

NWA-1100

802.11b/g Wireless Access Point

User's Guide

Version 1.00

7/2008

Edition 1



About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

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.
- 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.






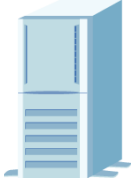

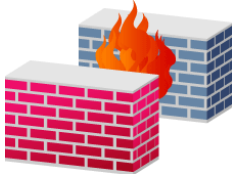



Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The NWA-1100 may be referred to as the “ZyXEL Device”, the “device” 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 > Configuration File > Backup** means you first click **Maintenance** in the navigation panel, then the **Configuration File** sub menu and finally the **Backup** button 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 	Printer 	Firewall 
Ethernet Switch 	Switch 	Router 

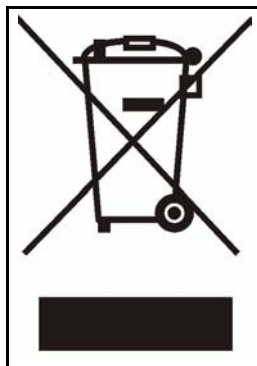
Safety Warnings



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.
- ONLY qualified service personnel should service or disassemble this device.
- 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.
- 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.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.

This product is recyclable. Dispose of it properly.



Contents Overview

Introduction	23
Introducing the ZyXEL Device	25
Introducing the Web Configurator	35
Status Screens	39
Tutorial	43
The Web Configurator	51
System Screens	53
Wireless Settings Screen	61
Wireless Security Screen	75
RADIUS Screen	89
MAC Filter Screen	93
IP Screen	97
Remote Management	101
Certificate Screen	111
Log Screens	115
Maintenance	121
Troubleshooting	129
Appendices and Index	133

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	17
List of Tables.....	21
Part I: Introduction.....	23
Chapter 1	
Introducing the ZyXEL Device	25
1.1 Introducing the ZyXEL Device	25
1.2 Applications for the ZyXEL Device	25
1.2.1 Access Point	25
1.2.2 Wireless Client	26
1.2.3 Bridge	27
1.2.4 AP + Bridge	29
1.3 Ways to Manage the ZyXEL Device	30
1.4 Configuring Your ZyXEL Device's Security Features	30
1.4.1 Control Access to Your Device	30
1.4.2 Wireless Security	31
1.5 Good Habits for Managing the ZyXEL Device	31
1.6 Hardware Connections	32
1.7 LEDs	32
Chapter 2	
Introducing the Web Configurator	35
2.1 Accessing the Web Configurator	35
2.2 Resetting the ZyXEL Device	36
2.2.1 Methods of Restoring Factory-Defaults	36
2.3 Navigating the Web Configurator	36

Chapter 3	
Status Screens	39
3.1 The Status Screen	39
3.1.1 System Statistics Screen	41
Chapter 4	
Tutorial	43
4.1 How to Configure the Wireless LAN	43
4.1.1 Choosing the Wireless Mode	43
4.1.2 Wireless LAN Configuration Overview	43
4.1.3 Further Reading	44
4.2 ZyXEL Device Setup in Wireless Client Mode	44
4.2.1 Scenario	45
4.2.2 Configuring the ZyXEL Device in Access Point Mode	45
4.2.3 Configuring the ZyXEL Device in Wireless Client Mode	46
4.2.4 Testing the Connection and Troubleshooting	49
Part II: The Web Configurator	51
Chapter 5	
System Screens	53
5.1 Overview	53
5.2 What You Can Do in the System Screens	53
5.3 What You Need To Know About the System Screens	54
5.4 General Screen	55
5.4.1 Password Screen	56
5.5 Time Screen	56
5.6 Technical Reference	58
5.6.1 Pre-defined NTP Time Servers List	58
Chapter 6	
Wireless Settings Screen	61
6.1 Overview	61
6.2 What You Can Do in the Wireless Settings Screen	61
6.3 What You Need To Know About Wireless Settings Screen	62
6.4 Wireless Settings Screen	63
6.4.1 Access Point Mode	63
6.4.2 Wireless Client Mode	65
6.4.3 Bridge Mode	68
6.4.4 AP + Bridge Mode	70
6.5 Technical Reference	71

6.5.1 WMM QoS	71
6.5.2 Spanning Tree Protocol (STP)	71
6.5.2.1 Rapid STP	71
6.5.2.2 STP Terminology	71
6.5.2.3 How STP Works	72
6.5.2.4 STP Port States	72
6.5.3 Additional Wireless Terms	73
Chapter 7	
Wireless Security Screen	75
7.1 Overview	75
7.2 What You Can Do in the Wireless Security Screen	75
7.3 What You Need To Know About Wireless Security	76
7.4 The Security Screen	77
7.4.1 Security: WEP	78
7.4.2 Security: 802.1x Only	79
7.4.2.1 Access Point	79
7.4.2.2 Wireless Client	80
7.4.3 Security: 802.1x Static 64-bit, 802.1x Static 128-bit	81
7.4.4 Security: WPA	83
7.4.4.1 Access Point	83
7.4.4.2 Wireless Client	84
7.4.5 Security: WPA2 or WPA2-MIX	85
7.4.5.1 Access Point	85
7.4.5.2 Wireless Client	86
7.4.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX	87
7.5 Technical Reference	87
Chapter 8	
RADIUS Screen	89
8.1 Overview	89
8.2 What You Can Do in the RADIUS Screen	89
8.3 What You Need to Know About RADIUS	89
8.4 The RADIUS Screen	90
Chapter 9	
MAC Filter Screen	93
9.1 Overview	93
9.2 What You Can Do in the MAC Filter	93
9.3 What You Need To Know About MAC Filter	93
9.4 MAC Filter Screen	94
Chapter 10	
IP Screen.....	97

10.1 Overview	97
10.2 What You Can Do in the IP Screen	97
10.3 What You Need to Know About IP	97
10.4 IP Screen	98
10.5 Technical Reference	99
10.5.1 WAN IP Address Assignment	99
Chapter 11	
Remote Management.....	101
11.1 Overview	101
11.2 What You Can Do in the Remote Management Screens	102
11.3 What You Need To Know About Remote Management	102
11.4 The Telnet Screen	104
11.5 The FTP Screen	104
11.6 The WWW Screen	105
11.7 The SNMP Screen	106
11.8 Technical Reference	108
11.8.1 MIB	108
11.8.2 Supported MIBs	108
11.8.3 SNMP Traps	108
Chapter 12	
Certificate Screen	111
12.1 Overview	111
12.2 What You Can Do in the Certificate Screen	111
12.3 What You Need To Know About Certificates	111
12.4 Certificate Screen	112
12.5 Technical Reference	112
12.5.1 Private-Public Certificates	113
12.5.2 Certification Authorities	113
12.5.3 Checking the Fingerprint of a Certificate on Your Computer	113
Chapter 13	
Log Screens	115
13.1 Overview	115
13.2 What You Can Do in the Log Screens	115
13.3 What You Need To Know About Logs	116
13.4 View Log Screen	116
13.5 Log Settings Screen	117
13.6 Technical Reference	118
13.6.1 Example Log Messages	119
13.7 Log Commands	119
13.7.1 Configuring What You Want the ZyXEL Device to Log	119

13.7.2 Displaying Logs	120
13.7.3 Command List	120
Chapter 14	
Maintenance	121
14.1 Overview	121
14.2 What You Can Do in the Maintenance Screens	121
14.3 What You Need To Know About the Maintenance Screens	121
14.4 Association List Screen	121
14.5 Channel Usage Screen	122
14.6 F/W Upload Screen	123
14.7 Configuration Screen	124
14.7.1 Backup Configuration	125
14.7.2 Restore Configuration	125
14.7.3 Back to Factory Defaults	126
14.8 Restart Screen	127
Chapter 15	
Troubleshooting.....	129
15.1 Power, Hardware Connections, and LEDs	129
15.2 ZyXEL Device Access and Login	129
15.3 Internet Access	131
Part III: Appendices and Index.....	133
Appendix A Product Specifications.....	135
Appendix B Power over Ethernet (PoE) Specifications	137
Appendix C Power Adaptor Specifications	139
Appendix D Setting up Your Computer's IP Address	141
Appendix E Wireless LANs	153
Appendix F Pop-up Windows, JavaScripts and Java Permissions	167
Appendix G IP Addresses and Subnetting	173
Appendix H Text File Based Auto Configuration	181
Appendix I How to Access and Use the CLI.....	187
Appendix J Legal Information.....	191
Appendix K Customer Support.....	195

Index.....201

List of Figures

Figure 1 Access Point Application	26
Figure 2 Wireless Client Application	26
Figure 3 Bridge Application	27
Figure 4 Bridging Example	28
Figure 5 Bridge Loop: Two Bridges Connected to Hub	28
Figure 6 Bridge Loop: Bridge Connected to Wired LAN	29
Figure 7 AP + Bridge Application	30
Figure 8 LEDs	32
Figure 9 Change Password Screen	35
Figure 10 Status Screen of the Web Configurator	37
Figure 11 The Status Screen	39
Figure 12 System Status: Show Statistics	41
Figure 13 Configuring Wireless LAN	44
Figure 14 FTP Server Connected to a Wireless Client	45
Figure 15 Access Point Mode Wireless Settings	46
Figure 16 Access Point Mode Security Settings	46
Figure 17 Wireless Client Mode Wireless Settings	47
Figure 18 Site Survey	48
Figure 19 Wireless Client Mode	48
Figure 20 Wireless Client Mode Security Settings	49
Figure 21 Wireless Client MAC Filtering	49
Figure 22 ZyXEL Device Setup	53
Figure 23 System: General	55
Figure 24 System: Password	56
Figure 25 System: Time	57
Figure 26 Wireless Mode	61
Figure 27 Wireless: Access Point	63
Figure 28 Wireless: Wireless Client	66
Figure 29 Wireless: Bridge	68
Figure 30 Wireless: AP+Bridge	70
Figure 31 Securing the Wireless Network	75
Figure 32 Security: None	78
Figure 33 Security: WEP	78
Figure 34 Security: 802.1x Only for Access Point	80
Figure 35 Security: 802.1x Only for Wireless Client	81
Figure 36 Security: 802.1x Static 64-bit, 802.1x Static 128-bit (AP mode)	82
Figure 37 Security: WPA for Access Point	83
Figure 38 Security: WPA for Wireless Client	84

