

NWA1300-NJ

802.11 b/g/n In-wall PoE Access Point

User's Guide

Default Login Details

User Name	admin
Password	1234

Firmware Version 1.0
Edition 1, 03/2011

www.zyxel.com

ZyXEL

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the NWA1300-NJ using the Web Configurator.

Tips for Reading User's Guides On-Screen

When reading a ZyXEL User's Guide On-Screen, keep the following in mind:

- If you don't already have the latest version of Adobe Reader, you can download it from <http://www.adobe.com>.
- Use the PDF's bookmarks to quickly navigate to the areas that interest you. Adobe Reader's bookmarks pane opens by default in all ZyXEL User's Guide PDFs.
- If you know the page number or know vaguely which page-range you want to view, you can enter a number in the toolbar in Reader, then press [ENTER] to jump directly to that page.
- Type [CTRL]+[F] to open the Adobe Reader search utility and enter a word or phrase. This can help you quickly pinpoint the information you require. You can also enter text directly into the toolbar in Reader.
- To quickly move around within a page, press the [SPACE] bar. This turns your cursor into a "hand" with which you can grab the page and move it around freely on your screen.
- Embedded hyperlinks are actually cross-references to related text. Click them to jump to the corresponding section of the User's Guide PDF.

Related Documentation

- Quick Start Guide

The Quick Start Guide is designed to help you get your NWA1300-NJ 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

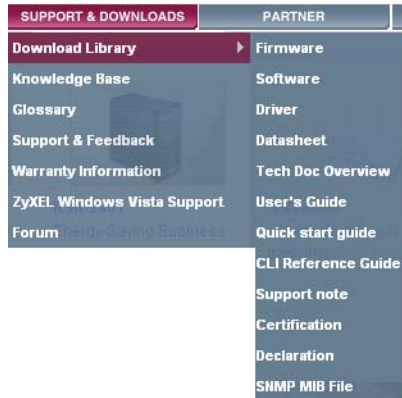
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

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.

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 NWA1300-NJ may be referred to as the “NWA1300-NJ”, 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 NWA1300-NJ icon is not an exact representation of your device.

NWA1300-NJ 	Computer 	Notebook computer 
Server 	DSLAM 	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).
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.

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

User's Guide 15

 Introduction 17

 The Web Configurator 21

 Tutorials 25

Technical Reference 29

 Network Setting 31

 Wireless LAN 35

 Administration 45

 System Tools 67

 Troubleshooting 69

Table of Contents

About This User's Guide	3
Document Conventions.....	6
Safety Warnings.....	8
Contents Overview	9
Table of Contents.....	11
 Part I: User's Guide.....	 15
 Chapter 1	
Introduction	17
1.1 Overview	17
1.2 Applications	18
1.3 Ways to Manage the NWA1300-NJ	18
1.4 Good Habits for Managing the NWA1300-NJ	18
1.5 Resetting the NWA1300-NJ	19
1.5.1 Procedure to Use the Reset Button	19
1.6 LEDs	20
 Chapter 2	
The Web Configurator	21
2.1 Overview	21
2.2 Accessing the Web Configurator	21
2.3 The Web Configurator Layout	23
2.3.1 Navigation Panel	23
2.3.2 Main Window	24
2.3.3 Status Bar	24
 Chapter 3	
Tutorials	25
3.1 Overview	25
3.2 Wireless Network Setup	25
3.2.1 Configuring the NWA1300-NJ Wireless Network Settings	26
3.2.2 Connecting to the NWA1300-NJ Wirelessly	28

Part II: Technical Reference 29**Chapter 4
Network Setting..... 31**

4.1 Overview	31
4.1.1 What You Can Do in this Chapter	31
4.2 What You Need To Know	31
4.3 LINK	33

**Chapter 5
Wireless LAN..... 35**

5.1 Overview	35
5.1.1 What You Can Do in this Chapter	36
5.1.2 What You Should Know	36
5.2 BASIC	38
5.3 ADVANCED	40
5.4 SECURITY	42

**Chapter 6
Administration..... 45**

6.1 Overview	45
6.1.1 What You Can Do in this Chapter	45
6.2 MANAGEMENT	46
6.3 FTP	48
6.4 FIRMWARE	49
6.4.1 Manual Firmware Upgrade Using the Web Configurator	50
6.4.2 Manual Firmware Upgrade via TFTP Server	50
6.4.3 Scheduled Firmware Upgrade	51
6.5 CONFIGURATION	53
6.5.1 Backup Configuration Using HTTP	53
6.5.2 Backup Configuration Using TFTP	55
6.5.3 Restore Configuration Using HTTP	56
6.5.4 Restore Configuration Using TFTP	57
6.5.5 Back to Factory Defaults	58
6.6 SNMP	58
6.6.1 SNMPv3 User Profile	61
6.7 SYSTEM STATUS	64
6.8 PING COMMAND	66

