HomePlug > Edit

Add/Edit Member

Device Information

Nickname: Bob's room

MAC Address: 00:13:49:EA:F0:BE

DAK Password: QLVK-SPSC-VSUH-LGMI

Note:

- Nickname is a friendly name for this device; name it if you like.
- You can find your MAC Address and DAK Password on your device back label, and the password format should be "XXXX-XXXX-XXXX-XXXX".

Apply Cancel

The following table describes the labels in the screen.

Table 22 Network > HomePlug > Edit

LABEL	DESCRIPTION
Device Information	
Nickname	Type a name you wish to use to identify a specific powerline adapter, for example, "Bob's room".
MAC Address	This is the MAC address of the HomePlug AV device. The MAC Address will appear in this field if the device's status is either Active or Not Member . If the device's status is Out of Network or your ZyXEL Device can not detect it, type the MAC Address here.

Table 22 Network > HomePlug > Edit

LABEL	DESCRIPTION
DAK Password	The DAK Password (DAK stands for Device Access Key), is used to verify that you are authorized to perform changes on a device. You can find the DAK printed on a sticker on the bottom of a HomePlug enabled device.
Apply	Click this button to apply add the device to the network or to apply your changes.
Cancel	Click this button to return to the previous screen.

PART III

Maintenance and Troubleshooting

System (81)
Logs (85)
Tools (89)
Configuration Mode (95)
Troubleshooting (97)

System

This chapter provides information on the **System** screens.

7.1 System General Screen

Click **Maintenance > System**. The following screen displays.

Figure 41 Maintenance > System > General

The screenshot shows a web interface for system configuration. At the top, there are two tabs: 'General' (selected) and 'Time Setting'. Below the tabs is a 'System Setup' section with three input fields: 'System Name', 'Domain Name', and 'Administrator Inactivity Timer' (set to 5 minutes). Below that is a 'Password Setup' section with three password input fields: 'Old Password', 'New Password', and 'Retype to Confirm'. At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 23 Maintenance > System > General

LABEL	DESCRIPTION
System Name	The system name is a unique name to identify the ZyXEL Device in an Ethernet network. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, your DHCP server may assign a domain name. The domain name entered by you is given priority over a DHCP-assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).

Table 23 Maintenance > System > General

LABEL	DESCRIPTION
Password Setup	Change your ZyXEL Device's password (recommended) using the fields as shown.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

7.2 Time Setting Screen

To change your ZyXEL Device's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown. Use this screen to configure the ZyXEL Device's time based on your local time zone.

Figure 42 Maintenance > System > Time Setting

The screenshot shows the 'Time Setting' configuration page. It includes sections for 'Current Time and Date', 'Time and Date Setup', and 'Time Zone Setup'. The 'Manual' option is selected for time and date setting, with fields for 'New Time (hh:mm:ss)' and 'New Date (yyyy/mm/dd)'. The 'Time Zone Setup' section includes a dropdown for 'Time Zone' and a checkbox for 'Daylight Savings'. The 'Start Date' and 'End Date' are both set to 'First Saturday of January (2000-01-01) at 0 o'clock'. 'Apply' and 'Reset' buttons are located at the bottom.

The following table describes the labels in this screen.

Table 24 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
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	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it. When you enter the time settings manually, the ZyXEL Device uses the new setting once you click Apply . Note: If you enter time settings manually, they revert to their defaults when power is lost.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set Time and Date Setup to Manual , enter the new time in this field and then click Apply .
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set Time and Date Setup to Manual , enter the new date in this field and then click Apply .
Get from Time Server	Select this radio button to have the ZyXEL Device get the time and date from the time server you specified below.
Auto	Select Auto to have the ZyXEL Device automatically search for an available time server and synchronize the date and time with the time server after you click Apply .
User Defined Time Server Address	Select User Defined Time Server Address and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
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. Select this option if you use Daylight Saving Time.

Table 24 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected Daylight Savings. The o'clock field uses the 24 hour format. Here are a couple of examples:</p> <p>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 you would select Second, Sunday, March and 2:00.</p> <p>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 select Last, Sunday, March. The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected Daylight Savings. The o'clock field uses the 24 hour format. Here are a couple of examples:</p> <p>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 select First, Sunday, November and 2:00.</p> <p>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 select Last, Sunday, October. The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

This chapter contains information about configuring general log settings and viewing the ZyXEL Device's logs. Refer to the appendices for example log message explanations.

8.1 View Log

The web configurator allows you to look at all of the ZyXEL Device's logs in one location. Click **Maintenance > Logs** to open the **View Log** screen.

Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Section 8.2 on page 86](#)). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, Java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 43 Maintenance > Logs > View Log

#	Time	Message	Source	Destination	Note
1	01/01/2000 02:57:08	Successful WEB login	192.168.1.33		User:admin
2	01/01/2000 01:42:26	Successful WEB login	192.168.1.33		User:admin
3	01/01/2000 00:28:27	Successful WEB login	192.168.1.33		User:admin
4	01/01/2000 00:14:41	Successful WEB login	192.168.1.33		User:admin

The following table describes the labels in this screen.

Table 25 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Display	The categories that you select in the Log Settings page (see Section 8.2 on page 86) display in the drop-down list box. Select a category of logs to view; select All Logs to view logs from all of the log categories that you selected in the Log Settings page.
Email Log Now	Click Email Log Now to send the log screen to the e-mail address specified in the Log Settings page (make sure that you have first filled in the Address Info fields in Log Settings).
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to delete all the logs.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the ZyXEL Device's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.

8.2 Log Settings

You can configure the ZyXEL Device's general log settings in one location.

Click **Maintenance > Logs > Log Settings** to open the **Log Settings** screen.

Use the **Log Settings** screen to configure to where the ZyXEL Device is to send logs; the schedule for when the ZyXEL Device is to send the logs and which logs and/or immediate alerts the ZyXEL Device to send.

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 or web sites with restricted web features such as cookies, active X and so on. 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.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

Figure 44 Maintenance > Logs > Log Settings

View Log		Log Settings	
E-mail Log Settings			
Mail Server	<input type="text"/>	(Outgoing SMTP Server NAME or IP Address)	
Mail Subject	<input type="text"/>		
Send Log to	<input type="text"/>	(E-Mail Address)	
Send Alerts to	<input type="text"/>	(E-Mail Address)	
<input type="checkbox"/> SMTP Authentication			
User Name	<input type="text"/>		
Password	<input type="text"/>		
Log Schedule	<input type="text" value="None"/>		
Day for Sending Log	<input type="text" value="Sunday"/>		
Time for Sending Log	<input type="text" value="0"/> (hour)	<input type="text" value="0"/> (minute)	
<input type="checkbox"/> Clear log after sending mail			
Syslog Logging			
<input type="checkbox"/> Active			
Syslog Server IP Address	<input type="text" value="0.0.0.0"/>	(Server NAME or IP Address)	
Log Facility	<input type="text" value="Local 1"/>		
Active Log and Alert			
Log	Send immediate alert		
<input checked="" type="checkbox"/> System Maintenance	<input type="checkbox"/> System Errors		
<input checked="" type="checkbox"/> System Errors			
<input type="checkbox"/> 802.1x			
<input type="checkbox"/> Wireless			
<input type="button" value="Apply"/> <input type="button" value="Reset"/>			

The following table describes the labels in this screen.

Table 26 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends. Not all ZyXEL Device models have this field.
Send Log To	The ZyXEL Device sends logs to the e-mail address specified in this field. If this field is left blank, the ZyXEL Device does not send logs via e-mail.
Send Alerts To	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.

Table 26 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Log Schedule	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none"> • Daily • Weekly • Hourly • When Log is Full • None. <p>If you select Weekly or Daily, specify a time of day when the E-mail should be sent. If you select Weekly, then also specify which day of the week the E-mail should be sent. If you select When Log is Full, an alert is sent when the log fills up. If you select None, no log messages are sent.</p>
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the checkbox to delete all the logs after the ZyXEL Device sends an E-mail of the logs.
Syslog Logging	The ZyXEL Device sends a log to an external syslog server.
Active	Click Active to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the ZyXEL Device to send E-mail alerts immediately.
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the ZyXEL Device.

9.1 Firmware Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a ".bin" extension, e.g., "ZyXEL Device.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the Firmware and Configuration File Maintenance chapter for upgrading firmware using FTP/TFTP commands.

Click **Maintenance > Tools**. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

Figure 45 Maintenance > Tools > Firmware

The following table describes the labels in this screen.

Table 27 Maintenance > Tools > Firmware

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 Browse... to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to begin the upload process. This process may take up to two minutes.



Do not turn off the ZyXEL Device while firmware upload is in progress!

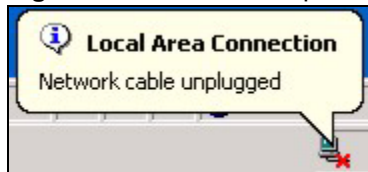
After you see the **Firmware Upload In Process** screen, wait five minutes before logging into the ZyXEL Device again.

Figure 46 Upload Warning



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 47 Network Temporarily Disconnected



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 **Return** to go back to the **Firmware** screen.

Figure 48 Upload Error Message



9.2 Configuration Screen

See the Firmware and Configuration File Maintenance chapter for transferring configuration files using FTP/TFTP commands.

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 49 Maintenance > Tools > Configuration

The screenshot shows a web interface with three tabs: 'Firmware', 'Configuration' (which is selected and highlighted in blue), and 'Restart'. Below the tabs, there are three main sections:

- Backup Configuration:** Contains the text 'Click Backup to save the current configuration of your system to your computer.' and a 'Backup' button.
- Restore Configuration:** Contains the text 'To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.' Below this is a 'File Path:' label followed by an empty text input field and a 'Browse...' button. Below the input field is an 'Upload' button.
- Back to Factory Defaults:** Contains the text 'Click **Reset** to clear all user-entered configuration information and return to factory defaults. After resetting, the' followed by two bullet points: '- Password will be 1234' and '- LAN IP address will be 192.168.1.2'. Below this is a 'Reset' button.

9.2.1 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.

9.2.2 Restore Configuration

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

Table 28 Maintenance 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 Browse... to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click Upload to begin the upload process.



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

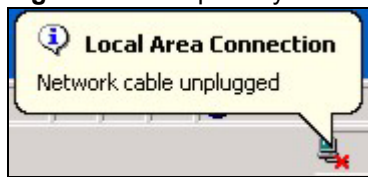
After you see a “configuration upload successful” screen, you must then wait one minute before logging into the ZyXEL Device again.

Figure 50 Configuration Restore Successful



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 51 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 ZyXEL Device IP address (192.168.1.2). See your Quick Start Guide for details on how to set up your computer’s IP address.

