

WAP3205

Wireless N Access Point

User's Guide

Default Login Details

IP Address	http://192.168.1.2
Password	1234



Firmware Version 1.0
Edition 1, 6/2009

www.zyxel.com

ZyXEL

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the WAP3205 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.

- Support Disc

Refer to the included CD for support documents.

Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- Download Library

Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- 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.

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.




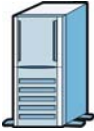

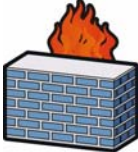



Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The WAP3205 may be referred to as the "WAP3205", 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 WAP3205 icon is not an exact representation of your device.

WAP3205 	Computer 	Notebook computer 
Server 	Modem 	Firewall 
Telephone 	Switch 	Router 

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT 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.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Contents Overview

Introduction	17
Getting to Know Your WAP3205	19
Introducing the Web Configurator	23
Monitor	29
WAP3205 Modes	33
Easy Mode	35
Access Point Mode	45
Client Mode	53
Universal Repeater Mode	65
Tutorials	73
Configuration	81
Wireless LAN	83
LAN	101
Maintenance and Troubleshooting	105
Maintenance	107
Troubleshooting	119
Product Specifications	125
Appendices and Index	129

Table of Contents

About This User's Guide	3
Document Conventions.....	5
Safety Warnings.....	7
Contents Overview	9
Table of Contents.....	11
Part I: Introduction.....	17
Chapter 1	
Getting to Know Your WAP3205	19
1.1 Overview	19
1.2 Applications	19
1.3 Ways to Manage the WAP3205	19
1.4 Good Habits for Managing the WAP3205	20
1.5 LEDs	20
Chapter 2	
Introducing the Web Configurator	23
2.1 Overview	23
2.2 Accessing the Web Configurator	23
2.2.1 Login Screen	24
2.2.2 Password Screen	25
2.2.3 Home Screen	25
2.3 Resetting the WAP3205	27
2.3.1 Procedure to Use the Reset Button	28
Chapter 3	
Monitor.....	29
3.1 Overview	29
3.2 What You Can Do	29
3.3 Log	29
3.4 Packet Statistics	30
3.5 WLAN Station Status	32

Chapter 4	
WAP3205 Modes	33
4.1 Overview	33
4.1.1 Web Configurator Modes	33
4.1.2 Device Modes	33
Chapter 5	
Easy Mode	35
5.1 Overview	35
5.2 What You Can Do	36
5.3 What You Need to Know	36
5.4 Navigation Panel	37
5.5 Network Map	37
5.6 Control Panel	38
5.6.1 Wireless Security	39
5.6.2 WPS	41
5.7 Status Screen in Easy Mode	42
Chapter 6	
Access Point Mode	45
6.1 Overview	45
6.2 What You Can Do	45
6.3 What You Need to Know	45
6.3.1 Setting your WAP3205 to AP Mode	46
6.3.2 Accessing the Web Configurator in Access Point Mode	46
6.3.3 Configuring your WLAN, LAN and Maintenance Settings	47
6.4 AP Mode Status Screen	47
Chapter 7	
Client Mode	53
7.1 Overview	53
7.2 What You Can Do	53
7.3 What You Need to Know	54
7.3.1 Setting your WAP3205 to Client Mode	54
7.3.2 Accessing the Web Configurator in Client Mode	54
7.4 Client Mode Status Screen	55
7.5 Wireless LAN Profile Screen	57
7.5.1 Adding a New WLAN Profile	58
7.5.2 Site Survey Screen	62
7.5.3 WPS Screen	63
Chapter 8	
Universal Repeater Mode	65

8.1 Overview	65
8.2 What You Can Do	65
8.3 What You Need to Know	66
8.3.1 Setting your WAP3205 to Universal Repeater Mode	66
8.3.2 Accessing the Web Configurator in Universal Repeater Mode	66
8.4 Universal Repeater Mode Status Screen	67
8.5 Universal Repeater Screen	69
8.5.1 No Security	70
8.5.2 Static WEP	70
8.5.3 WPA(2)-PSK	72
Chapter 9	
Tutorials	73
9.1 Overview	73
9.2 Connecting to the Internet from an Access Point	73
9.3 Configuring Wireless Security Using WPS	73
9.3.1 Push Button Configuration (PBC)	74
9.3.2 PIN Configuration	75
9.4 Enabling and Configuring Wireless Security (No WPS)	77
9.4.1 Configure Your Notebook	79
Part II: Configuration	81
Chapter 10	
Wireless LAN	83
10.1 Overview	83
10.2 What You Can Do	84
10.3 What You Should Know	84
10.3.1 Wireless Security Overview	84
10.4 General Wireless LAN Screen	87
10.5 Wireless Security Screen	88
10.5.1 No Security	88
10.5.2 WEP Encryption	89
10.5.3 WPA-PSK/WPA2-PSK	91
10.6 MAC Filter	92
10.7 Wireless LAN Advanced Screen	93
10.8 Quality of Service (QoS) Screen	95
10.9 WPS Screen	95
10.10 WPS Station Screen	97
10.11 Scheduling Screen	97
10.12 WDS Screen	99

Chapter 11	
LAN.....	101
11.1 Overview	101
11.2 What You Can Do	101
11.3 What You Need To Know	102
11.3.1 LAN TCP/IP	102
11.3.2 IP Alias	102
11.4 LAN IP Screen	103
11.5 IP Alias Screen	104
Part III: Maintenance and Troubleshooting	105
Chapter 12	
Maintenance	107
12.1 Overview	107
12.2 What You Can Do	107
12.3 General Screen	108
12.4 Password Screen	108
12.5 Time Setting Screen	109
12.6 Firmware Upgrade Screen	111
12.7 Configuration Backup/Restore Screen	113
12.8 Reset/Restart Screen	114
12.9 System Operation Mode Overview	115
12.10 Sys Op Mode Screen	116
Chapter 13	
Troubleshooting.....	119
13.1 Power, Hardware Connections, and LEDs	119
13.2 WAP3205 Access and Login	120
13.3 Internet Access	122
13.4 Resetting the WAP3205 to Its Factory Defaults	123
13.5 Wireless Router/AP Troubleshooting	124
Chapter 14	
Product Specifications	125
14.1 Wall-mounting Instructions	126
Part IV: Appendices and Index	129
Appendix A Pop-up Windows, JavaScripts and Java Permissions	131

Appendix B IP Addresses and Subnetting 139

Appendix C Setting up Your Computer's IP Address 149

Appendix D Wireless LANs 167

Appendix E Common Services..... 179

Appendix F Legal Information 183

Index..... 191

PART I

Introduction

Getting to Know Your WAP3205 (19)

Connection Wizard (25)

Introducing the Web Configurator (23)

WAP3205 Modes (33)

Monitor (29)

Tutorials (73)

Getting to Know Your WAP3205

1.1 Overview

This chapter introduces the main features and applications of the WAP3205.

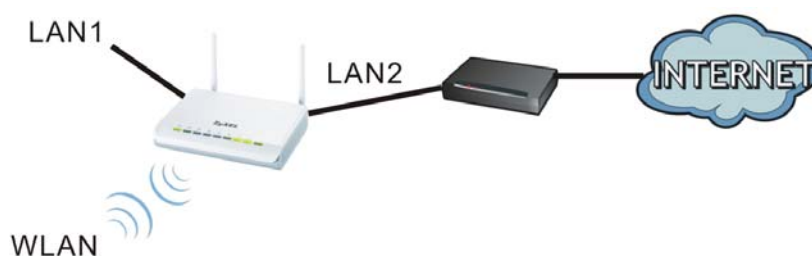
The WAP3205 extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices.

1.2 Applications

You can create the following networks using the WAP3205:

- **Wired.** You can connect to a broadband modem/router for Internet access and/or connect network devices via the Ethernet ports of the WAP3205 so that they can communicate with each other and access the Internet.
- **Wireless.** Wireless clients can connect to the WAP3205 to access network resources.

Figure 1 WAP3205 Network



1.3 Ways to Manage the WAP3205

Use any of the following methods to manage the WAP3205.

- **Web Configurator.** This is recommended for everyday management of the WAP3205 using a (supported) web browser.

- WPS (Wi-Fi Protected Setup) button. You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your ZyXEL Device.

1.4 Good Habits for Managing the WAP3205

Do the following things regularly to make the WAP3205 more secure and to manage the WAP3205 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 WAP3205 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the WAP3205. You could simply restore your last configuration.

1.5 LEDs

Figure 2 Front Panel



The following table describes the LEDs and the WPS button.

Table 1 Front Panel LEDs and WPS Button






LED	COLOR	STATUS	DESCRIPTION
POWER 	Green	On	The WAP3205 is receiving power and functioning properly.
		Off	The WAP3205 is not receiving power.
LAN 1-2  	Green	On	The WAP3205 has a successful 10/100MB Ethernet connection.
		Blinking	The WAP3205 is sending/receiving data through the LAN.
		Off	The LAN is not connected.

Table 1 Front Panel LEDs and WPS Button

LED	COLOR	STATUS	DESCRIPTION
WLAN 	Green	On	The WAP3205 is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The WAP3205 is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
WPS 	Green	On	WPS is enabled.
		Blinking	The WAP3205 is negotiating a WPS connection with a wireless client.
		Off	The wireless LAN is not ready or has failed.

Introducing the Web Configurator

2.1 Overview

This chapter describes how to access the WAP3205 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the WAP3205 via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions or Safari 2.0 or 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 ([Chapter 13 on page 119](#)) to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

- 1 Make sure your WAP3205 hardware is properly connected and prepare your computer or computer network to connect to the WAP3205 (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "http://192.168.1.2" as the website address.

Your computer must be in the same subnet in order to access this website address.

2.2.1 Login Screen


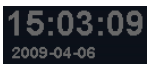
The Web Configurator initially displays the following login screen.

Figure 3 Login screen



The following table describes the labels in this screen.

Table 2 Login screen

LABEL	DESCRIPTION
Password	Type "1234" (default) as the password.
Language	Select the language you want to use to configure the Web Configurator. Click Login .
	This shows the current weather, either in celsius or fahrenheit, of the city you specify in Section 2.2.3.1 on page 26 .
	This shows the time (hh:mm:ss) and date (yyyy:mm:dd) of the timezone you select in Section 2.2.3.2 on page 27 or Section 12.5 on page 109 . The time is in 24-hour format, for example 15:00 is 3:00 PM.

2.2.2 Password Screen

You should see a screen asking you to change your password (highly recommended) as shown next.

Figure 4 Change Password Screen

The following table describes the labels in this screen.



Table 3 Change Password Screen

LABEL	DESCRIPTION
New Password	Type a new password.
Retype to Confirm	Retype the password for confirmation.
Apply	Click Apply to save your changes back to the WAP3205.
Ignore	Click Ignore if you do not want to change the password this time.

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to [Chapter 12 on page 107](#) to change this). Simply log back into the WAP3205 if this happens.

2.2.3 Home Screen

If you have previously logged into the Web Configurator but did not click **Logout**, you may be redirected to the **Home** screen.

You can also open this screen by clicking **Home** ( or ) in the **Easy Mode** or **Expert Mode** screens.


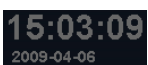
The Home screen displays as follows.

Figure 5 Home Screen



The following table describes the labels in this screen.

Table 4 Home Screen

LABEL	DESCRIPTION
Go	Click this to open the Easy mode Web Configurator.
Language	Select a language to go to the Easy mode Web Configurator in that language and click Login .
	(This is just an example). This shows the current weather, either in celsius or fahrenheit, of the city you specify in Section 2.2.3.1 on page 26 .
	(This is just an example). This shows the time (hh:mm:ss) and date (yyyy:mm:dd) of the timezone you select in Section 2.2.3.2 on page 27 or Section 12.5 on page 109 .

2.2.3.1 Weather Edit

You can change the temperature unit and select the location for which you want to know the weather.


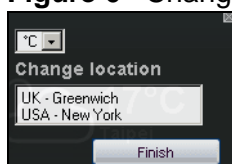
Click the  icon to change the Weather display.

Figure 6 Change Weather



The following table describes the labels in this screen.

Table 5 Change Weather

LABEL	DESCRIPTION
°C or °F	Choose which temperature unit you want the WAP3205 to display.
Change Location	Select the location for which you want to know the weather. If the city you want is not listed, choose one that is closest to it.
Finish	Click this to apply the settings and refresh the date and time display.

2.2.3.2 Time/Date Edit

One timezone can cover more than one country. You can choose a particular country in which the WAP3205 is located and have the WAP3205 display and use the current time and date for its logs.


Click the  icon to change the Weather display.

Figure 7 Change Password Screen



The following table describes the labels in this screen.

Table 6 Change Password Screen

LABEL	DESCRIPTION
Change time zone	Select the specific country whose current time and date you want the WAP3205 to display.
Finish	Click this to apply the settings and refresh the weather display.

Note: You can also edit the timezone in [Section 12.5 on page 109](#).

2.3 Resetting the WAP3205

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **RESET** button at the back of the WAP3205 to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to "1234" and the IP address will be reset to "192.168.1.2".

2.3.1 Procedure to Use the Reset Button

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for longer than 1 second to restart/reboot the WAP3205.
- 3 Press the **RESET** button for longer than five seconds to set the WAP3205 back to its factory-default configurations.

Monitor

3.1 Overview

This chapter discusses read-only information related to the device state of the WAP3205.

Note: To access the Monitor screens, you can also click the links in the Summary table of the Status screen to view the packets sent/received as well as the status of clients connected to the WAP3205.

3.2 What You Can Do

- Use the **Log** screen ([Section 3.3 on page 29](#)) to view the logs for the categories such as system maintenance, system errors, and so on.
- use the **Packet Statistics** screen ([Section 3.4 on page 30](#)) to view port status, packet specific statistics, the "system up time" and so on.
- Use the **WLAN Station Status** screen ([Section 3.5 on page 32](#)) to view the wireless stations that are currently associated to the WAP3205.

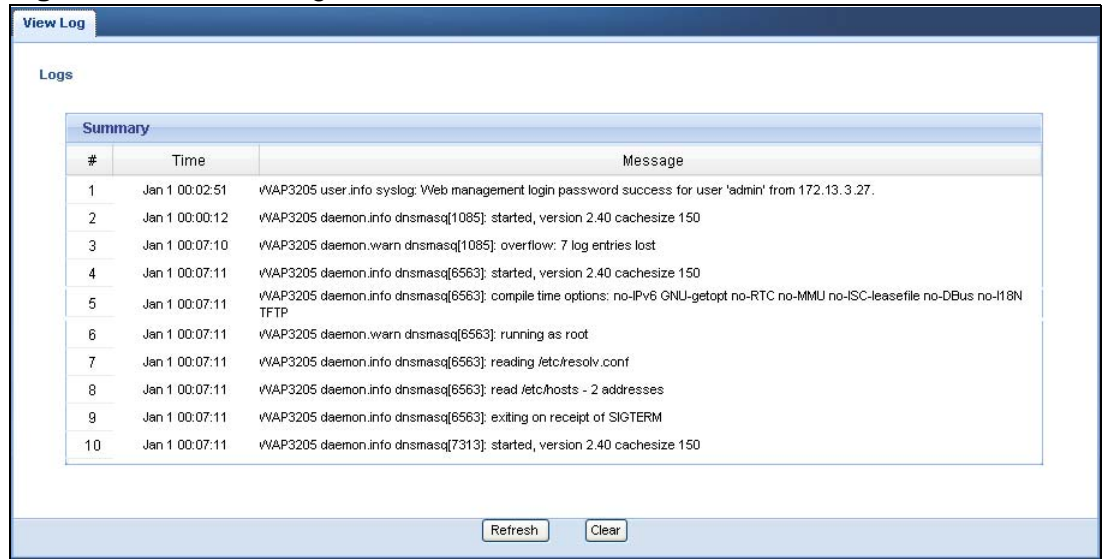
3.3 Log

Use the **View Log** screen to see the logged messages for the WAP3205.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills.

Click **Monitor > Log**.

Figure 8 Monitor > Log



The following table describes the labels in this screen.

Table 7 Monitor > Log

LABEL	DESCRIPTION
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Refresh	Click Refresh to renew the log screen.
Clear	Click Clear to delete all the logs.

3.4 Packet Statistics

Click the **Packet Statistics (Details...)** hyperlink in the **Status** screen or **Monitor > Packet Statistics**. Read-only information here includes port status,

packet specific statistics and the "system up time". The **Poll Interval(s)** field is configurable and is used for refreshing the screen.

Figure 9 Summary: Packet Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
LAN	100M	22338	32847	0	9493609	4383238	02:29:14
WLAN	300M	7040	623270	0	0	88856947	02:29:14

System Up Time : 2 hours, 29 mins, 20 secs

Poll Interval(s) : None

The following table describes the labels in this screen.

Table 8 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the WAP3205's port type.
Status	For the LAN ports, this displays the port speed 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.
Up Time	This is the total time the WAP3205 has been for each session.
System Up Time	This is the total time the WAP3205 has been on.
Poll Interval(s)	Enter the time interval in seconds 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.

3.5 WLAN Station Status

Click the **WLAN Station Status (Details...)** hyperlink in the **Status** screen or **Monitor > WLAN Station Status**. View the wireless stations that are currently associated to the WAP3205 in the **Association List**. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Note: This screen is not available when the WAP3205 is in Client mode.

Figure 10 Summary: Wireless Association List

#	MAC Address	Association Time
1	00:19:CB:32:BE:AC	02:43:51 2000/01/01

The following table describes the labels in this screen.

Table 9 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 WAP3205's WLAN network.
Refresh	Click Refresh to reload the list.

WAP3205 Modes

4.1 Overview

This chapter introduces the different modes available on your WAP3205. First, the term “mode” refers to two things in this User’s Guide.

- **Web Configurator mode.** This refers to the Web Configurator interface you want to use for editing WAP3205 features.
- **Device mode.** This is the operating mode of your WAP3205, or simply how the WAP3205 is being used in the network.

4.1.1 Web Configurator Modes

This refers to the configuration interface of the Web Configurator, which has two modes:

- **Easy.** The Web Configurator shows this mode by default. Refer to [Chapter 5 on page 35](#) for more information on the screens in this mode. This interface may be sufficient for users who just want to use the device.
- **Expert.** Advanced users can change to this mode to customize all the functions of the WAP3205. Click **Expert Mode** after logging into the Web Configurator. The User’s Guide [Chapter 2 on page 23](#) through [Chapter 12 on page 107](#) discusses the screens in this mode.

4.1.2 Device Modes

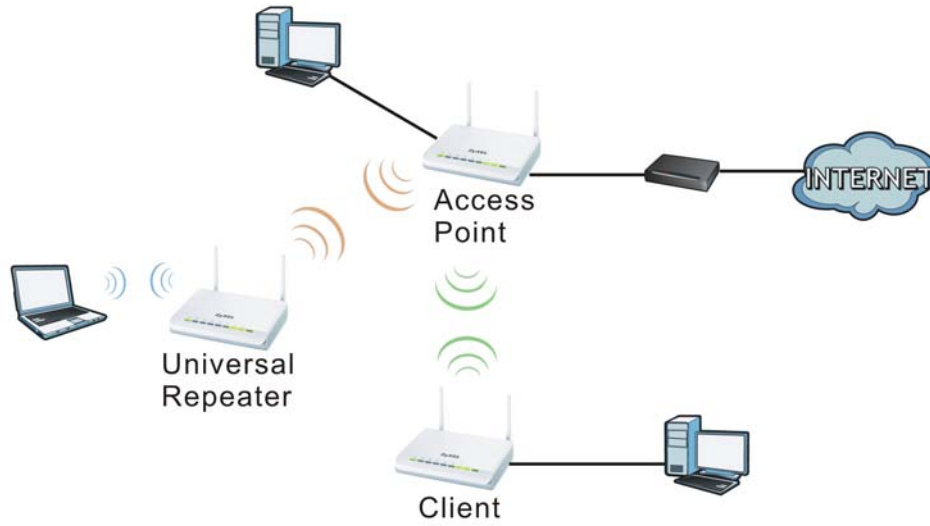
This refers to the operating mode of the WAP3205, which can act as a:

- **Access Point.** Use this mode if you want to extend your network by allowing network devices to connect to the WAP3205 wirelessly. Go to [Section 6.4 on page 47](#) view the **Status** screen in this mode.
- **Client.** Use this mode if there is an existing wireless router or access point in the network to which you want to connect your local network. Go to [Section 7.4 on page 55](#) to view the **Status** screen in this mode.

- **Universal Repeater.** In this mode, the WAP3205 can be an access point and a wireless client at the same time. Use this mode if there is an existing wireless router or access point in your network and you also want to allow clients to connect to the WAP3205 wirelessly. Go to [Section 6.4 on page 47](#) to view the **Status** screen in this mode.

The following figure is a simple illustration of the device configuration modes of the WAP3205.

Figure 11 Device Mode Example



For more information on these modes and to change the mode of your WAP3205, refer to [Chapter 12 on page 115](#).

The menu for changing device modes is available in **Expert** mode only.

Note: Choose your Device Mode carefully to avoid having to change it later.

In Client mode, you should know the SSID and wireless security details of the access point to which you want to connect.

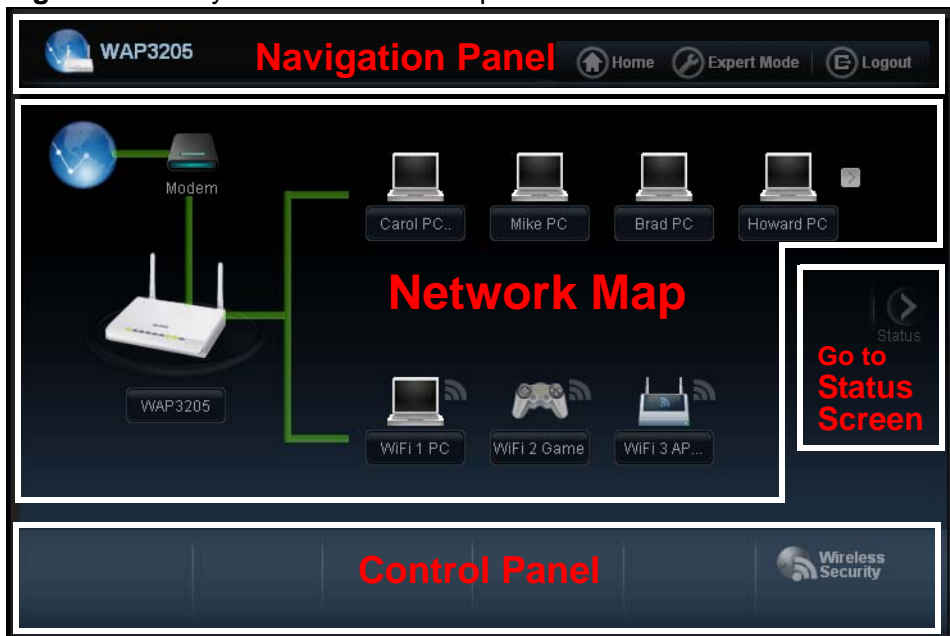
Easy Mode

5.1 Overview

The Web Configurator is set to **Easy Mode** by default. You can configure several key features of the WAP3205 in this mode. This mode is useful to users who are not fully familiar with some features that are usually intended for network administrators.

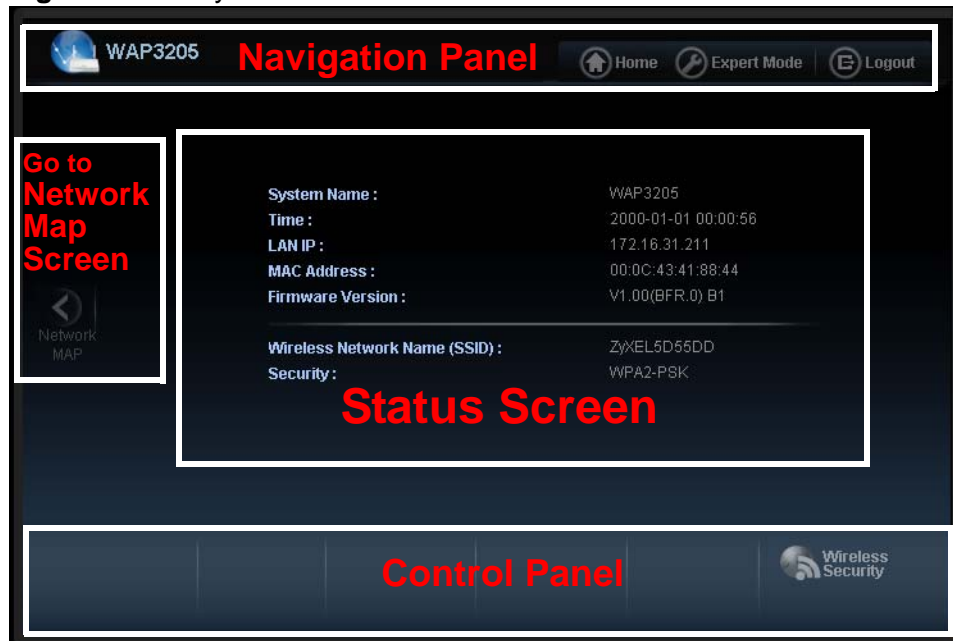
When you log in to the Web Configurator, the following screen opens.