Figure 39 Security:WPA2 or WPA2-MIX for Access Point	85
Figure 40 Security: WPA2 or WPA2-MIX for Wireless Client	86
Figure 41 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX	87
Figure 42 RADIUS Server Setup	89
Figure 43 Wireless > RADIUS	90
Figure 44 MAC Filtering	93
Figure 45 Wireless > MAC Filter	94
Figure 46 IP Setup	97
Figure 47 IP Setup	98
Figure 48 Remote Management Example	101
Figure 49 SNMP Management Mode	103
Figure 50 Remote Management: Telnet	104
Figure 51 Remote Management: FTP	105
Figure 52 Remote Management: WWW	106
Figure 53 Remote Management: SNMP	107
Figure 54 Certificates Example	111
Figure 55 Certificate	112
Figure 56 Certificates on Your Computer	113
Figure 57 Certificate Details	114
Figure 58 Accessing Logs in the Network	115
Figure 59 View Log	116
Figure 60 Log Settings	117
Figure 61 Association List	122
Figure 62 Channel Usage	122
Figure 63 Firmware Upload	123
Figure 64 Firmware Upload In Process	124
Figure 65 Network Temporarily Disconnected	124
Figure 66 Firmware Upload Error	124
Figure 67 Configuration	125
Figure 68 Configuration Upload Successful	126
Figure 69 Network Temporarily Disconnected	126
Figure 70 Configuration Upload Error	126
Figure 71 Reset Warning Message	127
Figure 72 Restart Screen	127
Figure 73 WIndows 95/98/Me: Network: Configuration	142
Figure 74 Windows 95/98/Me: TCP/IP Properties: IP Address	143
Figure 75 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	144
Figure 76 Windows XP: Start Menu	145
Figure 77 Windows XP: Control Panel	145
Figure 78 Windows XP: Control Panel: Network Connections: Properties	146
Figure 79 Windows XP: Local Area Connection Properties	146
Figure 80 Windows XP: Advanced TCP/IP Settings	147
Figure 81 Windows XP: Internet Protocol (TCP/IP) Properties	148

Figure 82 Macintosh OS 8/9: Apple Menu	149
Figure 83 Macintosh OS 8/9: TCP/IP	149
Figure 84 Macintosh OS X: Apple Menu	150
Figure 85 Macintosh OS X: Network	151
Figure 86 Peer-to-Peer Communication in an Ad-hoc Network	153
Figure 87 Basic Service Set	154
Figure 88 Infrastructure WLAN	155
Figure 89 RTS/CTS	156
Figure 90 WPA(2) with RADIUS Application Example	164
Figure 91 WPA(2)-PSK Authentication	164
Figure 92 Pop-up Blocker	167
Figure 93 Internet Options: Privacy	168
Figure 94 Internet Options: Privacy	169
Figure 95 Pop-up Blocker Settings	169
Figure 96 Internet Options: Security	170
Figure 97 Security Settings - Java Scripting	171
Figure 98 Security Settings - Java	171
Figure 99 Java (Sun)	172
Figure 100 Network Number and Host ID	174
Figure 101 Subnetting Example: Before Subnetting	176
Figure 102 Subnetting Example: After Subnetting	177
Figure 103 Text File Based Auto Configuration	181
Figure 104 Configuration File Format	183
Figure 105 WEP Configuration File Example	184
Figure 106 802.1X Configuration File Example	184
Figure 107 WPA-PSK Configuration File Example	185
Figure 108 WPA Configuration File Example	185
Figure 109 Wlan Configuration File Example	185

List of Tables

Table 1 LEDs	32
Table 2 The Status Screen	39
Table 3 System Status: Show Statistics	41
Table 4 Private IP Address Ranges	54
Table 5 System: General	55
Table 6 System: Password	56
Table 7 System: Time	57
Table 8 Default Time Servers	58
Table 9 Wireless: Access Point	64
Table 10 Wireless: Wireless Client	66
Table 11 Wireless: Bridge	68
Table 12 STP Path Costs	72
Table 13 STP Port States	72
Table 14 Additional Wireless Terms	73
Table 15 Wireless Security Levels	76
Table 16 Security: WEP	79
Table 17 Security: 802.1x Only for Access Point	80
Table 18 Security: 802.1x Only for Wireless Client	81
Table 19 Security: 802.1x Static 64-bit, 802.1x Static 128-bit	82
Table 20 Security: WPA for Access Point	83
Table 21 Security: WPA for Wireless Client	84
Table 22 Security: WPA2 or WPA2-MIX for Access Point	85
Table 23 Security: WPA2 or WPA2-MIX for Wireless Client	86
Table 24 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX	87
Table 25 Wireless > RADIUS	90
Table 26 Wireless > MAC Filter	94
Table 27 IP Setup	98
Table 28 Private IP Address Ranges	99
Table 29 Remote Management: Telnet	104
Table 30 Remote Management: FTP	105
Table 31 Remote Management: WWW	106
Table 32 Remote Management: SNMP	107
Table 33 SNMP Traps	108
Table 34 SNMP Interface Index to Physical and Virtual Port Mapping	109
Table 35 Certificate	112
Table 36 View Log	116
Table 37 Log Settings	117
Table 38 System Maintenance Logs	119

Table 39 Log Categories and Available Settings	120
Table 40 Log Command List	120
Table 41 Association List	122
Table 42 Channel Usage	123
Table 43 Firmware Upload	123
Table 44 Restore Configuration	125
Table 45 Hardware Specifications	135
Table 46 Firmware Specifications	135
Table 47 Power over Ethernet Injector Specifications	137
Table 48 Power over Ethernet Injector RJ-45 Port Pin Assignments	137
Table 49 North American Plug Standards	139
Table 50 European Plug Standards	139
Table 51 United Kingdom Plug Standards	139
Table 52 Australia and New Zealand Plug Standards	139
Table 53 IEEE 802.11g	157
Table 54 Wireless Security Levels	158
Table 55 Comparison of EAP Authentication Types	161
Table 56 Wireless Security Relational Matrix	165
Table 57 Subnet Masks	174
Table 58 Subnet Masks	175
Table 59 Maximum Host Numbers	175
Table 60 Alternative Subnet Mask Notation	175
Table 61 Subnet 1	177
Table 62 Subnet 2	178
Table 63 Subnet 3	178
Table 64 Subnet 4	178
Table 65 Eight Subnets	178
Table 66 24-bit Network Number Subnet Planning	179
Table 67 16-bit Network Number Subnet Planning	179
Table 68 Auto Configuration by DHCP	182
Table 69 Configuration via SNMP	182
Table 70 Displaying the File Version	182
Table 71 Displaying the File Version	183
Table 72 Displaying the Auto Configuration Status	183
Table 73 Default Management IP Address	187
Table 74 Default User Name and Password	187
Table 75 Common Command Input Values	188
Table 76 CLI Shortcuts and Help	189

PART I

Introduction

- Introducing the ZyXEL Device (25)
- Status Screens (39)
- Introducing the Web Configurator (35)
- Tutorial (43)

Introducing the ZyXEL Device

This chapter introduces the main applications and features of the ZyXEL Device. It also discusses the ways you can manage your ZyXEL Device.

1.1 Introducing the ZyXEL Device

Your ZyXEL Device extends the range of your existing wired network without additional wiring, providing easy network access to mobile users.

It controls network access with MAC address filtering and RADIUS server authentication. It also provides a high level of network traffic security, supporting IEEE 802.1x, Wi-Fi Protected Access (WPA), WPA2 and WEP data encryption. Its Quality of Service (QoS) features allow you to prioritize time-sensitive or highly important applications such as VoIP.

Your ZyXEL Device is easy to install, configure and use. The embedded Web-based configurator enables simple, straightforward management and maintenance.

See the Quick Start Guide for instructions on how to make hardware connections.

1.2 Applications for the ZyXEL Device

The ZyXEL Device can be configured to use the following WLAN operating modes

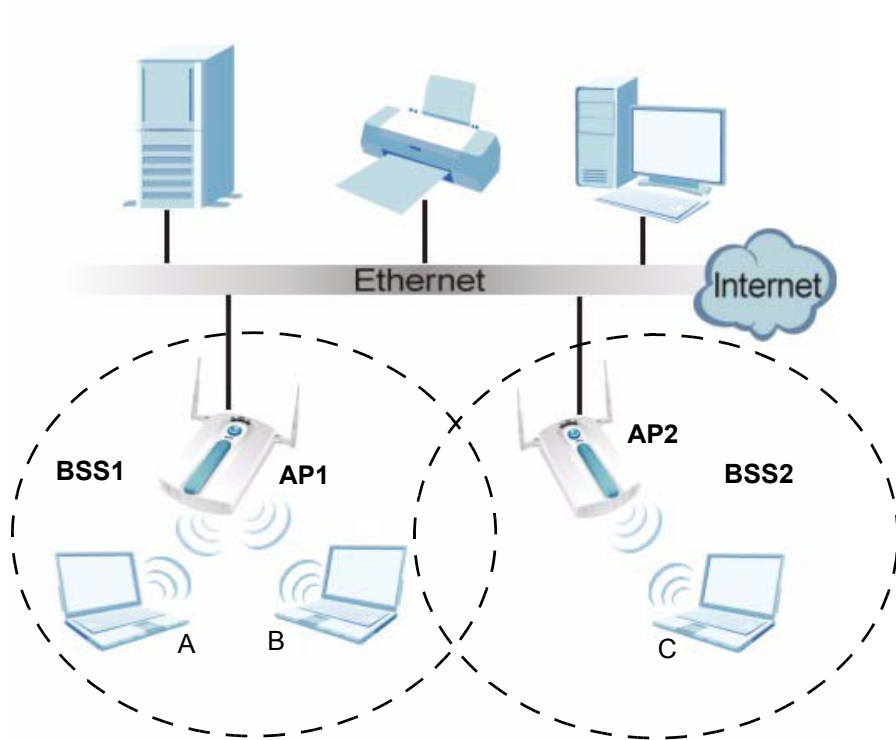
- 1 AP (Access Point)
- 2 Wireless Client
- 3 Bridge
- 4 AP + Bridge

Applications for each operating mode are shown below.

1.2.1 Access Point

The ZyXEL Device is an ideal access solution for wireless Internet connection. A typical Internet access application for your ZyXEL Device is shown as follows. Stations A, B and C can access the wired network through the ZyXEL Devices.

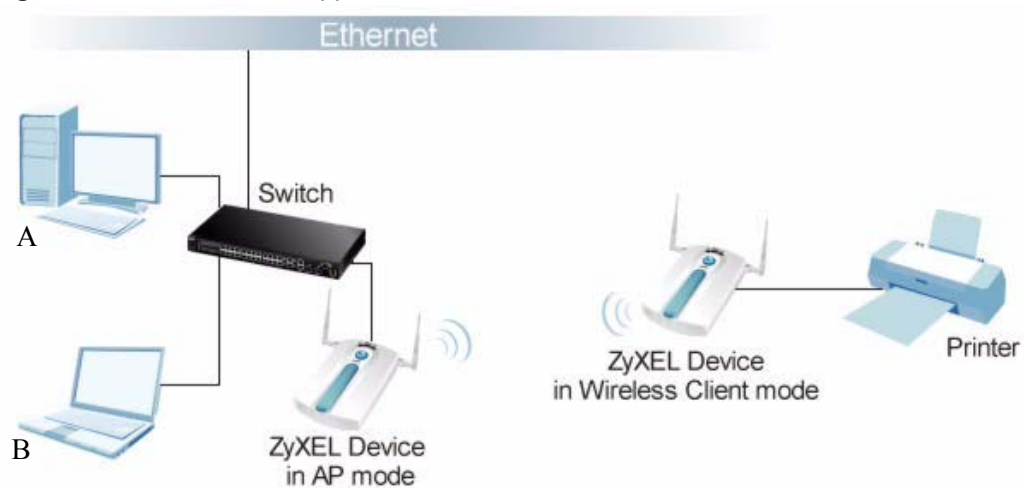
Figure 1 Access Point Application



1.2.2 Wireless Client

The ZyXEL Device can be used as a wireless client to communicate with an existing network. In the figure below, the printer can receive requests from the wired computer clients A and B via the ZyXEL Device in Wireless Client mode.