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

Figure 52 Configuration Restore Error



9.2.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the ZyXEL Device to its factory defaults.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device. Refer to the chapter about introducing the web configurator for more information on the **RESET** button.

9.3 Restart Screen

System restart allows you to reboot the ZyXEL Device without turning the power off.

Click **Maintenance > Tools > Restart**. Click **Restart** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

Figure 53 Maintenance > Tools > Restart



Configuration Mode

Click **Maintenance > Config Mode** to open the following screen. This screen allows you to hide or display the advanced screens of some features or the advanced features, such as MAC filter. **Basic** is selected by default and you cannot see the advanced screens or features. If you want to view and configure all screens including the advanced ones, select **Advanced** and click **Apply**.

Figure 54 Maintenance > Config Mode > General

The following table describes the labels in the screen.

Table 29 Maintenance > Config Mode > General

LABEL	DESCRIPTION
Configuration Mode	
Basic	Select Basic mode to enable or disable features and to monitor the status of your device.
Advanced	Select Advanced mode to set advanced settings.
Apply	Click on this to set the mode.
Reset	Click on this to reset your selection to the default (Advanced).

The following table lists the screens that you can view and configure only when you select **Advanced**.

Table 30 Advanced Configuration Options

CATEGORY	LINK	TAB
Network	Wireless LAN	MAC Filter
		Advanced
		QoS
Maintenance	Logs	Log Settings

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](#)
- [Resetting the ZyXEL Device to Its Factory Defaults](#)
- [Wireless Troubleshooting](#)
- [HomePlug AV Troubleshooting](#)
- [Advanced Features](#)

11.1 Power, Hardware Connections, and LEDs



The ZyXEL Device does not turn on. None of the LEDs turn on.

- 1 Make sure you are using the power adaptor or cord included with the ZyXEL Device.
- 2 Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
- 3 Disconnect and re-connect the power adaptor or cord to the ZyXEL Device.
- 4 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 1.4 on page 25](#).
- 2 Check the hardware connections. See the Quick Start Guide.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Disconnect and re-connect the power adaptor to the ZyXEL Device.
- 5 If the problem continues, contact the vendor.

11.2 ZyXEL Device Access and Login



I forgot the IP address for the ZyXEL Device.

- 1 The default IP address is **192.168.1.2**.
- 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 11.4 on page 100](#).



I forgot the password.

- 1 The default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 11.4 on page 100](#).



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 192.168.1.2.
 - If you changed the IP address ([Section 5.2 on page 68](#)), use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the ZyXEL Device](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See [Appendix B on page 109](#).
- 4 Make sure your computer is in the same subnet as the ZyXEL Device. (If you know that there are routers between your computer and the ZyXEL Device, skip this step.)
 - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Section 5.2 on page 68](#). Your ZyXEL Device is a DHCP server by default.
 - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the ZyXEL Device. See [Section 5.2 on page 68](#).
- 5 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See [Section 5.2 on page 68](#).

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

Advanced Suggestions

- If your computer is connected through the Internet or is connected wirelessly, use a computer that is connected to the LAN port.



I can see the **Login** screen, but I cannot log in to the ZyXEL Device.

- 1 Make sure you have entered the password correctly. The default password is **1234**. This 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 Disconnect and re-connect the power adaptor or cord to the ZyXEL Device.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 11.4 on page 100](#).



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.



I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

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

11.3 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.

- 2 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the ZyXEL Device.
- 3 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 4 If the problem continues, contact your ISP.



I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.4 on page 25](#).
- 2 Reboot the ZyXEL Device.
- 3 If the problem continues, contact your ISP.



The Internet connection is slow or intermittent.

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.4 on page 25](#). If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Check the signal strength. If the signal strength is low, try moving the ZyXEL Device closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
- 3 Reboot the ZyXEL Device.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

11.4 Resetting the ZyXEL Device to Its Factory Defaults

If you reset the ZyXEL Device, you lose all of the changes you have made. The ZyXEL Device re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.



You will lose all of your changes when you push the **RESET** button.

To reset the ZyXEL Device,

- 1 Make sure the **PWR LED** is on and not blinking.
- 2 Press and hold the **RESET** button for five to ten seconds. Release the **RESET** button when the **PWR LED** begins to blink. The default settings have been restored.

If the ZyXEL Device restarts automatically, wait for the ZyXEL Device to finish restarting, and log in to the web configurator. The password is “1234”.

If the ZyXEL Device does not restart automatically, disconnect and reconnect the ZyXEL Device’s power. Then, follow the directions above again.

11.5 Wireless Troubleshooting



I cannot access the ZyXEL Device or ping any computer from the WLAN.

- 1 Make sure the wireless LAN is enabled on the ZyXEL Device
 - 2 Make sure the wireless adapter on the wireless station is working properly.
 - 3 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the ZyXEL Device.
 - 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the ZyXEL Device.
 - 5 Check that both the ZyXEL Device and your wireless station are using the same wireless and wireless security settings.
- See the chapter on Wireless LAN in the User’s Guide for more information.

11.6 HomePlug AV Troubleshooting




I cannot start my power line device.

Check your power supply is working. Power line adapters operate from the power supplied by your home wiring and cannot operate without a working power supply. Remove the power line adapter from the outlet. Then connect an electrical device that you know works into the same power outlet. This checks the status of the power outlet.



I cannot access my power line network.

- 1 Make sure that the network password is the same on all the power line adapters in your network.

- 2 Check the DAK and MAC address for all power line adapters are typed correctly.
- 3 Make sure that all your power line adapters are HomePlug AV. Check the package it came in or ask your vendor. This ZyXEL Device can not detect earlier versions of HomePlug power line adapters such as HomePlug 1.0 or 1.0.1. (Although they can coexist on the same electrical wiring without interfering with each other.)
- 4 Make sure that the devices on your network are all on the same electrical wiring. Connect another power line adapter into an outlet close to your ZyXEL Device's power outlet. They are probably now on the same electrical wiring. Check the **Link**  LED. If it now lights up your power line adapter was probably previously on separate electrical wiring. Ask an electrician for more information on the electrical wiring in your building.
- 5 Check you do not have a power meter between power line adapters. Power line signals cannot pass this.



The signal on my power line network may be weak for the following reasons.

- 1 Your power line adapters may be connected to electrical surge protectors. Connect them to standard power outlets.
- 2 Your power line adapters may be located close to large appliances such as refrigerators or air-conditioners that cause interference with the power line signal. Move the adapters further away from such appliances to reduce interference.
- 3 Your power line adapters may be placed close to electrical devices such as electrical insect-killers which produce radio waves. These may interfere with the power line signals. Move the adapters further away from such electrical devices.
- 4 Your wiring may be old and/or low quality or with a long wiring path.

11.7 Advanced Features



I can log in, but I cannot see some of the screens or fields in the Web Configurator.

You may be accessing the Web Configurator in Basic mode. Some screens and fields are available only in Advanced mode. Use the **Maintenance > Config Mode** screen to select Advanced mode.

PART IV

Appendices and Index

Product Specifications and Wall-Mounting Instructions (105)

Pop-up Windows, JavaScripts and Java Permissions (109)

IP Addresses and Subnetting (115)

Setting up Your Computer's IP Address (123)

Wireless LANs (139)

Common Services (153)

Legal Information (157)

Customer Support (161)

Index (167)

Product Specifications and Wall-Mounting Instructions

The following tables summarize the ZyXEL Device's hardware and firmware features.

Table 31 Hardware Features

Dimensions (W x D x H)	190 x 128 x 33 mm
Power Specification	120~240 VAC, 50/60 Hz
Ethernet port	Auto-negotiating: This auto-negotiation feature allows the ZyXEL Device to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. Auto-crossover: Use either crossover or straight-through Ethernet cables.
Reset Button	The reset button is built into the rear panel. Use this button to restore the ZyXEL Device to its factory default settings. Press for 1 second to restart the device. Press for 5 seconds to restore to factory default settings.
Antenna	The ZyXEL Device is equipped with a 2dBi detachable antenna to provide clear radio transmission and reception on the wireless network.
Operating Temperature	0° C ~ 40° C
Storage Temperature	-20° C ~ 60° C
Operation Humidity	20% ~ 90% RH (Non-condensing)
Storage Humidity	20% ~ 90% RH (Non-condensing)
Distance between the centers of the holes on the device's back.	115 mm
Screw size for wall-mounting	use M3 screws made of plastic (not included)

Table 32 Firmware Features

FEATURE	DESCRIPTION
Default IP Address	192.168.1.2
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.33 to 192.168.1.64
Device Management	Use the web configurator to easily configure the rich range of features on the ZyXEL Device.

Table 32 Firmware Features

FEATURE	DESCRIPTION
Wireless Functionality	<p>Allows IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the ZyXEL Device wirelessly. IEEE 802.11g clients can connect using the super G function. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.</p> <p>Note: The ZyXEL Device may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.</p>
WPA(2)-PSK	WPA-PSK and WPA2-PSK allow you to implement the WPA and WPA2 encryption standards without using a RADIUS server. Instead, WPA(2)-PSK uses Pre-Shared Keys (PSKs) to authenticate devices on the wireless network. WPA-PSK and WPA2-PSK provide superior security to WEP.
Powerline Functionality	<p>The HomePlug AV standard specifies how network devices communicate using standard electrical wiring. It supports a data transfer rate of up to 200Mbps. Data is encrypted using 128-bit AES (Advanced Encryption Standard). HomePlug AV compatible devices co-exist with HomePlug 1.0 devices but do not detect each other.</p> <p>The range of a HomePlug AV network is 300 meters/984 feet in optimal conditions.</p> <p>HomePlug AV is compatible with all OSs</p> <p>Maximum number of powerline devices on a single network is 16.</p>
Firmware Upgrade	<p>Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyXEL Device.</p> <p>Note: Only upload firmware for your specific model!</p>
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration and put it back on the ZyXEL Device later if you decide you want to revert back to an earlier configuration.
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logging and Tracing	Use packet tracing and logs for troubleshooting. You can send logs from the ZyXEL Device to an external UNIX syslog server.

The following list, which is not exhaustive, illustrates the standards supported in the ZyXEL Device.

Table 33 Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol.
RFC 1112	IGMP v1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)

Table 33 Standards Supported (continued)

STANDARD	DESCRIPTION
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.1x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
Microsoft PPTP	MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)

Wall-mounting Instructions

Do the following to hang your ZyXEL Device on a wall.



See [Table 31 on page 105](#) for the size of screws to use and how far apart to place them.