Figure 12 Easy Mode: Network Map



Click **Status** to open the following screen screen.

Figure 13 Easy Mode: Status Screen



5.2 What You Can Do

You can do the following in this mode:

- Use this **Navigation Panel** (Section 5.4 on page 37) to opt out of the **Easy** mode.
- Use the **Network Map** screen (Section 5.5 on page 37) to check if your WAP3205 can ping the gateway and whether it is connected to the Internet. The **Network Map** screen is not applicable when the WAP3205 is in **Client Mode**.
- Use the **Control Panel** (Section 5.6 on page 38) to configure wireless security.
- Use the **Status Screen** screen (Section 5.7 on page 42) to view read-only information about the WAP3205, including the LAN IP, MAC Address of the WAP3205 and the firmware version.

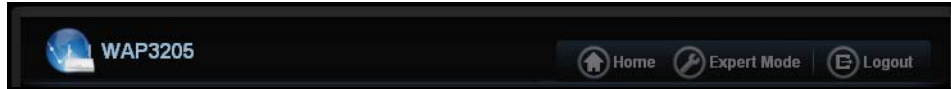
5.3 What You Need to Know

The **Network Map** screen is not applicable and **Wireless Security** in the control panel is not configurable when the WAP3205 is in Client mode.

5.4 Navigation Panel

Use this navigation panel to opt out of the **Easy** mode.

Figure 14 Control Panel



The following table describes the labels in this screen.

Table 10 Control Panel

ITEM	DESCRIPTION
Home	Click this to go to the Login page.
Expert Mode	Click this to change to Expert mode and customize features of the WAP3205.
Logout	Click this to end the Web Configurator session.

5.5 Network Map

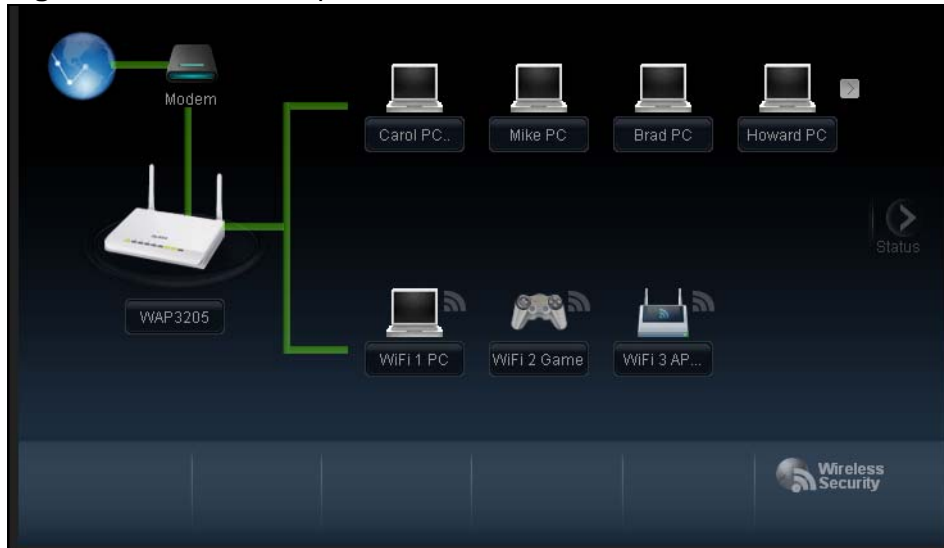
Note: The Network MAP is viewable by Windows XP (need to install patch), Windows Vista and Windows 7 users only. For Windows XP (Service Pack 2) users, you can see the network devices connected to the WAP3205 by downloading the LLTD (Link Layer Topology Discovery) patch from the Microsoft Website.

Note: Don't worry if the Network Map does not display in your web browser. This feature may not be supported by your system. You can still configure the Control Panel ([Section 5.6 on page 38](#)) in the Easy Mode and the WAP3205 features that you want to use in the Expert Mode.

Note: The Network Map is not applicable when the WAP3205 is in **Client Mode**.

When you log into the Web Configurator, the Network Map is shown as follows.

Figure 15 Network Map



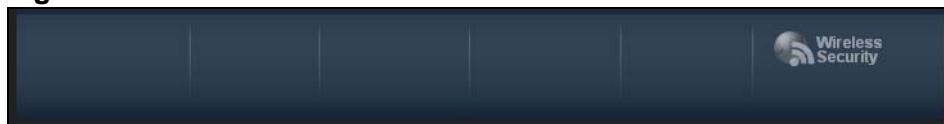
The line connecting the WAP3205 to the gateway becomes green when the WAP3205 is able to ping the gateway. It becomes red when the ping initiating from the WAP3205 does not get a response from the gateway. The same rule applies to the line connecting the gateway to the Internet.

You can also view the devices (represented by icons indicating the kind of network device) connected to the WAP3205, including those connecting wirelessly. Right-click on the WAP3205 icon to refresh the network map and go to the Wizard. Right click on the other icons to view information about the device.

5.6 Control Panel

The features configurable in **Easy Mode** are shown in the **Control Panel**.

Figure 16 Control Panel



Click the feature to open a screen where you can edit its settings.

The following table describes the labels in this screen.

Table 11 Control Panel

ITEM	DESCRIPTION
Wireless Security	Click this to configure the wireless security, such as SSID, security mode and WPS key on your WAP3205. Refer to Section 5.6.1 on page 39 to see this screen.

5.6.1 Wireless Security

Use this screen to configure security for your the Wireless LAN. You can enter the SSID and select the wireless security mode in the following screen.

Note: **Wireless Security** in the control panel is not configurable when the WAP3205 is in **Client Mode**.

Figure 17 Wireless Security

Wireless Security

Data transmitted wirelessly without encryption is not safe. Guard your wireless network with a security mode and the password you setup. And then, you can use WPS to connect your computers to your wireless network with just one single click.

Wireless Network Name (SSID): ZyXEL5D55DD

Security mode: WPA2-PSK

Wireless password: ●●●●●●

Verify password: ●●●●●●

WPS

Apply Cancel

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

Table 12 Wireless Security

LABEL	DESCRIPTION
Wireless Network Name (SSID)	<p>(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 keyboard characters) for the wireless LAN.</p> <p>The default SSID is WAP3205.</p>
Security mode	<p>Select WPA-PSK or WPA2-PSK to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen.</p> <p>Select No Security to allow any client to connect to this network without authentication.</p>
Wireless password	<p>This field appears when you choose wither WPA-PSK or WPA2-PSK as the security mode.</p> <p>Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.</p>
Verify password	<p>Type the password again to confirm.</p>
Apply	<p>Click Apply to save your changes back to the WAP3205.</p>
Cancel	<p>Click Cancel to close this screen.</p>
WPS	<p>Click this to configure the WPS screen.</p> <p>You can transfer the wireless settings configured here (Wireless Security screen) to another wireless device that supports WPS.</p>

5.6.2 WPS

Use this screen to add a wireless station to the network with the WAP3205's first SSID using WPS. Click **WPS** in the **Wireless Security** to open the following screen.

Figure 18 Wireless Security: WPS



The following table describes the labels in this screen.

Table 13 Wireless Security: WPS

LABEL	DESCRIPTION
Wireless Security	Click this to go back to the Wireless Security screen.
WPS	<p>Create a secure wireless network simply by pressing the button.</p> <p>The WAP3205 scans for a WPS-enabled device within the range and performs wireless security information synchronization.</p> <p>Note: After you click the WPS button on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.</p>

Table 13 Wireless Security: WPS

LABEL	DESCRIPTION
Register	Create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the WAP3205's interface and pushing this button. Type the same PIN number generated in the wireless station's utility. Then click Register to associate to each other and perform the wireless security information synchronization.
Exit	Click Exit to close this screen.

5.7 Status Screen in Easy Mode

In the Network Map screen, click **Status** to view read-only information about the WAP3205.

Figure 19 Status Screen in Easy Mode


System Name :	WAP3205
Time :	2000-01-01 00:00:56
LAN IP :	172.16.31.211
MAC Address :	00:0C:43:41:88:44
Firmware Version :	V1.00(BFR.0) B1
<hr/>	
Wireless Network Name (SSID) :	ZyXEL5D55DD
Security :	WPA2-PSK

The following table describes the labels in this screen.

Table 14 Status Screen in Easy Mode

ITEM	DESCRIPTION
Name	This is the name of the WAP3205 in the network. You can change this in the Maintenance > General screen in Section 12.3 on page 108 .
Time	This is the current system date and time. The date is in YYYY:MM:DD (Year-Month-Day) format. The time is in HH:MM:SS (Hour:Minutes:Seconds) format.
LAN IP	This is the IP address of the LAN port.
MAC Address	This is the MAC address of the WAP3205.
Firmware Version	This shows the firmware version of the WAP3205. The firmware version format shows the trunk version, model code and release number.

Table 14 Status Screen in Easy Mode

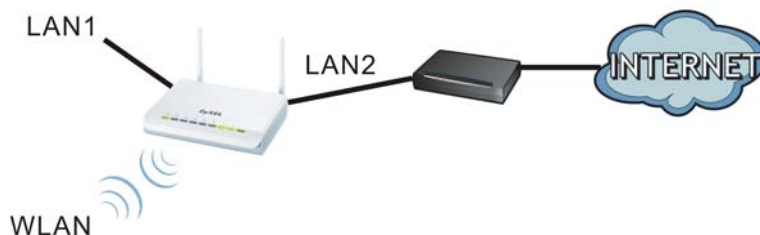
ITEM	DESCRIPTION
Wireless Network Name (SSID)	This shows the SSID of the wireless network. You can configure this in the Wireless Security screen (Section 5.6.1 on page 39 ; Section 10.3.1.1 on page 85).
Security	This shows the wireless security used by the WAP3205.

Access Point Mode

6.1 Overview

The WAP3205 is set to access point mode by default. In this mode your WAP3205 bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 20 Wireless Internet Access in Access Point Mode



Note: See [Chapter 9 on page 73](#) for an example of setting up a wireless network in Access Point mode.

6.2 What You Can Do

- Use the **Status** screen ([Section 6.4 on page 47](#)) to view read-only information about your WAP3205.
- Use the **LAN** screen ([Chapter 11 on page 101](#)) to set the IP address for your WAP3205 acting as an access point.
- Use the **Wireless LAN** screens ([Chapter 10 on page 83](#)) to configure the wireless settings and wireless security between the wireless clients and the WAP3205.

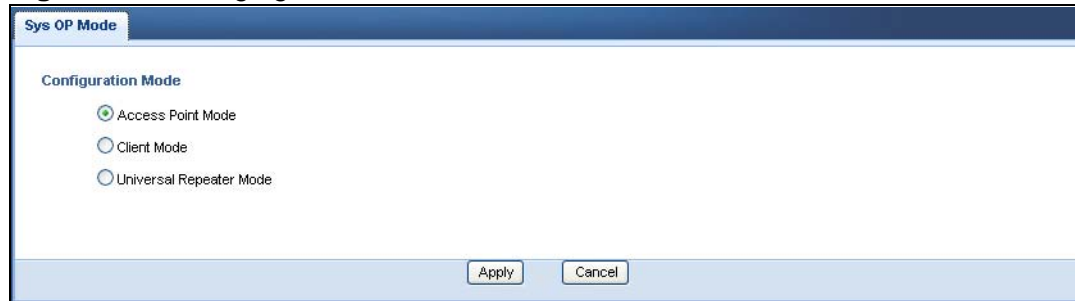
6.3 What You Need to Know

See [Chapter 9 on page 73](#) for a tutorial on setting up a network with the WAP3205 as an access point.

6.3.1 Setting your WAP3205 to AP Mode

- 1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.
- 2 To use your WAP3205 as an access point, go to **Maintenance > Sys OP Mode** and select **Access Point mode**.

Figure 21 Changing to Access Point mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your WAP3205 is already in Access Point mode.

6.3.2 Accessing the Web Configurator in Access Point Mode

Log in to the Web Configurator in Access Point mode, do the following:

- 1 Connect your computer to the LAN port of the WAP3205.
- 2 The default IP address of the WAP3205 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".
- 3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see [Appendix C on page 149](#) for information on changing your computer's IP address.
- 4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "192.168.1.2" as the web address in your web browser.

Note: After clicking **Login**, the Easy mode appears. Refer to [Section on page 35](#) for the Easy mode screens. Change to Expert mode to see the screens described in the sections following this.

6.3.3 Configuring your WLAN, LAN and Maintenance Settings

- See [Configuration \(81\)](#) for information on the configuring your wireless network and LAN settings.
- See [Maintenance and Troubleshooting \(105\)](#) for information on configuring your Maintenance settings.

6.4 AP Mode Status Screen


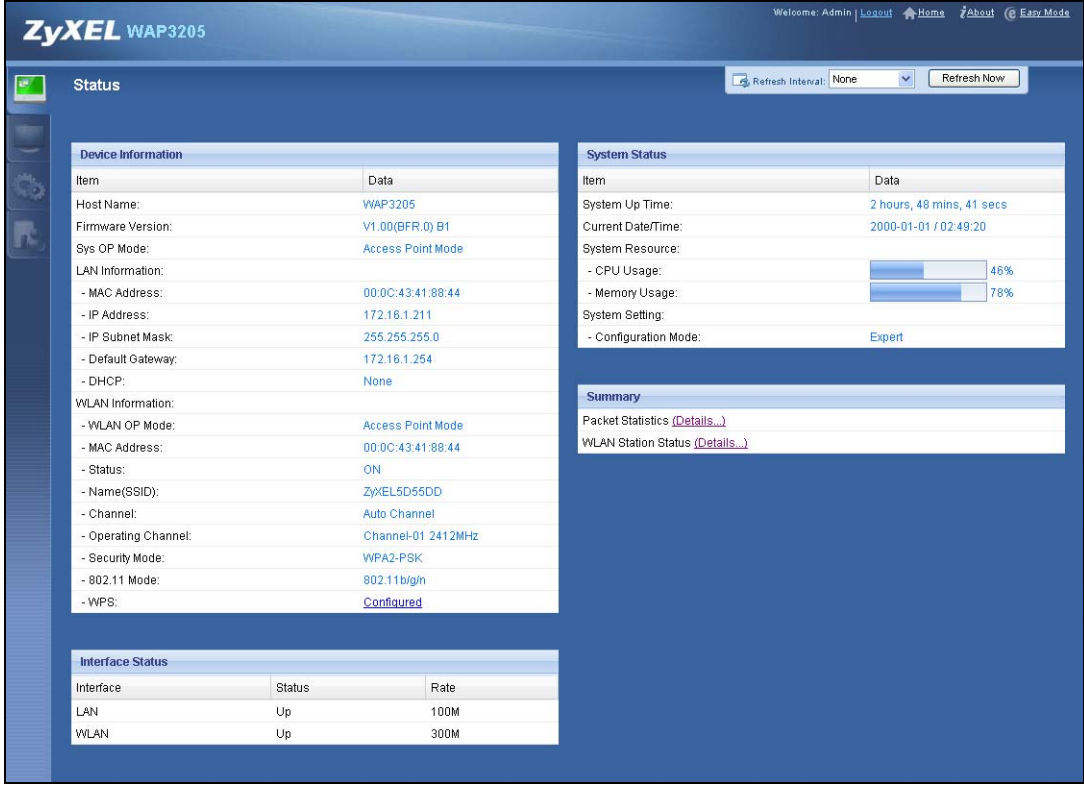
Click  to open the **Status** screen.

Figure 22 Status Screen: Access Point Mode



The screenshot shows the ZyXEL WAP3205 Status screen. The interface includes a navigation bar at the top with links for 'Welcome: Admin', 'Logout', 'Home', 'About', and 'Easy Mode'. A 'Refresh Interval' dropdown is set to 'None' with a 'Refresh Now' button. The main content is divided into several sections:

- Device Information:** A table listing items like Host Name (WAP3205), Firmware Version (V1.00(BFR.0) B1), Sys OP Mode (Access Point Mode), LAN Information (MAC Address: 00:0C:43:41:88:44, IP Address: 172.16.1.211, etc.), WLAN Information (WLAN OP Mode: Access Point Mode, MAC Address: 00:0C:43:41:88:44, Status: ON, etc.), and WPS (Configured).
- System Status:** A table showing System Up Time (2 hours, 48 mins, 41 secs), Current Date/Time (2000-01-01 / 02:49:20), System Resource (CPU Usage: 46%, Memory Usage: 78%), and System Setting (Configuration Mode: Expert).
- Interface Status:** A table showing LAN (Up, 100M) and WLAN (Up, 300M).
- Summary:** Links for Packet Statistics and WLAN Station Status.

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

Table 15 Status Screen Icon Key: Access Point Mode










ICON	DESCRIPTION
	Click this icon to view copyright and a link for related product information.
	Click this icon to go to Easy Mode. See Chapter 5 on page 35 .
	Click this to go to the Home page. See Chapter 3 on page 29 .

Table 15 Status Screen Icon Key: Access Point Mode (continued)

ICON	DESCRIPTION
	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.
	Click this icon to see the Status page. The information in this screen depends on the device mode you select.
	Click this icon to see the Monitor navigation menu.
	Click this icon to see the Configuration navigation menu.
	Click this icon to see the Maintenance navigation menu.

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

Table 16 Status Screen: Access Point Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the System Name you enter in the Maintenance > General screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 4.1.2 on page 33) to which the WAP3205 is set - Access Point Mode .
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.
Default Gateway	This shows the gateway IP address.
DHCP	This shows the LAN port's DHCP role - Client or None .
WLAN Information	
WLAN OP Mode	This is the device mode (Section 4.1.2 on page 33) to which the WAP3205's wireless LAN is set - Access Point Mode .
MAC Address	This shows the wireless adapter MAC Address of your device.
Status	This shows the current status of the Wireless LAN - ON .
Name (SSID)	This shows a descriptive name used to identify the WAP3205 in the wireless LAN.
Channel	This shows the channel number which you select manually or the WAP3205 automatically scans and selects.
Operating Channel	This shows the channel number which the WAP3205 is currently using over the wireless LAN.
Security Mode	This shows the level of wireless security the WAP3205 is using.
802.11 Mode	This shows the wireless standard.

Table 16 Status Screen: Access Point Mode

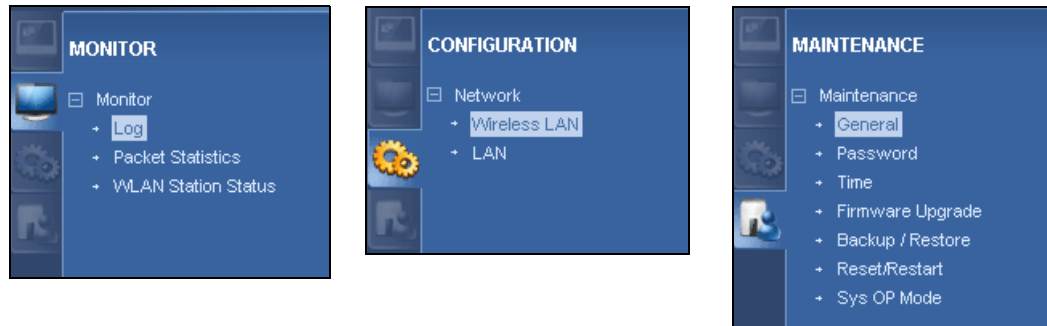
LABEL	DESCRIPTION
WPS	This displays Configured when the WPS has been set up. This displays Unconfigured if the WPS has not been set up. Click the status to display Network > Wireless LAN > WPS screen.
Interface Status	
Interface	This displays the WAP3205 port types. The port types are: LAN and WLAN .
Status	For the LAN ports, 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.
Rate	For the LAN ports, this displays the port speed 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.
System Status	
Item	This column shows the type of data the WAP3205 is recording.
Data	This column shows the actual data recorded by the WAP3205.
System Up Time	This is the total time the WAP3205 has been on.
Current Date/Time	This field displays your WAP3205's present date and time.
System Resource	
CPU Usage	This displays what percentage of the WAP3205's processing ability is currently used. When this percentage is close to 100%, the WAP3205 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management).
Memory Usage	This shows what percentage of the heap memory the WAP3205 is using.
System Setting	
Configuration Mode	This shows the web configurator mode you are viewing - Expert .
Summary	
Packet Statistics	Click Details... to go to the Monitor > Packet Statistics screen (Section 3.4 on page 30). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click Details... to go to the Monitor > WLAN Station Status screen (Section 3.5 on page 32). Use this screen to view the wireless stations that are currently associated to the WAP3205.

6.4.0.1 Navigation Panel

Use the menu in the navigation panel to configure WAP3205 features in Access Point mode.

The following screen and table show the features you can configure in Access Point mode.

Figure 23 Menu: Access Point Mode



The following table describes the sub-menus.

Table 17 Navigation Panel: Access Point Mode

LINK	TAB	FUNCTION
Status		This screen shows the WAP3205's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
MONITOR		
Log		Use this screen to view the list of activities recorded by your WAP3205.
Packet Statistics		Use this screen to view port status and packet specific statistics.
WLAN Station Status		Use this screen to view the wireless stations that are currently associated to the WAP3205.
CONFIGURATION		
Network		

Table 17 Navigation Panel: Access Point Mode

LINK	TAB	FUNCTION
Wireless LAN	General	Use this screen to configure general wireless LAN settings.
	Security	Use this screen to configure wireless security settings.
	MAC Filter	Use the MAC filter screen to configure the WAP3205 to block access to devices or block the devices from accessing the WAP3205.
	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.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
	WDS	Use this screen to set up Wireless Distribution System (WDS) on your WAP3205.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
	IP Alias	Use this screen to have the WAP3205 apply IP alias to create LAN subnets.
MAINTENANCE		
General		Use this screen to view and change administrative settings such as system and domain names.
Password	Password Setup	Use this screen to change the password of your WAP3205.
Time	Time Setting	Use this screen to change your WAP3205's time and date.
Firmware Upgrade		Use this screen to upload firmware to your WAP3205.
Backup/Restore		Use this screen to backup and restore the configuration or reset the factory defaults to your WAP3205.
Reset/Restart	Restart	This screen allows you to reboot the WAP3205 without turning the power off.
Sys OP Mode		This screen allows you to select whether your device acts as an access point, wireless client or both at the same time.

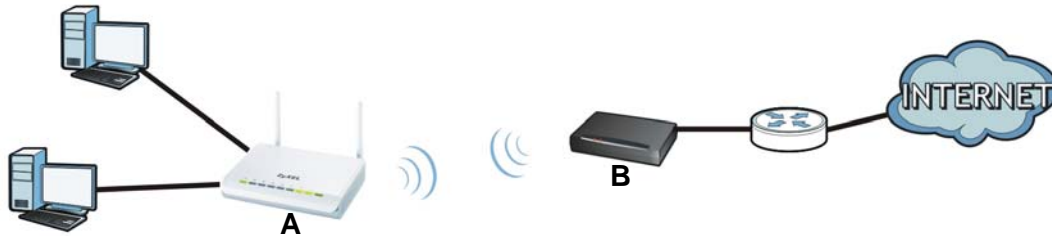
Client Mode

7.1 Overview

Your WAP3205 can act as a wireless client. In wireless client mode, it can connect to an existing network via an access point. Use this mode if you already have an access point or wireless router in your network.

In the example below, one WAP3205 (**A**) is configured as a wireless client and another is used as an access point (**B**). The WAP3205 has two clients that need to connect to the Internet. The WAP3205 wirelessly connects to the available access point (**B**).

Figure 24 Wireless Client Mode



After the WAP3205 and the access point connect, the WAP3205 acquires its WAN IP address from the access point. The clients of the WAP3205 can now surf the Internet.

7.2 What You Can Do

- Use the **Status** screen ([Section 7.4 on page 55](#)) to view read-only information about your WAP3205.
- Use the **LAN** screen ([Chapter 11 on page 101](#)) to set the IP address for your WAP3205.
- Use the **Wireless LAN** screen ([Section 7.5 on page 57](#)) to associate your WAP3205 (acting as a wireless client) with an existing access point.

7.3 What You Need to Know

With the exception of the **Wireless LAN** screens, the **LAN, Monitor, Configuration** and **Maintenance** screens in Client mode are similar to the ones in Access Point Mode. See [Chapter 11 on page 101](#) through [Chapter 12 on page 107](#) of this User's Guide.