Figure 2 Wireless Client Application



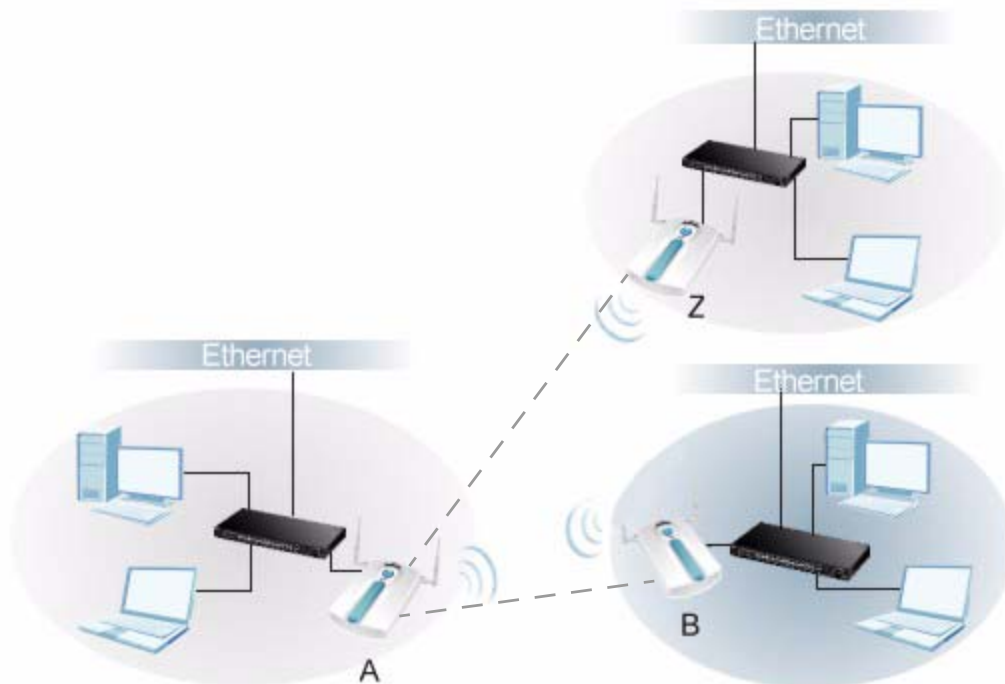
1.2.3 Bridge

The ZyXEL Device can act as a wireless network bridge and establish wireless links with other APs. In the figure below, the ZyXEL Devices (**A**, **B** and **Z**) are connected to independent wired networks and have a bridge connection (**A** can communicate with **B** and **Z**) at the same time. Security between bridged APs (the Wireless Distribution System or WDS) is independent of the security between the wired networks and their respective APs. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See [Section 6.4.3 on page 68](#) for more details.

Once the security settings of peer sides match one another, the connection between devices is made.

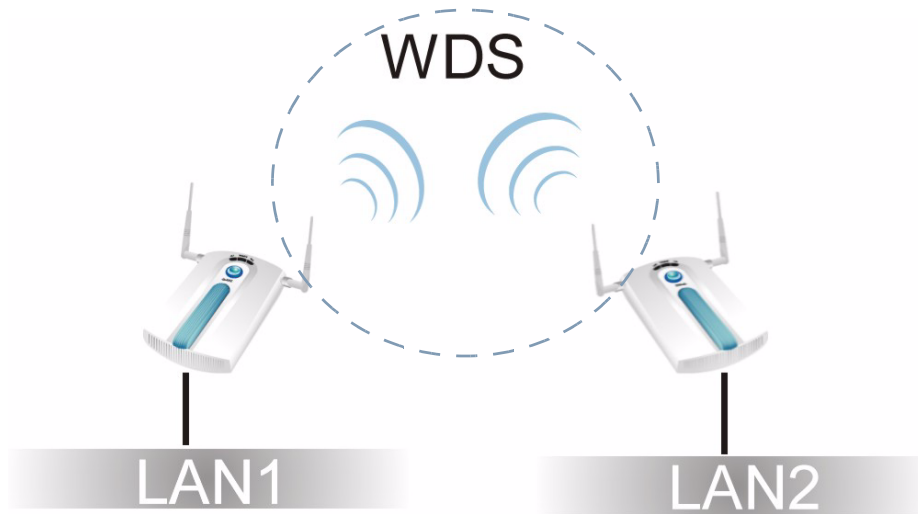
At the time of writing, WDS security is compatible with other ZyXEL NWA-series access points only. Refer to your other access point's documentation for details.

Figure 3 Bridge Application



In the example below, when both ZyXEL Devices are in Bridge mode, they form a WDS (Wireless Distribution System) allowing the computers in LAN 1 to connect to the computers in LAN 2.

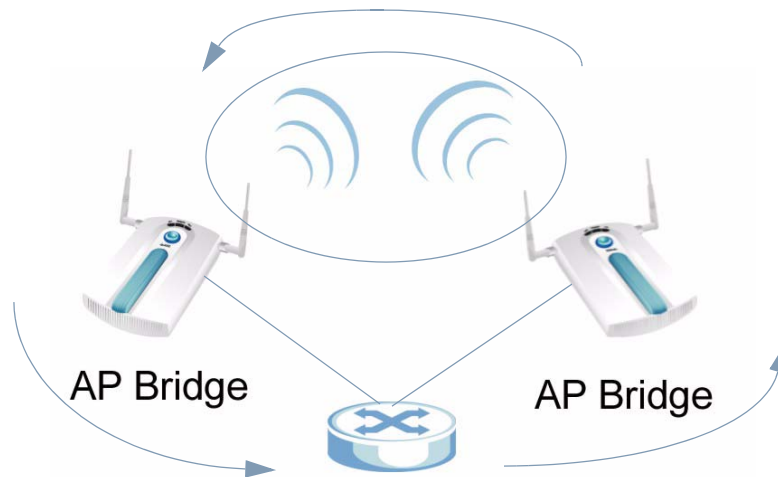
Figure 4 Bridging Example



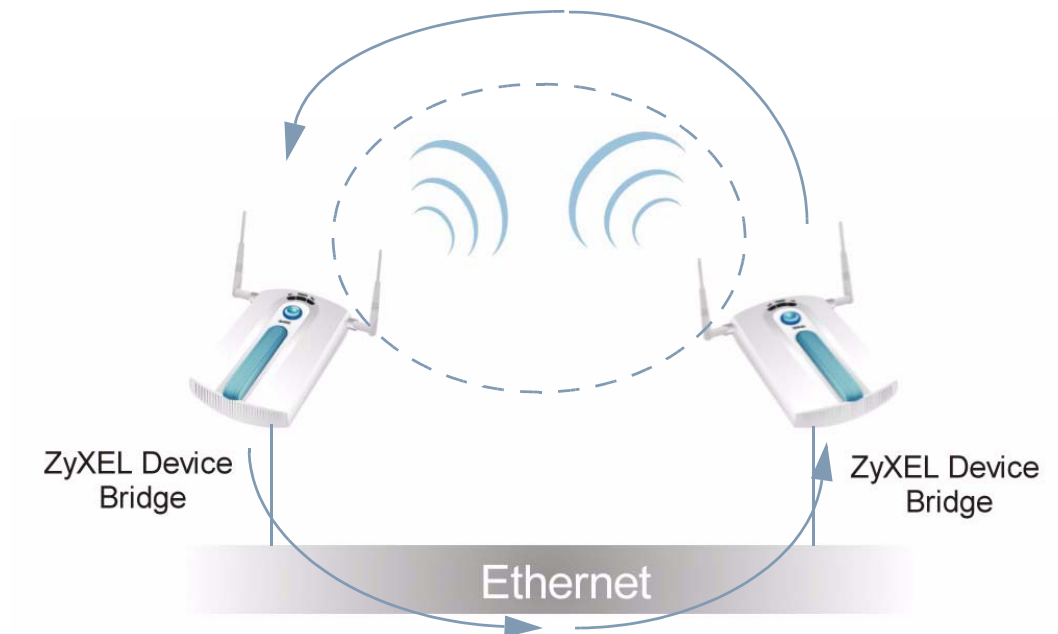
Be careful to avoid bridge loops when you enable bridging in the ZyXEL Device. Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and disruption of communications. The following examples show two network topologies that can lead to this problem:

- If two or more ZyXEL Devices (in bridge mode) are connected to the same hub.

Figure 5 Bridge Loop: Two Bridges Connected to Hub



- If your ZyXEL Device (in bridge mode) is connected to a wired LAN while communicating with another wireless bridge that is also connected to the same wired LAN.

Figure 6 Bridge Loop: Bridge Connected to Wired LAN

To prevent bridge loops, ensure that you enable STP in the **Wireless** screen or your ZyXEL Device is not set to bridge mode while connected to both wired and wireless segments of the same LAN.

1.2.4 AP + Bridge

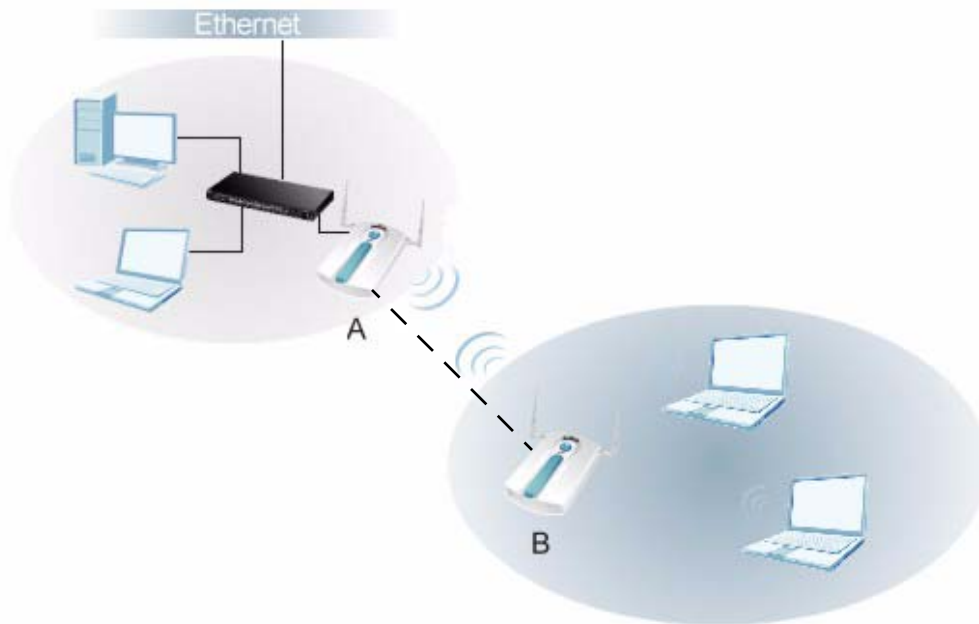
In **AP+Bridge** mode, the ZyXEL Device supports both AP and bridge connection at the same time.