**Chapter 7
System Tools..... 67**

7.1 Overview	67
7.1.1 What You Can Do in this Chapter	67

7.2 RESTART 67

Chapter 8

Troubleshooting..... 69

8.1 Overview 69

8.2 Power, Hardware Connections, and LEDs 69

8.3 NWA1300-NJ Access and Login 70

8.4 Internet Access 71

8.5 Wireless LAN Troubleshooting 72

Appendix A Product Specifications..... 73

Appendix B Pop-up Windows, JavaScripts and Java Permissions 75

Appendix C Setting Up Your Computer’s IP Address..... 87

Appendix D Wireless LANs 115

Appendix E Open Software Announcements 131

Appendix F Legal Information 157

Index..... 161

PART I

User's Guide

Introduction

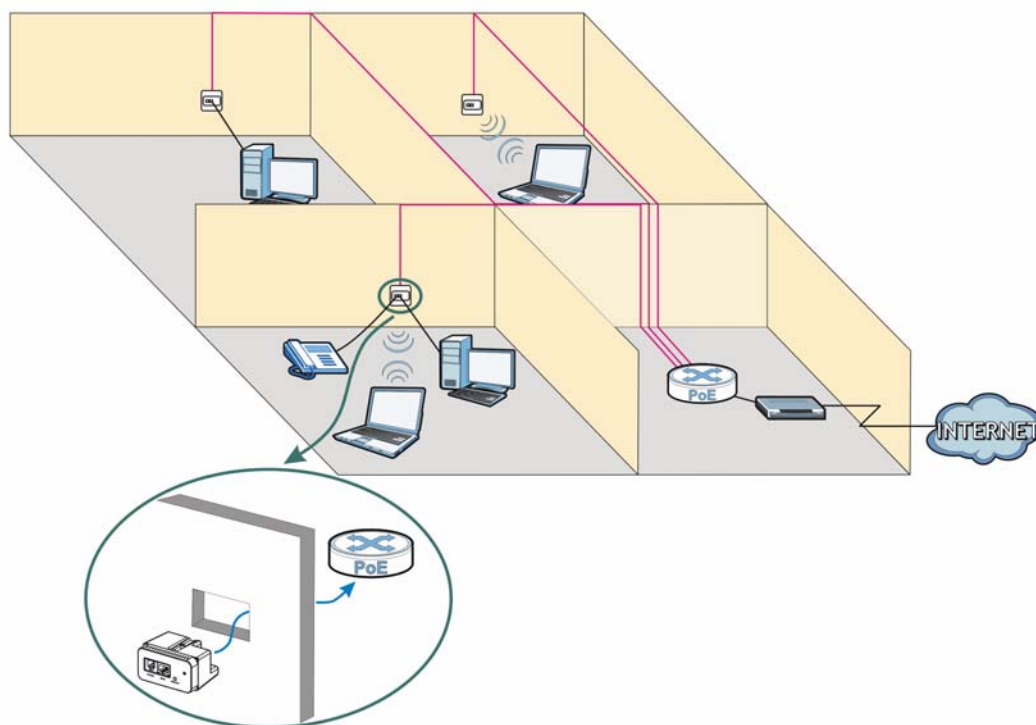
1.1 Overview

This chapter introduces the main features and applications of the NWA1300-NJ.

The NWA1300-NJ is an in-the-wall IEEE 802.11b/g/n wireless access point that supports Power over Ethernet (PoE) to eliminate the need for power sockets. The compact NWA1300-NJ can fit in a standard size wall outlet box, which allows you to hide it in the wall or wallboard with the wall jack faceplate.

The NWA1300-NJ 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.

In the following example, you connect a PoE switch to a broadband router/modem. You then use the switch to provide power and Internet access to three NWA1300-NJs in different rooms via Ethernet cables.

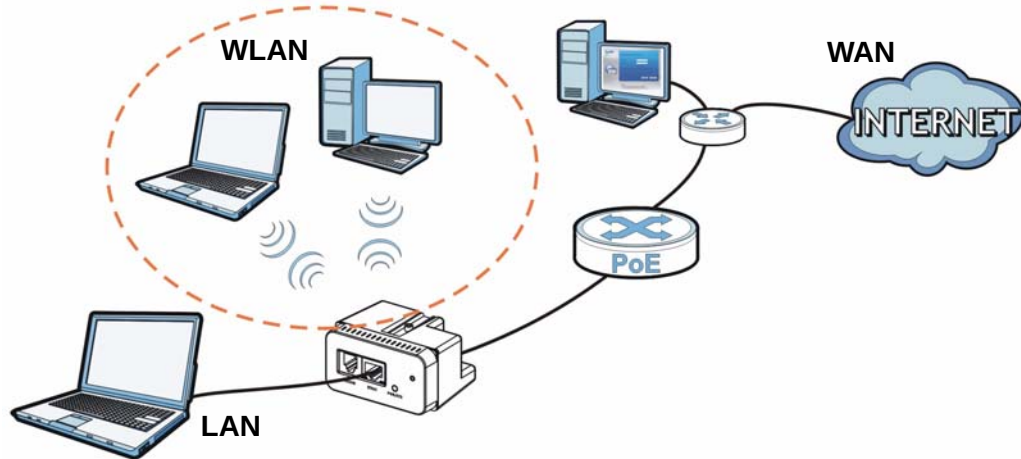


1.2 Applications

You can have the following networks on the NWA1300-NJ:

- **Wired.** You can connect network devices via the Ethernet port of the NWA1300-NJ so that they can communicate with each other and access the Internet.
- **Wireless.** Wireless clients can connect to the NWA1300-NJ to access network resources and the Internet.