7.3.1 Setting your WAP3205 to Client Mode

- 1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.
- 2 To set your WAP3205 to **Client Mode**, go to **Maintenance > Sys OP Mode** and select **Client Mode**.

Figure 25 Changing to Client mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your WAP3205 is already in Client mode.

7.3.2 Accessing the Web Configurator in Client Mode

To login to Web Configurator in Client mode, do the following:

- 1 Connect your computer to the LAN port of the WAP3205.
- 2 The default IP address of the WAP3205 is "192.168.1.2". If you did not change this, you can use the same IP address in Client mode. Open a web browser such as Internet Explorer and type "192.168.1.2" as the web address in your web browser.

If you changed the IP address of your WAP3205 while in Access Point mode, use this IP address in Client mode. The Client mode IP address is always the same as the Access Point mode IP address.

Note: After clicking **Login**, the Easy mode appears. Refer to [Chapter 5 on page 35](#) for the Easy mode screens. Click **Expert Mode** to see the screens described in the sections following this.

7.4 Client Mode Status Screen


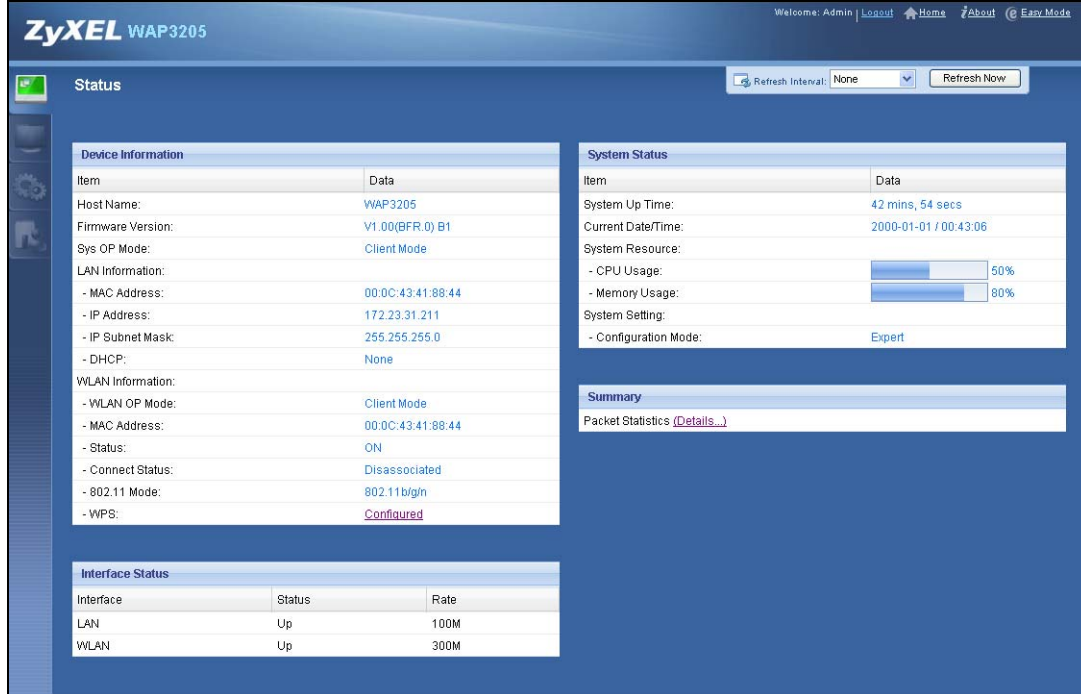
Click  to open the status screen.

Figure 26 Status: Client Mode



The screenshot shows the ZyXEL WAP3205 web interface. The top navigation bar includes 'Welcome: Admin | Logout | Home | About | Easy Mode'. The main content area is titled 'Status' and features a 'Refresh Interval' dropdown set to 'None' and a 'Refresh Now' button. The interface is divided into three main sections:

- Device Information:** A table with columns 'Item' and 'Data'.

Item	Data
Host Name:	WAP3205
Firmware Version:	V1.00(BFR.0) B1
Sys OP Mode:	Client Mode
LAN Information:	
- MAC Address:	00:0C:43:41:88:44
- IP Address:	172.23.31.211
- IP Subnet Mask:	255.255.255.0
- DHCP:	None
WLAN Information:	
- WLAN OP Mode:	Client Mode
- MAC Address:	00:0C:43:41:88:44
- Status:	ON
- Connect Status:	Disassociated
- 802.11 Mode:	802.11b/g/n
- WPS:	Configured
- System Status:** A table with columns 'Item' and 'Data'.

Item	Data
System Up Time:	42 mins, 54 secs
Current Date/Time:	2000-01-01 / 00:43:06
System Resource:	
- CPU Usage:	50%
- Memory Usage:	80%
System Setting:	Expert
- Interface Status:** A table with columns 'Interface', 'Status', and 'Rate'.

Interface	Status	Rate
LAN	Up	100M
WLAN	Up	300M

At the bottom, there is a 'Summary' section with a link for 'Packet Statistics (Details...)'.

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

Table 18 Status Screen: Client Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the System Name you enter in the Maintenance > General screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 4.1.2 on page 33) to which the WAP3205 is set - Client Mode .
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 - Client or None .
WLAN Information	
WLAN OP Mode	This is the device mode (Section 4.1.2 on page 33) to which the WAP3205's wireless LAN is set - Client Mode .
MAC Address	This shows the wireless adapter MAC Address of your device.

Table 18 Status Screen: Client Mode

LABEL	DESCRIPTION
Status	This shows the current status of the Wireless LAN - ON .
Name (SSID)	This shows a descriptive name used to identify the WAP3205 in the wireless LAN.
Connect Status	This shows whether or not the WAP3205 has successfully associated with an access point - Connected or Disassociated .
802.11 Mode	This shows the wireless standard.
WPS	This displays Configured when the WPS has been set up. This displays Unconfigured if the WPS has not been set up. Click the status to display Network > Wireless LAN > WPS screen.
Interface Status	
Interface	This displays the WAP3205 port types. The port types are: LAN and WLAN .
Status	For the LAN and WAN ports, 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.
Rate	For the LAN ports, this displays the port speed 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.
System Status	
Item	This column shows the type of data the WAP3205 is recording.
Data	This column shows the actual data recorded by the WAP3205.
System Up Time	This is the total time the WAP3205 has been on.
Current Date/Time	This field displays your WAP3205's present date and time.
System Resource	
CPU Usage	This displays what percentage of the WAP3205's processing ability is currently used. When this percentage is close to 100%, the WAP3205 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management).
Memory Usage	This shows what percentage of the heap memory the WAP3205 is using.
System Setting	
Configuration Mode	This shows the web configurator mode you are viewing - Expert .
Summary	
Packet Statistics	Click Details... to go to the Monitor > Packet Statistics screen (Section 3.4 on page 30). Use this screen to view port status and packet specific statistics.

7.5 Wireless LAN Profile Screen

Use this screen to view the wireless LAN profile settings of your WAP3205. Go to **Configuration > Wireless LAN > Profile** to open the following screen.

Figure 27 Client Mode: WLAN > Profile

#	Profile	SSID	Channel	Authentication	Encryption	Network Type
<input checked="" type="radio"/>	PROF001	ZyXEL	Auto	WPA-PSK	TKIP	Infrastructure
<input type="radio"/>	PROF002	TWexample	1	OPEN	NONE	Ad Hoc

The following table describes the labels in this screen.

Table 19 Client Mode: WLAN > Profile

LABEL	DESCRIPTION
Profile List	
#	Select a profile to remove, modify or enable it.
Profile	This displays the name of the pre-configured profile. indicates the profile is activated and the WAP3205 connects to the specified wireless network. indicates the profile is activated but the specified wireless network is not available or the WAP3205 fails to associate with the wireless network.
SSID	This displays the SSID of the wireless network with which this profile associates.
Channel	This displays the channel number used by this profile. Auto means the WAP3205 automatically scans for and selects an available channel.
Authentication	This displays the authentication method used by this profile.
Encryption	This displays the data encryption method used by this profile.
Network Type	This displays the network type (Infrastructure or Ad Hoc) of this profile.
Add	Click this button to create a new profile.
Delete	Select a profile and click this button to remove it.
Edit	Select a profile and click this button to modify it.
Activate	Select a profile and click this button to enable it. Note: You can activate only one profile at a time.

7.5.1 Adding a New WLAN Profile

Use this screen to create a new wireless LAN profile for your WAP3205. Click the **Add** button in the **Configuration > Wireless LAN > Profile** screen to open the following screen.

Figure 28 Client Mode: WLAN > Profile > Add

The following table describes the labels in this screen.

Table 20 Client Mode: WLAN > Profile > Add

LABEL	DESCRIPTION
Wireless Setup	
Profile Name	Enter a descriptive name for this profile.
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Security Mode	Select the security mode of the access point to which you want to connect.
Apply	Click Apply to save your changes back to the WAP3205.
Cancel	Click Cancel to go back to the previous screen.

7.5.1.1 No Security

Use this screen if the access point to which you want to connect does not use encryption.

Figure 29 Client Mode: WLAN > Profile: No Security

The following table describes the labels in this screen.

Table 21 Client Mode: WLAN > Profile: No Security

LABEL	DESCRIPTION
Wireless Setup	
Profile Name	Enter a descriptive name for this profile.
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Security Mode	Select No Security in this field.
Apply	Click Apply to save your changes back to the WAP3205.
Cancel	Click Cancel to go back to the previous screen.

7.5.1.2 Static WEP

Use this screen if the access point to which you want to connect to uses WEP security mode.

Figure 30 Client Mode: WLAN > Profile: WEP

The screenshot shows the configuration interface for a WEP profile. It includes sections for 'Wireless Setup' (Profile Name, Network Name (SSID)) and 'Security' (Security Mode: Static WEP, PassPhrase, WEP Encryption: 64-bits, Authentication Method: Open). A 'Note' section provides instructions for 64-bit and 128-bit WEP keys. Below the note, there are radio buttons for 'ASCII' and 'HEX' (selected). Four 'Key' input fields are provided, with 'Key 1' selected. At the bottom, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen..

Table 22 Client Mode: WLAN > Profile: WEP

LABEL	DESCRIPTION
Wireless Setup	
Profile Name	Enter a descriptive name for this profile.
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Security Mode	Select Static WEP to enable data encryption.
PassPhrase	Enter a Passphrase (up to 26 printable characters) and click Generate . A passphrase functions like a password. In WEP security mode, it is further converted by the WAP3205 into a complicated string that is referred to as the "key". This key is requested from all devices wishing to connect to a wireless network.
WEP Encryption	Select 64-bit WEP or 128-bit WEP . This dictates the length of the security key that the network is going to use.
Authentication Method	Select Open or Shared Key from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to log into the wireless network. Keep this setting at Open unless you want to force a key verification before communication between the wireless client and the ZyXEL Device occurs. Select Shared Key to force the clients to provide the WEP key prior to communication.
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 WAP3205 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 WAP3205.
Cancel	Click Cancel to go back to the previous screen.

7.5.1.3 WPA(2)-PSK

Use this screen if the access point to which you want to connect uses WPA(2)-PSK security mode.

Figure 31 Client Mode: WLAN > Profile: WPA-PSK/WPA2-PSK

The following table describes the labels in this screen. .

Table 23 Client Mode: WLAN > Profile: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Wireless Setup	
Profile Name	Enter a descriptive name for this profile.
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Security Mode	Select WPA-PSK or WPA2-PSK to add strong security on this wireless network.
Encryption Type	Select the type of wireless encryption employed by the access point to which you want to connect.
Pre-Shared Key	WPA-PSK or WPA2-PSK uses a simple common password for authentication. Type the pre-shared key employed by the access point to which you want to connect.
Apply	Click Apply to save your changes back to the WAP3205.
Cancel	Click Cancel to go back to the previous screen.

7.5.2 Site Survey Screen

Use this screen to scan for and connect to a wireless network automatically. Go to **Configuration > Wireless LAN > Site Survey** to open the following screen.

Figure 32 Client Mode: WLAN > Site Survey

#	SSID	BSSID	Signal Strength	Channel	Encryption	Authentication	Network Type
<input checked="" type="radio"/>	ZyXEL_Benny	00-13-49-C5-6E-08	10%	2	Not Use	OPEN	Infra.
<input checked="" type="radio"/>	ZyXEL_MIS	00-19-CB-4B-22-0F	39%	1	WEP	Unknown	Infra.
<input type="radio"/>	ZyXEL_MIS_WPA	06-19-CB-4B-22-0F	44%	1	TKIP, AES	WPA, WPA2	Infra.
<input type="radio"/>	ZyXEL_Guest	0A-19-CB-4B-22-0F	34%	1	TKIP, AES	WPA, WPA2	Infra.
<input type="radio"/>	ZyXEL_test_334SH	00-02-CF-98-6E-4C	10%	1	TKIP, AES	WPA-PSK, WPA2-PSK	Infra.
<input type="radio"/>	pqa-3260-p2602hwl	00-13-49-F5-1A-13	0%	3	AES	WPA2-PSK	Infra.
<input type="radio"/>	pqa-3237-test	00-19-CB-73-CC-BA	5%	4	TKIP	WPA-PSK	Infra.
<input type="radio"/>	TWexample	6E-A3-AB-58-F8-4F	91%	1	Not Use	OPEN	Ad Hoc

The following table describes the labels in this screen.

Table 24 Client Mode: WLAN > Site Survey

LABEL	DESCRIPTION
Station Site Survey	
#	Select a wireless device and click Add Profile to open a configuration screen where you can add the selected wireless device to a profile and then enable it.
SSID	This displays the SSID of the wireless device. <input checked="" type="checkbox"/> indicates the wireless device is added to an activated profile and the WAP3205 is connecting to it.
BSSID	This displays the MAC address of the wireless device.
Signal Strength	This displays the strength of the wireless signal. The signal strength mainly depends on the antenna output power and the distance between your WAP3205 and this device.
Channel	This displays the channel number used by this wireless device.
Encryption	This displays the data encryption method used by this wireless device.
Authentication	This displays the authentication method used by this wireless device.
Network Type	This displays the network type (Infrastructure or Ad Hoc) of this wireless device.
Rescan	Click this button to search for available wireless devices within transmission range and update this table.
Add Profile	Select a wireless device and click this button to add it to a profile.

7.5.3 WPS Screen

Use this screen to enable Wi-Fi Protected Setup (WPS) on the WAP3205. Go to **Configuration > Wireless LAN > WPS** to open the following screen.

Figure 33 Client Mode: WLAN > WPS

The screenshot shows the 'WPS' configuration screen. At the top, there are tabs for 'Profile', 'Site Survey', and 'WPS'. Below the tabs, the title is 'Wi-Fi Protected Setup (STA)'. Underneath, there is a 'Station Site Survey' table. The table has the following data:

No.	SSID	BSSID	Signal Strength	Ch.	Auth.	Encrypt	Ver.	Status
<input checked="" type="radio"/>	ZyXEL_test_334SH	0002CF986E4C	20%	1	WPA-PSK; WPA2-PSK	TKIP; AES	1.0	Conf.
<input type="radio"/>	pqa-3237-test	0019CB73CCBA	0%	4	WPA-PSK	TKIP	1.0	Conf.
<input type="radio"/>	ZyXEL	0000994610B0	5%	6	OPEN	Not Use	1.0	Unconf.
<input type="radio"/>	sky-NET	0023F803A4F8	15%	6	WPA2-PSK	AES	1.0	Conf.
<input type="radio"/>	bing-3265-1	00009987AAB1	0%	9	WPA2-PSK	AES	1.0	Unconf.
<input type="radio"/>	ZyLatte	0019CBBB6748	0%	6	OPEN	Not Use	1.0	Conf.

Below the table, there is a PIN field with the value '42947240' and buttons for 'Renew PIN', 'PIN Start', 'PBC Start', and 'Stop'. At the bottom center, there is a 'Rescan' button.

The following table describes the labels in this screen.

Table 25 Client Mode: WLAN > WPS

LABEL	DESCRIPTION
Station Site Survey	
#	Use the radio button to select the wireless device to which you want to connect using WPS.
SSID	This displays the SSID of the wireless device.
BSSID	This displays the MAC address of the wireless device.
Signal Strength	This displays the strength of the wireless signal. The signal strength mainly depends on the antenna output power and the distance between your WAP3205 and this device.
Ch.	This displays the channel number used by this wireless device.
Auth.	This displays the authentication method used by this wireless device.
Encrypt	This displays the data encryption method used by this wireless device.
Ver.	This displays the firmware version running on the wireless device.
Status	This displays Conf. (configured) when WPS has been set up on the wireless device. This displays Unconf. (unconfigured) if WPS has not been set up on the wireless device.
PIN	This displays the PIN number of the WAP3205.
Renew PIN	Click this button to generate a new PIN and display it in the PIN field.
PIN Start	Click this button to perform wireless security information synchronization using the PIN configuration method.
PBC Start	Click this button to perform wireless security information synchronization using the Push Button Configuration (PBC) method.

Table 25 Client Mode: WLAN > WPS (continued)

LABEL	DESCRIPTION
Stop	Click this button to cancel wireless security information synchronization.
Rescan	Click this button to search for available for WPS-enabled devices within transmission range and update this table.

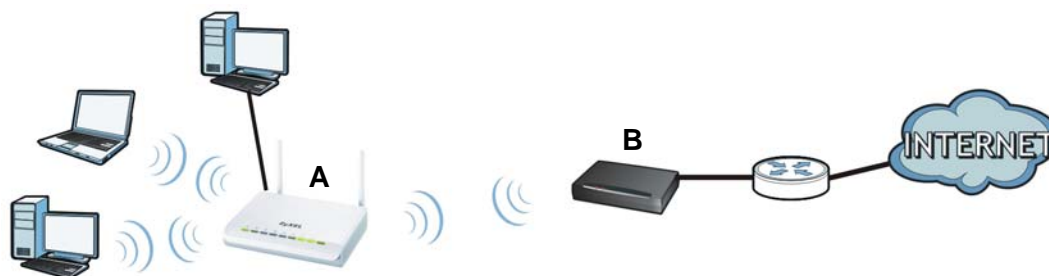
Universal Repeater Mode

8.1 Overview

Your WAP3205 can act as an access point and wireless client at the same time. In this mode, the WAP3205 can connect to an existing network through another access point and also lets wireless clients connect to the network through it. This helps you expand wireless coverage when you have an access point or wireless router already in your network.

In the example below, the WAP3205 (**A**) is configured as a universal repeater. It has three clients that want to connect to the Internet. The WAP3205 wirelessly connects to the available access point (**B**).

Figure 34 Universal Repeater Mode



After the WAP3205 and the access point connect, the WAP3205 acquires its IP address from the access point. The clients of the WAP3205 can now surf the Internet.

8.2 What You Can Do

- Use the **Status** screen ([Section 7.4 on page 55](#)) to view read-only information about your WAP3205.
- Use the **LAN** screen ([Chapter 11 on page 101](#)) to set the IP address for your WAP3205.
- Use the **Wireless LAN > Universal Repeater** screen ([Section 7.5 on page 57](#)) to configure the security between the WAP3205 and another access point.

- Use other **Wireless LAN** screens ([Chapter 10 on page 83](#)) to configure the wireless settings and wireless security between the wireless clients and the WAP3205.

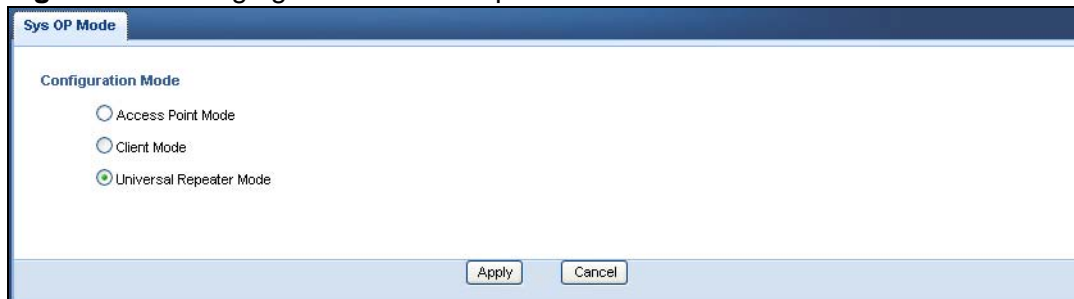
8.3 What You Need to Know

With the exception of the **Wireless LAN > Universal Repeater** screen, other configuration screens in Universal Repeater mode are similar to the ones in Access Point Mode. See [Chapter 11 on page 101](#) through [Chapter 12 on page 107](#) of this User's Guide.

8.3.1 Setting your WAP3205 to Universal Repeater Mode

- 1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.
- 2 To set your WAP3205 to **Universal Repeater Mode**, go to **Maintenance > Sys OP Mode** and select **Universal Repeater Mode**.

Figure 35 Changing to Universal Repeater mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your WAP3205 is already in Universal Repeater mode.

8.3.2 Accessing the Web Configurator in Universal Repeater Mode

To login to Web Configurator in Client mode, do the following:

- 1 Connect your computer to the LAN port of the WAP3205.

- 2 The default IP address of the WAP3205 is "192.168.1.2". If you did not change this, you can use the same IP address in Universal Repeater mode. Open a web browser such as Internet Explorer and type "192.168.1.2" as the web address in your web browser.

If you changed the IP address of your WAP3205 while in Access Point mode, use this IP address in Universal Repeater mode. The Universal Repeater mode IP address is always the same as the Access Point mode IP address.

Note: After clicking **Login**, the Easy mode appears. Refer to [Chapter 5 on page 35](#) for the Easy mode screens. Click **Expert Mode** to see the screens described in the sections following this.

8.4 Universal Repeater Mode Status Screen


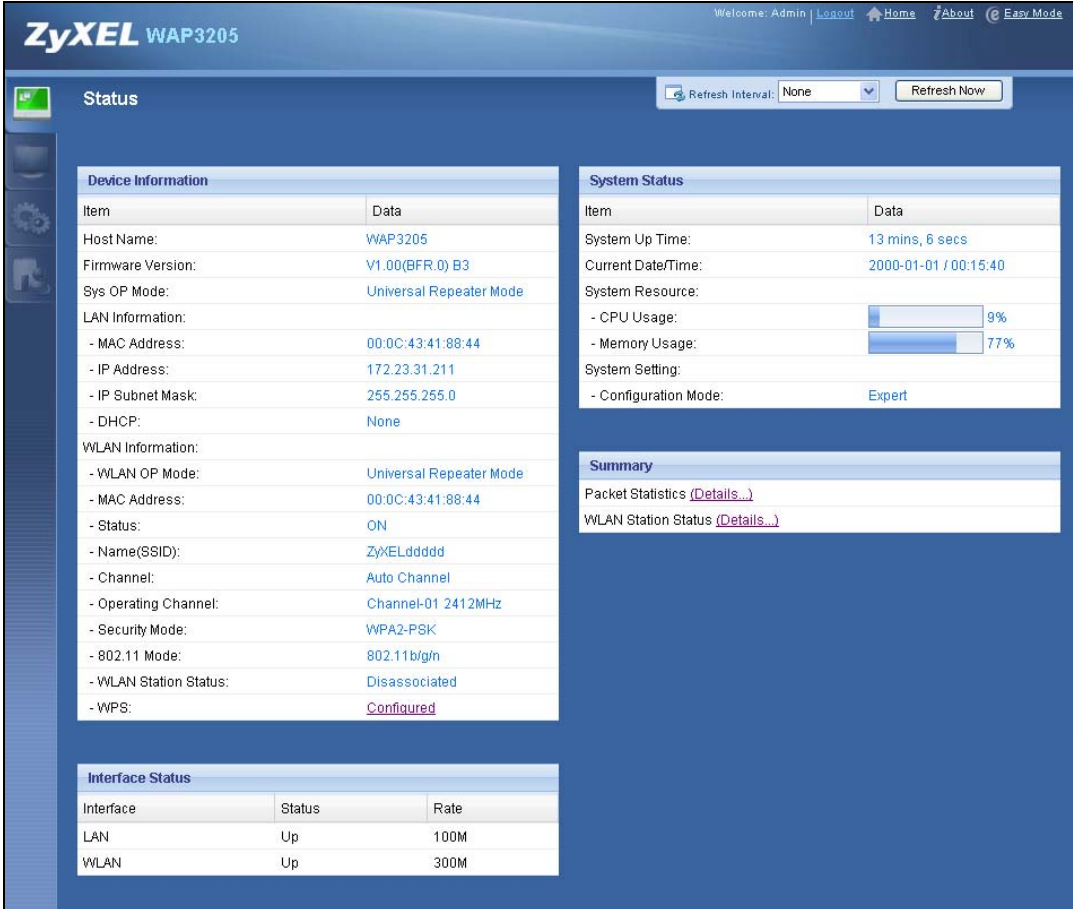
Click  to open the status screen.