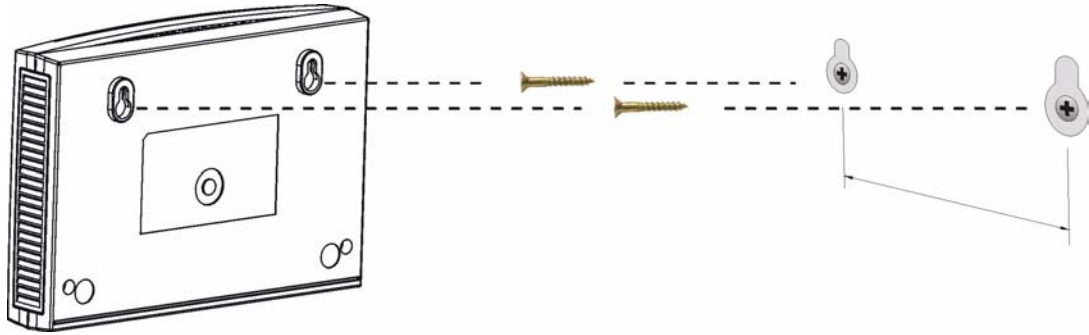
- 1 Locate a high position on a wall that is free of obstructions. Use a sturdy wall.
- 2 Drill two holes for the screws. Make sure the distance between the centers of the holes matches what is listed in the product specifications appendix.



Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

- 3 Do not screw the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.
- 4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the ZyXEL Device with the connection cables.
- 5 Align the holes on the back of the ZyXEL Device with the screws on the wall. Hang the ZyXEL Device on the screws.

Figure 55 Wall-mounting Example



Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).



Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

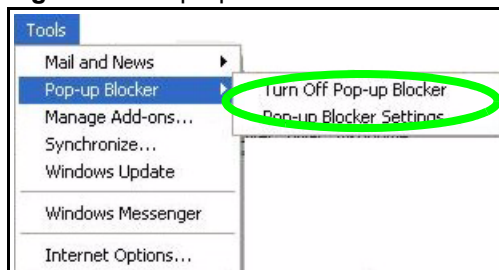
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 56 Pop-up Blocker

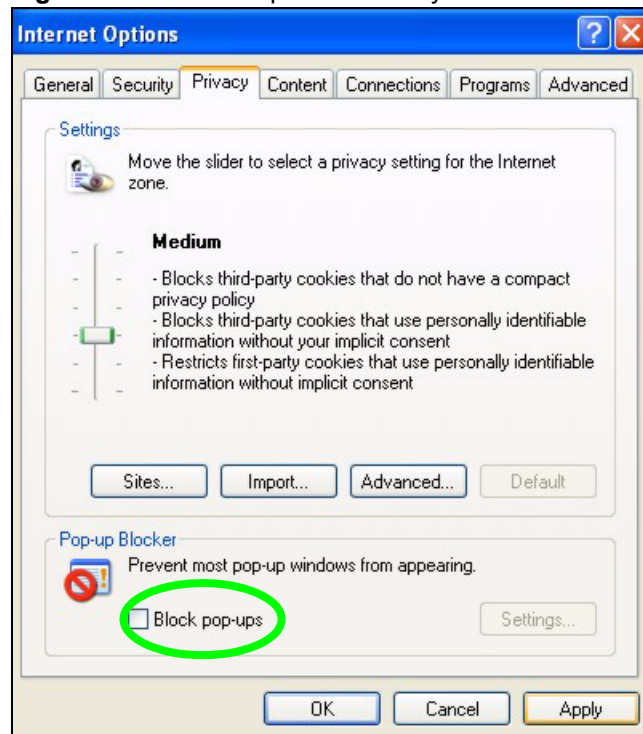


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.

- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 57 Internet Options: Privacy

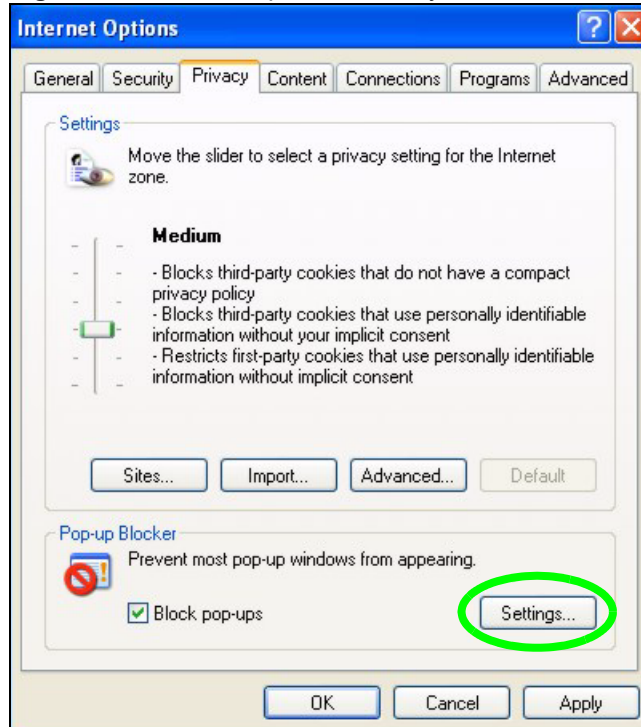


- 3 Click **Apply** to save this setting.

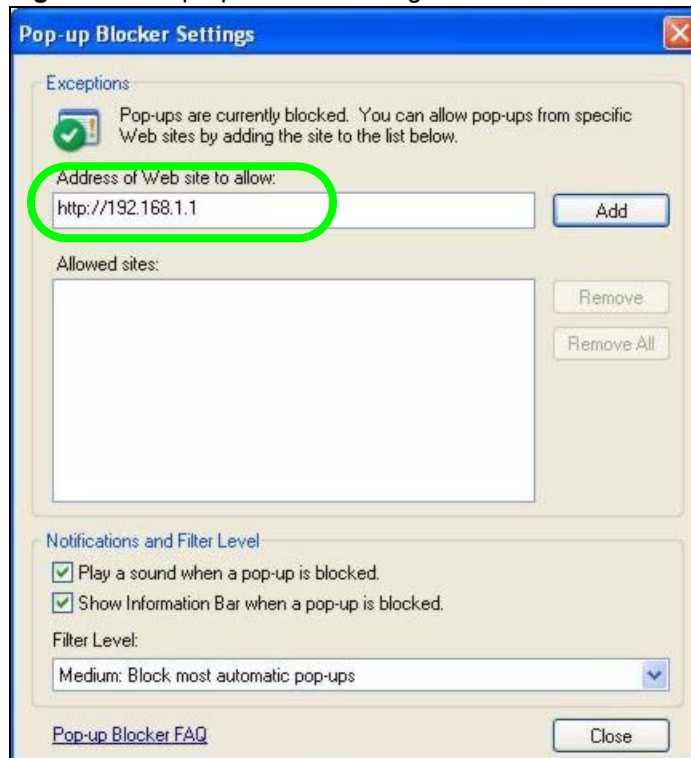
Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

Figure 58 Internet Options: Privacy

- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.
- 4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 59 Pop-up Blocker Settings

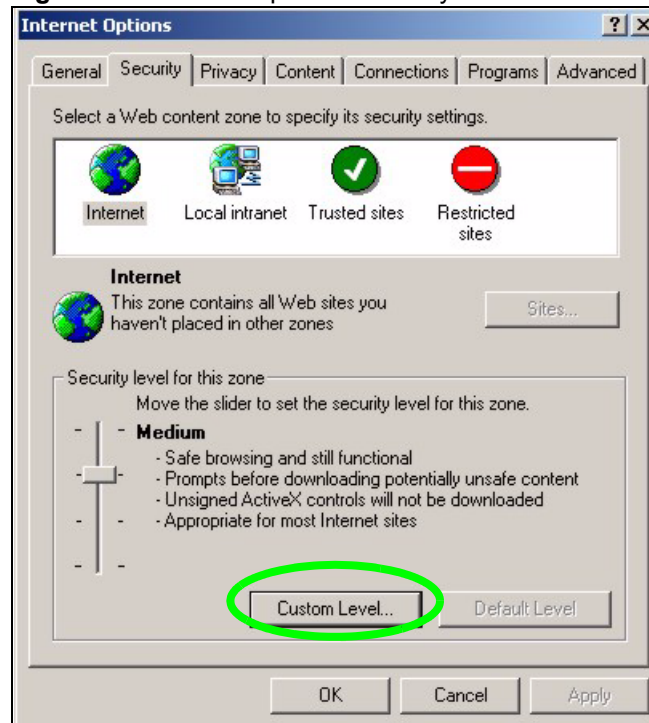
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

JavaScripts

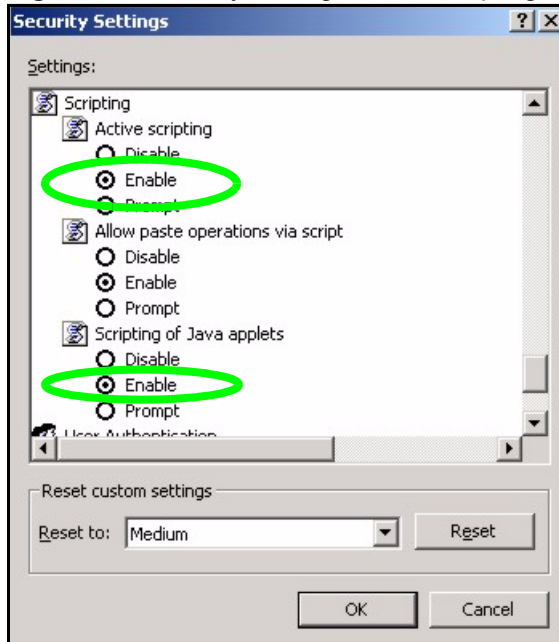
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

- 1 In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.

Figure 60 Internet Options: Security

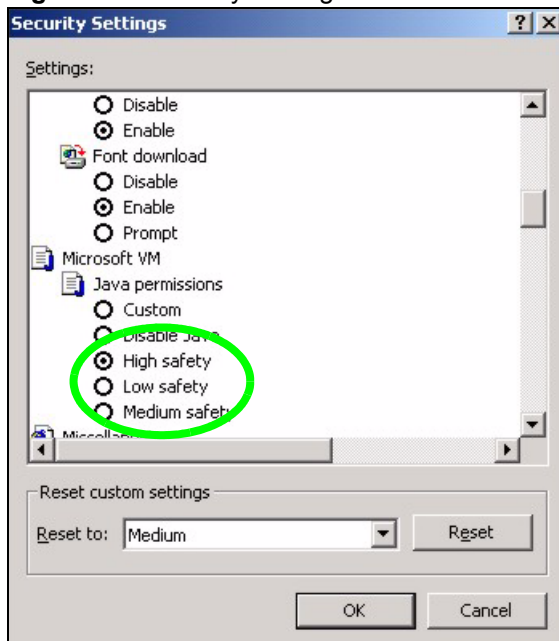


- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6 Click **OK** to close the window.