Using AP + Bridge mode, your ZyXEL Device can extend the range of the WLAN. In the figure below, **A** and **B** act as AP + Bridge devices that forward traffic between associated wireless workstations and the wired LAN.

When the ZyXEL Device is in **AP+Bridge** mode, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See [Section 6.4.4 on page 70](#) for more details.

Unless specified, the term “security settings” refers to the traffic between the wireless stations and the ZyXEL Device.

Figure 7 AP + Bridge Application



1.3 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.
- CLI (Command Line Interface). Line commands are mostly used for troubleshooting by service engineers.
- FTP (File Transfer Protocol) for firmware upgrades.
- SNMP (Simple Network Management Protocol). The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.

1.4 Configuring Your ZyXEL Device's Security Features

Your ZyXEL Device comes with a variety of security features. This section summarizes these features and provides links to sections in the User's Guide to configure security settings on your ZyXEL Device. Follow the suggestions below to improve security on your ZyXEL Device and network.

1.4.1 Control Access to Your Device

Ensure only people with permission can access your ZyXEL Device.

- Control physical access by locating devices in secure areas, such as locked rooms. Most ZyXEL Devices have a reset button. If an unauthorized person has access to the reset button, they can then reset the device's password to its default password, log in and reconfigure its settings.

- Change any default passwords on the ZyXEL Device, such as the password used for accessing the ZyXEL Device's web configurator (if it has a web configurator). Use a password with a combination of letters and numbers and change your password regularly. Write down the password and put it in a safe place.
- Avoid setting a long timeout period before the ZyXEL Device's web configurator automatically times out. A short timeout reduces the risk of unauthorized person accessing the web configurator while it is left idle.
- See [Chapter 5 on page 53](#) for instructions on changing your password and setting the timeout period.
- Configure remote management to control who can manage your ZyXEL Device. See [Chapter 11 on page 101](#) for more information. If you enable remote management, ensure you have enabled remote management only on the IP addresses, services or interfaces you intended and that other remote management settings are disabled.

1.4.2 Wireless Security

Wireless devices are especially vulnerable to attack. If your ZyXEL Device has a wireless function, take the following measures to improve wireless security.

- Enable wireless security on your ZyXEL Device. Choose the most secure encryption method that all devices on your network support. See [Section 7.4 on page 77](#) for directions on configuring encryption. If you have a RADIUS server, enable IEEE 802.1x or WPA(2) user identification on your network so users must log in. This method is more common in business environments.
- Hide your wireless network name (SSID). The SSID can be regularly broadcast and unauthorized users may use this information to access your network. See [Section 6.4 on page 63](#) for directions on using the web configurator to hide the SSID.
- Enable the MAC filter to allow only trusted users to access your wireless network or deny unwanted users access based on their MAC address. See [Section 9.4 on page 94](#) for directions on configuring the MAC filter.

1.5 Good Habits for Managing the ZyXEL Device

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

- Change the password often. 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 won't have to totally re-configure the ZyXEL Device; you can simply restore your last configuration.

1.6 Hardware Connections

See your Quick Start Guide for information on making hardware connections.

1.7 LEDs

Figure 8 LEDs

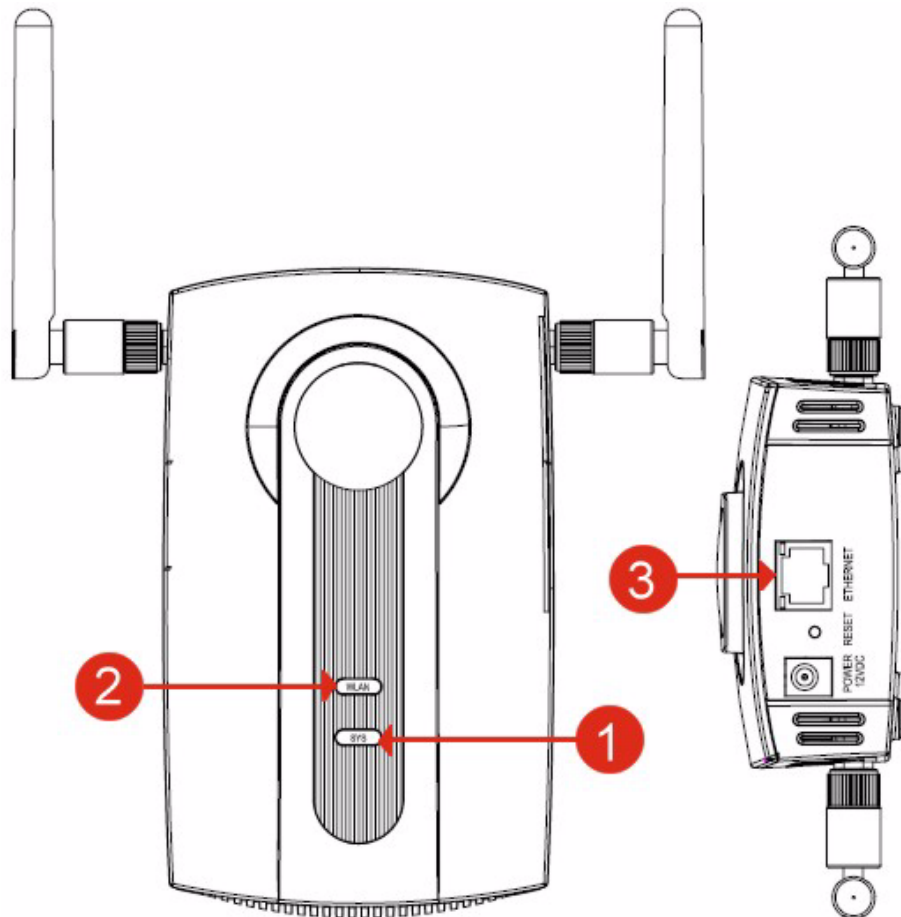


Table 1 LEDs

LABEL	LED	COLOR	STATUS	DESCRIPTION
1	SYS	Green	On	The ZyXEL Device is in AP + Bridge or Bridge mode, and has successfully established a Wireless Distribution System (WDS) connection.
		Amber	Flashing	The ZyXEL Device is starting up.
			Off	Either <ul style="list-style-type: none"> The ZyXEL Device is in Access Point or mode and is functioning normally. The ZyXEL Device is in AP+Bridge or Bridge mode and has not established a Wireless Distribution System (WDS) connection. or <ul style="list-style-type: none"> The ZyXEL Device is not receiving power.
2	WLAN	Green	On	The wireless adaptor WLAN is active.

Table 1 LEDs (continued)

LABEL	LED	COLOR	STATUS	DESCRIPTION
			Blinking	The wireless adaptor WLAN is active, and transmitting or receiving data.
			Off	The wireless adaptor WLAN is not active.
3	ETHERNET	Green	On	The ZyXEL Device has a 10 Mbps Ethernet connection.
			Blinking	The ZyXEL Device has a 10 Mbps Ethernet connection and is sending or receiving data.
		Yellow	On	The ZyXEL Device has a 100 Mbps Ethernet connection.
			Blinking	The ZyXEL Device has a 100 Mbps Ethernet connection and is sending/receiving data.
			Off	The ZyXEL Device does not have an Ethernet connection.

Introducing the Web Configurator

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

2.1 Accessing the Web Configurator

- 1 Make sure your 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 "192.168.1.2" as the URL (default).
- 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) then click **Apply**. Alternatively, click **Ignore**.



If you do not change the password, the following screen appears every time you login.

Figure 9 Change Password Screen

Use the screen to change password.

New Password

Retype to Confirm

You should now see the **Status** screen. See [Chapter 2 on page 35](#) for details about the **Status** screen.



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.

2.2 Resetting the ZyXEL Device

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button. This replaces the current configuration file with the factory-default configuration file. This means that you will lose all the settings you previously configured. The password will be reset to 1234.

2.2.1 Methods of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in two ways:

Use the **RESET** button to upload the default configuration file. Hold this button in for about 10 seconds (the lights will begin to blink). Use this method for cases when the password or IP address of the ZyXEL Device is not known.

Use the web configurator to restore defaults (refer to [Section 14.7 on page 124](#)).

2.3 Navigating the Web Configurator

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

Check the status bar at the bottom of the screen when you click **Apply** or **OK** to verify that the configuration has been updated.

Figure 10 Status Screen of the Web Configurator

ZyXEL

Status

Refresh Interval : None Refresh Now

System Information

Device Name : ZyXEL
 Operation Mode : AP
 MAC Address : 00:60:b3:aa:bb:cc
 Firmware Version : NWA1100 V1.00 (AAQ.0)

Ethernet Information :

- IP Address : 192.168.1.2
- Subnet Mask : 255.255.255.0
- Gateway IP Address : 0.0.0.0

WLAN Information :

- SSID : ZyXEL NWA1100
- Channel : 6
- MAC Filter : Disable
- Security Mode : Disable

System Resources

System Up Time : 2000-1-1 00:00:00

System Resources :

- CPU Usage : 6%
- Memory Usage : 66%

Interface Status

Interface	Status	Channel	Rate
LAN	Up		100M/Full
WLAN	Up	6	54M

System Status

Statistics Association List View Log

Status Ready

- Click the links on the left of the screen to configure advanced features such as **SYSTEM** (General, Password and Time), **WIRELESS** (Wireless Settings, Security, RADIUS, MAC Filter), **IP**, **REMOTE MGNT** (Telnet, FTP, WWW and SNMP), **CERTIFICATES**, and **LOGS** (View Log and Log Settings).
- Click **MAINTENANCE** to view information about your ZyXEL Device or upgrade configuration and firmware files. Maintenance features include **Association List**, **Channel Usage**, **F/W (firmware) Upload**, **Configuration File** (Backup, Restore and Default) and **Restart**.
- Click **LOGOUT** at any time to exit the web configurator.

Status Screens

The **Status** screens display when you log into the ZyXEL Device, or click **Status** in the navigation menu.