Figure 36 Status: Universal Repeater Mode



The screenshot shows the ZyXEL WAP3205 web interface in Universal Repeater Mode. The page title is "ZyXEL WAP3205" and the user is logged in as "Admin". The status screen is divided into several sections:

- Device Information:** A table listing various system parameters.
- System Status:** A table showing system up time, current date/time, and resource usage (CPU and Memory).
- Interface Status:** A table showing the status and rate of the LAN and WLAN interfaces.

Item	Data
Host Name:	WAP3205
Firmware Version:	V1.00(BFR.0) B3
Sys OP Mode:	Universal Repeater Mode
LAN Information:	
- MAC Address:	00:0C:43:41:88:44
- IP Address:	172.23.31.211
- IP Subnet Mask:	255.255.255.0
- DHCP:	None
WLAN Information:	
- WLAN OP Mode:	Universal Repeater Mode
- MAC Address:	00:0C:43:41:88:44
- Status:	ON
- Name(SSID):	ZyXELdddd
- Channel:	Auto Channel
- Operating Channel:	Channel-01 2412MHz
- Security Mode:	WPA2-PSK
- 802.11 Mode:	802.11b/g/n
- WLAN Station Status:	Disassociated
- WPS:	Configured

Item	Data
System Up Time:	13 mins, 6 secs
Current Date/Time:	2000-01-01 / 00:15:40
System Resource:	
- CPU Usage:	9%
- Memory Usage:	77%
System Setting:	
- Configuration Mode:	Expert

Interface	Status	Rate
LAN	Up	100M
WLAN	Up	300M

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

Table 26 Status Screen: Universal Repeater Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the System Name you enter in the Maintenance > General screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 4.1.2 on page 33) to which the WAP3205 is set - Universal Repeater Mode .
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 - Client or None .
WLAN Information	
WLAN OP Mode	This is the device mode (Section 4.1.2 on page 33) to which the WAP3205's wireless LAN is set - Universal Repeater Mode .
MAC Address	This shows the wireless adapter MAC Address of your device.
Status	This shows the current status of the Wireless LAN - ON .
Name (SSID)	This shows a descriptive name used to identify the WAP3205 in the wireless LAN.
Channel	This shows the channel number which you select manually or the WAP3205 automatically scans and selects.
Operating Channel	This shows the channel number which the WAP3205 is currently using over the wireless LAN.
Security Mode	This shows the level of wireless security the WAP3205 is using.
802.11 Mode	This shows the wireless standard.
WLAN Station Status	This shows whether a wireless station is currently associated with the WAP3205.
WPS	This displays Configured when the WPS has been set up. This displays Unconfigured if the WPS has not been set up. Click the status to display Network > Wireless LAN > WPS screen.
Interface Status	
Interface	This displays the WAP3205 port types. The port types are: LAN and WLAN .
Status	For the LAN and WAN ports, 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.

Table 26 Status Screen: Universal Repeater Mode

LABEL	DESCRIPTION
Rate	For the LAN ports, this displays the port speed 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.
System Status	
Item	This column shows the type of data the WAP3205 is recording.
Data	This column shows the actual data recorded by the WAP3205.
System Up Time	This is the total time the WAP3205 has been on.
Current Date/Time	This field displays your WAP3205's present date and time.
System Resource	
CPU Usage	This displays what percentage of the WAP3205's processing ability is currently used. When this percentage is close to 100%, the WAP3205 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management).
Memory Usage	This shows what percentage of the heap memory the WAP3205 is using.
System Setting	
Configuration Mode	This shows the web configurator mode you are viewing - Expert .
Summary	
Packet Statistics	Click Details... to go to the Monitor > Packet Statistics screen (Section 3.4 on page 30). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click Details... to go to the Monitor > WLAN Station Status screen (Section 3.5 on page 32). Use this screen to view the wireless stations that are currently associated to the WAP3205.

8.5 Universal Repeater Screen

Use this screen to enter the SSID and select the wireless security mode used by the wireless device to which you want to connect. Go to **Configuration > Wireless LAN > Universal Repeater** to open the **Universal Repeater** screen. The screen varies depending on security mode.

8.5.1 No Security

Figure 37 Universal Repeater Mode: Wireless LAN > Universal Repeater: No Security

The screenshot shows the 'Universal Repeater' configuration page. At the top, there are tabs for 'General', 'Security', 'MAC Filter', 'Advanced', 'QoS', 'WPS', 'WPS Station', 'Scheduling', and 'Universal Repeater'. The 'Universal Repeater' tab is selected. Below the tabs, the 'Universal Repeater Parameters' section contains three input fields: 'SSID', 'MAC Address (Optional)', and 'Security Mode'. The 'Security Mode' dropdown menu is set to 'No Security'. At the bottom of the page, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 27 Universal Repeater Mode: Wireless LAN > Universal Repeater: No Security

LABEL	DESCRIPTION
Universal Repeater Parameters	
SSID	Enter the name of the access point to which you are connecting.
MAC Address (Optional)	Enter the MAC address of the access point to which you are connecting.
Security Mode	Select No Security if the access point to which you want to connect does not use encryption.
Apply	Click Apply to save your changes back to the WAP3205.
Reset	Click Reset to reload the previous configuration for this screen.

8.5.2 Static WEP

Figure 38 Universal Repeater Mode: Wireless LAN > Universal Repeater: Static WEP

The screenshot shows the 'Universal Repeater' configuration page for Static WEP mode. At the top, there are tabs for 'General', 'Security', 'MAC Filter', 'Advanced', 'QoS', 'WPS', 'WPS Station', 'Scheduling', and 'Universal Repeater'. The 'Universal Repeater' tab is selected. Below the tabs, the 'Universal Repeater Parameters' section contains four input fields: 'SSID', 'MAC Address (Optional)', 'Security Mode', and 'Encryption Type'. The 'Security Mode' dropdown menu is set to 'Static WEP' and the 'Encryption Type' dropdown menu is set to 'Open'. Below this section is the 'WEP Key' section, which contains a 'WEP Default Key' dropdown menu set to 'Key 1', and four rows of 'WEP Key' input fields (Key 1 through Key 4), each with an 'ASCII' dropdown menu. At the bottom of the page, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 28 Universal Repeater Mode: Wireless LAN > Universal Repeater: Static WEP

LABEL	DESCRIPTION
Universal Repeater Parameters	
SSID	Enter the name of the access point to which you are connecting.
MAC Address (Optional)	Enter the MAC address of the access point to which you are connecting.
Security Mode	Select Static WEP if the access point to which you want to connect uses WEP data encryption.
Encryption Type	Select Open or Shared Key from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to log into the wireless network. Keep this setting at Open unless you want to force a key verification before communication between the wireless client and the ZyXEL Device occurs. Select Shared Key to force the clients to provide the WEP key prior to communication.
WEP Key	
WEP Default Key	Select a default WEP key to use for data encryption.
WEP Key 1 ~ WEP Key 4	The WEP keys are used to encrypt data. Both the WAP3205 and the access point must use the same WEP key for data transmission. If you chose HEX , enter 10 or 26 hexadecimal characters in the range of "A-F", "a-f" and "0-9" (for example, 11AA22BB33) for a 64-bit or 128-bit WEP key respectively. If you chose ASCII , enter any 5 or 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for a 64-bit or 128-bit WEP key respectively. You must configure at least one key, only one key can be activated at any one time.
Apply	Click Apply to save your changes back to the WAP3205.
Reset	Click Reset to reload the previous configuration for this screen.

8.5.3 WPA(2)-PSK

Figure 39 Universal Repeater Mode: Wireless LAN > Universal Repeater: WPA(2)-PSK

The screenshot shows a web interface for configuring a Universal Repeater. At the top, there are several tabs: General, Security, MAC Filter, Advanced, QoS, WPS, WPS Station, Scheduling, and Universal Repeater. The 'Universal Repeater' tab is selected. Below the tabs, the 'Universal Repeater Parameters' section contains the following fields:

- SSID: A text input field.
- MAC Address (Optional): A text input field.
- Security Mode: A dropdown menu with 'WPA2-PSK' selected.
- Encryption Type: A dropdown menu with 'AES' selected.
- Pre-Shared Key: A text input field.

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 29 Universal Repeater Mode: Wireless LAN > Universal Repeater: WPA(2)-PSK

LABEL	DESCRIPTION
Universal Repeater Parameters	
SSID	Enter the name of the access point to which you are connecting.
MAC Address (Optional)	Enter the MAC address of the access point to which you are connecting.
Security Mode	Select WPA-PSK or WPA2-PSK if the access point to which you want to connect uses WPA-PSK or WPA2-PSK.
Encryption Type	Select the type of wireless encryption employed by the access point to which you want to connect.
Pre-Shared Key	WPA-PSK or WPA2-PSK uses a simple common password for authentication. Type the password employed by the access point to which you want to connect.
Apply	Click Apply to save your changes back to the WAP3205.
Reset	Click Reset to reload the previous configuration for this screen.

9.1 Overview

This chapter provides tutorials for your WAP3205 (in access point or universal repeater mode) as follows:

- [Connecting to the Internet from an Access Point](#)
- [Configuring Wireless Security Using WPS](#)
- [Enabling and Configuring Wireless Security \(No WPS\)](#)

9.2 Connecting to the Internet from an Access Point

This section gives you an example of how to set up an access point (AP) and wireless client (a notebook (**B**), in this example) for wireless communication. **B** can access the Internet through the access point (**A**) wirelessly.

Figure 40 Wireless Access Point Connection to the Internet



9.3 Configuring Wireless Security Using WPS

This section gives you an example of how to set up wireless network using WPS. This example uses the WAP3205 as the AP and NWD-211AN as the wireless client which connects to a notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCI card).

There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See [Section 9.3.1 on page 74](#). This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the WAP3205's interface. See [Section 9.3.2 on page 75](#). This is the more secure method, since one device can authenticate the other.

9.3.1 Push Button Configuration (PBC)

- 1 Make sure that your WAP3205 is turned on and that it is within range of your computer.
- 2 Make sure that you have installed the wireless client (this example uses the NWD-211AN) driver and utility in your notebook.
- 3 In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button)
- 4 Log into WAP3205's Web Configurator and press the **Push Button** button in the **Network > Wireless Client > WPS Station** screen.

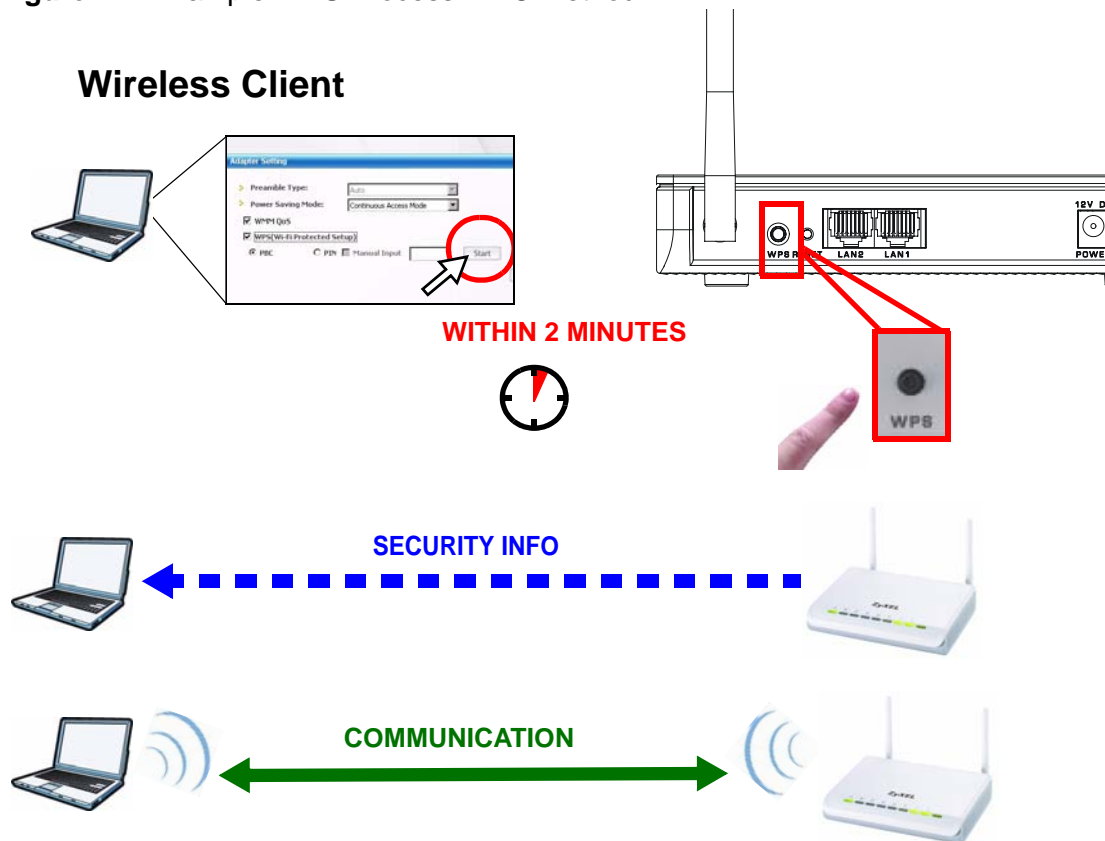
Note: Your WAP3205 has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The WAP3205 sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the WAP3205 securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both WAP3205 and wireless client (the NWD-211AN in this example).

Figure 41 Example WPS Process: PBC Method



9.3.2 PIN Configuration

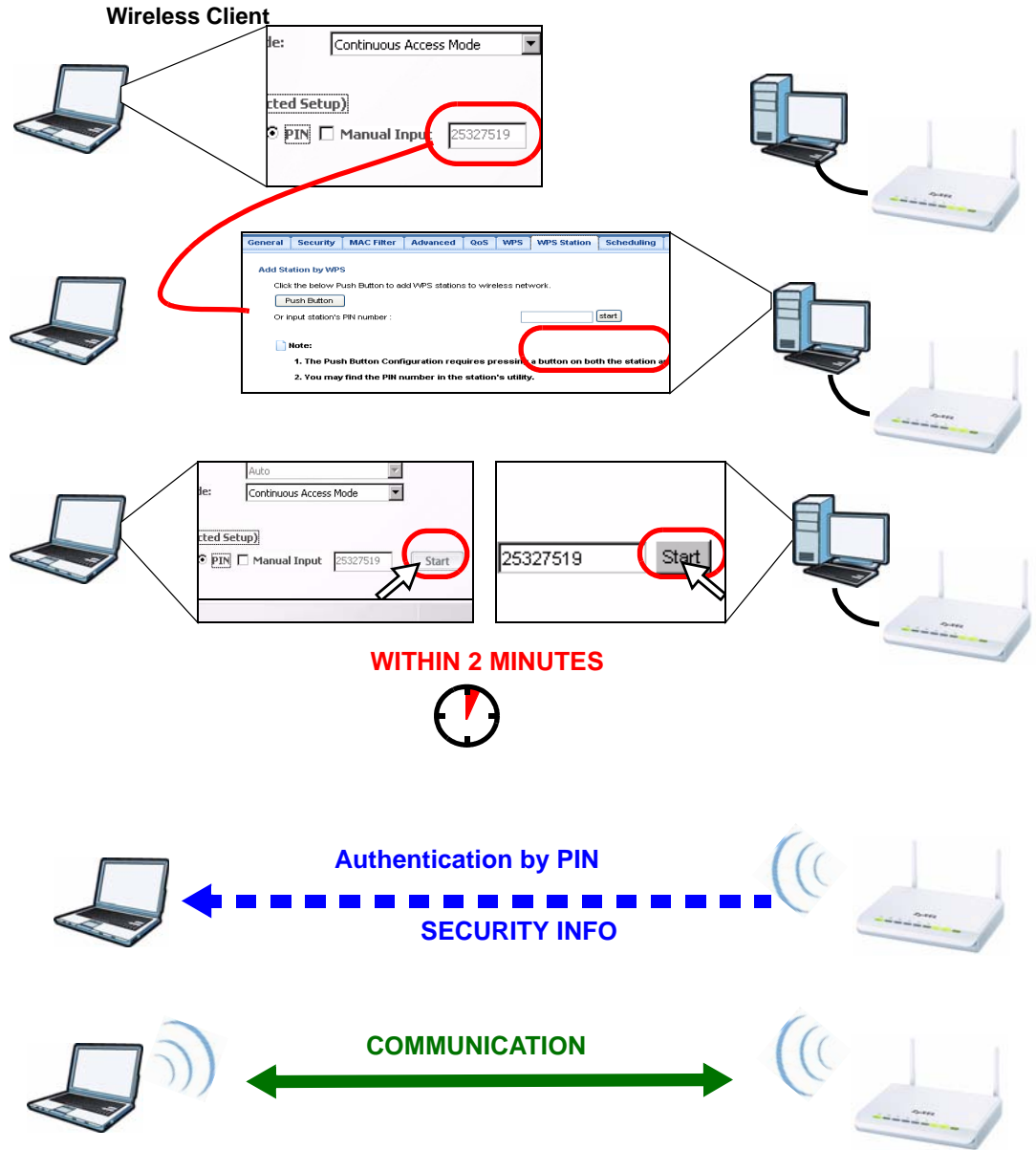
When you use the PIN configuration method, you need to use both WAP3205's configuration interface and the client's utilities.

- 1 Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.
- 2 Enter the PIN number to the **PIN** field in the **Network > Wireless LAN > WPS Station** screen on the WAP3205.
- 3 Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the WAP3205's **WPS Station** screen within two minutes.

The WAP3205 authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the WAP3205 securely.

The following figure shows you the example to set up wireless network and security on WAP3205 and wireless client (ex. NWD-211AN in this example) by using PIN method.

Figure 42 Example WPS Process: PIN Method



9.4 Enabling and Configuring Wireless Security (No WPS)

This example shows you how to configure wireless security settings with the following parameters on your WAP3205.

SSID	SSID_Example3
Channel	Auto
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your WAP3205.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see [Section 2.2 on page 23](#)).

- 1 Open the **Wireless LAN > General** screen in the AP's Web Configurator.
- 2 Enter **SSID_Example3** as the SSID and select a channel or select **Auto Channel Selection** to have the WAP3205 scans for and select an available channel automatically. Click **Apply**.

Figure 43 Tutorial: Network > Wireless LAN > General

The screenshot shows the 'Wireless Setup' configuration page. The 'Wireless LAN' status is 'ON'. The 'Network Name (SSID)' field is set to 'SSID_Example3'. The 'Channel Selection' dropdown is set to 'Channel-01 2412MHz' and the 'Auto Channel Selection' checkbox is checked. The 'Operating Channel' is 'Channel-01 2412MHz'. There are 'Apply' and 'Cancel' buttons at the bottom.

- 3 Click the **Security** tab.

- Select the SSID (**SSID_Example3**) for which you want to configure the security. Set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Figure 44 Tutorial: Network > Wireless LAN > Security

The screenshot shows the Security configuration page for the ZyXEL WAP3205. The Security Mode is set to WPA-PSK, the Pre-Shared Key is 'ThisismyWPA-PSKpre-sharedkey', and the Group Key Update Timer is 3600 seconds. A note states: 'Note: WPA-PSK and WPA2-PSK can be configured when WPS enabled'. The Apply and Cancel buttons are visible at the bottom.

- 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 45 Tutorial: Checking Wireless Settings

The screenshot shows the Status page for the ZyXEL WAP3205. The WLAN Information section is highlighted with a red box, showing settings like WLAN OP Mode (Access Point Mode), MAC Address (00:0C:43:41:88:44), Status (ON), Name (SSID_Example3), Channel (Auto Channel), Operating Channel (Channel-01 2412MHz), Security Mode (WPA-PSK), 802.11 Mode (802.11b/g/n), and WPS (Configured). The Interface Status section is also highlighted with a red box, showing WLAN as Up with a rate of 300M.

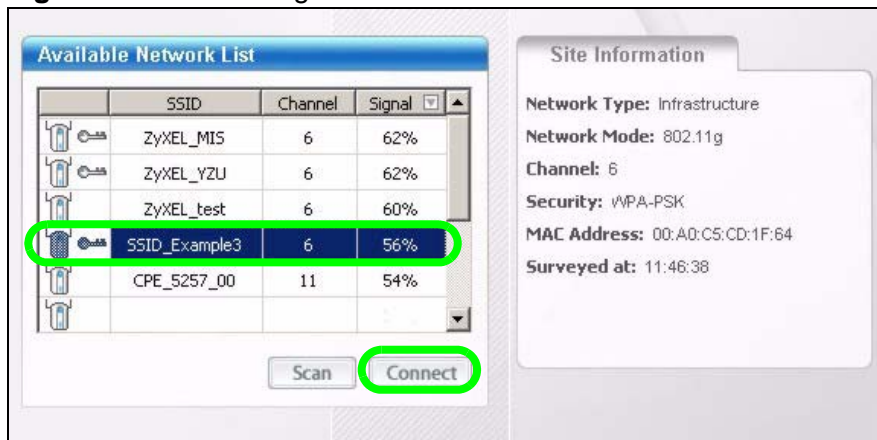
Item	Data	
Host Name:	WAP3205	
Firmware Version:	V1.00(BFR.0) B1	
Sys OP Mode:	Access Point Mode	
LAN Information:		
- MAC Address:	00:0C:43:41:88:44	
- IP Address:	172.23.31.211	
- IP Subnet Mask:	255.255.255.0	
- Default Gateway:	172.23.31.254	
- DHCP:	None	
WLAN Information:		
- WLAN OP Mode:	Access Point Mode	
- MAC Address:	00:0C:43:41:88:44	
- Status:	ON	
- Name(SSID):	SSID_Example3	
- Channel:	Auto Channel	
- Operating Channel:	Channel-01 2412MHz	
- Security Mode:	WPA-PSK	
- 802.11 Mode:	802.11b/g/n	
- WPS:	Configured	
Interface Status		
Interface	Status	Rate
LAN	Up	100M
WLAN	Up	300M

9.4.1 Configure Your Notebook

Note: We use the ZyXEL NWD-211AN wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

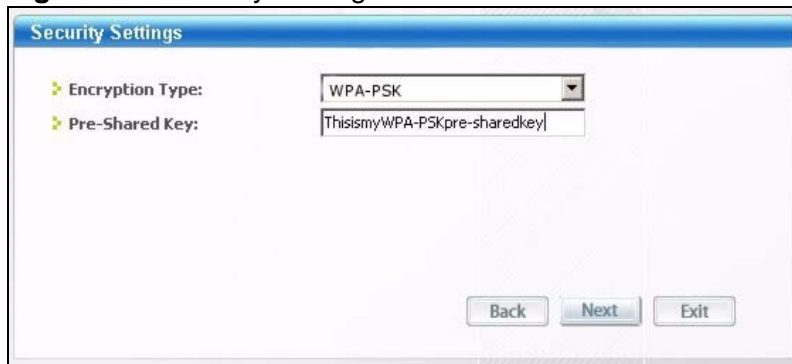
- 1 The WAP3205 supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.
- 2 Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless adapter's User's Guide for information on how to do that.
- 3 After you've installed the utility, open it. If you cannot see your utility's icon on your screen, go to **Start > Programs** and click on your utility in the list of programs that appears. The utility displays a list of APs within range, as shown in the example screen below.
- 4 Select SSID_Example3 and click **Connect**.

Figure 46 Connecting a Wireless Client to a Wireless Network

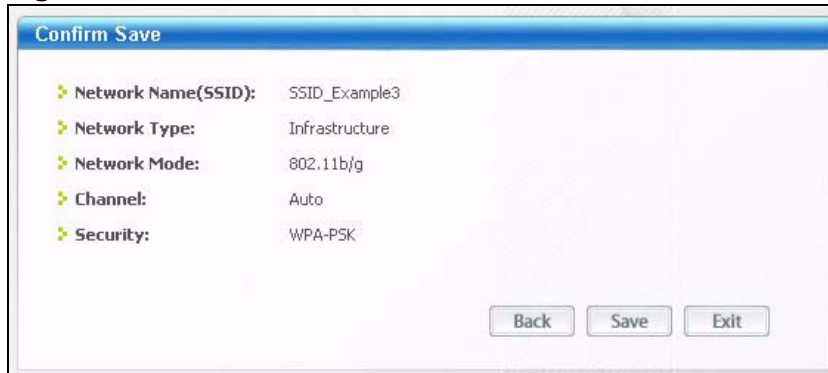


- 5 Select WPA-PSK and type the security key in the following screen. Click **Next**.