Figure 61 Security Settings - Java Scripting

Java Permissions

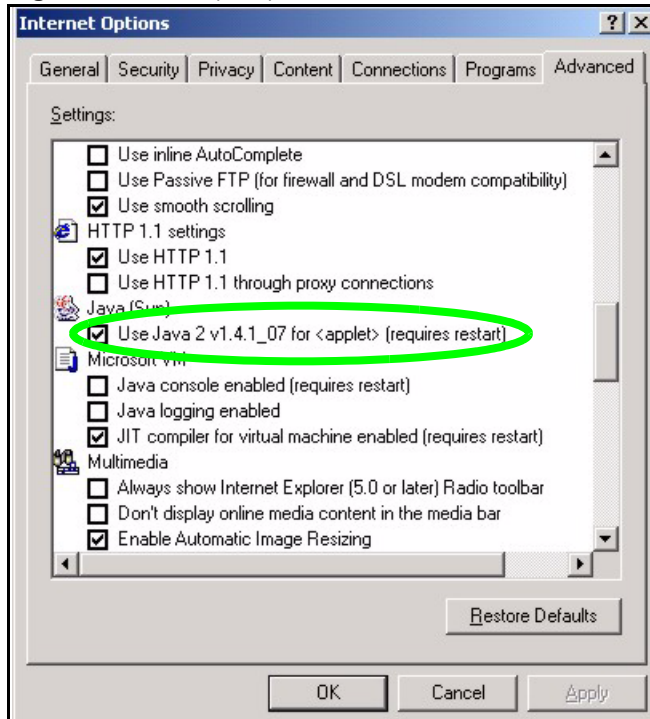
- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

Figure 62 Security Settings - Java

JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

Figure 63 Java (Sun)



IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

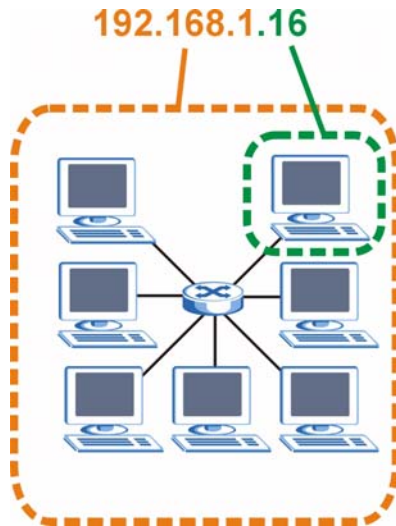
One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 64 Network Number and Host ID

How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 34 Subnet Mask - Identifying Network Number

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	11111111	11111111	11111111	00000000
Network Number	11000000	10101000	00000001	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 35 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 36 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 37 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 37 Alternative Subnet Mask Notation (continued)

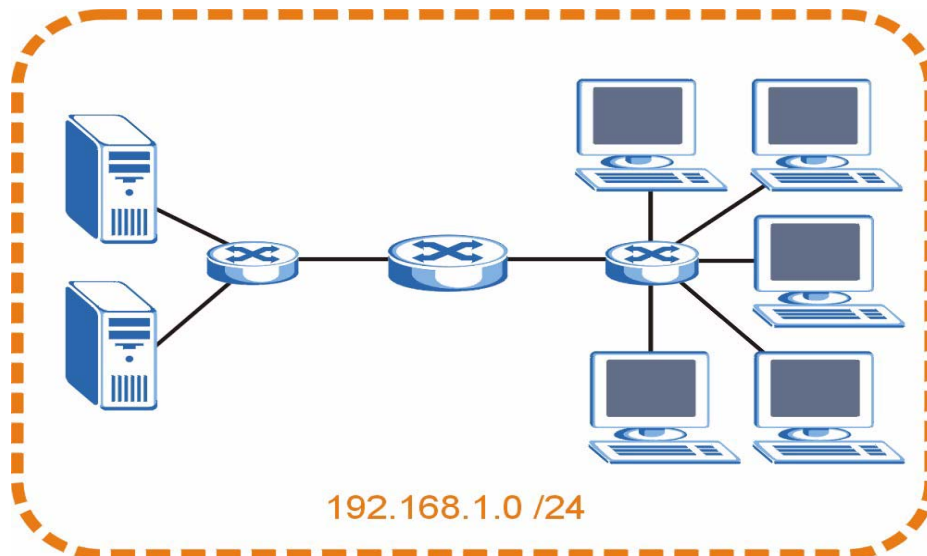
SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

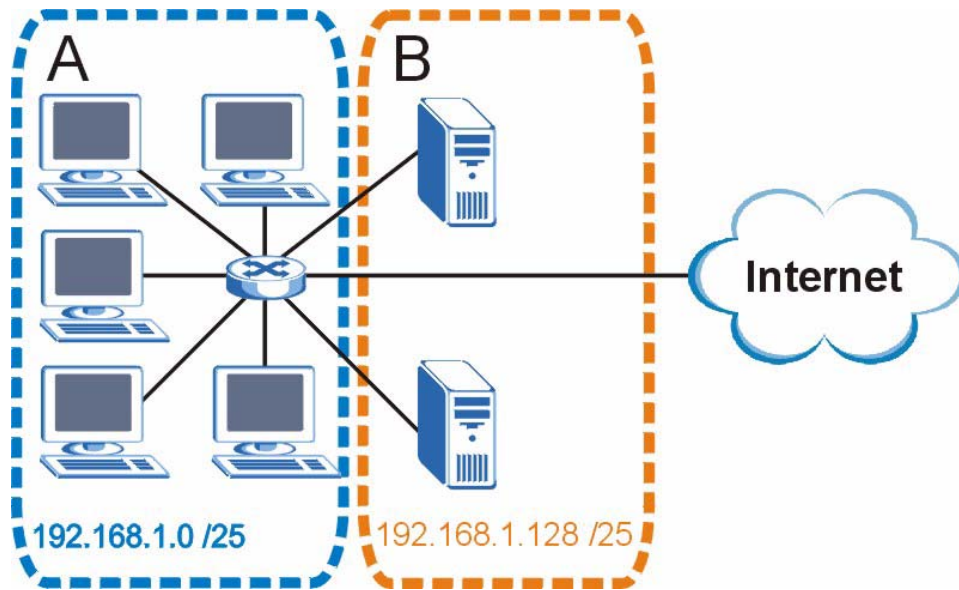
The following figure shows the company network before subnetting.

Figure 65 Subnetting Example: Before Subnetting

You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 66 Subnetting Example: After Subnetting

In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to “borrow” two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 38 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 39 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 40 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 41 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 42 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 42 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 43 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 44 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 44 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

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. 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. You must also enable Network Address Translation (NAT) on your router that connects to the Internet.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) 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 don't 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 (running only between two branch offices, for example) 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.

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*.

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

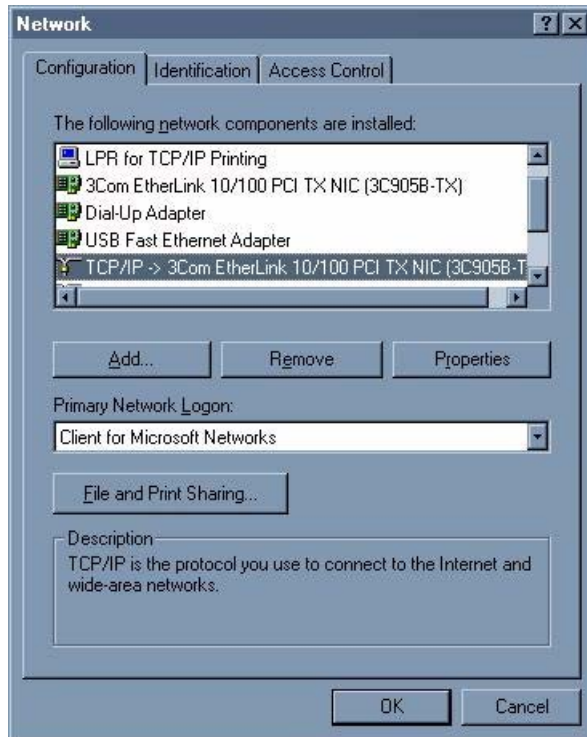
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 67 Windows 95/98/Me: Network: Configuration

Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.
- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

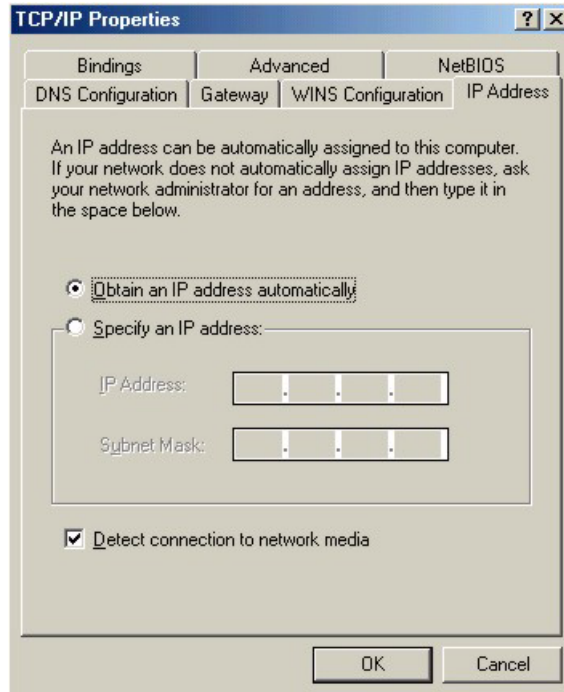
If you need Client for Microsoft Networks:

- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.
- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

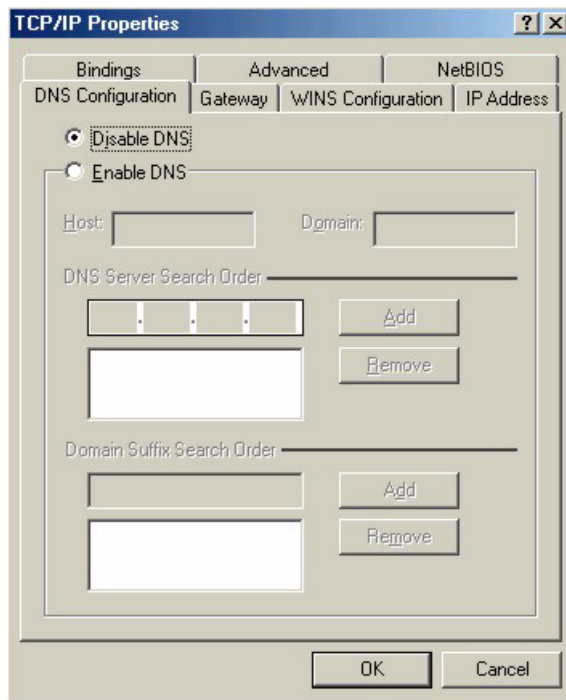
Configuring

- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
 - If your IP address is dynamic, select **Obtain an IP address automatically**.
 - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 68 Windows 95/98/Me: TCP/IP Properties: IP Address



- 3 Click the **DNS Configuration** tab.
 - If you do not know your DNS information, select **Disable DNS**.
 - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 69 Windows 95/98/Me: TCP/IP Properties: DNS Configuration

- 4 Click the **Gateway** tab.
 - If you do not know your gateway's IP address, remove previously installed gateways.
 - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
- 5 Click **OK** to save and close the **TCP/IP Properties** window.
- 6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
- 7 Turn on your Prestige and restart your computer when prompted.