Figure 1 NWA1300-NJ Applications



1.3 Ways to Manage the NWA1300-NJ

Use any of the following methods to manage the NWA1300-NJ.

- **ENC.** You can use a computer with the Enterprise Network Center (ENC) installed to provision and manage multiple NWA1300-NJs at the same time. The ENC supports DHCP option 224 which allows the ENC to discover and provision the NWA1300-NJ automatically.
- **Web Configurator.** This is for everyday management of the NWA1300-NJ using a (supported) web browser. By default, the NWA1300-NJ is in DHCP client mode. You need to connect the NWA1300-NJ to a DHCP server to obtain an IP address first before accessing the web configurator.
- **SNMP.** The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.

1.4 Good Habits for Managing the NWA1300-NJ

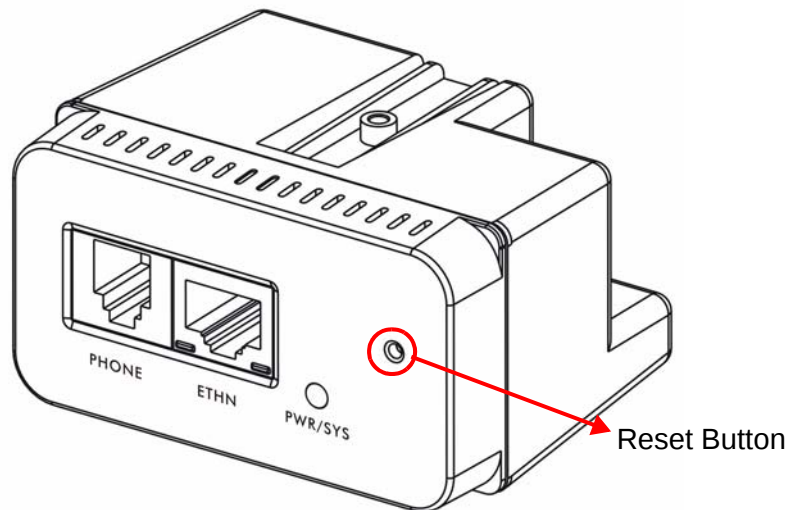
Do the following things regularly to make the NWA1300-NJ more secure and to manage the NWA1300-NJ more effectively.

- 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 NWA1300-NJ to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NWA1300-NJ. You could simply restore your last configuration.

1.5 Resetting the NWA1300-NJ

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the reset button on the front panel of the NWA1300-NJ 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 configured IP address will be reset to a dynamically assigned IP address from a DHCP server (if available).

Figure 2 NWA1300-NJ Reset Button

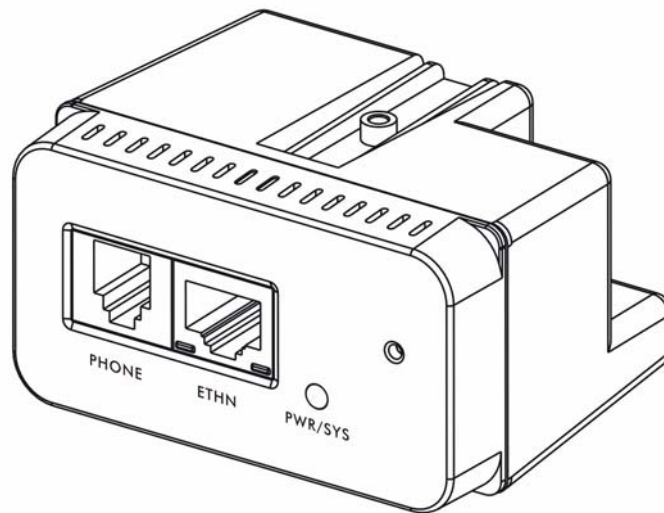


1.5.1 Procedure to Use the Reset Button

- 1 Make sure the power LED is on.
- 2 Press the reset button for longer than five seconds to set the NWA1300-NJ back to its factory-default configurations.

1.6 LEDs

Figure 3 Front Panel



The following table describes the LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS	Green	On	The NWA1300-NJ is receiving power and starts up.
		Blinking	The NWA1300-NJ is self-testing.
		Off	The NWA1300-NJ is not receiving power or the NWA1300-NJ is ready for use.
ETHN	Yellow	On	The NWA1300-NJ is receiving power and starts up.
	Green	On	The NWA1300-NJ is receiving power and starts up.
		Blinking	The NWA1300-NJ is sending/receiving data through the LAN.
		Off	The port is not connected. The LED also turns off when the NWA1300-NJ is ready or the NWA1300-NJ has a successful 10/100MB Ethernet connection.