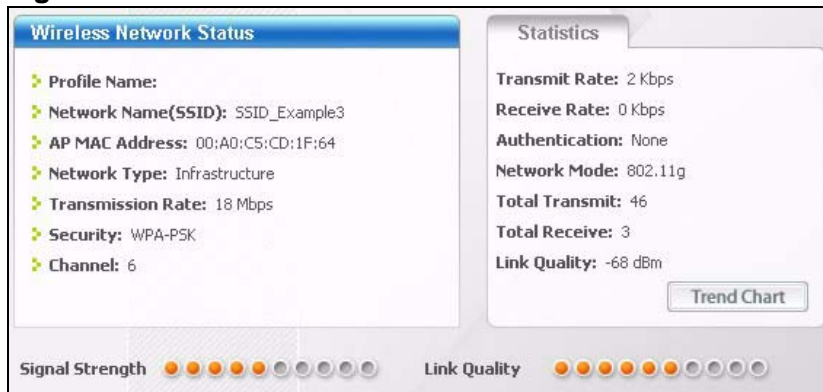
Figure 47 Security Settings



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

Figure 48 Confirm Save

- Check the status of your wireless connection in the screen below. If your wireless connection is weak or you have no connection, see the Troubleshooting section of this User's Guide.

Figure 49 Link Status

If your connection is successful, 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.

PART II

Configuration

Wireless LAN (83)

LAN (101)

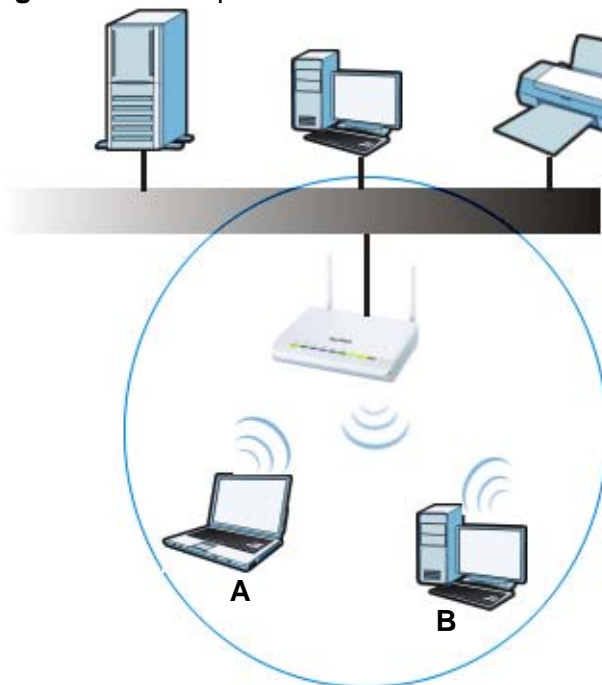
Wireless LAN

10.1 Overview

This chapter discusses how to configure the wireless network settings in your WAP3205. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 50 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 WAP3205 is the AP.

10.2 What You Can Do

- Use the **General** screen ([Section 10.4 on page 87](#)) to enter the SSID, enable intra-BSS traffic and select the channel.
- Use the **Security** screen ([Section 10.5 on page 88](#)) to configure wireless security between the WAP3205 and the wireless clients.
- Use the **MAC Filter** screen ([Section 10.6 on page 92](#)) to allow or deny wireless stations based on their MAC addresses from connecting to the WAP3205.
- Use the **Advanced** screen ([Section 10.7 on page 93](#)) to configure wireless advanced features, such as set the RTS/CTS Threshold and HT physical mode.
- Use the **QoS** screen ([Section 10.8 on page 95](#)) to enable Wifi MultiMedia Quality of Service (WMMQoS). This allows the WAP3205 to automatically set priority levels to services, such as e-mail, VoIP, chat, and so on.
- Use the **WPS** screen ([Section 10.9 on page 95](#)) to quickly set up a wireless network with strong security, without having to configure security settings manually.
- Use the **WPS Station** screen ([Section 10.10 on page 97](#)) to add a wireless station using WPS.
- Use the **Scheduling** screen ([Section 10.11 on page 97](#)) to set the times your wireless LAN is turned on and off.
- Use the **WDS** screen ([Section 10.12 on page 99](#)) to configure Wireless Distribution System on your WAP3205.

10.3 What You Should Know

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.

10.3.1 Wireless Security Overview

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

10.3.1.1 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.

10.3.1.2 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.

10.3.1.3 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.

-
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.

The types of encryption you can choose depend on the type of user authentication.

Table 30 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION
Weakest	No Security
↕	WEP
↕	WPA-PSK
Strongest	WPA2-PSK

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA-PSK. Therefore, you should set up **WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK** or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

When you select **WPA2-PSK** in your WAP3205, 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** (depending on the type of wireless network login) and select the **WPA Compatible** option in the WAP3205.

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.

10.3.1.4 WPS

WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the [Section 9.3 on page 73](#).

10.3.1.5 WDS

Wireless Distribution System or WDS security is used between bridged APs. It 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.

10.4 General Wireless LAN Screen

Use this screen to enter the SSID, select the channel and enable intra-BSS traffic.

Note: If you are configuring the WAP3205 from a computer connected to the wireless LAN and you change the WAP3205'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 WAP3205's new settings.

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

Figure 51 Network > Wireless LAN > General

The screenshot shows the 'General' tab of the 'Wireless Setup' configuration page. The 'Wireless LAN' status is 'ON'. The 'Network Name(SSID)' is 'ZyXEL'. There are three 'Name(SSID)' fields (SSID1, SSID2, SSID3) and a 'Channel Selection' dropdown set to 'Channel-01 2412MHz'. The 'Operating Channel' is 'Channel-10 2457MHz'. There are checkboxes for 'Hide' and 'Enable Intra-BSS Traffic' for each SSID and for 'Auto Channel Selection'.

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

Table 31 Network > Wireless LAN > General

LABEL	DESCRIPTION
Wireless Setup	
Wireless LAN	This is turned on by default. The current wireless state is reflected in this field.
Network Name(SSID) or Name(SSID1 ~3)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN. You can configure up to four SSIDs to enable multiple BSSs (Basic Service Sets) on the WAP3205. This allows you to use one access point to provide several BSSs simultaneously. You can then assign varying security types to different SSIDs. Wireless clients can use different SSIDs to associate with the same access point.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a wireless client cannot obtain the SSID through scanning using a site survey tool.

Table 31 Network > Wireless LAN > General

LABEL	DESCRIPTION
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 clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other.
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 frequency band and the country you are in. This option is only available if Auto Channel Selection is disabled.
Auto Channel Selection	Select the check box to have the WAP3205 automatically scan for and select a channel which is not used by another device.
Operating Channel	This displays the channel the WAP3205 is currently using.
Apply	Click Apply to save your changes back to the WAP3205.
Reset	Click Reset to reload the previous configuration for this screen.

10.5 Wireless Security Screen

Use this screen to select the wireless security mode for each SSID. Click **Network > Wireless LAN > Security** to open the **Security** screen. The screen varies depending on what you select in the **Security Mode** field.

10.5.1 No Security

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

Note: If you do not enable any wireless security on your WAP3205, your network is accessible to any wireless networking device that is within range.

Figure 52 Network > Wireless LAN > Security: No Security

The screenshot shows the configuration page for Wireless LAN Security. The 'Security' tab is active. The 'SSID' dropdown menu is set to 'ZyXEL'. The 'Security Mode' dropdown menu is set to 'No Security'. Below these fields, there is a note: 'Note: WPA-PSK and WPA2-PSK can be configured when WPS enabled'. At the bottom of the page, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 32 Network > Wireless LAN > Security: No Security

LABEL	DESCRIPTION
SSID	Select the SSID for which you want to configure the security.
Security Mode	Choose No Security from the drop-down list box.
Apply	Click Apply to save your changes back to the WAP3205.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.5.2 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 WAP3205 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.

Select **Static WEP** from the **Security Mode** list.

Figure 53 Network > Wireless LAN > Security: Static WEP

The screenshot shows the configuration page for Static WEP. At the top, there are tabs for General, Security, MAC Filter, Advanced, QoS, WPS, WPS Station, Scheduling, and WDS. The Security tab is active. The SSID is set to ZyXEL. The Security Mode is set to Static WEP. There is a PassPhrase field with a Generate button. The WEP Encryption is set to 64-bits. The Authentication Method is set to Shared Key. A Note indicates that for 64-bit WEP, 5 ASCII or 10 hexadecimal characters are needed for each key, and for 128-bit WEP, 13 ASCII or 26 hexadecimal characters are needed. Below this, there are radio buttons for ASCII and HEX, and four key input fields labeled Key 1 through Key 4. A final Note states that WPA-PSK and WPA2-PSK can be configured when WPS is enabled. At the bottom, there are Apply and Cancel buttons.

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

Table 33 Network > Wireless LAN > Security: Static WEP

LABEL	DESCRIPTION
SSID	Select the SSID for which you want to configure the security.
Security Mode	Select Static WEP to enable data encryption.
PassPhrase	Enter a Passphrase (up to 26 printable characters) and click Generate. A passphrase functions like a password. In WEP security mode, it is further converted by the WAP3205 into a complicated string that is referred to as the "key". This key is requested from all devices wishing to connect to a wireless network.
WEP Encryption	Select 64-bits or 128-bits . This dictates the length of the security key that the network is going to use.
Authentication Method	Select Auto or Shared Key from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Keep this setting at Auto unless you want to force a key verification before communication between the wireless client and the WAP3205 occurs. Select Shared Key to force the clients to provide the WEP key prior to communication.
ASCII	Select this option in order to enter ASCII characters as WEP key.

Table 33 Network > Wireless LAN > Security: Static WEP

LABEL	DESCRIPTION
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 WAP3205 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 WAP3205.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.5.3 WPA-PSK/WPA2-PSK

Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 54 Network > Wireless LAN > Security: WPA-PSK/WPA2-PSK

The following table describes the labels in this screen.

Table 34 Network > Wireless LAN > Security: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
SSID	Select the SSID for which you want to configure the security.
Security Mode	Select WPA-PSK or WPA2-PSK to enable data encryption.
WPA Compatible	This field appears when you choose WPA2-PSK as the Security Mode . Check this field to allow wireless devices using WPA-PSK security mode to connect to your WAP3205.

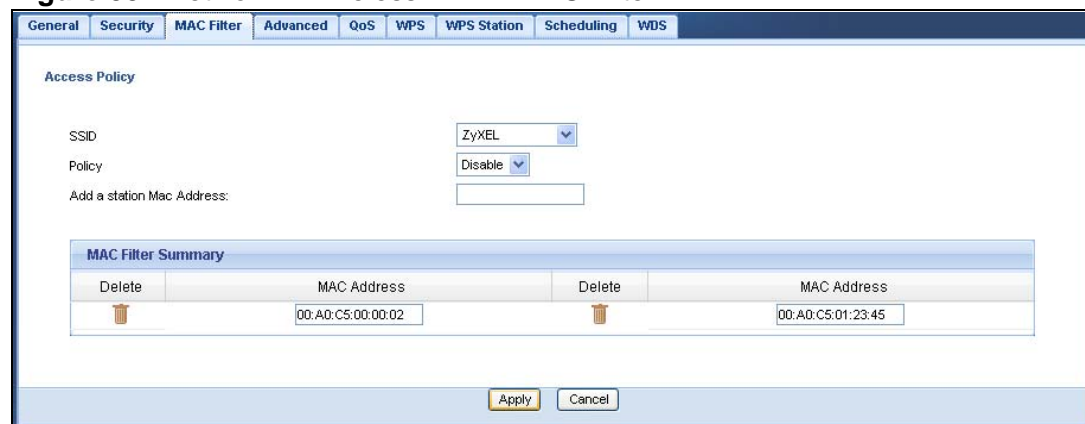
Table 34 Network > Wireless LAN > Security: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Pre-Shared Key	WPA-PSK/WPA2-PSK uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP sends a new group key out to all clients. The default is 3600 seconds (60 minutes).
Apply	Click Apply to save your changes back to the WAP3205.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.6 MAC Filter

The MAC filter screen allows you to configure the WAP3205 to give exclusive access to devices (Allow) or exclude devices from accessing the WAP3205 (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 WAP3205's MAC filter settings, click **Network > Wireless LAN > MAC Filter**. The screen appears as shown.

Figure 55 Network > Wireless LAN > MAC Filter

The following table describes the labels in this menu.

Table 35 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Access Policy	
SSID	Select the SSID for which you want to configure MAC filtering.

Table 35 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Policy	<p>Define the filter action for the list of MAC addresses in the MAC Address table.</p> <p>Select Disable to deactivate the MAC filtering rule you configure below.</p> <p>Select Allow to permit access to the WAP3205, MAC addresses not listed will be denied access to the WAP3205.</p> <p>Select Reject to block access to the WAP3205, MAC addresses not listed will be allowed to access the WAP3205</p>
Add a station Mac Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the WAP3205 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. Click Add .
MAC Filter Summary	
Delete	Click the delete icon to remove the MAC address from the list.
MAC Address	This is the MAC address of the wireless station that are allowed or denied access to the WAP3205.
Apply	Click Apply to save your changes back to the WAP3205.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.7 Wireless LAN Advanced Screen

Use this screen to allow wireless advanced features, such as the output power, RTS/CTS Threshold and high-throughput physical mode settings.

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

Figure 56 Network > Wireless LAN > Advanced

The screenshot displays the 'Wireless Advanced Setup' configuration page. At the top, there are tabs for 'General', 'Security', 'MAC Filter', 'Advanced', 'QoS', 'WPS', 'WPS Station', 'Scheduling', and 'WDS'. The 'Advanced' tab is selected. The settings are as follows:

- RTS/CTS Threshold: 2346 (range 256 ~ 2346)
- Fragmentation Threshold: 2346 (range 256 ~ 2346)
- Output Power: 100%
- Network Mode: 11b/g/n mixed mode
- HT Physical Mode:
 - Operating Mode: Mixed Green
 - Channel Band/Width: 20 20/40
 - Guard Interval: long Auto
 - Extension Channel: AUTO

At the bottom of the screen, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 36 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 256 and 2432.
Fragmentation Threshold	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 .
Output Power	Set the output power of the WAP3205 in this field. If there is a high density of APs in an area, decrease the output power of the WAP3205 to reduce interference with other APs. Select one of the following 100% , 90% , 75% , 50% , 25% or 10% . See the product specifications for more information on your WAP3205's output power.
Network Mode	Select 11b only to allow only IEEE 802.11b compliant WLAN devices to associate with the WAP3205. Select 11g only to allow only IEEE 802.11g compliant WLAN devices to associate with the WAP3205. Select 11 b/g mixed mode to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the WAP3205. The transmission rate of your WAP3205 might be reduced. Select 11 b/g/n mixed mode to allow both IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the WAP3205. The transmission rate of your WAP3205 might be reduced.
HT (High Throughput) Physical Mode - Use the fields below to configure the 802.11 wireless environment of your WAP3205.	
Operating Mode	Choose this according to the wireless mode(s) used in your network. Mixed - Select this if the wireless clients in your network use different wireless modes (for example, IEEE 802.11b/g and IEEE 802.11n modes) Green - Select this if the wireless clients in your network uses only one type of wireless mode (for example, IEEE 802.11 n only)
Channel Bandwidth	Select the channel bandwidth you want to use for your wireless network. It is recommended that you select 20/40 (20/40 MHz). Select 20 MHz if you want to lessen radio interference with other wireless devices in your neighborhood.
Guard Interval	Select Auto to increase data throughput. However, this may make data transfer more prone to errors. Select Long to prioritize data integrity. This may be because your wireless network is busy and congested or the WAP3205 is located in an environment prone to radio interference.
Extension Channel	This is set to Auto by default. If you select 20/40 as your Channel Bandwidth , the extension channel enables the WAP3205 to get higher data throughput. This also lowers radio interference and traffic.

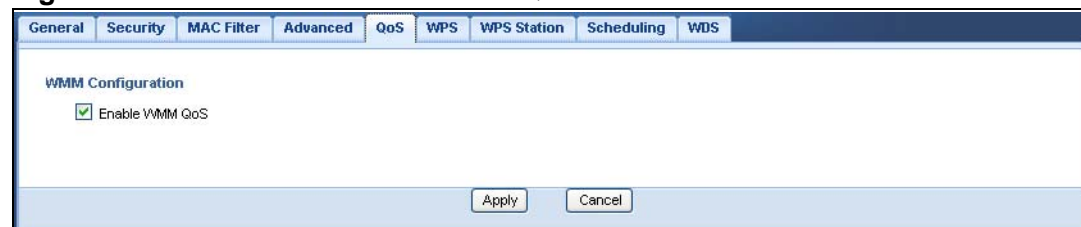
Table 36 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the WAP3205.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.8 Quality of Service (QoS) Screen

The QoS screen allows you to automatically give a service (such as VoIP and video) a priority level.

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

Figure 57 Network > Wireless LAN > QoS

The following table describes the labels in this screen.

Table 37 Network > Wireless LAN > QoS

LABEL	DESCRIPTION
Enable WMM QoS	Check this to have the WAP3205 automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Apply	Click Apply to save your changes to the WAP3205.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.9 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Network > Wireless LAN > WPS** tab.

Note: With WPS, wireless clients can only connect to the wireless network using the first SSID on the WAP3205.

Figure 58 Network > Wireless LAN > WPS

The following table describes the labels in this screen.

Table 38 Network > Wireless LAN > WPS

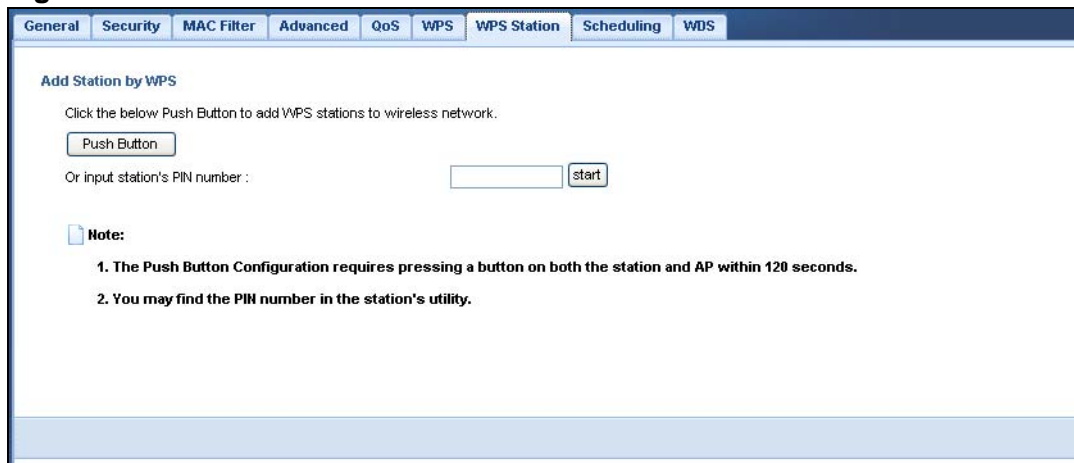
LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select this to enable the WPS feature.
PIN Number	This displays a PIN number last time system generated. Click Generate to generate a new PIN number.
Status	
Status	This displays Configured when the WAP3205 has connected to a wireless network using WPS or when Enable WPS is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays Unconfigured if WPS is disabled and there are no wireless or wireless security changes on the WAP3205 or you click Release_Configuration to remove the configured wireless and wireless security settings.
Release Configuration	This button is only available when the WPS status displays Configured . Click this button to remove all configured wireless and wireless security settings for WPS connections on the WAP3205.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the WAP3205.
SSID	This is the name of the wireless network (the WAP3205's first SSID).
Security	This is the type of wireless security employed by the network.
Apply	Click Apply to save your changes back to the WAP3205.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.10 WPS Station Screen

Use this screen when you want to add a wireless station using WPS. To open this screen, click **Network > Wireless LAN > WPS Station** tab.

Note: After you click **Push Button** on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.

Figure 59 Network > Wireless LAN > WPS Station



The following table describes the labels in this screen.

Table 39 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. See Section 9.3.1 on page 74 . Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Or input station's PIN number	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings. See Section 9.3.2 on page 75 . Type the same PIN number generated in the wireless station's utility. Then click Start to associate to each other and perform the wireless security information synchronization.

10.11 Scheduling Screen

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn

on or off on certain days and at certain times. To open this screen, click **Network > Wireless LAN > Scheduling** tab.

Figure 60 Network > Wireless LAN > Scheduling

Wireless LAN Scheduling

Enable Wireless LAN Scheduling

WLAN status	Day	For the following times (24-Hour Format)			
<input type="radio"/> On <input checked="" type="radio"/> Off	<input checked="" type="checkbox"/> Everyday	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Mon	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Tue	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Wed	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Thu	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Fri	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Sat	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Sun	00 (hour)	00 (min)	~	00 (hour) 00 (min)

Note: Specify the same begin time and end time means the whole day schedule.

Apply Cancel

The following table describes the labels in this screen.

Table 40 Network > Wireless LAN > Scheduling

LABEL	DESCRIPTION
Wireless LAN Scheduling	
Enable Wireless LAN Scheduling	Select this to enable Wireless LAN scheduling.
Scheduling	
WLAN Status	Select On or Off to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the Day and For the following times fields.
Day	Select Everyday or the specific days to turn the Wireless LAN on or off. If you select Everyday you can not select any specific days. This field works in conjunction with the For the following times field.
For the following times (24-Hour Format)	Select a begin time using the first set of hour and minute (min) drop down boxes and select an end time using the second set of hour and minute (min) drop down boxes. If you have chosen On earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. If you have chosen Off earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields.
Apply	Click Apply to save your changes back to the WAP3205.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.12 WDS Screen

A Wireless Distribution System (WDS) is a wireless connection between two or more APs. Use this screen to set the operating mode of your WAP3205 to **AP + Bridge** or **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.

Note: You must enable the same wireless security settings on the WAP3205 and on all wireless clients that you want to associate with it.

Click **Network > Wireless LAN > WDS** tab. The following screen opens with the **Basic Setting** set to **Disabled**, and **Security Mode** set to **No Security**.

Figure 61 Network > Wireless LAN > WDS

The following table describes the labels in this screen.

Table 41 Network > Wireless LAN > WDS

LABEL	DESCRIPTION
WDS Setup	
Basic Settings	<p>Select the operating mode for your WAP3205.</p> <ul style="list-style-type: none"> • Disable - The WAP3205 works as an access point only and cannot establish wireless links with other APs. • AP + Bridge - The WAP3205 functions as a bridge and access point simultaneously. • Bridge - The WAP3205 acts as a wireless network bridge and establishes wireless links with other APs. <p>You need to know the MAC address of the peer device, which also must be in bridge mode. The WAP3205 can establish up to five wireless links with other APs.</p>
Local MAC Address	This is the MAC address of your WAP3205.

Table 41 Network > Wireless LAN > WDS

LABEL	DESCRIPTION
Phy Mode	Select the Phy mode you want the WAP3205 to use. This dictates the maximum size of packets during data transmission. This field is not available when you select Disable in the Basic Setting field.
Remote MAC Address	This is the MAC address of the peer device that your WAP3205 wants to make a bridge connection with. You can connect to up to 4 peer devices.
Security	
EncrypType	Select whether to use WEP , TKIP or AES encryption for your WDS connection in this field. Otherwise, select No Security .
EncrypKey	The Encryp key is used to encrypt data. Peers must use the same key for data transmission.
Apply	Click Apply to save your changes to WAP3205.
Cancel	Click Cancel to reload the previous configuration for this screen.

11.1 Overview

This chapter describes how to configure LAN settings.

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. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

Figure 62 LAN Example



The LAN screens can help you manage IP addresses.

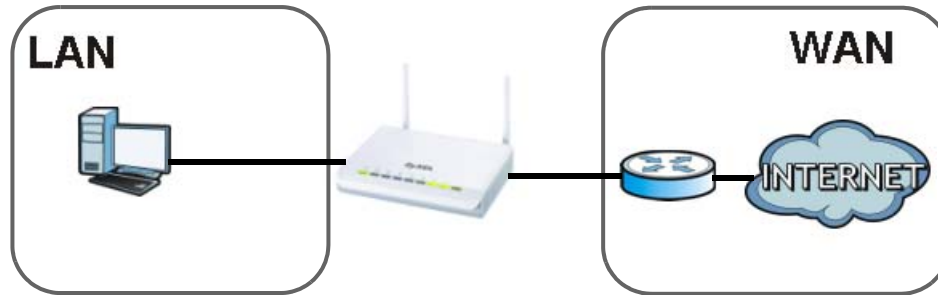
11.2 What You Can Do

- Use the **IP** screen ([Section 11.4 on page 103](#)) to change the IP address for your WAP3205 and DNS server information.
- Use the **IP Alias** screen ([Section 11.5 on page 104](#)) to have the WAP3205 apply IP alias to create LAN subnets.