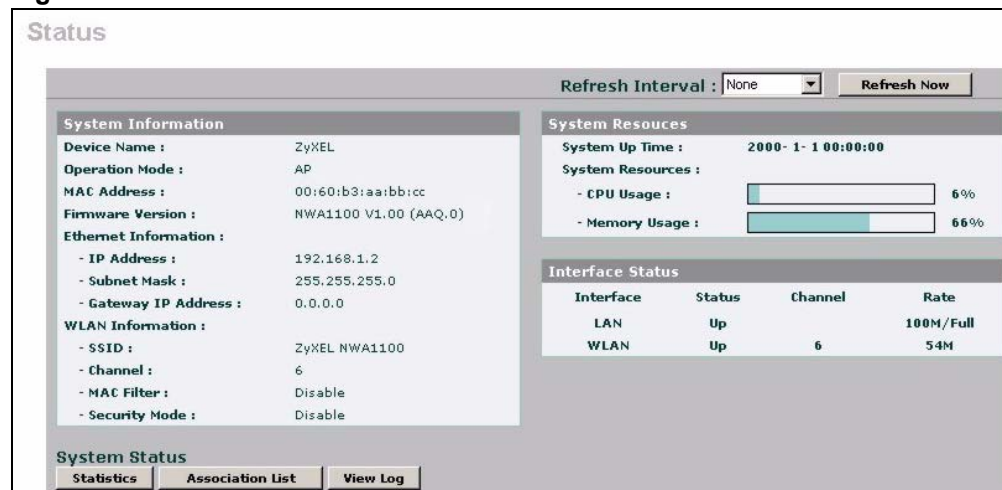
Use the **Status** screens to look at the current status of the device, system resources, and interfaces. The **Status** screens also provide detailed information about system statistics, associated wireless clients, and logs.

3.1 The Status Screen

Use this screen to get a quick view of system, Ethernet, WLAN and other information regarding your ZyXEL Device.

Click **Status**. The following screen displays.

Figure 11 The Status Screen



The following table describes the labels in this screen.

Table 2 The Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the ZyXEL Device to update this screen.
Refresh Now	Click this to update this screen immediately.
System Information	

Table 2 The Status Screen

LABEL	DESCRIPTION
Device Name	This field displays the ZyXEL Device system name. It is used for identification. You can change this in the System > General screen's Device Name field.
Operation Mode	This field displays the current operating mode of the first wireless module (AP, Wireless Client, Bridge or AP+Bridge). You can change the operating mode in the Wireless > Wireless Settings screen.
MAC Address	This displays the MAC (Media Access Control) address of the ZyXEL Device on the LAN. Every network device has a unique MAC address which identifies it across the network.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. You can change the firmware version by uploading new firmware in Maintenance > F/W Upload .
Ethernet Information	
IP Address	This field displays the current IP address of the ZyXEL Device on the network.
Subnet Mask	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.
Gateway IP Address	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN port. The gateway helps forward packets to their destinations.
WLAN Information	
SSID	This field displays the SSID (Service Set Identifier).
Channel	The channel or frequency used by the ZyXEL Device to send and receive information.
MAC Filter	Media Access Control filtering checks incoming frames based on MAC (Media Access Control) address(es) that you specify.
Security Mode	This displays the security mode the ZyXEL Device is using.
System Resources	
System Up Time	This field displays the elapsed time since the ZyXEL Device was turned on.
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently being used. The higher the CPU usage, the more likely the ZyXEL Device is to slow down.
Memory Usage	This field displays what percentage of the ZyXEL Device's volatile memory is currently in use. The higher the memory usage, the more likely the ZyXEL Device is to slow down. Some memory is required just to start the ZyXEL Device and to run the web configurator.
Interface Status	
Interface	This column displays each interface of the ZyXEL Device.
Status	This field indicates whether or not the ZyXEL Device is using the interface. For each interface, this field displays Up when the ZyXEL Device is using the interface and Down when the ZyXEL Device is not using the interface.
Channel	Click this to see which wireless channels are currently in use in the local area. See Section 14.5 on page 122 .
Rate	For the LAN port this displays the port speed and duplex setting. For the WLAN interface, it displays the downstream and upstream transmission rate or N/A if the interface is not in use.

Table 2 The Status Screen

LABEL	DESCRIPTION
LAN	This field displays the number of wireless clients currently associated to the first wireless module. Each wireless module supports up to 32 concurrent associations.
WLAN	This field displays the number of wireless clients currently associated to the second wireless module. Each wireless module supports up to 32 concurrent associations.
System Status	
Statistics	Click this link to view port status and packet specific statistics. See Section 3.1.1 on page 41 .
Association List	Click this to see a list of wireless clients currently associated to each of the ZyXEL Device's wireless modules. See Section 14.4 on page 121 .
View Log	Click this to see a list of logs produced by the ZyXEL Device. See Chapter 13 on page 115 .

3.1.1 System Statistics Screen

Use this screen to view read-only information, including 802.11 Mode, Channel ID, Retry Count and FCS Error Count. Also provided is the "poll interval". The **Poll Interval** field is configurable. The fields in this screen vary according to the current wireless mode of each WLAN adaptor.

Click **Status > Show Statistics**. The following screen pops up.

Figure 12 System Status: Show Statistics

Description	802.11 Mode	Channel ID	RX PKT	TX PKT	Retry Count	FCS Error
ZyXEL	802.11b+g	6	8139	22175	18761	36

Poll Interval : (0-65534) sec

The following table describes the labels in this screen.

Table 3 System Status: Show Statistics

LABEL	DESCRIPTION
Description	
802.11 Mode	This field shows which mode (802.11b Only, 802.11g Only, 802.11b+g) the ZyXEL Device is using.
Channel ID	Click this to see which wireless channels are currently in use in the local area. See Section 14.5 on page 122 .
RX PKT	This is the number of received packets on this port.
TX PKT	This is the number of transmitted packets on this port.
Retry Count	This is the total number of retries for transmitted packets (TX).
FCS Error	This is the ratio percentage showing the total number of checksum error of received packets (RX) over total RX.

Tutorial

This chapter first provides an overview of how to configure the wireless LAN on your ZyXEL Device, and then gives step-by-step guidelines showing how to configure your ZyXEL Device for some example scenarios.

4.1 How to Configure the Wireless LAN

This section illustrates how to choose which wireless operating mode to use on the ZyXEL Device and how to set up the wireless LAN in each wireless mode. See [Section 4.1.3 on page 44](#) for links to more information on each step.

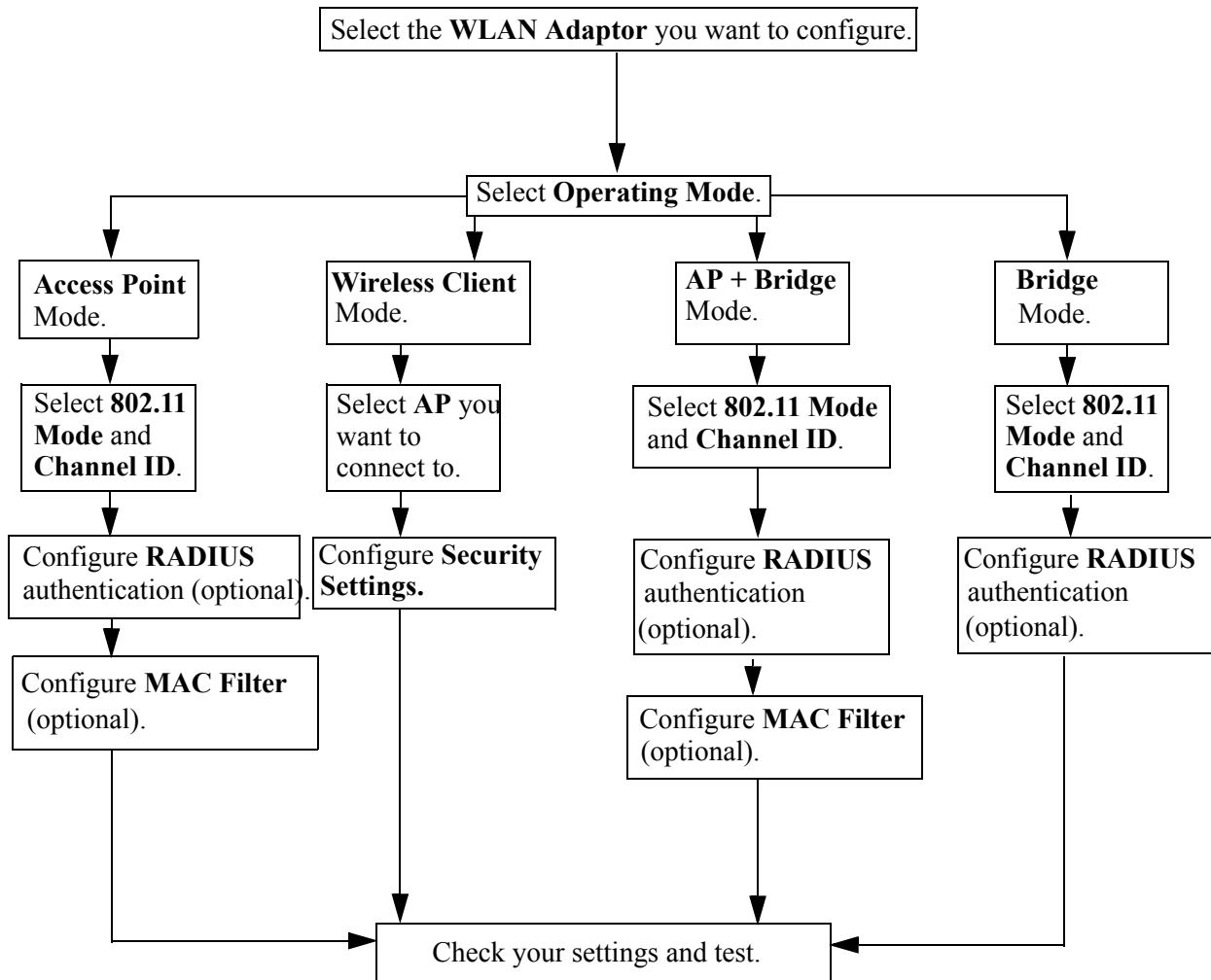
4.1.1 Choosing the Wireless Mode

- Use **Access Point** operating mode if you want to allow wireless clients to access your wired network, all using the same security and Quality of Service (QoS) settings. See [Section 1.2.1 on page 25](#) for details.
- Use **Wireless Client** operating mode if you want to use the ZyXEL Device to access a wireless network. See [Section 1.2.2 on page 26](#) for details.
- Use **Bridge** operating mode if you want to use the ZyXEL Device to communicate with other access points. See [Section 1.2.2 on page 26](#) for details.
The ZyXEL Device is a bridge when other APs access your wired Ethernet network through the ZyXEL Device.
- Use **AP + Bridge** operating mode if you want to use the ZyXEL Device as an access point (see above) while also communicating with other access points. See [Section 1.2.4 on page 29](#) for details.

4.1.2 Wireless LAN Configuration Overview

The following figure shows the steps you should take to configure the wireless settings according to the operating mode you select. Use the Web Configurator to set up your ZyXEL Device's wireless network (see your Quick Start Guide for information on setting up your ZyXEL Device and accessing the Web Configurator).

Figure 13 Configuring Wireless LAN



4.1.3 Further Reading

Use these links to find more information on the steps:

- Selecting a **WLAN Adaptor**: see [Section 6.4.1 on page 63](#).
- Choosing **802.11 Mode**: see [Section 6.4.1 on page 63](#).
- Choosing a wireless **Channel ID**: see [Section 6.4.1 on page 63](#).
- Choosing a **Security** mode: see [Section 7.4.1 on page 78](#).
- Configuring an external **RADIUS** server: see [Section 8.4 on page 90](#).
- Configuring **MAC Filtering**: see [Section 9.1 on page 93](#).