The Web Configurator

2.1 Overview

This chapter describes how to access the NWA1300-NJ 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 NWA1300-NJ via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

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

2.2 Accessing the Web Configurator

- 1 Make sure your NWA1300-NJ hardware is properly connected and prepare your computer or computer network to connect to the NWA1300-NJ (refer to the Quick Start Guide).
- 2 The NWA1300-NJ's Ethernet port is set to DHCP client mode by default. Make sure the NWA1300-NJ is connected to a DHCP server. Check your DHCP server to know the IP address assigned to the NWA1300-NJ by the DHCP server.
- 3 Launch your web browser.
- 4 Type the NWA1300-NJ's IP address as the website address.

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

- 5 Type "admin" (default) as the user name and "1234" (default) as the password and click **Submit**. In some versions, the default password appears automatically - if this is the case, click **Submit**.

Figure 4 Password Screen



NWA1300-NJ

Username: admin

Password:

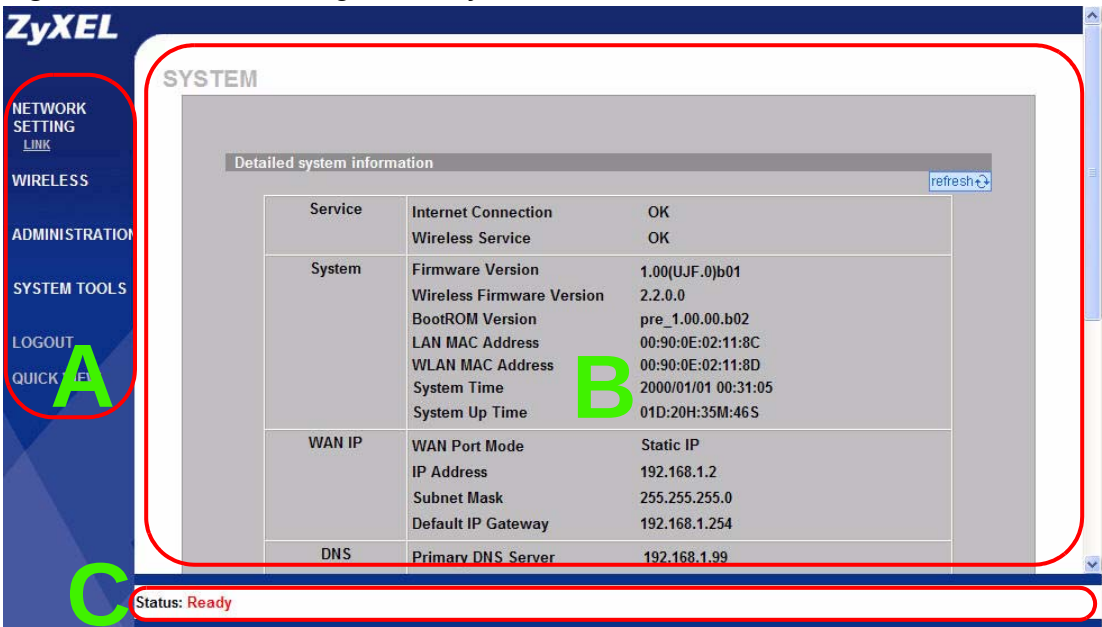
Submit Reset

Note: For security reasons, the NWA1300-NJ automatically logs you out if you do not use the web configurator for five minutes (default). Simply log back into the NWA1300-NJ if this happens.

Right after you log in, the **SYSTEM STATUS** screen is displayed. See [Chapter 6 on page 45](#) for more information about the **SYSTEM STATUS** screen.

2.3 The Web Configurator Layout

Figure 5 The Web Configurator Layout



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

- **A** - navigation panel
- **B** - main window
- **C** - status bar

2.3.1 Navigation Panel

Use the sub-menus on the navigation panel to configure NWA1300-NJ features.

The following table describes the sub-menus.

Table 2 Screens Summary

LINK	TAB	FUNCTION
NETWORK SETTING		
LINK		Use this screen to configure NWA1300-NJ's IP address and subnet mask, and DNS server settings.
WIRELESS		
BASIC		Use this screen to configure general wireless LAN settings.
ADVANCED		Use this screen to configure advanced wireless settings.
SECURITY		Use this screen to configure wireless security settings.
ADMINISTRATION		

Table 2 Screens Summary

LINK	TAB	FUNCTION
MANAGEMENT		Use this screen to change administrative settings such as system password and your NWA1300-NJ's time and date.
FTP		Use this screen to configure from which IP address(es) users can use FTP to access the NWA1300-NJ.
FIRMWARE	Manual Firmware Upgrade	Use this screen to manually upload firmware to your NWA1300-NJ.
	Scheduled Firmware Upgrade	Use this screen to automatically download the latest firmware from a TFTP server according to a schedule.
CONFIGURATION		Use this screen to backup and restore the configuration or reset the factory defaults to your NWA1300-NJ.
SNMP		Use this screen to configure the NWA1300-NJ SNMP settings.
SYSTEM STATUS		This screen shows the current state of the NWA1300-NJ.
PING COMMAND		Use this screen to test the Internet connection.
SYSTEM TOOLS		
RESTART		Use this screen to reboot the NWA1300-NJ without turning the power off.
LOGOUT		Click this to log out of the Web Configurator.