11.3 What You Need To Know

There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 63 LAN and WAN IP Addresses



The LAN parameters of the WAP3205 are preset in the factory with the following values:

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

11.3.1 LAN TCP/IP

The WAP3205 has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

11.3.2 IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The WAP3205 supports three logical LAN interfaces via its single physical Ethernet interface with the WAP3205 itself as the gateway for each LAN network.

11.4 LAN IP Screen

Use this screen to change the IP address for your WAP3205. Click **Network > LAN > IP**.

Figure 64 Network > LAN > IP

The following table describes the labels in this screen.

Table 42 Network > LAN > IP

LABEL	DESCRIPTION
Get from DHCP Server	<p>Click this to deploy the WAP3205 as an access point in the network.</p> <p>When you enable this, the WAP3205 gets its IP address from the network's DHCP server (for example, your ISP or router). Users connected to the WAP3205 can now access the network (i.e., the Internet if the IP address is given by the ISP or a router with Internet access).</p> <p>The Web Configurator may no longer be accessible unless you know the IP address assigned by the DHCP server to the WAP3205. Otherwise, you need to reset the WAP3205 to be able to access the Web Configurator again (see Section 12.7 on page 113 for details on how to reset the WAP3205).</p> <p>Also when you select this, you cannot enter an IP address for your WAP3205 in the field below.</p>
Use Defined LAN IP Address	Click this if you want to specify the IP address of your WAP3205. Or if your ISP or network administrator gave you a static IP address to access the network or the Internet.
IP Address	Type the IP address in dotted decimal notation. The default setting is 192.168.1.2. If you change the IP address you will have to log in again with the new IP address.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your WAP3205 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the WAP3205.

Table 42 Network > LAN > IP

LABEL	DESCRIPTION
Gateway IP Address	Enter a gateway IP address (if your ISP or network administrator gave you one) in this field.
DNS Assignment	
First DNS Server	Select From ISP if your ISP or router to which the WAP3205 connects dynamically assigns DNS server information (and the WAP3205's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.
Second DNS Server	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 computer in order to access it.
Apply	Click Apply to save your changes back to the WAP3205.
Reset	Click Reset to begin configuring this screen afresh.

11.5 IP Alias Screen

Use this screen to have the WAP3205 apply IP alias to create LAN subnets. Click **LAN > IP Alias**.

Figure 65 Network > LAN > IP Alias

The following table describes the labels in this screen.

Table 43 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias	Check this to enable IP alias.
IP Address	Type the IP alias address of your WAP3205 in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your WAP3205 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the WAP3205.
Apply	Click Apply to save your changes back to the WAP3205.
Reset	Click Reset to begin configuring this screen afresh.

PART III

Maintenance and Troubleshooting

Maintenance (107)

Troubleshooting (119)

Maintenance

12.1 Overview

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

12.2 What You Can Do

- Use the **General** screen ([Section 12.3 on page 108](#)) to set the timeout period of the management session.
- Use the **Password** screen ([Section 12.4 on page 108](#)) to change your WAP3205's system password.
- Use the **Time** screen ([Section 12.5 on page 109](#)) to change your WAP3205's time and date.
- Use the **Firmware Upgrade** screen ([Section 12.6 on page 111](#)) to upload firmware to your WAP3205.
- Use the **Backup/Restore** screen ([Section 12.8 on page 114](#)) to view information related to factory defaults, backup configuration, and restoring configuration.
- Use the **Reset/Restart** screen ([Section 12.8 on page 114](#)) to reboot the WAP3205 without turning the power off.
- Use the **Sys OP Mode** screen ([Section 12.10 on page 116](#)) to select how you want to use your WAP3205.

12.3 General Screen

Use this screen to set the management session timeout period. Click **Maintenance > General**. The following screen displays.

Figure 66 Maintenance > General

The following table describes the labels in this screen.

Table 44 Maintenance > General

LABEL	DESCRIPTION
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).
Apply	Click Apply to save your changes back to the WAP3205.
Reset	Click Reset to begin configuring this screen afresh.

12.4 Password Screen

It is strongly recommended that you change your WAP3205's password.

If you forget your WAP3205's password (or IP address), you will need to reset the device. See [Section 12.8 on page 114](#) for details

Click **Maintenance > Password**.

Figure 67 Maintenance > Password

The following table describes the labels in this screen.

Table 45 Maintenance > Password

LABEL	DESCRIPTION
Password Setup	Change your WAP3205'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 WAP3205.
Reset	Click Reset to begin configuring this screen afresh.

12.5 Time Setting Screen

Use this screen to configure the WAP3205's time based on your local time zone. To change your WAP3205's time and date, click **Maintenance > Time**. The screen appears as shown.

Figure 68 Maintenance > Time

The screenshot displays the 'Time Setting' configuration page. It is divided into three main sections:

- Current Time and Date:** Shows the current system time as 04:43:45 and the current date as 2000-01-01.
- Current Time and Date (Configuration):** Offers two methods:
 - Manual:** Selected with a radio button. Fields for 'New Time (hh:mm:ss)' are set to 4:42:52, and 'New Date (yyyy/mm/dd)' are set to 2000/1/1.
 - Get from Time Server:** Includes an 'Auto' radio button and a 'User Defined Time Server Address' field containing '192.5.41.41'.
- Time Zone Setup:** Features a dropdown menu for 'Time Zone' set to '(GMT+08:00) Perth, Taipei'. Below it, there are checkboxes for 'Daylight Savings' and input fields for 'start Date (mm/dd)' and 'End Date', each followed by 'at' and 'o'clock' labels.

At the bottom of the form, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 46 Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your WAP3205. Each time you reload this page, the WAP3205 synchronizes the time with the time server.
Current Date	This field displays the date of your WAP3205. Each time you reload this page, the WAP3205 synchronizes the date with the time server.
Current Time and Date	
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.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you select 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 select Manual , enter the new date in this field and then click Apply .
Get from Time Server	Select this radio button to have the WAP3205 get the time and date from the time server you specified below.
Auto	Select Auto to have the WAP3205 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 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 46 Maintenance > Time

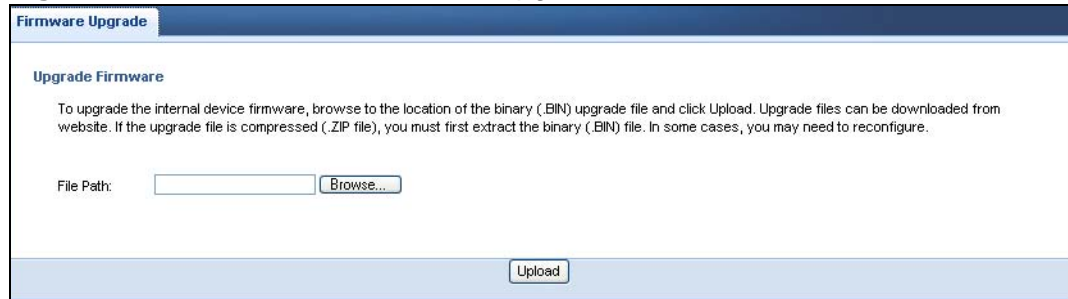
LABEL	DESCRIPTION
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected Daylight Savings. The o'clock field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each 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 First, Sunday, April and type 2 in the o'clock field.</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 last Sunday of October. 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 Last, Sunday, October and type 2 in the o'clock field.</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 WAP3205.
Reset	Click Reset to begin configuring this screen afresh.

12.6 Firmware Upgrade Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a `*.bin` extension, e.g., `WAP3205.bin`. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your WAP3205.

Figure 69 Maintenance > Firmware Upgrade



The following table describes the labels in this screen.

Table 47 Maintenance > Firmware Upgrade

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.

Note: Do not turn off the WAP3205 while firmware upload is in progress!

After you see the **Firmware Upload In Progress** screen, wait two minutes before logging into the WAP3205 again.

The WAP3205 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 70 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, an error message appears. Click **Return** to go back to the **Firmware Upgrade** screen.

12.7 Configuration Backup/Restore Screen

Backup configuration allows you to back up (save) the WAP3205's current configuration to a file on your computer. Once your WAP3205 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.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your WAP3205.

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 71 Maintenance > Backup/Restore

Backup / Restore

Backup Configuration

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

Restore Configuration

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

File Path:

Back to Factory Defaults

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

- Password will be 1234
- LAN IP address will be 192.168.1.2

The following table describes the labels in this screen.

Table 48 Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup	Click Backup to save the WAP3205's current configuration to your computer.
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.

Table 48 Maintenance > Backup/Restore

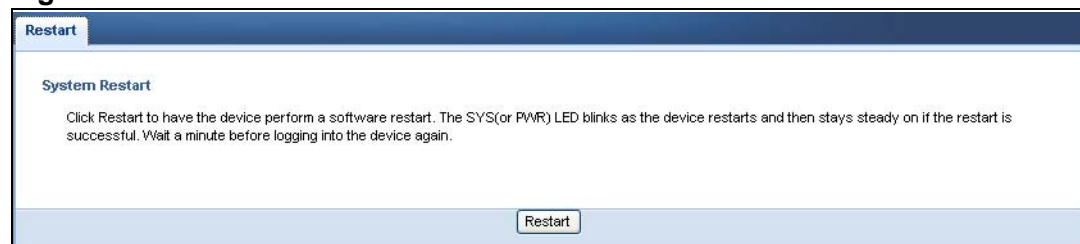
LABEL	DESCRIPTION
Upload	<p>Click Upload to begin the upload process.</p> <p>Note: Do not turn off the WAP3205 while configuration file upload is in progress.</p> <p>After you see a “configuration upload successful” screen, you must then wait one minute before logging into the WAP3205 again. The WAP3205 automatically restarts in this time causing a temporary network disconnect.</p> <p>If you see an error screen, click Back to return to the Backup/Restore screen.</p>
Reset	<p>Pressing the Reset button in this section clears all user-entered configuration information and returns the WAP3205 to its factory defaults.</p> <p>You can also press the RESET button on the rear panel to reset the factory defaults of your WAP3205. Refer to the chapter about introducing the Web Configurator for more information on the RESET button.</p>

Note: 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 WAP3205 IP address (192.168.1.2). See [Appendix C on page 149](#) for details on how to set up your computer’s IP address.

12.8 Reset/Restart Screen

System restart allows you to reboot the WAP3205 without turning the power off.

Click **Maintenance > Reset/Restart** to open the following screen.

Figure 72 Maintenance > Reset/Restart

Click **Restart** to have the WAP3205 reboot. This does not affect the WAP3205's configuration.

12.9 System Operation Mode Overview

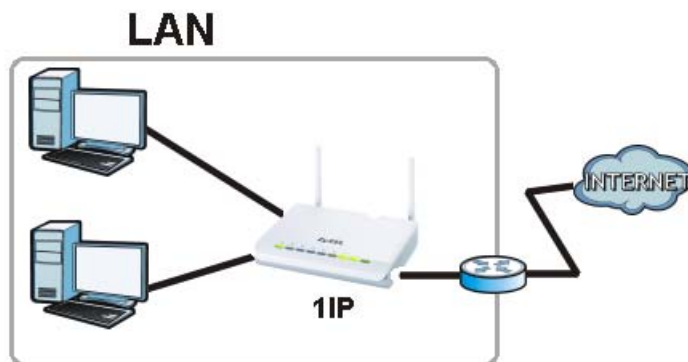
The **Sys OP Mode** (System Operation Mode) function lets you configure your WAP3205 as an access point, wireless client or both at the same time. You can choose between **Access Point Mode**, **Client Mode** and **Universal Repeater Mode** depending on your network topology and the features you require from your device.

The following describes the device modes available in your WAP3205.

Access Point

An access point enabled all ethernet ports to be bridged together and be in the same subnet. To connect to the Internet, another device, such as a router, is required.

Figure 73 Access Point Mode



Client

WAP3205 in client mode connects to an existing access point wirelessly. It acts just like a wireless client in notebooks/computers.

Figure 74 Client Mode



Universal Repeater

WAP3205 in Universal Repeater mode work as an access point and wireless client simultaneously.

Figure 75 Universal Repeater Mode



12.10 Sys Op Mode Screen

Use this screen to select how you want to use your WAP3205.

Figure 76 Maintenance > Sys OP Mode

The following table describes the labels in the **General** screen.

Table 49 Maintenance > Sys OP Mode

LABEL	DESCRIPTION
System Operation Mode	
Access Point	Select Access Point Mode if your device bridges traffic between clients on the same network. <ul style="list-style-type: none"> In Access Point mode all Ethernet ports have the same IP address. The default IP address of the device on the local network is 192.168.1.2.

LABEL	DESCRIPTION
Client Mode	<p>Select Client Mode if your device needs a wireless client to connect to an existing access point.</p> <ul style="list-style-type: none"> • You cannot configure wireless LAN settings like MAC filtering, QoS, WDS and scheduling in the client mode. • The IP address of the device on the local network is the same as the IP address given to the WAP3205 while in access point mode (default is 192.168.1.2).
Universal Repeater Mode	<p>Select Universal Repeater Mode if you want to have wireless clients associate with the WAP3205 and also want to connect the WAP3205 to an existing access point.</p> <ul style="list-style-type: none"> • In addition to wireless LAN settings between the WAP3205 and wireless clients, you also need to configure security and wireless settings between the WAP3205 and another access point. • WDS is not available when the WAP3205 is in universal repeater mode. • The IP address of the device on the local network is the same as the IP address given to the WAP3205 while in access point mode (default is 192.168.1.2).
Apply	Click Apply to save your settings.
Reset	Click Reset to return your settings to the default (Router)

Note: If you select the incorrect System Operation Mode you may not be able to connect to the Internet.

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](#)
- [WAP3205 Access and Login](#)
- [Internet Access](#)
- [Resetting the WAP3205 to Its Factory Defaults](#)
- [Wireless Router/AP Troubleshooting](#)

13.1 Power, Hardware Connections, and LEDs

The WAP3205 does not turn on. None of the LEDs turn on.

- 1 Make sure you are using the power adaptor or cord included with the WAP3205.
- 2 Make sure the power adaptor or cord is connected to the WAP3205 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 WAP3205.
- 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 1.5 on page 20](#).
- 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 WAP3205.
- 5 If the problem continues, contact the vendor.

13.2 WAP3205 Access and Login

I don't know the IP address of my WAP3205.

- 1 The default IP address is **192.168.1.2**.
- 2 If you changed the IP address and have forgotten it,
 - and your WAP3205 is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.
 - reset your WAP3205 to change all settings back to their default. This means your current settings are lost. See [Section 13.4 on page 123](#) in the **Troubleshooting** for information on resetting your WAP3205.

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 13.4 on page 123](#).

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 11.4 on page 103](#)), use the new IP address.

- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I don't know the IP address of my WAP3205](#).
- 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 A on page 131](#).
 - 4 Make sure your computer is in the same subnet as the WAP3205. (If you know that there are routers between your computer and the WAP3205, skip this step.)
 - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Section 14.3 on page 139](#).
 - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the WAP3205. See [Appendix B on page 139](#).
 - 5 Reset the device to its factory defaults, and try to access the WAP3205 with the default IP address. See [Section 12.7 on page 113](#).
 - 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestion

- If your computer is connected wirelessly, use a computer that is connected to a **LAN** port.

I can see the **Login** screen, but I cannot log in to the WAP3205.

- 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 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
- 3 Disconnect and re-connect the power adaptor or cord to the WAP3205.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 13.4 on page 123](#).

13.3 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 Make sure the WAP3205 is connected to a broadband modem or router with Internet access.
- 3 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 AP.
 - Go to **Network > Wireless LAN > General > WDS** and check if the WAP3205 is set to bridge mode. Select **Disable** and try to connect to the Internet again.
- 4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 5 Go to **Maintenance > Sys OP Mode**. Check your System Operation Mode setting.
 - Select **Access Point Mode** if your WAP3205 bridges traffic between clients on the same network.
 - Select **Client Mode** if your WAP3205 needs a wireless client to connect to an existing access point.
 - Select **Universal Repeater Mode** if you want to have wireless clients associate with the WAP3205 and also want to connect the WAP3205 to an existing access point.
- 6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the WAP3205), 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 1.5 on page 20](#).
- 2 Reboot the WAP3205.
- 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 1.5 on page 20](#). If the WAP3205 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 clients 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 WAP3205.
- 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.

13.4 Resetting the WAP3205 to Its Factory Defaults

If you reset the WAP3205, you lose all of the changes you have made. The WAP3205 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 WAP3205,

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for longer than 1 second to restart/reboot the WAP3205.
- 3 Press the **RESET** button for longer than five seconds to set the WAP3205 back to its factory-default configurations.

If the WAP3205 restarts automatically, wait for the WAP3205 to finish restarting, and log in to the Web Configurator. The password is "1234".

If the WAP3205 does not restart automatically, disconnect and reconnect the WAP3205's power. Then, follow the directions above again.

13.5 Wireless Router/AP Troubleshooting

I cannot access the WAP3205 or ping any computer from the WLAN (wireless AP or router).

- 1 Make sure the wireless adapter on the wireless station is working properly.
- 2 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the WAP3205.
- 3 Make sure your computer (with a wireless adapter installed) is within the transmission range of the WAP3205.
- 4 Check that both the WAP3205 and your wireless station are using the same wireless and wireless security settings.

Product Specifications

The following tables summarize the WAP3205's hardware and firmware features.

Table 50 Hardware Features

Dimensions (W x D x H)	162 mm x 115 mm x 33 mm
Weight	245 g
Power Specification	Input: 100~240 V AC, 50~60 Hz Output: 12 V DC 1A
Two Ethernet ports	Auto-negotiating: 10 Mbps, 100 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
LEDs	PWR, LAN1-2 WLAN, WPS
Reset Button	The reset button is built into the rear panel. Use this button to restore the WAP3205 to its factory default settings. Press for 1 second to restart the device. Press for 5 seconds to restore to factory default settings.
WPS button	Press the WPS on two WPS enabled devices within 120 seconds for a security-enabled wireless connection.
Antenna	The WAP3205 is equipped with two 2dBi (2.4GHz) detachable antennas to provide clear radio transmission and reception on the wireless network.
Operation Environment	Temperature: 0° C ~ 40° C / 32°F ~ 104°F Humidity: 20% ~ 90%
Storage Environment	Temperature: -30° C ~ 70° C / -22°F ~ 158°F Humidity: 20% ~ 95%

Table 51 Firmware Features

FEATURE	DESCRIPTION
Default IP Address	192.168.1.2
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Wireless Interface	Wireless LAN
Default Wireless SSID	ZyXEL

Table 51 Firmware Features

FEATURE	DESCRIPTION
Device Management	Use the Web Configurator to easily configure the rich range of features on the WAP3205.
Wireless Functionality	Allows IEEE 802.11b, IEEE 802.11g and/or IEEE 802.11n wireless clients to connect to the WAP3205 wirelessly. Enable wireless security (WPA(2)-PSK) and/or MAC filtering to protect your wireless network. Note: The WAP3205 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.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the Web Configurator to put it on the WAP3205. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the WAP3205's configuration and put it back on the WAP3205 later if you decide you want to revert back to an earlier configuration.
Wireless LAN Scheduler	You can schedule the times the wireless LAN is enabled/disabled.
Time and Date	Get the current time and date from an external server when you turn on your WAP3205. You can also set the time manually. These dates and times are then used in logs.
IP Multicast	IP Multicast is used to send traffic to a specific group of computers. The WAP3205 supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Logging	Use logs for troubleshooting. You can view logs in the Web Configurator.

14.1 Wall-mounting Instructions

Complete the following steps to hang your WAP3205 on a wall.

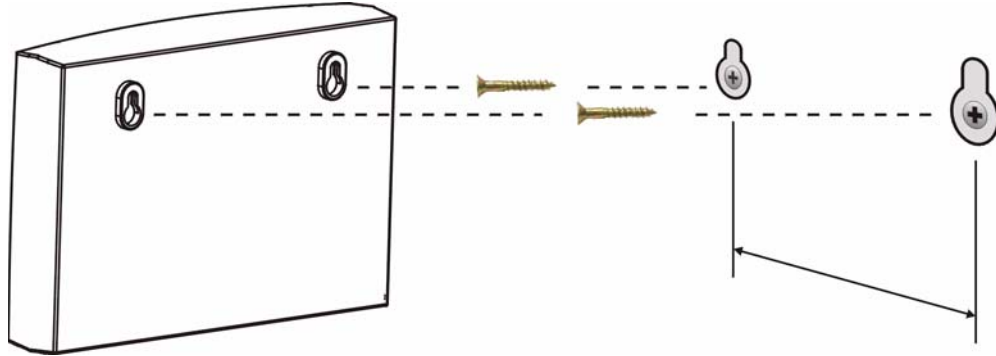
- 1 Select a position free of obstructions on a sturdy wall.
- 2 Drill two holes for the screws.

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

- 3 Do not insert 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.

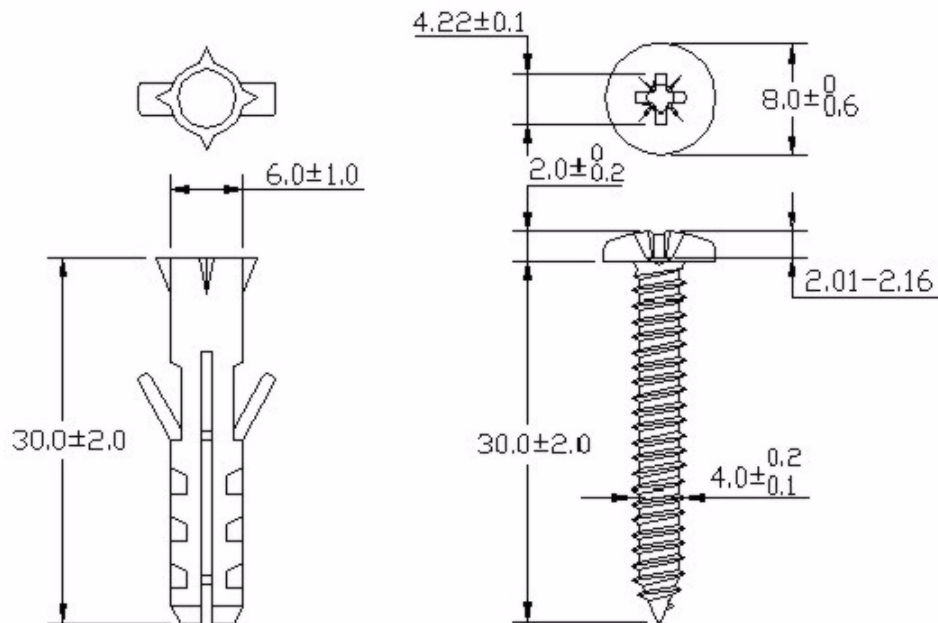
- 4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the WAP3205 with the connection cables.
- 5 Align the holes on the back of the WAP3205 with the screws on the wall. Hang the WAP3205 on the screws.

Figure 77 Wall-mounting Example



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

Figure 78 Masonry Plug and M4 Tap Screw



PART IV

Appendices and Index

Pop-up Windows, JavaScripts and Java
Permissions (131)

IP Addresses and Subnetting (139)

Setting up Your Computer's IP Address
(149)

Wireless LANs (167)

Common Services (179)

Legal Information (183)

Index (191)

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).

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

Internet Explorer Pop-up Blockers

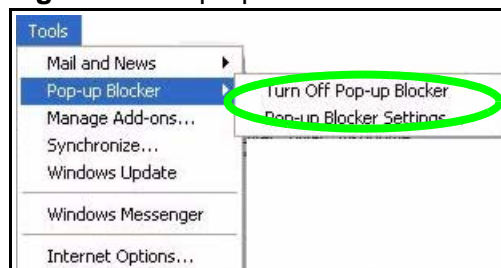
You may have to disable pop-up blocking to log into your device.

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**.