Verifying Settings

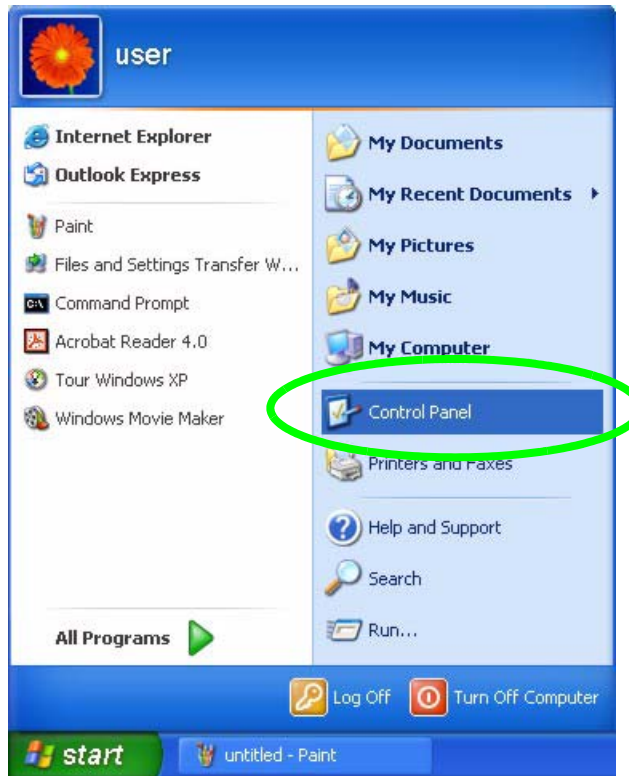
- 1 Click **Start** and then **Run**.
- 2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

- 1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 70 Windows XP: Start Menu



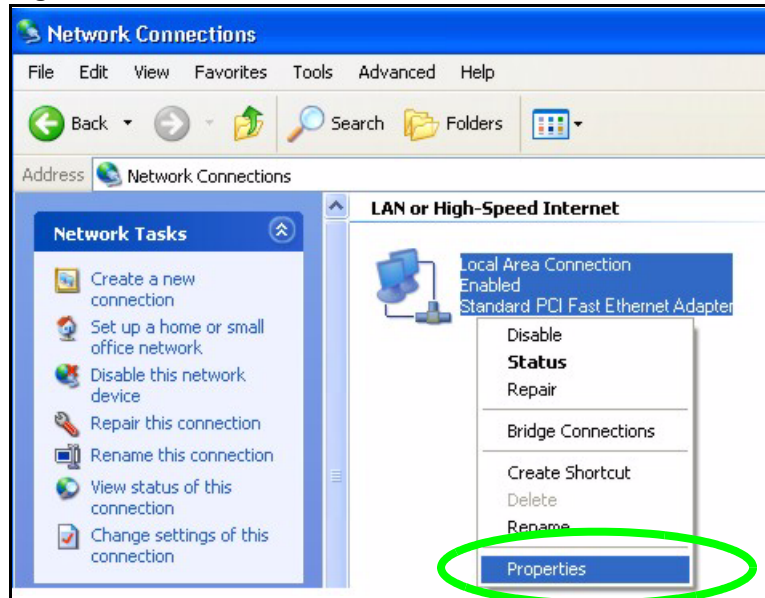
- 2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 71 Windows XP: Control Panel



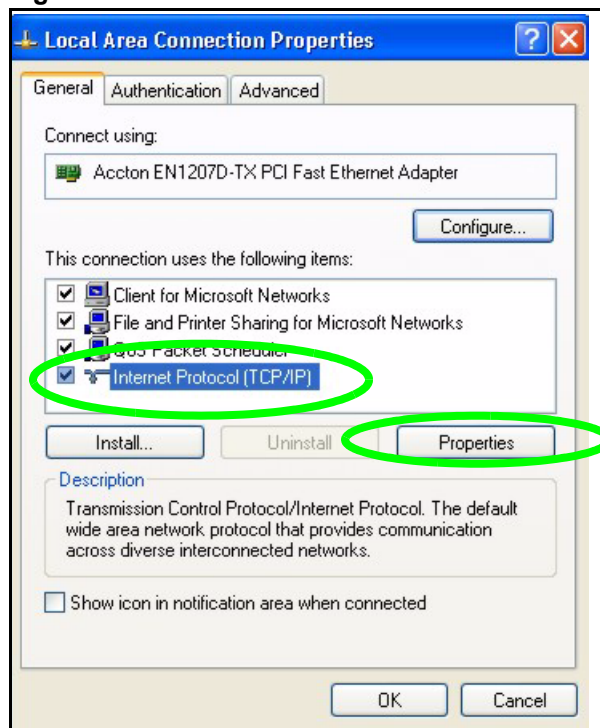
- 3 Right-click **Local Area Connection** and then click **Properties**.

Figure 72 Windows XP: Control Panel: Network Connections: Properties



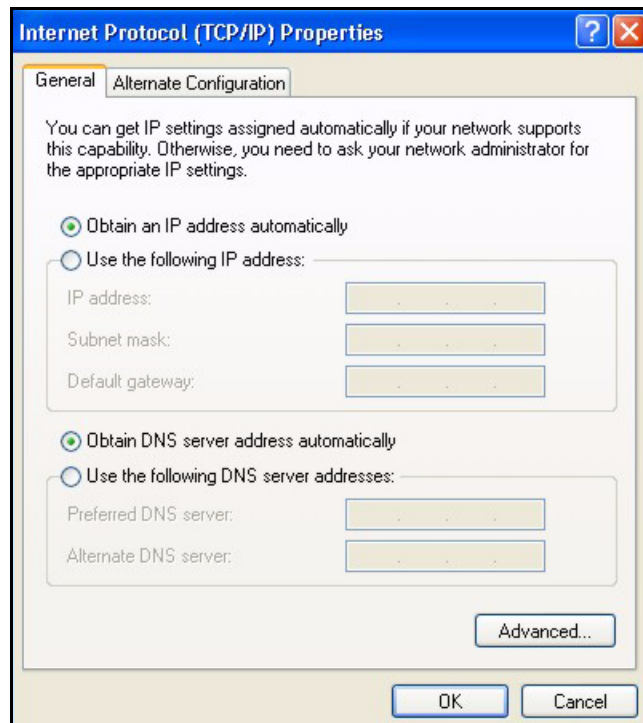
4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 73 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

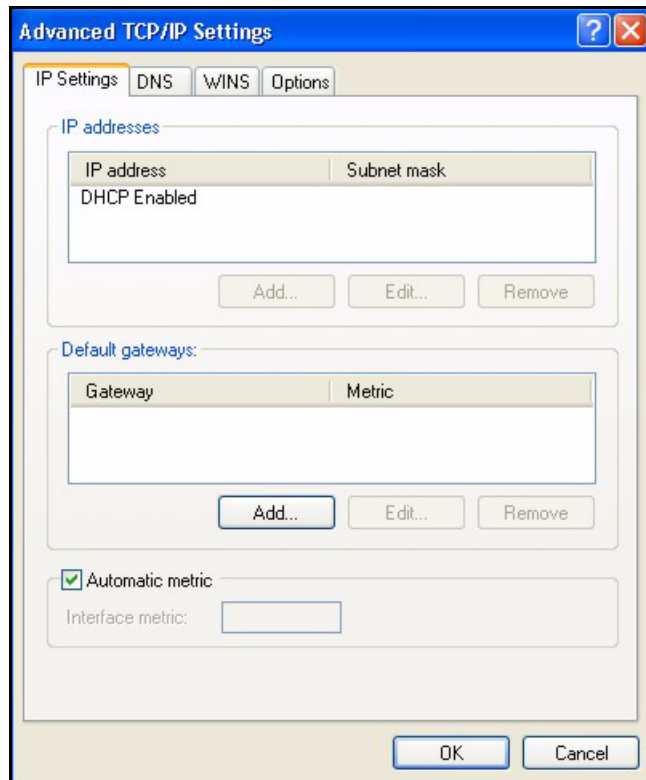
- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 74 Windows XP: Internet Protocol (TCP/IP) Properties

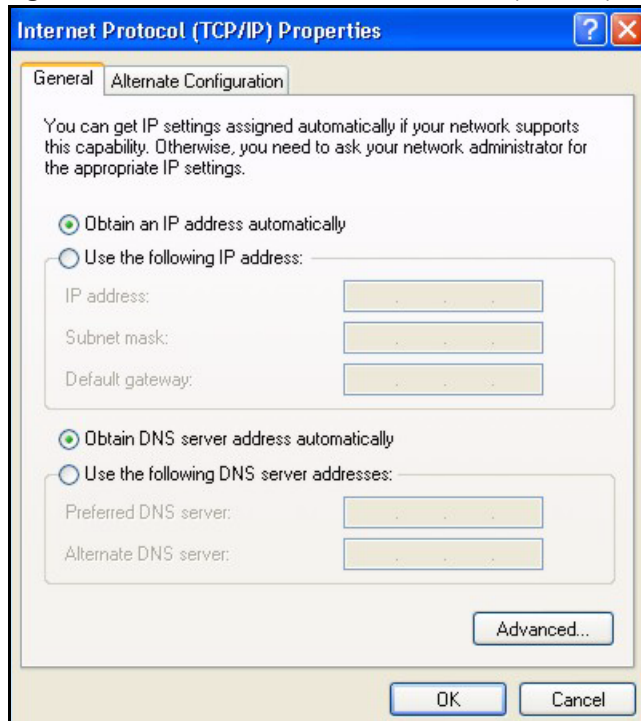
- 6** If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 75 Windows XP: Advanced TCP/IP Properties

- 7** In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):
- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
 - If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.
- If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 76 Windows XP: Internet Protocol (TCP/IP) Properties

- 8** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9** Click **Close (OK in Windows 2000/NT)** to close the **Local Area Connection Properties** window.
- 10** Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).
- 11** Turn on your Prestige and restart your computer (if prompted).