2.3.2 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

2.3.3 Status Bar

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

Tutorials

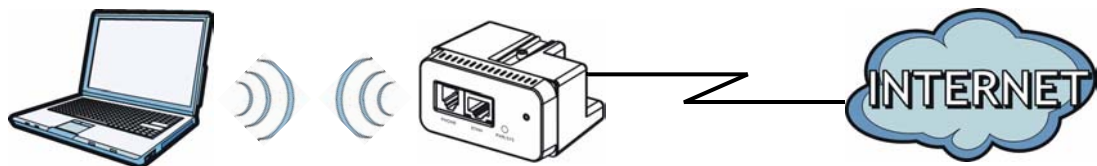
3.1 Overview

This chapter describes how to set up a wireless network.

Note: The tutorials featured in this chapter require a basic understanding of connecting to and using the Web Configurator on your NWA1300-NJ. For details, see the included Quick Start Guide. For field descriptions of individual screens, see the related technical reference in this User's Guide.

3.2 Wireless Network Setup

The NWA1300-NJ is connected to a broadband modem with Internet access. Thomas wants to set up a wireless network so that the users can use their notebooks or computers to wirelessly access the Internet through the NWA1300-NJ. In this wireless network, the NWA1300-NJ serves as an access point (AP), and the notebook with a wireless network card or USB/PCI adapter is the wireless client. The wireless client can access the Internet through the AP.



Thomas has to configure the wireless network settings on the NWA1300-NJ. Then users can set up a wireless network using manual configuration ([Section 3.2.2 on page 28](#)).

3.2.1 Configuring the NWA1300-NJ Wireless Network Settings

This example uses the following parameters to set up a wireless network.

SSID	SSID_Example
Channel	6
Security Mode	WPA-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork
802.11 Mode	IEEE 802.11b/g/n (Mixed)

Follow the steps below to configure the wireless settings on the NWA1300-NJ.

Note: To see the current SSID, go to the **ADMINISTRATION > SYSTEM STATUS** or the **QUICK VIEW** screen.

- 1 Open the **WIRELESS > BASIC** screen in the NWA1300-NJ's web configurator. Configure the screen using the provided parameters (see [page 26](#)).
- 2 Enter "SSID_Example" as the ESSID and select a channel (6 in this example) which is not used by another AP.
- 3 Select **802.11n + 802.11g + 802.11b** in the **802.11 Mode** field. Click **Apply**.

The screenshot shows the 'BASIC WIRELESS SETTINGS' web page. Under the 'General Setting' tab, the following fields are visible: ESSID (text box with 'SSID_Example'), Channel (dropdown menu with '6' selected), 802.11 Mode (dropdown menu with '802.11n + 802.11g + 802.11b' selected), Channel Width (dropdown menu with 'Auto 20/40 MHZ' selected), and Transmit Power (dropdown menu with '50%' selected). An 'Apply' button is located at the bottom right of the settings area.

- 4 Go to **WIRELESS > SECURITY**.

- 5 Set security mode to **WPA**, select the **Use WPA with Pre-shared Key** option and enter “DoNotStealMyWirelessNetwork” in the **Pre-shared Key** field. Click **Apply**.

SECURITY WIRELESS SETTINGS

Security: ☐ Disable ☒ **WPA** ☐ WPA2 ☐ WPA/WPA2

Group Key Rekeying: Per 86400 seconds

☒ **Use WPA with Pre-shared Key**
Pre-shared Key: DoNotStealMyWirelessNetwork (8~63 characters)

☐ Use WPA with RADIUS Server
Server IP:
Authentication Port:
Shared Secret Key: (8~63 characters)

☐ WEP
Encryption: ☐ 64bit ☐ 128bit
Mode: HEX
WEP Key:
☐ 1.
☐ 2.
☐ 3.
☐ 4.

Note: You have to restart the system to apply the WEP settings

Authentication Method: ☐ Open System ☐ Shared Key ☒ Both

- 6 Click **QUICK VIEW** to open the system status screen. Verify your wireless and wireless security settings and check if the WLAN connection is up.

ZyXEL

NETWORK SETTING

WIRELESS

ADMINISTRATION

MANAGEMENT

FTP

FIRMWARE

CONFIGURATION

SNMP

SYSTEM STATUS

PING COMMAND

SYSTEM TOOLS

LOGOUT

QUICK VIEW

Detailed system information [refresh](#)

Service	Internet Connection	OK
	Wireless Service	OK
System	Firmware Version	1.00(UJF.0)b01_alpha1
	Wireless Firmware Version	2.2.0.0
	BootROM Version	pre_1.00.00.b02
	LAN MAC Address	00:90:0E:02:11:8C
	WLAN MAC Address	00:90:0E:02:11:8D
	System Time	2000/01/01 05:30:24
	System Up Time	01D:20H:35M:46S
WAN IP	WAN Port Mode	Static IP
	IP Address	192.168.1.2
	Subnet Mask	255.255.255.0
	Default IP Gateway	192.168.1.254
DNS	Primary DNS Server	192.168.1.99
	Secondary DNS Server	
Wireless	ESSID	SSID_Example
	Channel	6
	Encryption	WPA
Network Traffic	WAN Traffic	Tx Data:2568666

Status: **Ready**

- 7 The user can now use the notebook's wireless client to search for the NWA1300-NJ (see [Section 3.2.2 on page 28](#)).