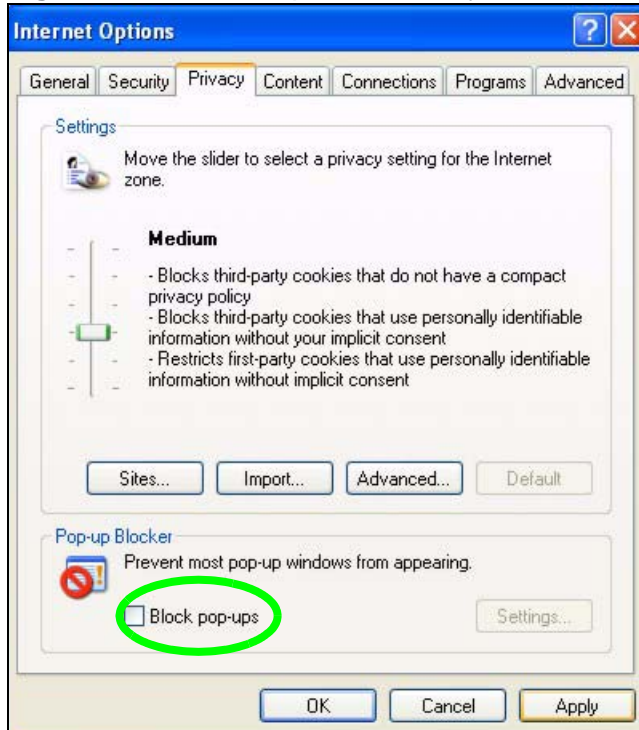
Figure 79 Pop-up Blocker



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 80 Internet Options: Privacy



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

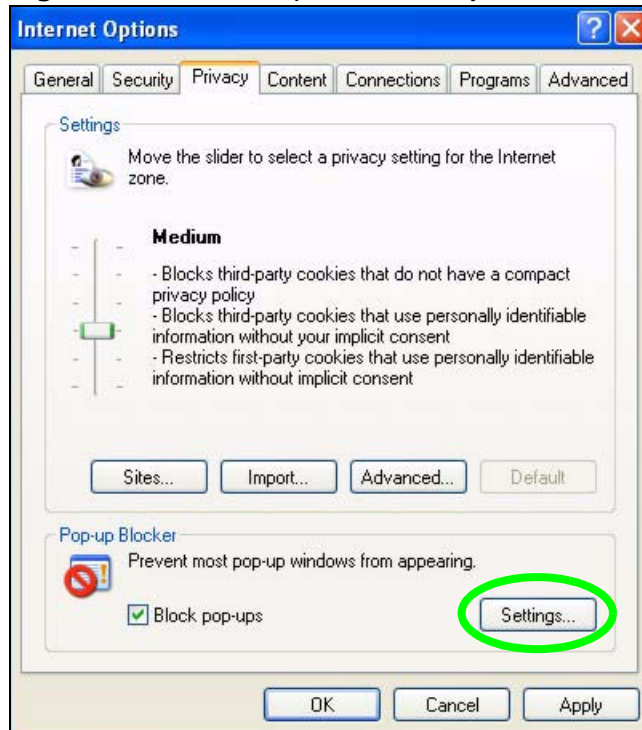
Enable pop-up Blockers with Exceptions

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.

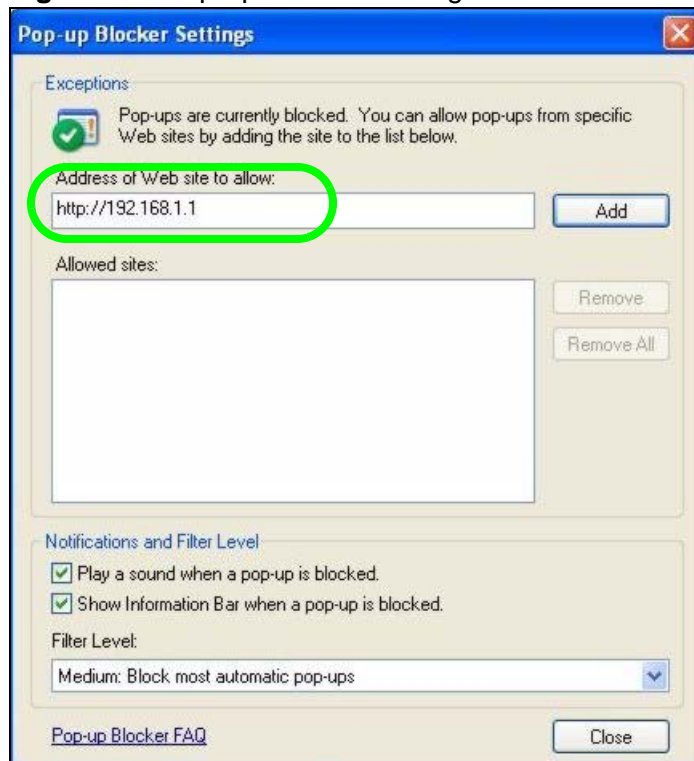
Figure 81 Internet Options: Privacy



- 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 82 Pop-up Blocker Settings



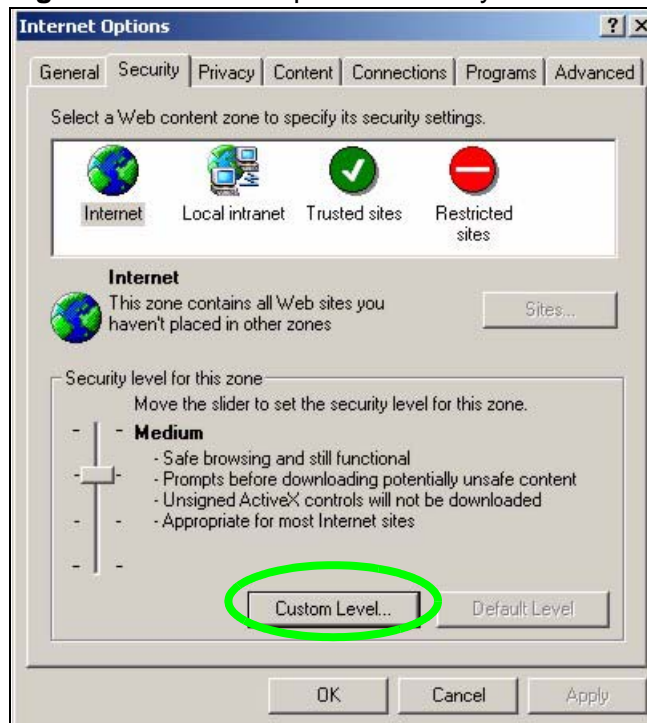
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

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.

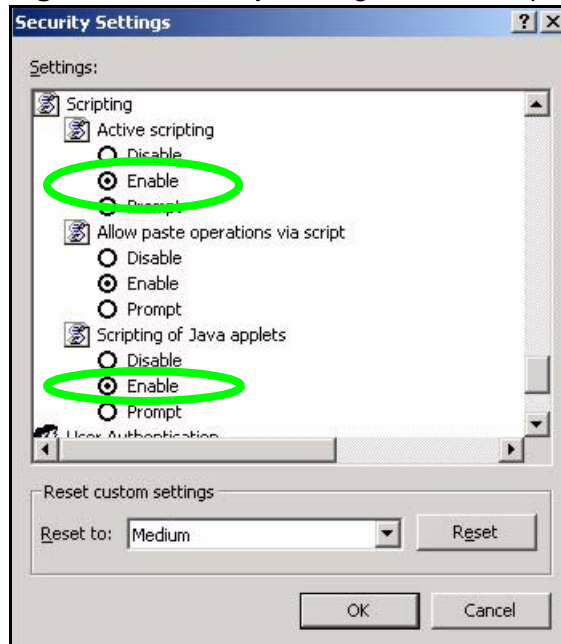
Figure 83 Internet Options: Security



- 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 84 Security Settings - Java Scripting

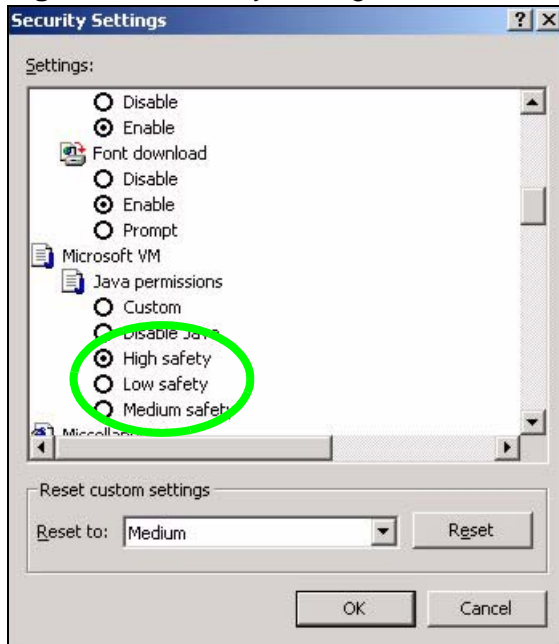


Java Permissions

- 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 85 Security Settings - Java

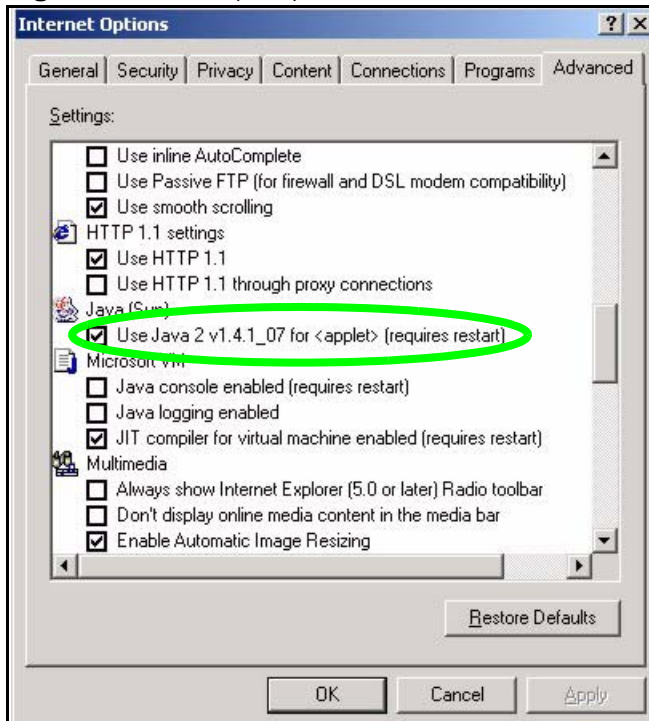


JAVA (Sun)

- 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 86 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.

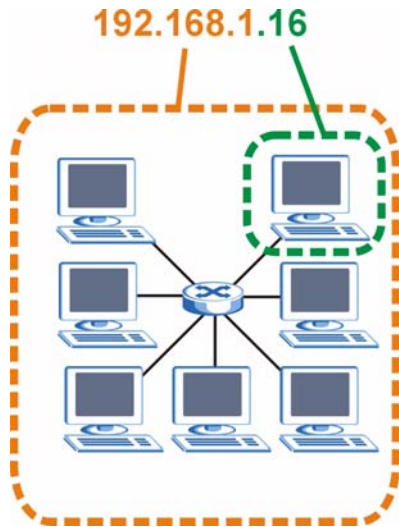
Structure

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 87 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 52 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

Table 52 Subnet Mask - Identifying Network Number

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
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 53 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 54 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 55 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
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

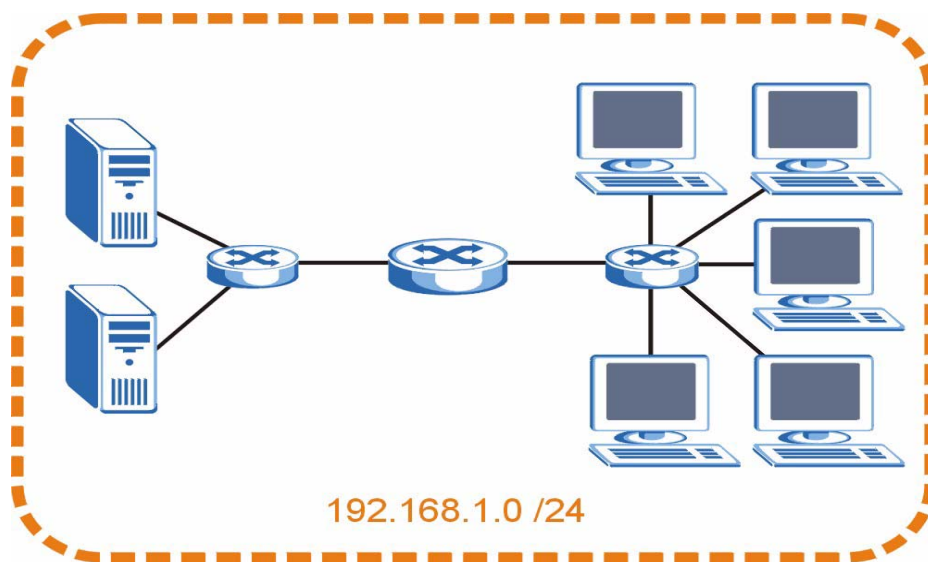
Subnetting

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 88 Subnetting Example: Before Subnetting

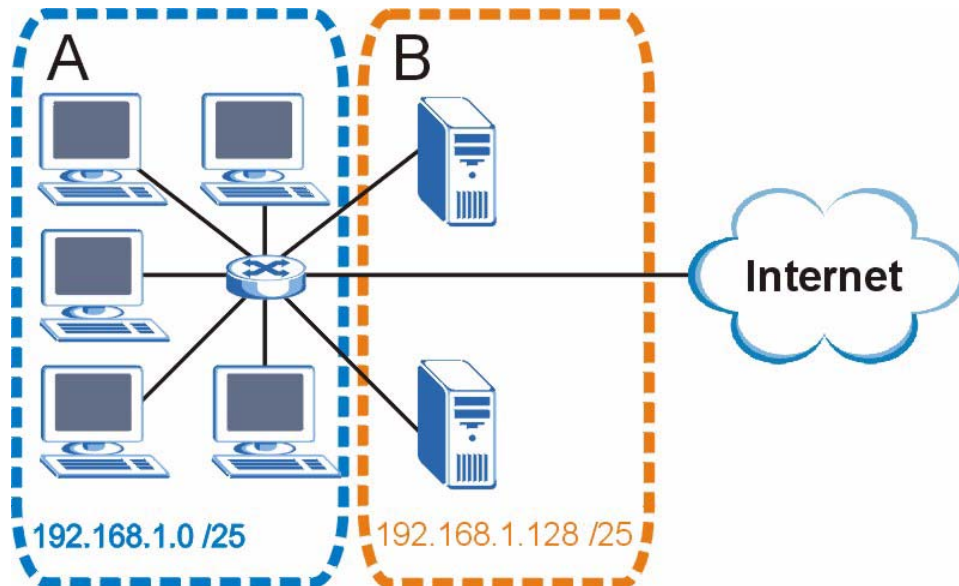


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 89 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 56 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 57 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 58 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 59 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

Table 59 Subnet 4 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
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 60 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
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 61 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 62 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
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 the WAP3205.

Once you have decided on the network number, pick an IP address for your WAP3205 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 WAP3205 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 WAP3205 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.

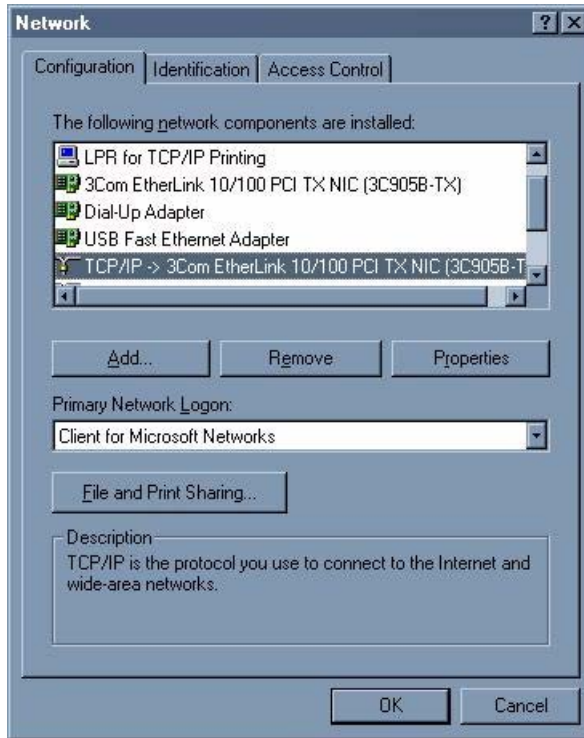
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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 90 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**.

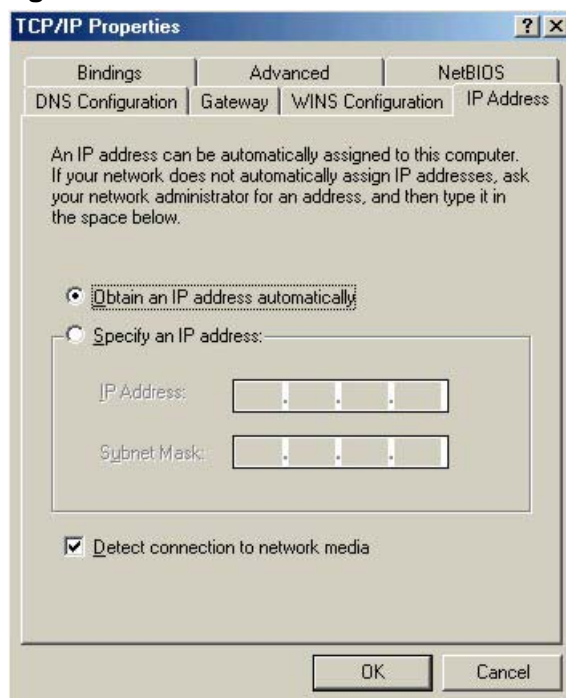
If you need Client for Microsoft Networks:

- 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

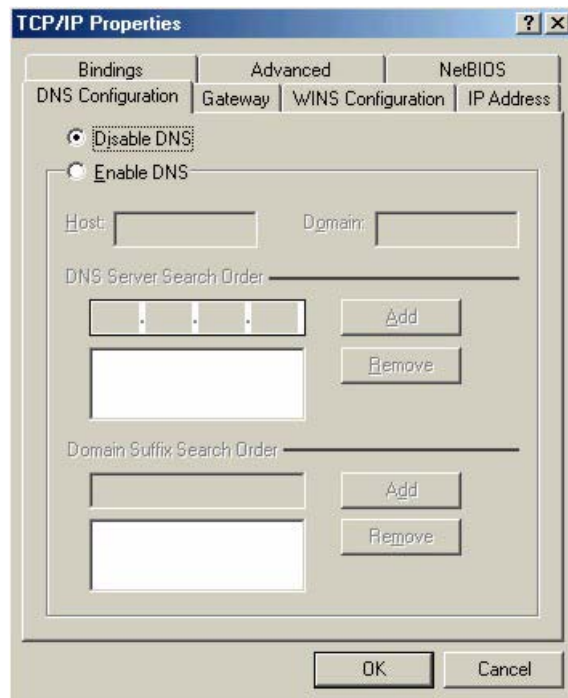
- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
 - If your IP address is dynamic, select **Obtain an IP address automatically**.
 - If you have a static IP address, select **Specify an IP address**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

Figure 91 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 92 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.

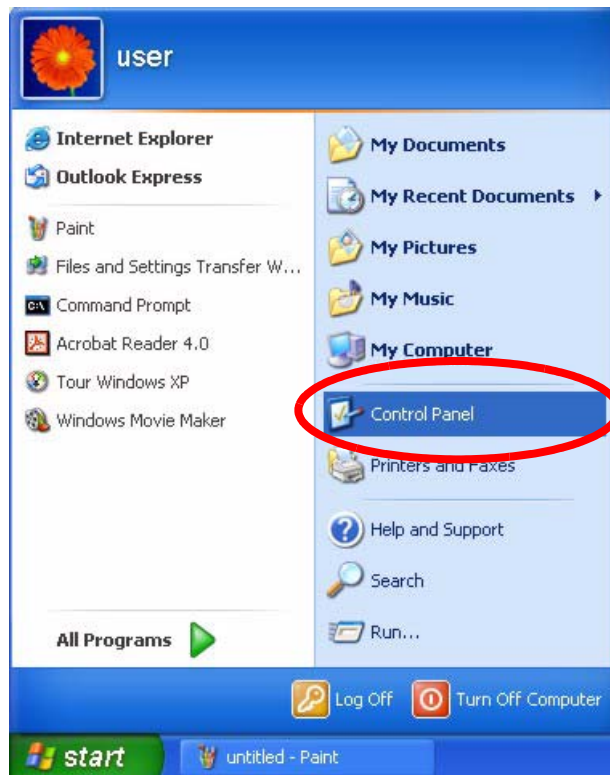
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

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 93 Windows XP: Start Menu



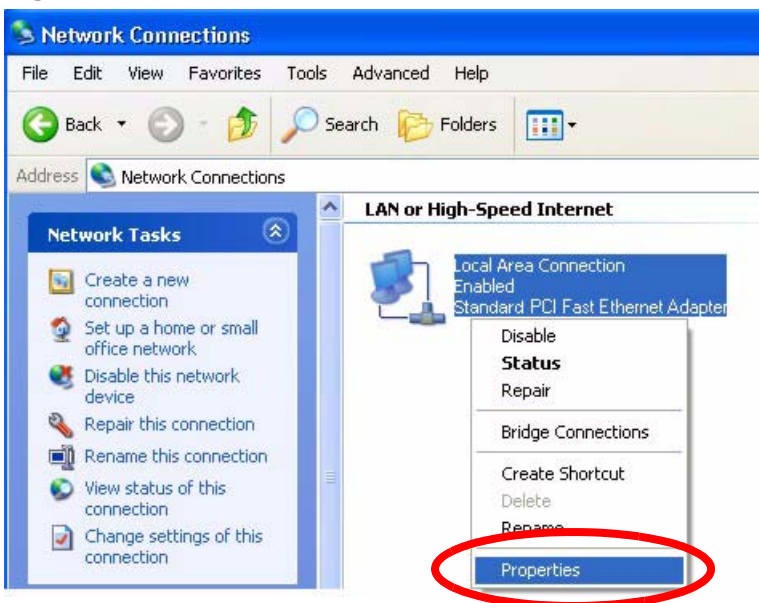
- 2 In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections)** in Windows 2000/NT).

Figure 94 Windows XP: Control Panel



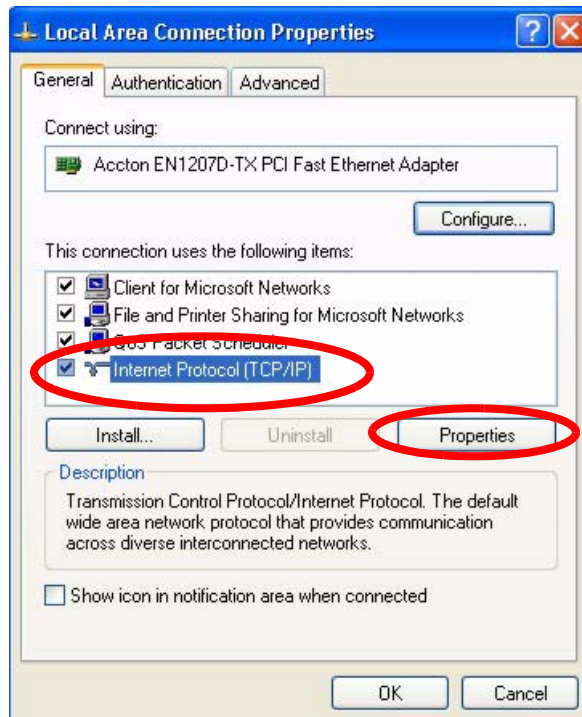
- 3 Right-click **Local Area Connection** and then click **Properties**.