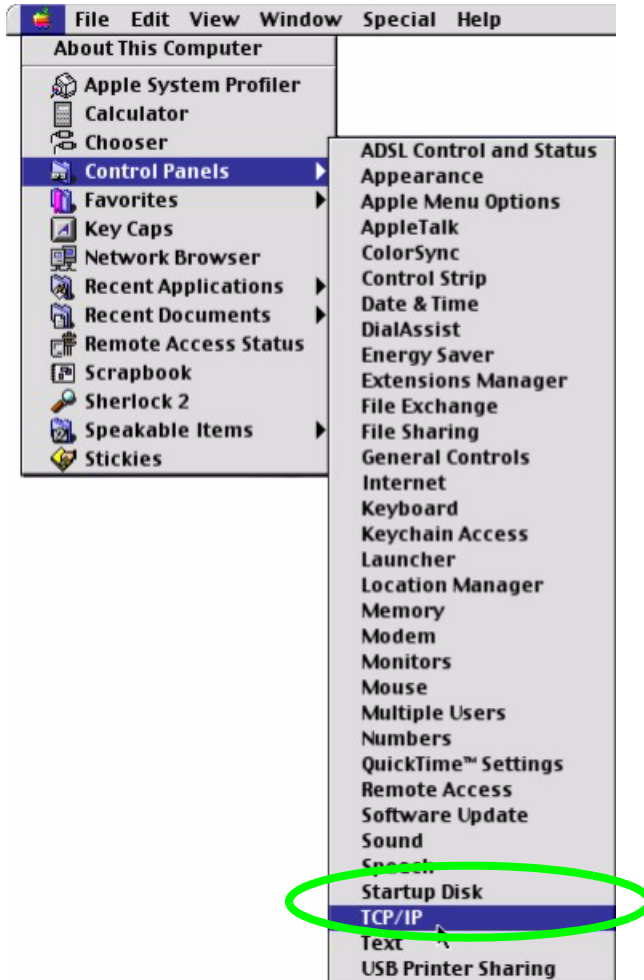
Verifying Settings

- 1** Click **Start, All Programs, Accessories** and then **Command Prompt**.
- 2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

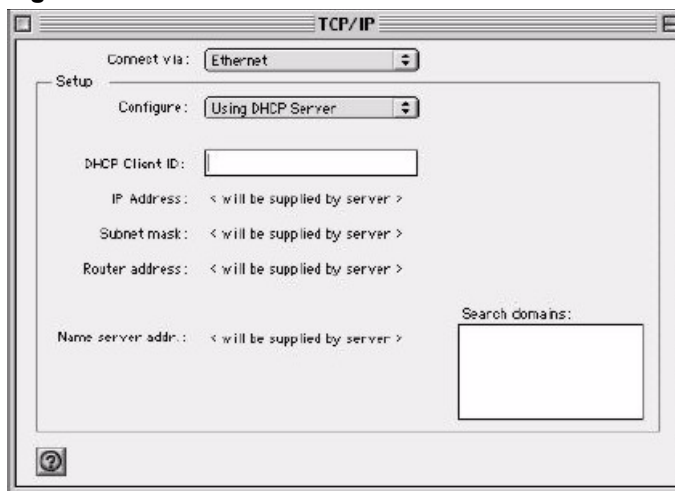
- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 77 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 78 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your Prestige in the **Router address** box.
- 5 Close the **TCP/IP Control Panel**.
 - 6 Click **Save** if prompted, to save changes to your configuration.
 - 7 Turn on your Prestige and restart your computer (if prompted).

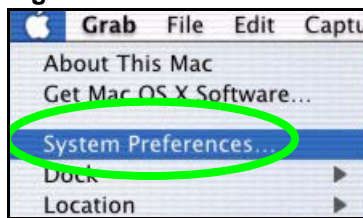
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

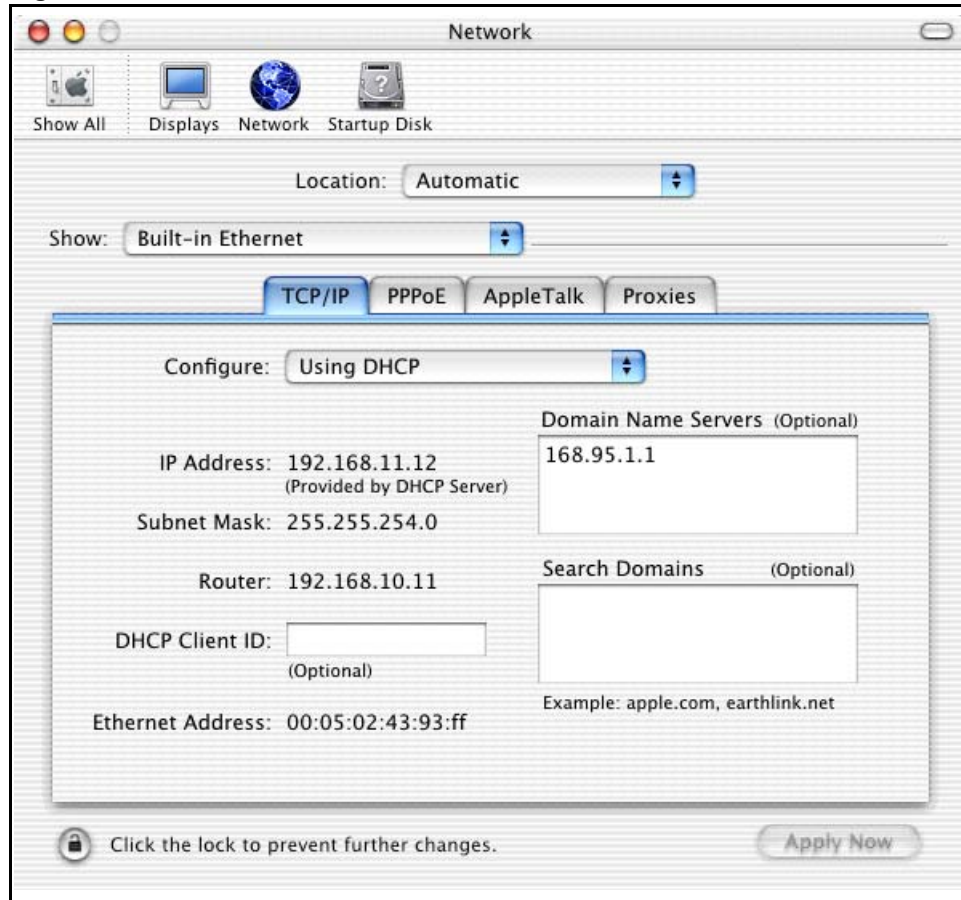
Macintosh OS X

- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 79 Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
 - Select **Automatic** from the **Location** list.
 - Select **Built-in Ethernet** from the **Show** list.
 - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 80 Macintosh OS X: Network

- 4 For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your Prestige in the **Router address** box.
- 5 Click **Apply Now** and close the window.
- 6 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.



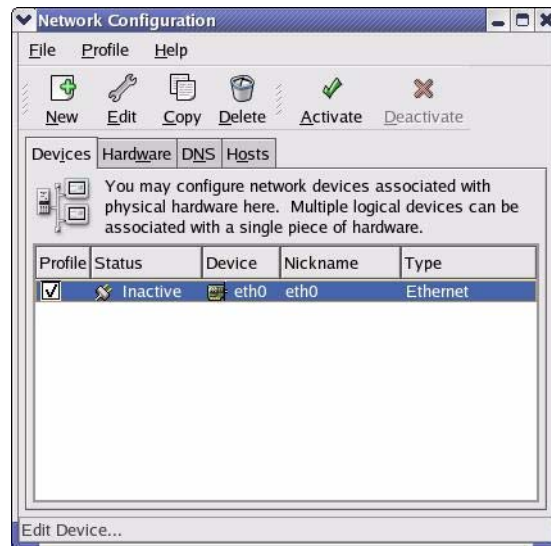
Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

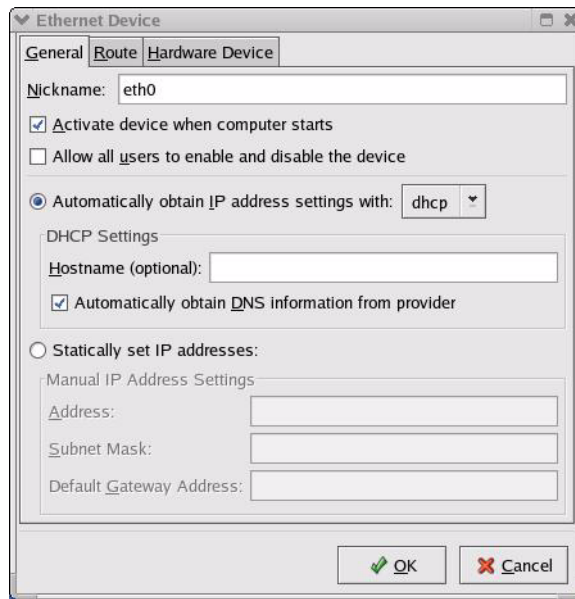
Follow the steps below to configure your computer IP address using the KDE.

- 1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

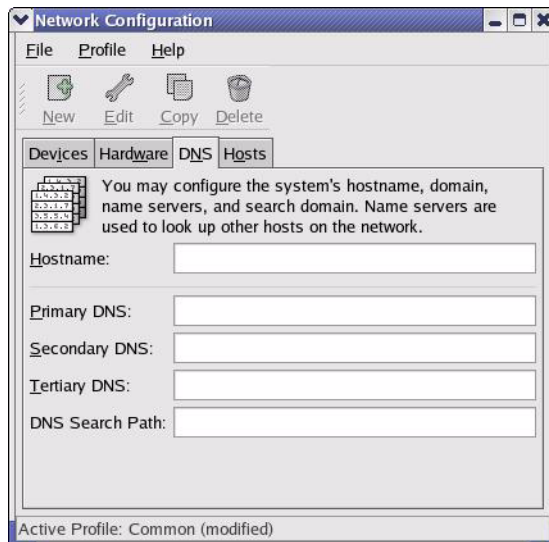
Figure 81 Red Hat 9.0: KDE: Network Configuration: Devices



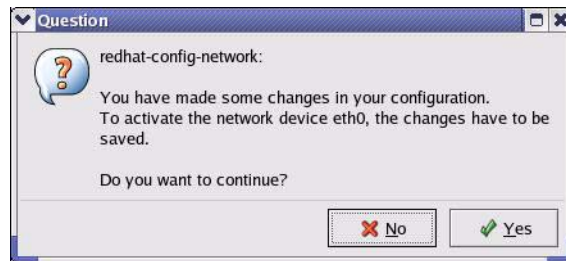
- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Figure 82 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
 - If you have a static IP address click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.
- 3 Click **OK** to save the changes and close the **Ethernet Device General** screen.
 - 4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 83 Red Hat 9.0: KDE: Network Configuration: DNS

- 5 Click the **Devices** tab.
- 6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens**.