3.2.2 Connecting to the NWA1300-NJ Wirelessly

Use the wireless adapter's utility installed on the notebook to search for the "SSID_Example" SSID. Then enter the "DoNotStealMyWirelessNetwork" pre-shared key to establish an wireless Internet connection.

Note: The NWA1300-NJ 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.

PART II

Technical Reference

Network Setting

4.1 Overview

This chapter describes how to configure your NWA1300-NJ's IP address to communicate with the wired network to which the NWA1300-NJ is connected.

4.1.1 What You Can Do in this Chapter

Use the **LINK** ([Section 4.3 on page 33](#)) screen to change your IP address assignment.

4.2 What You Need To Know

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

WAN IP Address Assignment

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

Table 3 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

DNS Server Address Assignment

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

Maximum Transmission Unit

A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes) that can be sent in a packet- or frame-based network. The Transmission Control Protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission. Too large an MTU size may mean retransmissions if the packet encounters a router that can't handle that large a packet. Too small an MTU size means relatively more header overhead and more acknowledgements that have to be sent and handled.

4.3 LINK

Use this screen to change your IP settings. The NWA1300-NJ's Ethernet port is set to DHCP client mode by default. Click **NETWORK SETTING > LINK**.

Figure 6 NETWORK SETTING > LINK

The following table describes the labels in this screen.

Table 4 NETWORK SETTING > LINK

LABEL	DESCRIPTION
DHCP Client	Select this option if your NWA1300-NJ is using a dynamically assigned IP address from a DHCP server each time. Note: You must know the IP address assigned to the NWA1300-NJ (by the DHCP server) to access the NWA1300-NJ again.
MTU Setting	Enter the MTU (Maximum Transmission Unit) size for the Ethernet interface.
Static IP	Select this option if you were assigned a fixed IP address (and DNS server settings) to use for Internet access
IP Address	Enter the IP address of your NWA1300-NJ in dotted decimal notation. Note: If you change the NWA1300-NJ's IP address, you must use the new IP address if you want to access the web configurator again.
Subnet Mask	Enter the subnet mask that specifies the network number portion of an IP address.

Table 4 NETWORK SETTING > LINK (continued)

LABEL	DESCRIPTION
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your NWA1300-NJ that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your NWA1300-NJ; over the WAN, the gateway must be the IP address of one of the remote nodes.
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
MTU Setting	Enter the MTU (Maximum Transmission Unit) size for the Ethernet interface.
ENC IP Address	Enter the IP addresses of the connected ENC (Enterprise Network Center) server for central management. If the NWA1300-NJ is connected to a DHCP server that supports option 224, the NWA1300-NJ can obtain the ENC server's IP address automatically from the DHCP server.
Apply	Click Apply to save your changes back to the NWA1300-NJ.

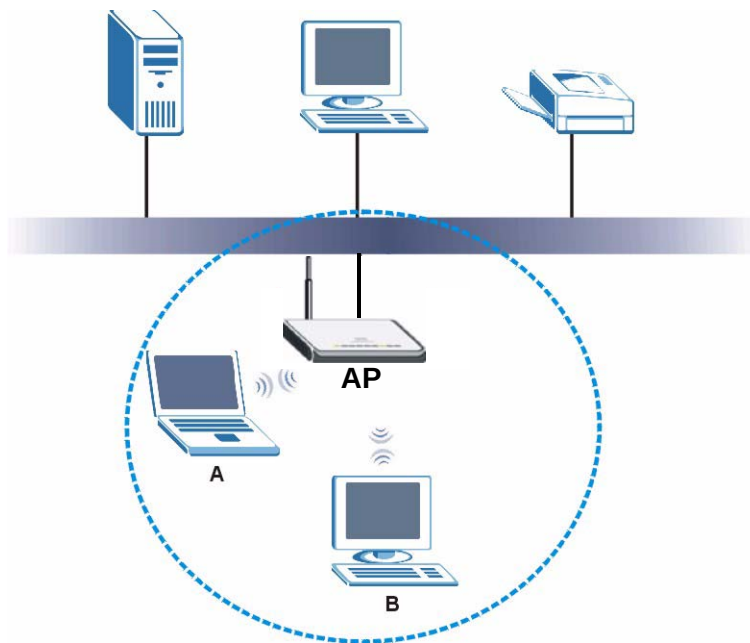
Wireless LAN

5.1 Overview

This chapter discusses how to configure the wireless network settings in your NWA1300-NJ. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 7 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 NWA1300-NJ is the AP.

5.1.1 What You Can Do in this Chapter

- Use the **BASIC** screen ([Section 5.2 on page 38](#)) to configure the general wireless settings, such as the SSID, channel and 802.11 mode.
- Use the **ADVANCED** screen ([Section 5.3 on page 40](#)) to configure the advanced wireless settings, such as the RTS/CTS Threshold and preamble type.
- Use the **SECURITY** screen ([Section 5.4 on page 42](#)) to configure the wireless security settings.

5.1.2 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.

Wireless Security Overview

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

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.