Figure 95 Windows XP: Control Panel: Network Connections: Properties



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

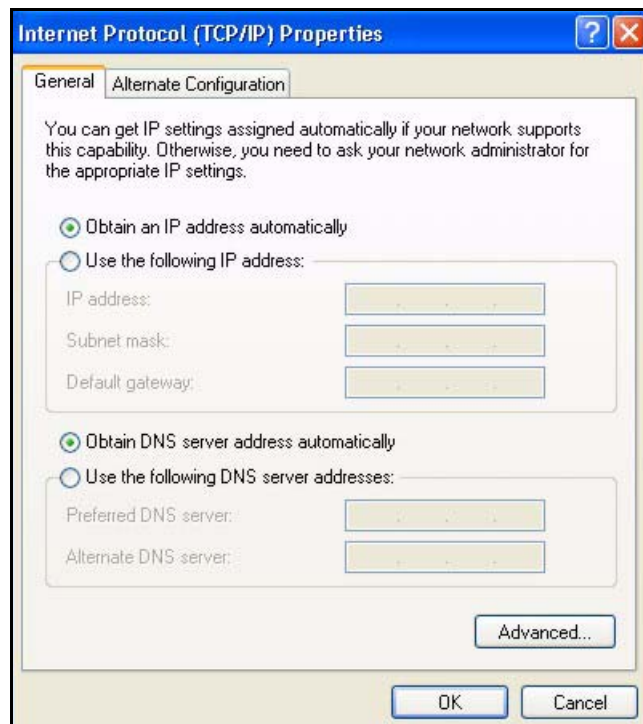
Figure 96 Windows XP: Local Area Connection Properties



- 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 97 Windows XP: Internet Protocol (TCP/IP) Properties



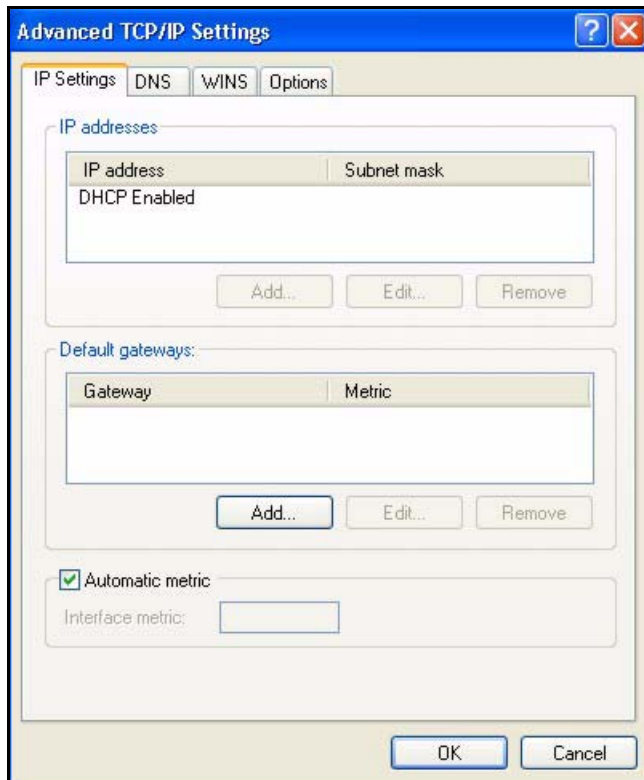
- 6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

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 98 Windows XP: Advanced TCP/IP Properties

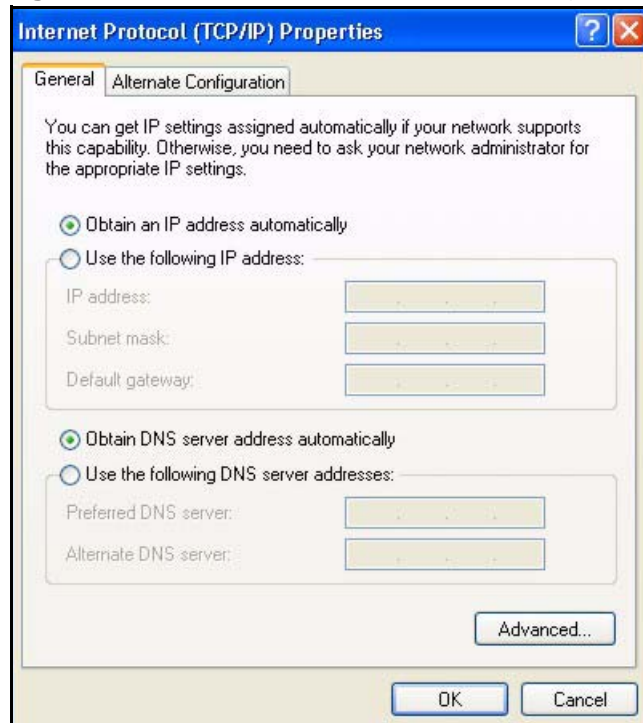


7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- 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 99 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).

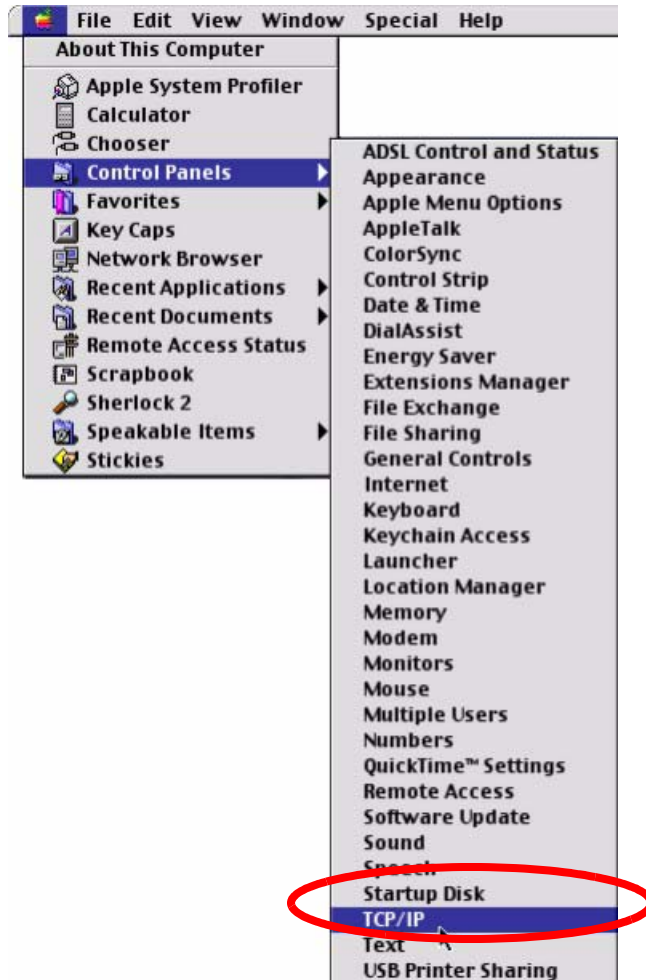
Verifying Settings

- 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

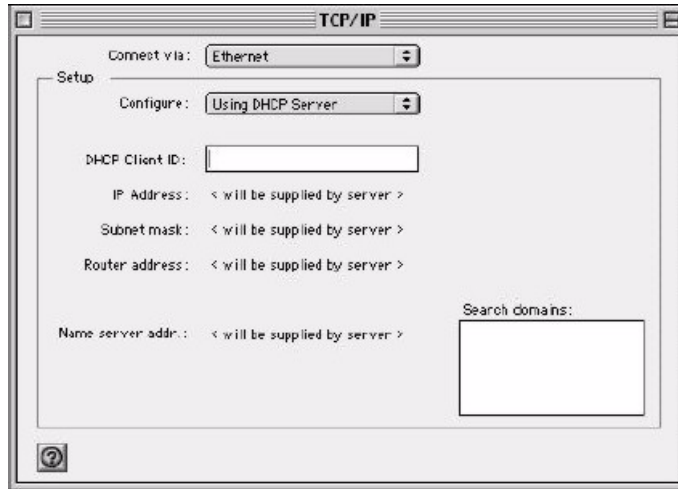
- 1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 100 Macintosh OS 8/9: Apple Menu



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

Figure 101 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).

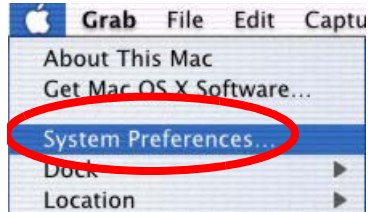
Verifying Settings

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

Macintosh OS X

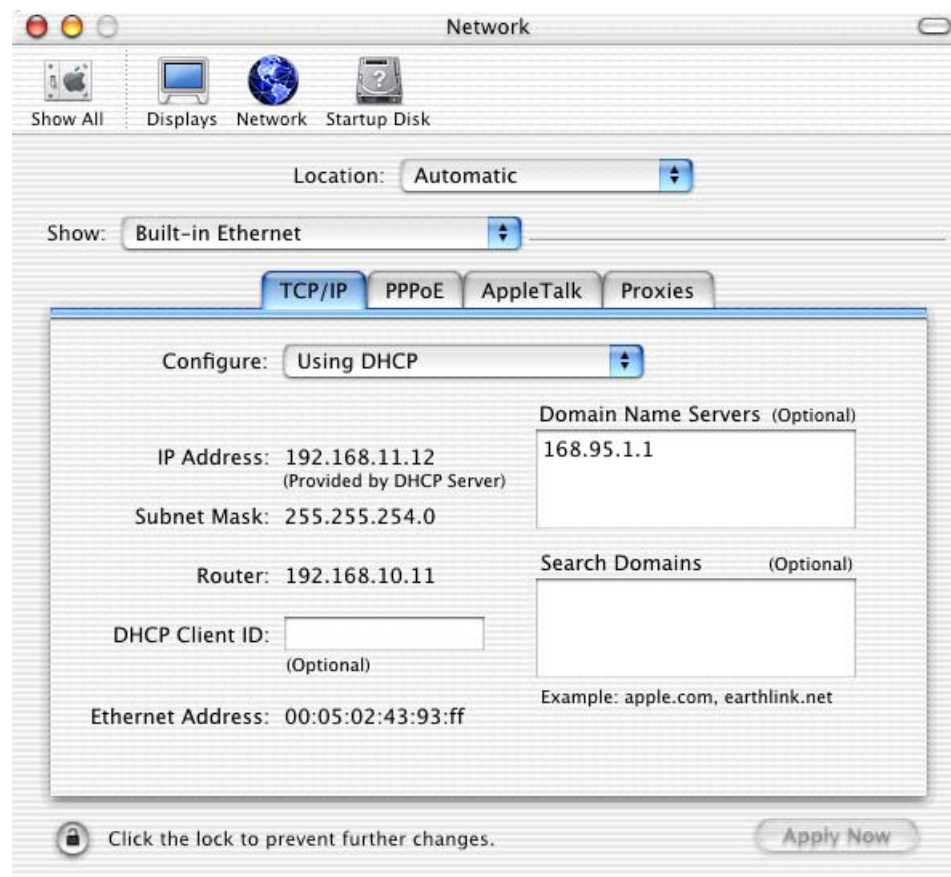
- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 102 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 103 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.

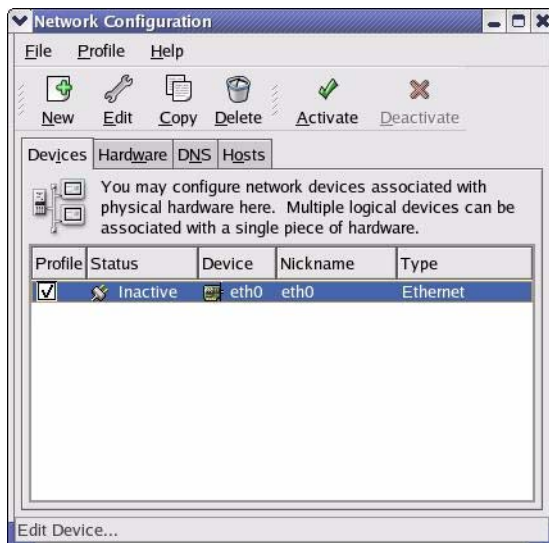
Note: Make sure you are logged in as the root administrator.

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 104 Red Hat 9.0: KDE: Network Configuration: Devices



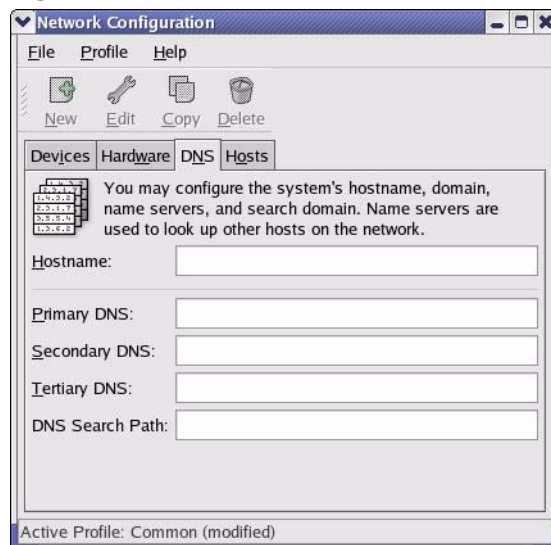
- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Figure 105 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 106 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 107 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 108 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 109 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 110 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 111 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]
```

Verifying Settings

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

Figure 112 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

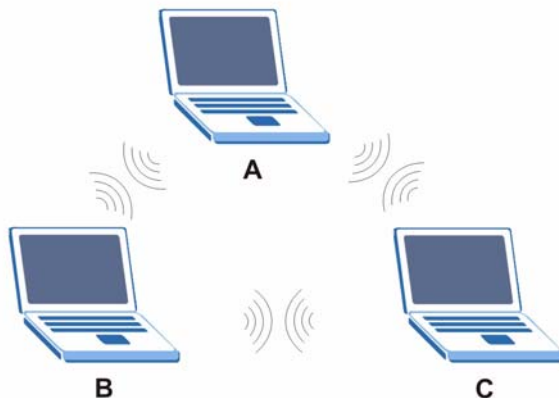
Wireless LAN Topologies

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 stations (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 113 Peer-to-Peer Communication in an Ad-hoc Network



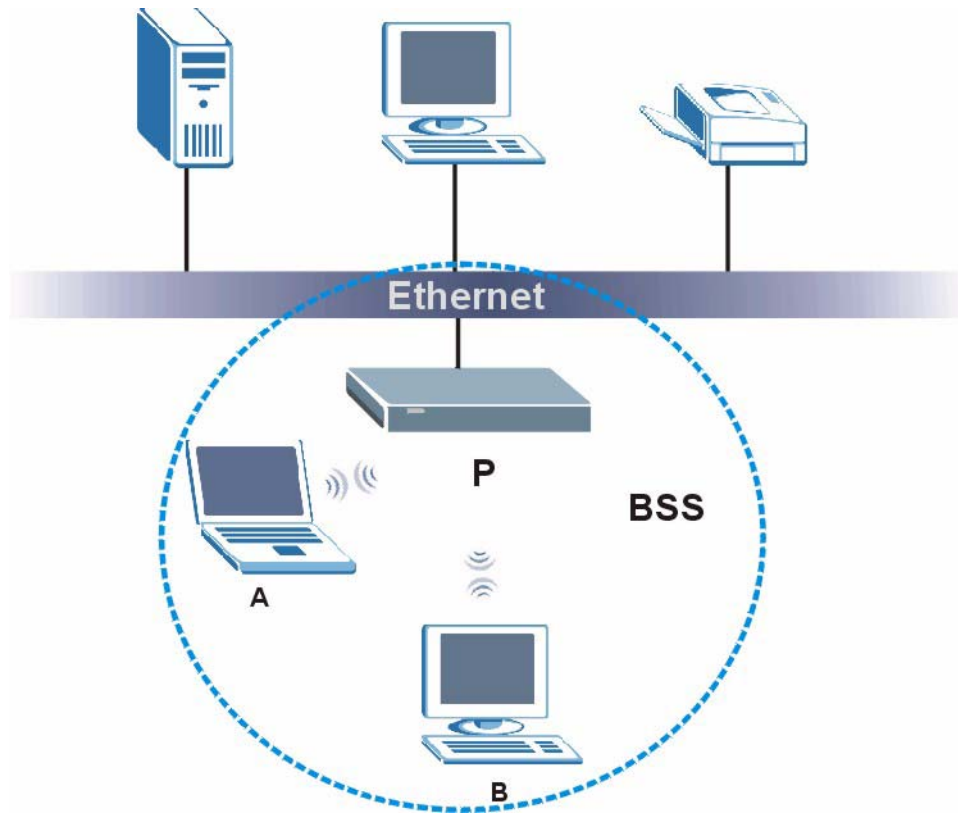
BSS

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

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate

with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 114 Basic Service Set



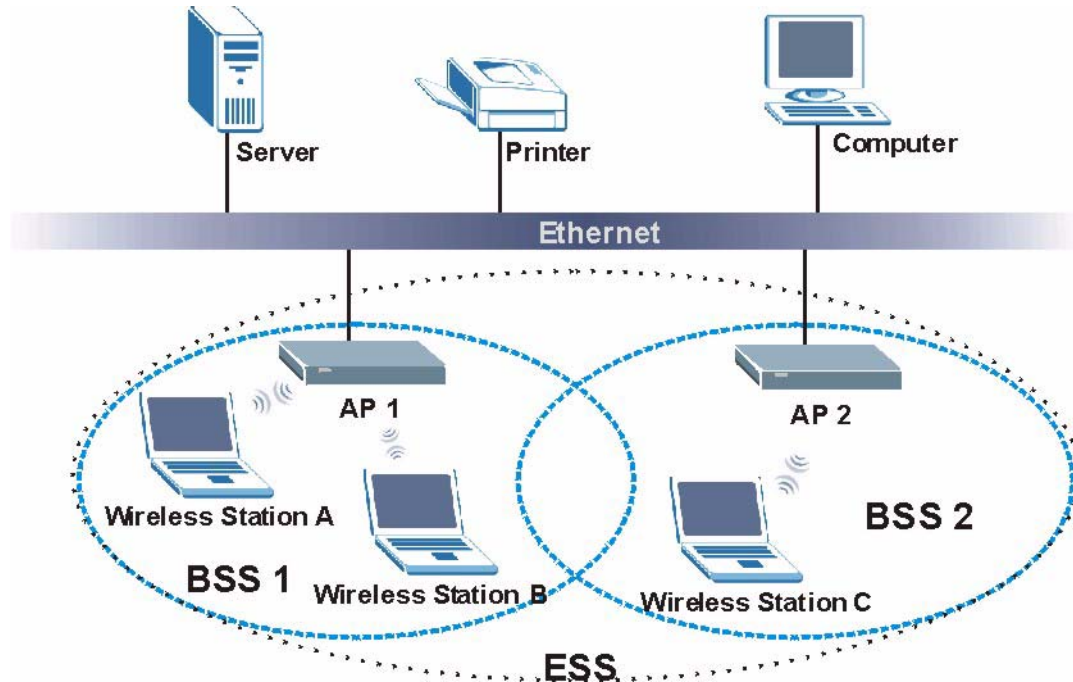
ESS

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 stations within the same ESS must have the same ESSID in order to communicate.

Figure 115 Infrastructure WLAN



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. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

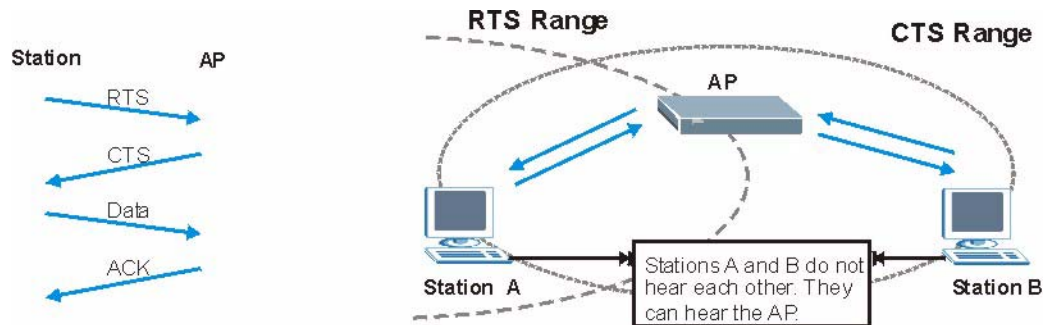
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel 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 116 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.

Note: 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

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

Note: The AP and the wireless stations **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 63 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)

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 stations.

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 station 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 Authentication

This appendix discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station '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 stations 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 screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

Note: 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 64 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(2)

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(2) and WEP are improved data encryption and user authentication.

Encryption

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

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes 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.

TKIP regularly changes and rotates 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 pair-wise key 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.

WPA2 AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael.

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), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

User Authentication

WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

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.

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 (only) allows it to join the network if the password matches.
- 3 The AP derives and distributes keys to the wireless clients.
- 4 The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 117 WPA(2)-PSK Authentication



WPA(2) with RADIUS Application Example

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 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 pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Security Parameters Summary

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

Table 65 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	No	Enable
WPA-PSK	TKIP	Yes	Enable
WPA2	AES	No	Enable
WPA2-PSK	AES	Yes	Enable

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 66 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.

Table 66 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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).

Table 66 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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.

Table 66 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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 © 2009 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.

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.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

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。減少電磁波影響，請妥適使用。

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.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

- 1 this device may not cause interference and
- 2 this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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 your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

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.

End-User License Agreement for "WAP3205"

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

1 Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2 Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3 Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4 Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL on its Open Source web site (<ftp://opensource.zyxel.com>) (collectively the "Open-Sourced Components") You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise

permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the online electronic documentation for the Software (<ftp://opensource.zyxel.com>), and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5 Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6 No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7 Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8 Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9 Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10 Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11 General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

Note: NOTE: Some components of the Vantage CNM 2.3 incorporate source code covered under the Apache License, GPL License, LGPL License, Sun License, and Castor License. To obtain the source code covered under those Licenses, please check <ftp://opensource.zyxel.com> to get it.

Index

A

alternative subnet mask notation [142](#)

AP [19](#)

AP (Access Point) [169](#)

AP Mode

 menu [49](#)

 status screen [47](#), [55](#), [67](#)

AP+Bridge [19](#)

B

Bridge/Repeater [19](#)

bridged APs, security [86](#)

BSS [167](#)

C

CA [174](#)

Certificate Authority [174](#)

certifications [183](#)

 notices [184](#)

 viewing [185](#)

Channel [48](#), [68](#), [169](#)

 Interference [169](#)

channel [84](#)

Configuration

 restore [113](#)

copyright [183](#)

CPU usage [49](#), [56](#), [69](#)

CTS (Clear to Send) [170](#)

D

Daylight saving [110](#)

Dimensions [125](#)

disclaimer [183](#)

Dynamic WEP Key Exchange [174](#)

E

EAP Authentication [173](#)

Encryption [175](#)

encryption [85](#)

 key [86](#)

 WPA compatible [86](#)

ESS [168](#)

Extended Service Set [168](#)

F

FCC interference statement [183](#)

Firmware upload [111](#)

 file extension

 using HTTP

firmware version [48](#), [55](#), [68](#)

Fragmentation Threshold [171](#)

G

General wireless LAN screen [87](#)

H

Hidden Node [169](#)

I

IANA [148](#)

IBSS [167](#)

IEEE 802.11g [171](#)
Independent Basic Service Set [167](#)
Internet Assigned Numbers Authority
 See IANA
IP Address [104](#)
IP alias [102](#)

L

LAN [101](#)
LAN overview [101](#)
LAN setup [101](#)
LAN TCP/IP [102](#)
Language [114](#)
Link type [49, 56, 68](#)
Local Area Network [101](#)
Log [29](#)

M

MAC [92](#)
MAC address [85](#)
MAC address filter [85](#)
MAC address filtering [92](#)
MAC filter [92](#)
managing the device
 good habits [20](#)
 using the web configurator. See web configurator.
 using the WPS. See WPS.
MBSSID [19](#)
Media access control [92](#)
Memory usage [49, 56, 69](#)
mode [19](#)

N

NAT [147](#)
Navigation Panel [49](#)
navigation panel [49](#)

O

Operating Channel [48, 68](#)
operating mode [19](#)

P

port speed [49, 56, 69](#)
Power Specification [125](#)
Preamble Mode [171](#)
product registration [186](#)

Q

Quality of Service (QoS) [95](#)

R

RADIUS [172](#)
 Shared Secret Key [173](#)
RADIUS Message Types [173](#)
RADIUS Messages [173](#)
registration
 product [186](#)
related documentation [3](#)
Reset button [27](#)
Reset the device [27](#)
Restore configuration [113](#)
RF (Radio Frequency) [126](#)
Roaming [93](#)
RTS (Request To Send) [170](#)
RTS Threshold [169, 170](#)
RTS/CTS Threshold [84, 93, 94](#)

S

safety warnings [7](#)
Scheduling [97](#)
Security Parameters [178](#)

Service Set [40, 87](#)
Service Set IDentification [40, 87](#)
Service Set IDentity. See SSID.
SSID [40, 48, 56, 68, 84, 87](#)
subnet [139](#)
Subnet Mask [104](#)
subnet mask [140](#)
subnetting [143](#)
Summary
 Packet statistics [30](#)
 Wireless station status [32](#)
syntax conventions [5](#)
System General Setup [108](#)
System restart [114](#)

example [83](#)
MAC address filter [85](#)
overview [83](#)
security [84](#)
SSID [84](#)
Wireless security [84](#)
 overview [84](#)
 type [84](#)
Wireless tutorial [73](#)
 WPS [73](#)
WLAN
 Interference [169](#)
 Security Parameters [178](#)
WPA compatible [86](#)
WPA, WPA2 [175](#)
WPS [20](#)

T

Temperature [125](#)
Time setting [109](#)

U

Use Authentication [176](#)

W

warranty [186](#)
 note [186](#)
Web Configurator
 how to access [23](#)
 Overview [23](#)
web configurator [19](#)
WEP Encryption [60, 61, 70, 71, 72, 90, 91](#)
WEP encryption [89](#)
WEP key [89](#)
Wireless association list [32](#)
wireless LAN scheduling [97](#)
Wireless network
 basic guidelines [84](#)
 channel [84](#)
 encryption [85](#)