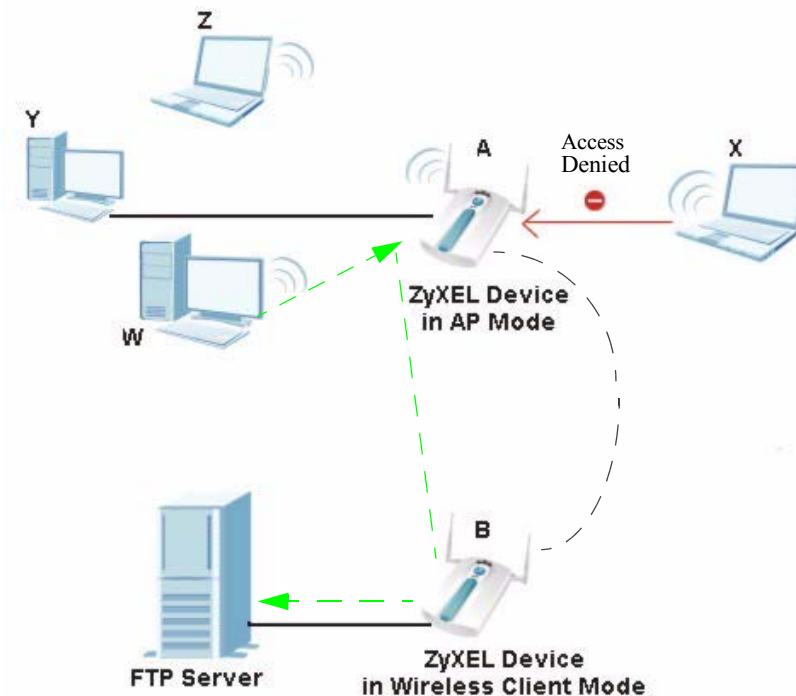
4.2 ZyXEL Device Setup in Wireless Client Mode

This example shows you how to restrict wireless access to your ZyXEL Device.

4.2.1 Scenario

In the figure below, there are two ZyXEL Devices (**A** and **B**) in the network. **A** is in Access Point (AP) mode while **B** is in Wireless Client mode. Station **B** is connected to a File Transfer Protocol (FTP) server. You want only specified wireless clients to be able to access station **B**. You also want to allow wireless traffic between **B** and wireless clients connected to **A** (**W**, **Y** and **Z**). Other wireless devices (**X**) must not be able to connect to the FTP server.

Figure 14 FTP Server Connected to a Wireless Client



4.2.2 Configuring the ZyXEL Device in Access Point Mode

Before setting up the ZyXEL Device as a wireless client (**B**), you need to make sure there is an access point to connect to. Use the Ethernet port on your ZyXEL Device to configure it via a wired connection.

Open the Web Configurator and go to the **Wireless > Wireless Settings** screen.

Figure 15 Access Point Mode Wireless Settings

Wireless Settings	Security	Radius	MAC Filter
Basic Settings			
Operation Mode	AP		
SSID	ZyXEL NWA1100 A		(max.32 printable characters) <input type="checkbox"/> Hide SSID
Channel	6		
Wireless Mode	802.11b+g		
Advanced Settings			
Beacon Interval	100 (25-1000)		
Intra-BSS Traffic	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
DTIM Interval	1 (1~255)		
WMM	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Number of Wireless Stations Allowed to Associate	32 (1~32)		
Radio Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Output Power Management	Full		
Preamble Type	Dynamic		
RTS/CTS Threshold	2346 (1~2346)		
Fragmentation Threshold	2346 (1~2346)		

- 1 Set the **Operation Mode** to **AP**.
- 2 Enter an **SSID** name, such as “NWA-1100 A”.
- 3 Choose the channel you want the ZyXEL Device to use.
- 4 Select the **Wireless Mode**.
- 5 Set the **Intra-BSS Traffic** to **Enable**.
- 6 Go to **Wireless > Security** to configure the ZyXEL Device to use WPA-PSK security mode.

Figure 16 Access Point Mode Security Settings

Wireless Settings	Security	Radius	MAC Filter
Security Settings			
Security Mode	WPA-PSK		
Pre-Shared Key	ThePreSharedKey (8~63 ASCII characters)		
<input type="button" value="Apply"/> <input type="button" value="Reset"/>			

4.2.3 Configuring the ZyXEL Device in Wireless Client Mode

Your ZyXEL Device should have a wired connection before it can be set to wireless client operating mode. Connect your ZyXEL Device to the FTP server. Open the Web Configurator ZyXEL Device and go to the **Wireless > Wireless Settings** screen. Follow these steps to configure Station B.

- 1 Select **Wireless Client** as **Operating Mode**. Wait for the screen to refresh.

- 2 You should now see a tab that says **Site Survey** (refer to [Figure 18](#)). Click on this. A window should pop up which contains a list of all available wireless devices within your ZyXEL Device's range. Copy the SSID of the AP you want your wireless client to connect to (refer to [Figure 19](#)).
- 3 For this example, you want to connect to the access point, A. The SSID that you should copy is **ZyXEL NWA-1100 A** (refer to [Figure 15](#) to check the SSID of Station A).
- 4 Go back to the screen in [Figure 17](#). In the **SSID** field, enter **ZyXEL NWA-1100 A** (refer to [Figure 18](#)).
- 5 Set the **Wireless Mode** to the same one set for the access point. **Click Apply**.

Figure 17 Wireless Client Mode Wireless Settings

Wireless Settings	Security	Radius	MAC Filter
Basic Settings			
Operation Mode	Wireless Client		
SSID	<input type="text" value=""/> (max. 32 printable characters)		Site Survey
Wireless Mode	802.11b+g		
Advanced Settings			
MAC Address Clone	<input checked="" type="radio"/> Auto <input type="radio"/> Manual	00:1c:c4:84:e0:4b	
Radio Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Output Power Management	Full		
Preamble Type	Dynamic		
RTS/CTS Threshold	2346 (1~2346)		
Fragmentation	2346 (256~2346)		
Rates Configuration			
Rate	Configuration	Rate	Configuration
1 Mbps	Basic	2 Mbps	Basic
5.5 Mbps	Basic	11 Mbps	Basic
6 Mbps	Optional	9 Mbps	Optional
12 Mbps	Optional	18 Mbps	Optional
24 Mbps	Optional	36 Mbps	Optional
48 Mbps	Optional	54 Mbps	Optional
<input type="checkbox"/> Enable Antenna Diversity <input checked="" type="checkbox"/> Enable Spanning Tree Protocol(STP)			
<input type="button" value="Apply"/> <input type="button" value="Reset"/>			

Figure 18 Site Survey

SSID	BSSID	Channel	Wireless Mode	Security	Signal Strength
ZyXEL_MIS	00:13:49:26:C7:05	1	802.11g only	WEP	60%
ZyXEL_MIS	00:00:AA:77:00:54	6	802.11g only	none	71%
ZyXEL_MIS	00:13:49:26:C7:05	6	802.11g only	WEP	60%
ZyXEL NWA-1100 A	06:13:49:DF:42:A8	6	802.11g only	none	90%
USG280_Flashed	00:13:49:AF:40:8F	6	802.11g only	WEP	71%
USG280_Flashed_01	00:13:49:AF:40:8F	6	802.11g only	none	72%
USG280_Flashed_02	00:13:49:AF:40:8F	6	802.11g only	WPA-PSK	72%
6072-wifi	08:19:CE:86:D7:7B	3	802.11g only	WPA-PSK	60%
FOA_3295_DEMAREY2	08:19:CE:86:D7:7B	3	802.11g only	none	56%
NSO480_NORM	00:19:CB:5A:28:6A	6	802.11g only	WPA-PSK	53%
Casper_test	08:19:CE:86:D7:7B	6	802.11g only	WPA	56%
ZyXEL	08:19:CE:77:88:11	6	802.11g only	none	55%
ZyXEL_MIS	00:13:49:26:C7:05	6	802.11g only	WEP	67%
WALL-Fixed-Router	00:13:49:7A:5F:01	3	802.11g only	none	55%

Figure 19 Wireless Client Mode

Wireless Settings | Security | Radius | MAC Filter

Basic Settings

Operation Mode: Wireless Client

SSID: ZyXEL NWA-1100 A (max.32 printable characters) Site Survey

Wireless Mode: 802.11b+g

Advanced Settings

MAC Address Clone: Auto Manual 00:1c:c4:84:e0:4b

Radio Enable: Yes No

Output Power Management: Full

Preamble Type: Dynamic

RTS/CTS Threshold: 2346 (1-2346)

Fragmentation: 2346 (256-2346)

Rates Configuration

Rate	Configuration	Rate	Configuration
1 Mbps	Basic	2 Mbps	Basic
5.5 Mbps	Basic	11 Mbps	Basic
6 Mbps	Optional	9 Mbps	Optional
12 Mbps	Optional	18 Mbps	Optional
24 Mbps	Optional	36 Mbps	Optional
48 Mbps	Optional	54 Mbps	Optional

Enable Antenna Diversity

Enable Spanning Tree Protocol(STP)

Apply Reset

- Go to **Wireless > Security** to configure the ZyXEL Device to use WPA-PSK security mode.

Figure 20 Wireless Client Mode Security Settings

The screenshot shows the 'Security Settings' section of the ZyXEL Web Configurator. It has four tabs: 'Wireless Settings', 'Security', 'Radius', and 'MAC Filter'. The 'Security' tab is active. Under 'Security Settings', there are two fields: 'Security Mode' with a dropdown menu set to 'WPA-PSK', and 'Pre-Shared Key' with a text input field containing 'ThePreSharedKey' and a note '(8-63 ASCII characters)'. Below these fields are 'Apply' and 'Reset' buttons. A red oval highlights the 'Security Mode' dropdown and the 'Pre-Shared Key' text field.

- 7 One way to ensure that only specified wireless clients can access the FTP server is by enabling MAC filtering on the ZyXEL Device. See [Chapter 9 on page 93](#) for more information on the MAC Filter screen.
- 8 Still in the Web Configurator, go to **Wireless > MAC Filter**. Click on **Active** then highlight **Allow the following MAC Address to associate**. Enter the MAC Addresses of the wireless clients (**W**, **Y** and **Z**) you want to associate with the ZyXEL Device. Click **Apply**.

Figure 21 Wireless Client MAC Filtering

The screenshot shows the 'MAC Address Filter' section of the ZyXEL Web Configurator. It has four tabs: 'Wireless Settings', 'Security', 'Radius', and 'MAC Filter'. The 'MAC Filter' tab is active. Under 'MAC Address Filter', there is a checkbox for 'Active' which is checked. Below it are two radio button options: 'Allow the following MAC Address to associate' (selected) and 'Deny the following MAC address to associate'. Below these options is a table with columns for '#', 'MAC Address', '#', and 'MAC Address'. The table contains three rows of data, representing clients W, Y, and Z.