User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

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

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

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

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

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

Encryption

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

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

Table 5 Types of Encryption for Each Type of Authentication

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

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

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

Note: It is recommended that wireless networks use WPA-PSK, WPA, 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.

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

If you want to use WPA2 in your NWA1300-NJ, you can select to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should select the **WPA / WPA2** option in the NWA1300-NJ.

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.

5.2 BASIC

Use this screen to enter the SSID, and select the channel and 802.11 mode.

Note: If you are configuring the NWA1300-NJ from a computer connected to the wireless LAN and you change the NWA1300-NJ'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 NWA1300-NJ's new settings.

Click **WIRELESS > BASIC**.

Figure 8 WIRELESS > BASIC

The screenshot shows the 'BASIC WIRELESS SETTINGS' configuration window. It has a title bar 'General Setting' and a list of settings: ESSID (text field with 'Wireless'), Channel (dropdown menu with '6'), 802.11 Mode (dropdown menu with '802.11g + 802.11b'), Channel Width (dropdown menu with 'Auto 20/40 MHZ'), and Transmit Power (dropdown menu with '25%'). An 'Apply' button is located at the bottom right of the settings area.

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

Table 6 WIRELESS > BASIC

LABEL	DESCRIPTION
ESSID	The SSID (Service Set IDentity) identifies the Service Set with which a wireless station is associated. Wireless clients associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Channel	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. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible.
802.11 Mode	Select 802.11n + 802.11g + 802.11b to allow both IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NWA1300-NJ. The transmission rate of your NWA1300-NJ might be reduced. Select 802.11n + 802.11g to allow either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the NWA1300-NJ. Select 802.11g + 802.11b to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the NWA1300-NJ. The NWA1300-NJ adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. Select 802.11n Only to only allow IEEE 802.11n compliant WLAN devices to associate with the NWA1300-NJ. Select 802.11g Only to only allow IEEE 802.11g compliant WLAN devices to associate with the NWA1300-NJ. Select 802.11b Only to only allow IEEE 802.11b compliant WLAN devices to associate with the NWA1300-NJ.
Channel Width	Select whether the NWA1300-NJ uses a wireless channel width of 20 or 40 MHz. A standard 20 MHz channel offers transfer speeds of up to 150Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps. Because not all devices support 40 MHz channels, select Auto 20/40 MHz to allow the NWA1300-NJ to adjust the channel bandwidth automatically. Select 20 MHz if you want to lessen radio interference with other wireless devices in your neighborhood.
Transmit Power	Set the output power of the NWA1300-NJ in this field. If there is a high density of APs in an area, decrease the output power of the NWA1300-NJ to reduce interference with other APs. Select one of the following 100 %, 50 % or 25 %.
Apply	Click Apply to save your changes back to the NWA1300-NJ.

5.3 ADVANCED

Use this screen to configure the advanced wireless settings. Click **WIRELESS > ADVANCED**. The screen appears as shown.

Figure 9 WIRELESS > ADVANCED

ADVANCED WIRELESS SETTINGS

Do not change any setting below unless you make sure you understand all the meaning of setting. , You can press "DEFAULT" to restore the wireless factory default setting?once you made setting changed to cause wireless not work.

Beacon Interval: (msec, range:1~1000, default:100)

RTS Threshold: (range:256~2432, default:2432)

Fragmentation Threshold: (range:800~2432, default:2346, even number only)

Preamble Type: ☒ Dynamic Preamble ☐ Short Preamble ☐ Long Preamble

The following table describes the labels in this screen.

Table 7 WIRELESS > ADVANCED

LABEL	DESCRIPTION
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. This value can be set from 1ms to 1000ms. A high value helps save current consumption of the access point.
RTS 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 to enable an RTS/CTS handshake to avoid retransmitting due to hidden nodes.
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 800 and 2432.

Table 7 WIRELESS > ADVANCED

LABEL	DESCRIPTION
Preamble Type	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. Select Long Preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks. Select Short Preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications. Select Dynamic Preamble to automatically use short preamble when all wireless devices on the network support it, otherwise the NWA1300-NJ uses long preamble. Note: If a wireless device uses a different preamble mode than the NWA1300-NJ does, it cannot communicate with the NWA1300-NJ.
Default	Click Default to reload the default configuration for this screen.
Apply	Click Apply to save your changes back to the NWA1300-NJ.

5.4 SECURITY

Use this screen to configure the wireless security settings. Click **WIRELESS > SECURITY**. The screen appears as shown.

Figure 10 WIRELESS > SECURITY

The following table describes the labels in this screen.

Table 8 WIRELESS > SECURITY

LABEL	DESCRIPTION
Security	
Disable	Select this to allow wireless stations to communicate with the access points without any data encryption or authentication. Note: If you do not enable any wireless security on your NWA1300-NJ, your network is accessible to any wireless networking device that is within range.