Figure 84 Red Hat 9.0: KDE: Network Configuration: Activate

- 7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

- 1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.
 - If you have a dynamic IP address, enter `dhcp` in the `BOOTPROTO=` field. The following figure shows an example.

Figure 85 Red Hat 9.0: Dynamic IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter `static` in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 86 Red Hat 9.0: Static IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- 2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 87 Red Hat 9.0: DNS Settings in `resolv.conf`

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

- 3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 88 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

11.7.1 Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 89 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

Wireless LANs

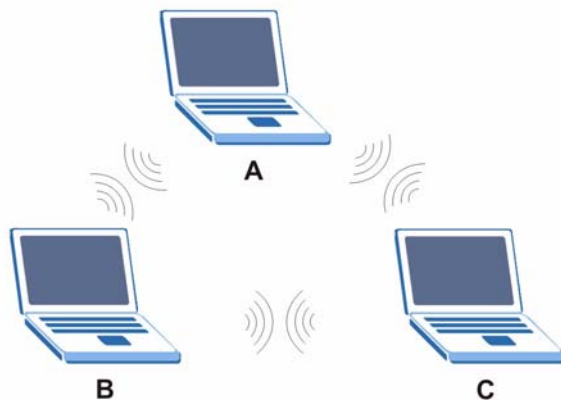
Wireless LAN Topologies

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

Ad-hoc Wireless LAN Configuration

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

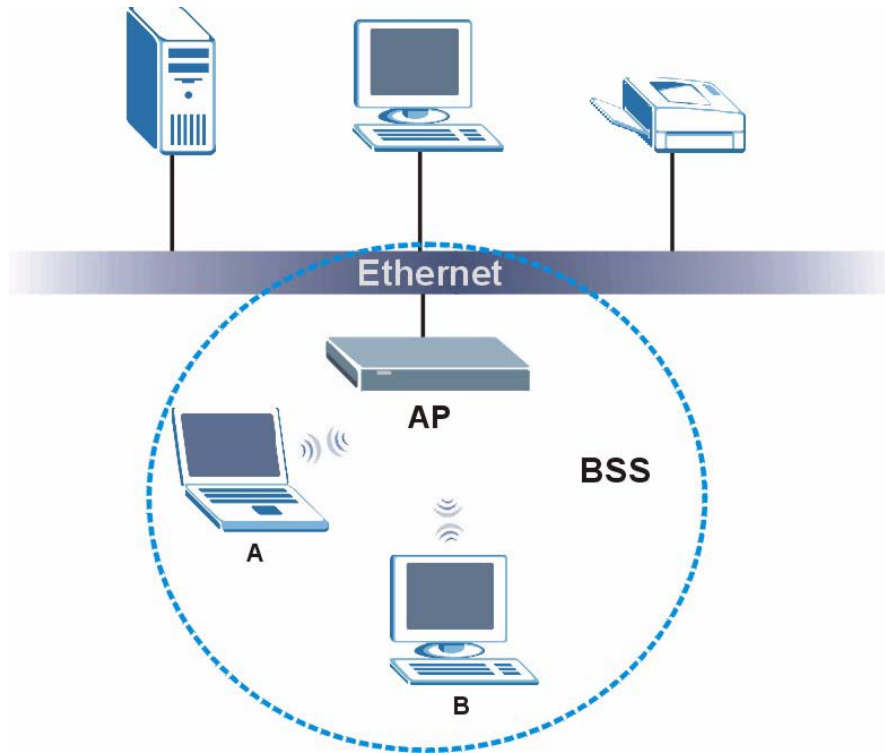
Figure 90 Peer-to-Peer Communication in an Ad-hoc Network



BSS

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

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

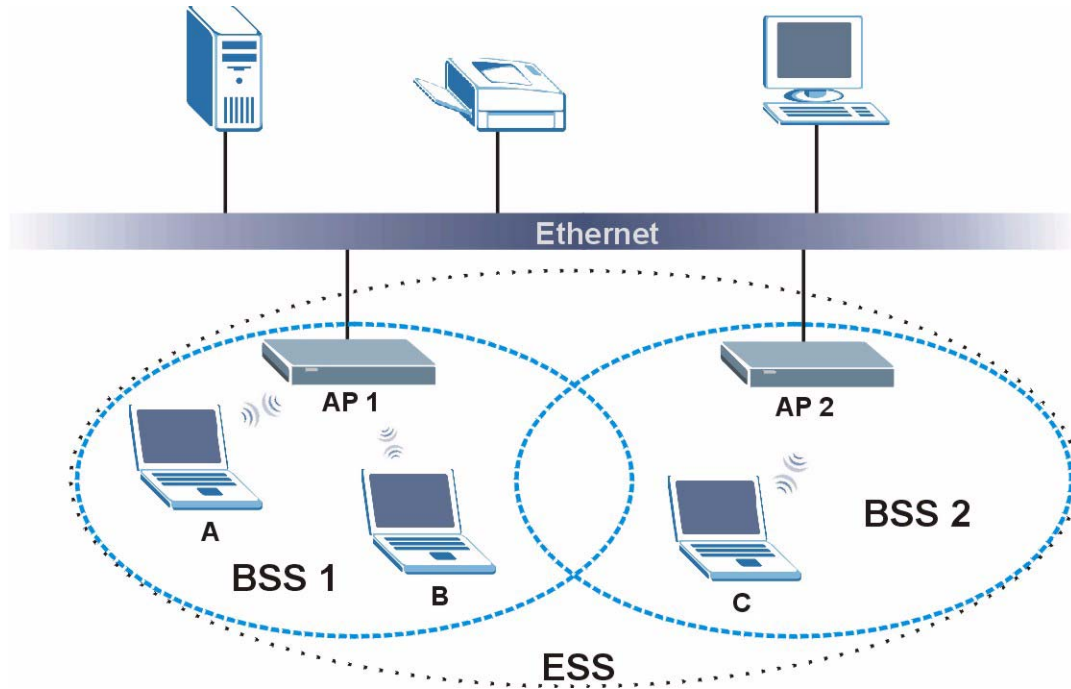
Figure 91 Basic Service Set

ESS

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

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

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

Figure 92 Infrastructure WLAN

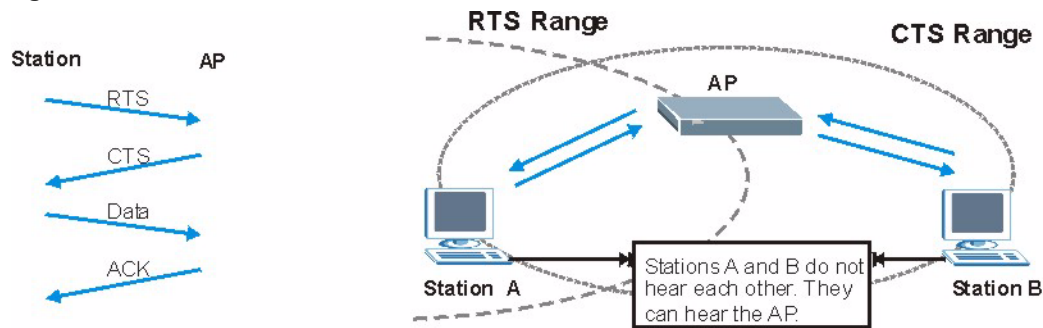
Channel

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

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

RTS/CTS

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

Figure 93 RTS/CTS

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

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

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

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

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

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



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

Fragmentation Threshold

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

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

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

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the ZyXEL Device uses long preamble.



The wireless devices **MUST** use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

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

Table 45 IEEE 802.11g

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

Wireless Security Overview

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

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

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

Table 46 Wireless Security Levels

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



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

IEEE 802.1x

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

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

RADIUS

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

- Authentication
 - Determines the identity of the users.
- Authorization

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

- Accounting
Keeps track of the client's network activity.

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

Types of RADIUS Messages

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

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

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

- Accounting-Request
Sent by the access point requesting accounting.
- Accounting-Response
Sent by the RADIUS server to indicate that it has started or stopped accounting.

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

Types of EAP Authentication

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

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

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

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

EAP-MD5 (Message-Digest Algorithm 5)

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

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

EAP-TLS (Transport Layer Security)

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

EAP-TTLS (Tunneled Transport Layer Service)

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

PEAP (Protected EAP)

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

LEAP

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

Dynamic WEP Key Exchange

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

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



EAP-MD5 cannot be used with Dynamic WEP Key Exchange

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

Table 47 Comparison of EAP Authentication Types

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

WPA and WPA2

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

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

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

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

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

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

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

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

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

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

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

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

User Authentication

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

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

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

Wireless Client WPA Supplicants

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

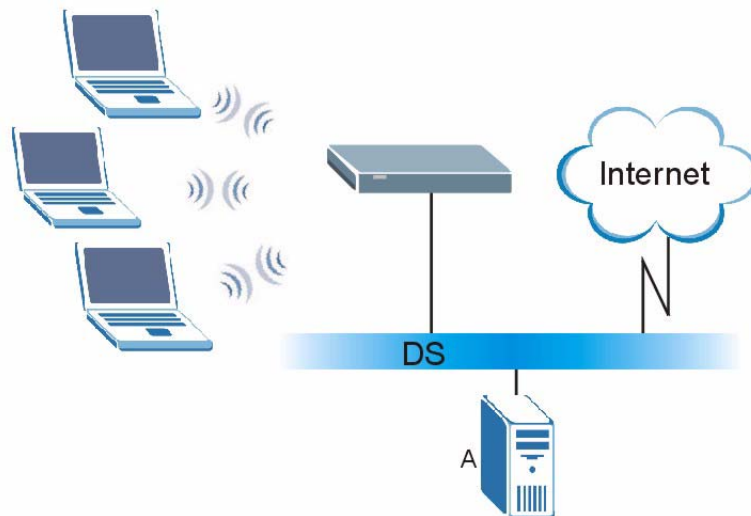
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

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

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

Figure 94 WPA(2) with RADIUS Application Example



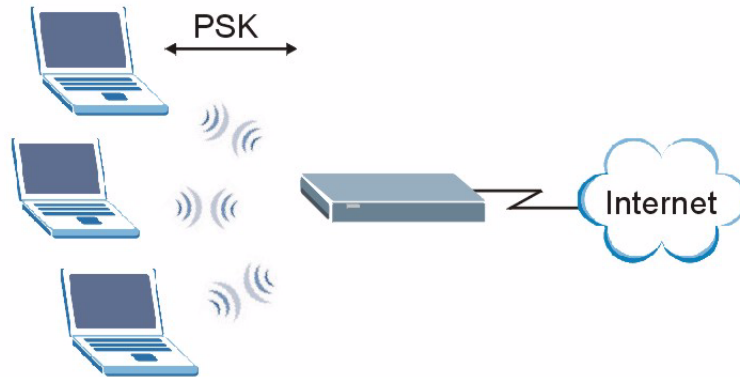
WPA(2)-PSK Application Example

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

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

- 3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.
- 4 The AP and wireless clients use the TKIP or AES encryption process, to encrypt data exchanged between them.