#	MAC Address	#	MAC Address
1	11:AF:FA:22:00:AA	33	ZZ:AA:YY:BB:WA:00
2	00:FA:FA:CC:BB:11	34	AB:CD:EF:GH:IJ:KL

After following this tutorial, you should now have the same setup as shown in [Figure 14](#).

4.2.4 Testing the Connection and Troubleshooting

This section discusses how you can check if you have correctly configured your network setup as described in this tutorial.

- Try accessing the FTP server from wireless clients **W**, **Y** or **Z**. Test if you can send or retrieve a file. If you cannot establish a connection with the FTP server, do the following steps.
 - 1 Make sure **W**, **Y** and **Z** use the same wireless security settings as **A** and can access **A**.
 - 2 Make sure **B** uses the same wireless and wireless security settings as **A** and can access **A**.
 - 3 Make sure intra-BSS traffic is enabled on **A**.
- Try accessing the FTP server from **X**. If you are able to access the FTP server, do the following.
 - 1 Make sure MAC filtering is enabled.
 - 2 Make sure **X**'s MAC address is not entered in the list of allowed devices.

PART II

The Web Configurator

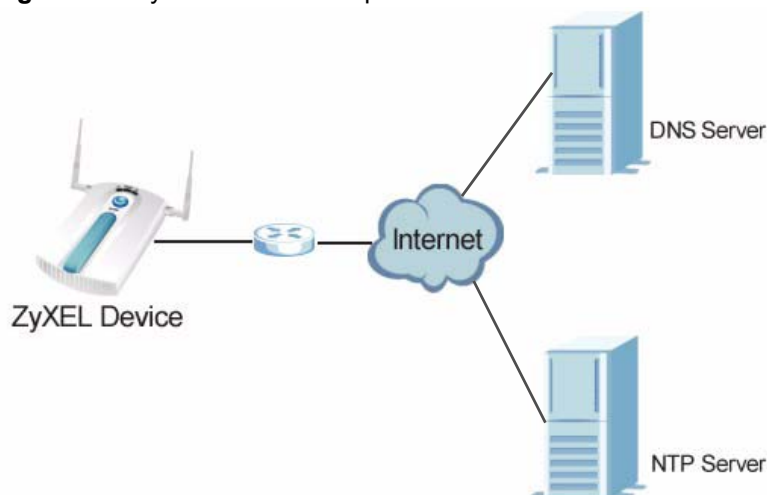
System Screens (53)
Wireless Settings Screen (61)
Wireless Security Screen (75)
RADIUS Screen (89)
MAC Filter Screen (93)
IP Screen (97)
Remote Management (101)
Certificate Screen (111)
Log Screens (115)
Maintenance (121)
Troubleshooting (129)

System Screens

5.1 Overview

This chapter provides information and instructions on how to identify and manage your ZyXEL Device over the network.

Figure 22 ZyXEL Device Setup



In the figure above, the ZyXEL Device connects to a Domain Name Server (DNS) server to avail of a domain name. It also connects to an Network Time Protocol (NTP) server to set the time on the device.

5.2 What You Can Do in the System Screens

- Use the **System > General** screen (see [Section on page 55](#)) to specify the **Device name** and **Administrator Inactivity Timer** value. You can also configure your **System DNS Servers** in this screen.
- Use the **System > Password** screen (see [Section 5.4.1 on page 56](#)) to manage the password for your ZyXEL Device.
- Use the **System > Time Setting** screen (see [Section 5.5 on page 56](#)) to change your ZyXEL Device's time and date. This screen allows you to configure the ZyXEL Device's time based on your local time zone.

5.3 What You Need To Know About the System Screens

IP Address Assignment

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

Table 4 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

You can obtain your IP address from the IANA, from an ISP or have it assigned by 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.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, 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, 192.168.1.2, for your 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 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 device unless you are instructed to do otherwise.

5.4 General Screen

Use the General screen to identify your ZyXEL Device over the network. Click **System > General**. The following screen displays.

Figure 23 System: General

The following table describes the labels in this screen.

Table 5 System: General

LABEL	DESCRIPTION
Device Settings	
Device Name	Type a descriptive name to identify the ZyXEL Device in the Ethernet network. This name can be up to 15 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted.
Administrator Inactivity Timer	Type how many minutes a management session (via web configurator) 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).
System DNS Servers	
First DNS Server Second DNS Server Third DNS Server	The field to the right displays the (read-only) DNS server IP address that the DHCP assigns. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. The default setting is None .

Table 5 System: General

LABEL	DESCRIPTION
Apply	Click Apply to save your changes.
Reset	Click Reset to reload the previous configuration for this screen.

5.4.1 Password Screen

Use this screen to control access to your ZyXEL Device by assigning a password to it. Click **System > Password**. The following screen displays.

Figure 24 System: Password.

The following table describes the labels in this screen.

Table 6 System: Password

LABEL	DESCRIPTIONS
Password Setup	
Current Password	Type in your existing system password ("1234" is the default password).
New Password	Type your new system password (max 19 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.
Apply	Click Apply to save your changes.
Reset	Click Reset to reload the previous configuration for this screen.

5.5 Time Screen

Use this screen to change your ZyXEL Device's time and date, click **System > Time**. The following screen displays.

Figure 25 System: Time

General	Password	Time
Current Time and Date		
Current Date	2000 1 2	(YY:MM:DD)
Current Time	0 25 51	(HH:MM:SS)
Time and Date Setup		
<input type="checkbox"/> Enable NTP client update		
<input type="radio"/> 192.5.41.41 - North America <input checked="" type="checkbox"/> Random		
<input checked="" type="radio"/> User Defined Time Server 0.0.0.0		
Time Zone Setup		
Time Zone: (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London		
Daylight Saving Setup		
<input type="checkbox"/> Daylight Savings		
Start Date	First Sunday of January (2000-1-2)	at 0 o'clock
End Date	First Sunday of January (2000-1-2)	at 0 o'clock
<input type="button" value="Apply"/> <input type="button" value="Reset"/>		

The following table describes the labels in this screen.

Table 7 System: Time

LABEL	DESCRIPTION
Current Time and Date	
Current Date	This field displays the last updated date from the time server.
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 (if configured).
Time and Date Setup	
Enable NTP client update	Select this to have the ZyXEL Device use the predefined list of Network Time Protocol (NTP) servers.
Random	Select this to have the ZyXEL Device select which NTP server to use.
User Defined Time Server	Enter the IP address or URL 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 Saving Setup	
Daylight Savings	Select this option if you use daylight savings time. Daylight saving 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.

Table 7 System: Time

LABEL	DESCRIPTION
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected Enable Daylight Saving. The at 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 at 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 Enable Daylight Saving. 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 at 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.
Reset	Click Reset to reload the previous configuration for this screen.

5.6 Technical Reference

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

5.6.1 Pre-defined NTP Time Servers List

When you turn on the ZyXEL Device for the first time, the date and time start at 2000-01-01 00:00:00. When you select **Auto** in the **System > Time Setting** screen, the ZyXEL Device then attempts to synchronize with one of the following pre-defined list of NTP time servers.

The ZyXEL Device continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 8 Default Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil

Table 8 Default Time Servers (continued)

ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

When the ZyXEL Device uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the ZyXEL Device goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

Wireless Settings Screen

6.1 Overview

This chapter discusses the steps to configure the Wireless Settings screen on the ZyXEL Device. It also introduces the wireless LAN (WLAN) and some basic scenarios.

Figure 26 Wireless Mode



In the figure above, the ZyXEL Device allows access to another bridge device (A) and a notebook computer (B) upon verifying their settings and credentials. It denies access to other devices (C and D) with configurations that do not match those specified in your ZyXEL Device.

6.2 What You Can Do in the Wireless Settings Screen

Use the **Wireless > Wireless Settings** screen (see [Section 6.4 on page 63](#)) to configure the ZyXEL Device to operate in AP (Access Point), Wireless Client, Bridge or AP + Bridge.

6.3 What You Need To Know About Wireless Settings Screen

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.

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).

Operating Mode

The ZyXEL Device can run in four operating modes as follows:

- **AP (Access Point).** The ZyXEL Device is wireless access point that allows wireless communication to other devices in the network.
- **Wireless Client.** The ZyXEL Device acts as a wireless client to access a wireless network.
- **Bridge.** The ZyXEL Device acts as a wireless network bridge and establishes wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode. The ZyXEL Device can establish up to five wireless links with other APs.
- **AP+Bridge Mode.** The ZyXEL Device functions as a bridge and access point simultaneously.

Refer to [Chapter 1 on page 25](#) for illustrations of these wireless applications.

SSID

The SSID (Service Set Identifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID.

Normally, the ZyXEL Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the ZyXEL Device 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 wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

Channel

A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference.

Wireless Mode

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. Your ZyXEL Device can support **802.11b Only**, **802.11g Only** and **802.11b+g**.

6.4 Wireless Settings Screen

Use this screen to choose the operating mode for your ZyXEL Device. Click **Wireless > Wireless Settings**. The screen varies depending upon the operating mode you select.

6.4.1 Access Point Mode

Use this screen to use your ZyXEL Device as an access point. Select **AP** as the **Operation Mode**. The following screen displays.

Figure 27 Wireless: Access Point

Wireless Settings	Security	Radius	MAC Filter
Basic Settings			
Operation Mode	AP		
SSID	ZyXEL NWA1100 (max.32 printable characters)		<input type="checkbox"/> Hide SSID
Channel	6		
Wireless Mode	802.11b+g		
Advanced Settings			
Beacon Interval	100 (25-1000)		
Intra-BSS Traffic	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
DTIM Interval	1 (1-255)		
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Number of Wireless Stations Allowed to Associate	32 (1-32)		
Radio Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Output Power Management	Full		
Preamble Type	Dynamic		
RTS/CTS Threshold	2346 (1-2346)		
Fragmentation	2346 (256-2346)		
Rates Configuration			
Rate	Configuration	Rate	Configuration
1 Mbps	Basic	2 Mbps	Basic
5.5 Mbps	Basic	11 Mbps	Basic
6 Mbps	Optional	9 Mbps	Optional
12 Mbps	Optional	18 Mbps	Optional
24 Mbps	Optional	36 Mbps	Optional
48 Mbps	Optional	54 Mbps	Optional
<input type="checkbox"/> Enable Antenna Diversity			
<input checked="" type="checkbox"/> Enable Spanning Tree Protocol(STP)			
<input type="button" value="Apply"/> <input type="button" value="Reset"/>			