Figure 95 WPA(2)-PSK Authentication



Security Parameters Summary

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

Table 48 Wireless Security Relational Matrix

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

Antenna Overview

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

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

Antenna Characteristics

Frequency

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

Radiation Pattern

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

Antenna Gain

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

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

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

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

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

Positioning Antennas

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

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

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

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
 - If the **Protocol** is **TCP, UDP, or TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 49 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.

Table 49 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.

Table 49 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

Legal Information

Copyright

Copyright © 2007 by ZyXEL Communications Corporation.

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 Communications Corporation.

Published by ZyXEL Communications Corporation. 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.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined 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:

- 1 Reorient or relocate the receiving antenna.
- 2 Increase the separation between the equipment and the receiver.
- 3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4 Consult the dealer or an experienced radio/TV technician for help.



FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

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

Note

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

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

Please have the following information ready when you contact customer support.

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.

“+” is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- FTP: [ftp.zyxel.com](ftp://ftp.zyxel.com), [ftp.europe.zyxel.com](ftp://ftp.europe.zyxel.com)
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: [ftp.zyxel.co.cr](ftp://ftp.zyxel.co.cr)
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz

- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Česká Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: <http://www.zyxel.in>
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: <http://zyxel.kz/support>
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: <http://www.zyxel.com.my>
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.us.zyxel.com
- FTP: <ftp.us.zyxel.com>

- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: <http://zyxel.ru/support>
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: <http://www.zyxel.com.sg>
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: <http://www.zyxel.co.th>
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index

Numerics

802.11 mode [62](#)
802.11b [62](#)
802.11b/g [62](#)
802.11g [62](#)

A

administrator inactivity timer [81](#)
Advanced Encryption Standard (AES) [72](#), [148](#)
advanced mode [37](#)
Advanced Setup [36](#)
AES [72](#), [148](#)
alert [86](#)
alternative subnet mask notation [117](#)
antenna
 directional [151](#)
 gain [151](#)
 omni-directional [151](#)
AP (access point) [141](#)

B

backup configuration [91](#)
basic mode [37](#)
Basic Service Set, See BSS [139](#)
Basic Setup [36](#)
BSS [139](#)

C

CA [146](#)
Certificate Authority (CA) [146](#)
certifications [157](#)
 notices [158](#)
 viewing [158](#)
changing the NMK [72](#)
channel [39](#), [47](#), [141](#)

interference [141](#)
configuration [91](#)
 backup [91](#)
 reset the factory defaults [92](#)
 restore [91](#)
configuration mode [37](#)
contact information [161](#)
copyright [157](#)
CPU usage [39](#)
CTS (Clear to Send) [142](#)
customer support [161](#)

D

date [39](#), [83](#)
Daylight Saving Time [83](#)
defaults
 LAN [67](#)
 login [35](#)
 resetting to [92](#)
device reset [37](#)
DHCP [81](#)
dimensions [105](#)
disclaimer [157](#)
domain name [81](#)
duplex setting [40](#)
dynamic WEP key exchange [147](#)

E

EAP authentication [145](#)
e-mail [65](#)
encryption [50](#), [72](#), [148](#)
 and local (user) database [50](#)
 key [51](#)
 WPA compatible [50](#)
ESS [140](#)
ESSID [101](#)
Extended Service Set, See ESS [140](#)

F

factory LAN defaults [67](#)
FCC interference statement [157](#)
File Transfer Protocol, (FTP) [65](#)
firmware
 file extension
 HTTP upload
 upload [89](#)
 version [39](#)
fragmentation threshold [62](#), [142](#)
FTP [24](#), [65](#)
Funk Software Odyssey client [149](#)

G

general setup [81](#)

H

hidden node [141](#)
HomePlug [42](#)
 network status [42](#)
HomePlug AV [23](#), [71](#)
 AES [72](#)
HTTP [65](#)
humidity [105](#)

I

IANA [122](#)
IBSS [139](#)
IEEE 802.11b [62](#)
IEEE 802.11g [62](#), [143](#)
IMAP [65](#)
Independent Basic Service Set
 See IBSS [139](#)
initialization vector (IV) [148](#)
Internet Assigned Numbers Authority
 See IANA
IP address [67](#), [68](#)
 assignment [67](#)
 dynamic [68](#)

K

key [51](#)
 length [51](#)
 strength [51](#)
 WEP [55](#)

L

LAN [67](#)
 defaults [67](#)
 overview [67](#)
 setup [67](#)
link type [39](#)
local (user) database [49](#)
 and encryption [50](#)
Local Area Network, See LAN [67](#)
log [85](#)
login [35](#)
 defaults [35](#)

M

MAC [60](#)
MAC address [49](#), [60](#)
 filter [49](#), [60](#)
management [35](#)
 login [35](#)
 session timeout [81](#)
managing the device
 good habits [24](#)
 using FTP. See FTP.
 using the web configurator. See web configurator.
Media Access Control address, See MAC address [60](#)
memory usage [39](#)
Message Integrity Check (MIC) [148](#)

N

name [81](#)
NAT [122](#)
navigation panel [40](#)
network
 encryption [72](#)
 Ethernet [67](#)
 HomePlug AV [71](#)
 powerline [71](#), [72](#)

- wireless [47](#)
- Network Membership Key, See NMK [72](#)
- network name [72](#)
- network password [72](#)
- NMK [72](#)
 - changing [72](#)

O

- Odyssey client [149](#)
- operating channel [39](#)
- output power [62](#)

P

- packet statistics [41](#)
- Pairwise Master Key (PMK) [148](#), [150](#)
- password [35](#)
- PMK [148](#)
- POP3 [65](#)
- port speed [40](#)
- power
 - adaptor specification [105](#)
 - wireless [62](#)
- powerline [71](#), [72](#)
 - encryption [72](#)
 - scenario [72](#)
- preamble mode [143](#)
- priorities [53](#)
- private network [72](#)
- product registration [159](#)
- PSK [148](#)

Q

- QoS [53](#), [62](#)
- QoS priorities [53](#)
- Quality of Service, See QoS [62](#)

R

- RADIUS [144](#)
 - message types [145](#)

- messages [145](#)
 - server [49](#)
 - shared secret key [145](#)
- registration
 - product [159](#)
- related documentation [3](#)
- reset button [37](#), [92](#)
- resetting the device [37](#)
- restart [93](#)
- restore configuration [91](#)
- RF (Radio Frequency) [106](#)
- roaming [51](#), [61](#)
 - requirements [52](#)
- RTS (Request To Send) [142](#)
 - threshold [141](#), [142](#)
- RTS/CTS threshold [61](#)

S

- safety warnings [6](#)
- security [48](#), [150](#)
 - encryption [50](#)
 - wireless [48](#), [49](#)
- Service Set [54](#)
- Service Set IDentity, See SSID [54](#)
- Service Set IDentity. See SSID.
- Simple Mail Transfer Protocol [87](#)
- SMTP [65](#), [87](#)
- SSID [39](#), [47](#), [54](#)
- static WEP [50](#)
- statistics [41](#)
- status [37](#)
- sub-menus [40](#)
- subnet [115](#)
- subnet mask [68](#), [116](#)
- subnetting [118](#)
- summary
 - HomePlug network status [42](#)
 - packet statistics [41](#)
 - wireless station status [42](#)
- Super G [62](#)
 - with Dynamic Turbo [62](#)
 - without Dynamic Turbo [62](#)
- syntax conventions [4](#)
- system
 - general setup [81](#)
 - restart [93](#)
- system name [81](#)

T

temperature [105](#)
Temporal Key Integrity Protocol (TKIP) [148](#)
time [39](#), [83](#)
 server [83](#)
 setting [82](#)
 zone [83](#)
trademarks [157](#)

U

user authentication [49](#)
 local (user) database [49](#)
 RADIUS server [49](#)

W

warranty [159](#)
 note [159](#)
web configurator [24](#)
 default password [35](#)
 how to access [35](#)
 navigating [37](#)
 navigation panel [40](#)
 overview [35](#)
 password [35](#)
WEP [50](#)
 encryption [55](#), [56](#)
 key [55](#)
 key exchange [147](#)
Wi-Fi Multimedia QoS, See WMM [53](#)
Wi-Fi Protected Access, See WPA [147](#)
Windows XP Zero Configuration [149](#)
wireless
 association list [42](#)
 basic guidelines [47](#)
 channel [47](#), [101](#)
 Dynamic Turbo [62](#)
 encryption [50](#)
 general screen [53](#)
 IEEE 802.11b [62](#)
 IEEE 802.11g [62](#)
 interference [141](#)
 LAN [101](#)
 MAC address filter [49](#)
 network example [47](#)
 output power [62](#)
 security [48](#), [49](#), [101](#), [143](#)
 security parameters [150](#)

 SSID [47](#)
 stations [42](#)
 Super G [62](#)
 tutorial [27](#)
wireless client
 WPA supplicants [149](#)
WLAN
 interference [141](#)
 security parameters [150](#)
WMM [53](#)
 priorities [53](#)
World Wide Web, See WWW. [65](#)
WPA [50](#), [147](#)
 compatible [50](#)
 key caching [148](#)
 pre-authentication [148](#)
 supplicants [149](#)
 user authentication [148](#)
 vs WPA-PSK [148](#)
 wireless client supplicant [149](#)
 with RADIUS application example [149](#)
WPA2 [50](#), [147](#)
 user authentication [148](#)
 vs WPA2-PSK [148](#)
 wireless client supplicant [149](#)
 with RADIUS application example [149](#)
WPA2-Pre-Shared Key, See WPA2-PSK [147](#)
WPA2-PSK [50](#), [147](#), [148](#)
 application example [149](#)
WPA-PSK [50](#), [147](#), [148](#)
 application example [149](#)
WWW [65](#)

Z

Zero Configuration [149](#)
ZyNOS [39](#)