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

Table 9 Wireless: Access Point

LABEL	DESCRIPTION
Basic Settings	
Operation Mode	Select AP from the drop-down list.
SSID	<p>The SSID (Service Set Identifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Select an SSID Profile from the drop-down list box.</p> <p>Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID 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.</p>
Hide SSID	If you hide the SSID, then the ZyXEL Device cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of "hiding" the ZyXEL Device may be inconvenience for some valid WLAN clients.
Channel	<p>Set the operating frequency/channel depending on your particular region.</p> <p>To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box. Click MAINTENANCE and then the Channel Usage tab to open the Channel Usage screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.</p> <p>To have the ZyXEL Device automatically select a channel, click Scan instead.</p>
Wireless Mode	<p>Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device.</p> <p>Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device.</p> <p>Select 802.11b+g to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.</p>
Advanced Settings	
Beacon Interval	<p>When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in lowpower mode before waking up to handle the beacon. This value can be set from 20ms to 1000ms. A high value helps save current consumption of the access point.</p>
Intra-BSS Traffic	<p>When Intra-BSS is enabled, wireless client can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client can still access the wired network but cannot communicate with each other.</p>
DTIM Interval	<p>Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 100.</p>
WMM	<p>Select this to turn on WMM QoS (Wireless MultiMedia Quality of Service). The ZyXEL Device assigns priority to packets based on the IEEE 802.1q or DSCP information in their headers. If a packet has no WMM information in its header, it is assigned the default priority.</p>

Table 9 Wireless: Access Point

LABEL	DESCRIPTION
Number of Wireless Stations Allowed to Associate	Specify how many wireless stations can associate with your ZyXEL Device.
Radio Enable	Select Yes to enable WLAN radio, and No to turn it off. The ZyXEL Device cannot be accessed wirelessly if radio is turned off.
Output Power Management	Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power of the ZyXEL Device to reduce interference with other APs. Select one of the following Full (Full Power), 50% , 25% , 12.5% or Min (Minimum). See the product specifications for more information on your ZyXEL Device's output power.
Preamble Type	Select Dynamic to have the AP automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble. Select Long if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.
RTS/CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to its smallest value (1) turns on the RTS/CTS handshake. Enter a value between 1 and 2346 .
Fragmentation	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between 256 and 2346 .
Rates Configuration	This section controls the data rates permitted for clients. For each Rate , select an option from the Configuration list. The options are: <ul style="list-style-type: none"> • Basic (1~11 Mbps only): Clients can always connect to the access point at this speed. • Optional: Clients can connect to the access point at this speed, when permitted to do so by the AP. • Disable: Clients cannot connect to the access point at this speed.
Enable Antenna Diversity	Select this to use antenna diversity. Antenna diversity uses multiple antennas to reduce signal interference.
Enable Spanning Tree Control (STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP - compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the ZyXEL Device.
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

6.4.2 Wireless Client Mode

Use this screen to turn your ZyXEL Device into a wireless client. Select **Wireless Client** as the **Operation Mode**. The following screen displays.

Figure 28 Wireless: Wireless Client

Wireless Settings	Security	Radius	MAC Filter
Basic Settings			
Operation Mode	vWireless Client		
SSID	ZyXEL NWA1100 (max.32 printable characters)		Site Survey
Wireless Mode	802.11b+g		
Advanced Settings			
MAC Address Clone	<input checked="" type="radio"/> Auto <input type="radio"/> Manual		
Radio Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Output Power Management	Full		
Preamble Type	Dynamic		
RTS/CTS Threshold	2346 (1-2346)		
Fragmentation	2346 (256-2346)		
Rates Configuration			
Rate	Configuration	Rate	Configuration
1 Mbps	Basic	2 Mbps	Basic
5.5 Mbps	Basic	11 Mbps	Basic
6 Mbps	Optional	9 Mbps	Optional
12 Mbps	Optional	18 Mbps	Optional
24 Mbps	Optional	36 Mbps	Optional
48 Mbps	Optional	54 Mbps	Optional
<input type="checkbox"/> Enable Antenna Diversity <input checked="" type="checkbox"/> Enable Spanning Tree Protocol(STP)			
Apply		Reset	

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

Table 10 Wireless: Wireless Client

LABEL	DESCRIPTION
Basic Settings	
Operation Mode	Select Wireless Client from the drop-down list. Click Apply to make the Site Survey button appear next to the SSID field. Click this button to get a pop up window of available APs.
SSID	<p>The SSID (Service Set IDentifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID.</p> <p>In this field, enter the SSID of the AP you want to use (click Site Survey button for a list of available APs). Click Apply. Set the security configuration for this operating mode in the Wireless > Security screen. Check the Status screen to check if the settings you set show in the WLAN information.</p> <p>Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device’s SSID 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.</p>

Table 10 Wireless: Wireless Client

LABEL	DESCRIPTION
Site Survey	Click this to view a list of available wireless access points within the range.
Wireless Mode	Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select 802.11b+g to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Advanced Settings	
MAC Address Clone	Choose Manual to configure the ZyXEL Device's MAC address by cloning the MAC address from a computer on your LAN. Choose Auto to use the factory default MAC address of your ZyXEL Device.
Radio Enable	Select Yes to enable WLAN radio, and No to turn it off. The ZyXEL Device cannot be accessed wirelessly if radio is turned off.
Output Power Management	Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power of the ZyXEL Device to reduce interference with other APs. Select one of the following Full (Full Power), 50% , 25% , 12.5% or Min (Minimum). See the product specifications for more information on your ZyXEL Device's output power.
Preamble Type	Select Dynamic to have the ZyXEL Device automatically use short preamble when the wireless network your ZyXEL Device is connected to supports it, otherwise the ZyXEL Device uses long preamble. Select Long preamble if you are unsure what preamble mode the wireless device your ZyXEL Device is connected to supports, and to provide more reliable communications in busy wireless networks.
RTS/CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to its smallest value (1) turns on the RTS/CTS handshake. Enter a value between 1 and 2346 .
Fragmentation	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between 256 and 2346 .
Rates Configuration	This section controls the data rates permitted for clients. For each Rate , select an option from the Configuration list. The options are: <ul style="list-style-type: none"> • Basic (1~11 Mbps only): Clients can always connect to the access point at this speed. • Optional: Clients can connect to the access point at this speed, when permitted to do so by the AP. • Disable: Clients cannot connect to the access point at this speed.
Enable Antenna Diversity	Select this to use antenna diversity. Antenna diversity uses multiple antennas to reduce signal interference.
Enable Spanning Tree Control (STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP - compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the ZyXEL Device.
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

6.4.3 Bridge Mode

Use this screen to have the ZyXEL Device act as a wireless network bridge and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

Use this screen to use the ZyXEL Device as a wireless bridge. Select **Bridge** as the **Operation Mode**.

Figure 29 Wireless: Bridge

Wireless Settings	Security	Radius	MAC Filter
Basic Settings			
Operation Mode	Bridge		
Channel	6		
Wireless Mode	802.11b+g		
WDS Settings			
Local MAC Address	00	60	b3 : aa : bb : cc
Remote MAC Address 1			
Remote MAC Address 2			
Remote MAC Address 3			
Remote MAC Address 4			
Advanced Settings			
Radio Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Output Power Management	Full		
Preamble Type	Dynamic		
RTS/CTS Threshold	2346 (1~2346)		
Fragmentation	2346 (256~2346)		
Rates Configuration			
Rate	Configuration	Rate	Configuration
1 Mbps	Basic	2 Mbps	Basic
5.5 Mbps	Basic	11 Mbps	Basic
6 Mbps	Optional	9 Mbps	Optional
12 Mbps	Optional	18 Mbps	Optional
24 Mbps	Optional	36 Mbps	Optional
48 Mbps	Optional	54 Mbps	Optional
<input type="checkbox"/> Enable Antenna Diversity <input checked="" type="checkbox"/> Enable Spanning Tree Protocol(STP)			
<input type="button" value="Apply"/> <input type="button" value="Reset"/>			

The following table describes the bridge labels in this screen.

Table 11 Wireless: Bridge

LABEL	DESCRIPTIONS
Basic Settings	
Operation Mode	Select Bridge in this field.

Table 11 Wireless: Bridge

LABEL	DESCRIPTIONS
Channel	<p>Set the operating frequency/channel depending on your particular region.</p> <p>To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box. Click MAINTENANCE and then the Channel Usage tab to open the Channel Usage screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.</p> <p>To have the ZyXEL Device automatically select a channel, click Scan instead.</p>
Wireless Mode	<p>Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device.</p> <p>Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device.</p> <p>Select 802.11b+g to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.</p>
WDS Settings	
Local Mac Address Remote MAC Address 1 - 4	<p>A Wireless Distribution System is a wireless connection between two or more APs.</p> <p>Note: WDS security is independent of the security settings between the ZyXEL Device and any wireless clients.</p> <p>Local MAC Address is the MAC address of your ZyXEL Device. You can specify up to 4 remote devices' MAC addresses in this section.</p>
Advanced Settings	
Radio Enable	<p>Select Yes to enable WLAN radio, and No to turn it off. The ZyXEL Device cannot be accessed wirelessly if radio is turned off.</p>
Output Power Management	<p>Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power of the ZyXEL Device to reduce interference with other APs. Select one of the following Full (Full Power), 50%, 25%, 12.5% or Min (Minimum). See the product specifications for more information on your ZyXEL Device's output power.</p>
Preamble Type	<p>Select Dynamic to have the ZyXEL Device automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble.</p> <p>Select Long preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.</p>
RTS/CTS Threshold	<p>(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to 1 turns on the RTS/CTS handshake. Enter a value between 1 and 2346.</p>
Fragmentation	<p>The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between 256 and 2346.</p>
Rates Configuration	<p>This section controls the data rates permitted for clients.</p> <p>For each Rate, select an option from the Configuration list. The options are:</p> <ul style="list-style-type: none"> • Basic (1~11 Mbps only): Clients can always connect to the access point at this speed. • Optional: Clients can connect to the access point at this speed, when permitted to do so by the AP. • Disable: Clients cannot connect to the access point at this speed.

Table 11 Wireless: Bridge

LABEL	DESCRIPTIONS
Enable Antenna Diversity	Select this to use antenna diversity. Antenna diversity uses multiple antennas to reduce signal interference.
Enable Spanning Tree Protocol(STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP - compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the ZyXEL Device.

6.4.4 AP + Bridge Mode

Use this screen to have the ZyXEL Device function as a bridge and access point simultaneously. Select **AP + Bridge** as the **Operation Mode**. The following screen displays.

Figure 30 Wireless: AP+Bridge

The screenshot shows the 'Wireless Settings' screen for the ZyXEL NWA-1100. The 'Operation Mode' is set to 'AP+Bridge'. The SSID is 'ZyXEL NWA1100' and the channel is '6'. The 'Wireless Mode' is '802.11b+g'. Under 'WDS Settings', there are fields for 'Local MAC Address' and four 'Remote MAC Address' fields. The 'Advanced Settings' section includes 'Beacon Interval' (100), 'Intra-BSS Traffic' (Enable), 'DTIM Interval' (1), 'WMM' (Disable), 'Number of Wireless Stations Allowed to Associate' (32), 'Radio Enable' (Yes), 'Output Power Management' (Full), 'Preamble Type' (Dynamic), 'RTS/CTS Threshold' (2346), and 'Fragmentation' (2346). The 'Rates Configuration' table lists rates from 1 Mbps to 54 Mbps with their respective configurations. At the bottom, 'Enable Spanning Tree Protocol (STP)' is checked, and there are 'Apply' and 'Reset' buttons.