Table 8 WIRELESS > SECURITY (continued)

LABEL	DESCRIPTION
WPA	Select this to configure and enable WPA or WPA-PSK authentication and encryption.
WPA2	Select this to configure and enable WPA2 or WPA2-PSK authentication and encryption.
WPA/WPA2	Select this to have both WPA2 and WPA wireless clients be able to communicate with the NWA1300-NJ even when the NWA1300-NJ is using WPA2 or WPA2-PSK.
Group Key Rekeying	Enter the rate at which the AP or the RADIUS server sends a new group key out to all clients.
Use WPA with Pre-shared Key	Select this option if you do not have a RADIUS server in your network and want to use a pre-shared key WPA or WPA2.
Pre-shared Key	The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Use WPA with RADIUS Server	Select this option if you have a RADIUS server in your network and want to use it for user authentication and encryption.
Server IP	Enter the IP address of the external authentication server in dotted decimal notation.
Authentication Port	Enter the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret Key	Enter a password (from 8 to 63 case-sensitive ASCII characters) as the key to be shared between the external authentication server and the NWA1300-NJ. The key must be the same on the external authentication server and your NWA1300-NJ. The key is not sent over the network.
WEP	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 clients and the access points must use the same WEP key. Select this to configure and enable WEP encryption.
Encryption	The NWA1300-NJ 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.
Mode	Select the type of input mode from the drop-down list box. Select ASCII to enter ASCII characters as WEP key. Select HEX to enter hexadecimal characters as a WEP key.

Table 8 WIRELESS > SECURITY (continued)

LABEL	DESCRIPTION
WEP Key	The WEP keys are used to secure your data from eavesdropping by unauthorized wireless users. Both the NWA1300-NJ and the wireless clients must use the same WEP key for data transmission. If you chose 64bit in the Encryption field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each key. If you chose 128bit in the Encryption field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each key. You must configure all four keys. Only one key can be activated at any one time. Select a default key to use for data encryption.
Authentication Method	Select Open System, Shared Key or Both. This field specifies whether the wireless clients have to provide the WEP key to login to the wireless network. Keep this setting at Both or Open System unless you want to force a key verification before communication between the wireless client and the NWA1300-NJ occurs. Select Shared Key to force the clients to provide the WEP key prior to communication.
Default	Click Default to reload the default configuration for this screen.
Apply	Click Apply to save your changes back to the NWA1300-NJ.

Administration

6.1 Overview

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

6.1.1 What You Can Do in this Chapter

- Use the **MANAGEMENT** screen ([Section 6.2 on page 46](#)) to set the password, change your NWA1300-NJ's time and date and configure from which IP address(es) users can manage the NWA1300-NJ.
- Use the **FTP** screen ([Section 6.3 on page 48](#)) to configure from which IP address(es) users can use FTP to access the NWA1300-NJ.
- Use the **FIRMWARE** screen ([Section 6.4 on page 49](#)) to upload firmware to your NWA1300-NJ.
- Use the **CONFIGURATION** screen ([Section 6.5 on page 53](#)) to backup and restore device configurations. You can also reset your device settings back to the factory default.
- Use the **SNMP** screen ([Section 6.6 on page 58](#)) to configure your SNMP settings.
- Use the **SYSTEM STATUS** screen ([Section 6.7 on page 64](#)) to look at the current state of the NWA1300-NJ.
- Use the **PING COMMAND** screen ([Section 6.8 on page 66](#)) to test the Internet connection.

6.2 MANAGEMENT

Use this screen to set the password and configure the NWA1300-NJ's time based on your local time zone. Click **ADMINISTRATION > MANAGEMENT**. The following screen displays.

Figure 11 ADMINISTRATION > MANAGEMENT

MANAGEMENT

Administrator Setting

Please be sure to change your password:

Username:

Password:

Date/Time

Date: 2002 1 1 (Year/Month/Day)

Time: 5 55 7 (Hour : Minute : Second)

☐ Use NTP (Network Time Protocol) Time Server

Server IP/Domain Name:

Time Zone: GMT -12:00

Update Time: 0 hours

☐ Daylight Saving Time

Start Date: 4 Month/ 1 Day

End Date: 10 Month/ 31 Day

LED Setting

☒ Enable

☐ Disable

Secure Administrator IP Address

☒ Any

☐ Specify

	~	
	~	
	~	
	~	
	~	

Allow remote user to ping the device

☒ Enable ☐ Disable

The following table describes the labels in this screen.

Table 9 ADMINISTRATION > MANAGEMENT

LABEL	DESCRIPTION
Administrator Setting	
Username	Type your new system user name (up to 20 case-sensitive alphanumeric characters).
Password	Type your new system password (up to 20 case-sensitive alphanumeric characters). Note that as you type a password, the screen displays a dot (.) for each character you type.
Date/Time	
Date	This field displays the date of your NWA1300-NJ. Each time you reload this page, the NWA1300-NJ synchronizes the date with the time server. Select the new date manually and then click Apply. This field is not configurable if you select Use NTP (Network Time Protocol) Time Server.
Time	This field displays the time of your NWA1300-NJ. Each time you reload this page, the NWA1300-NJ synchronizes the time with the time server. Select the new time manually and then click Apply. This field is not configurable if you select Use NTP (Network Time Protocol) Time Server.
Get from My Computer	Click this button to set the time and date on the NWA1300-NJ to be the same as the management computer. This button is not available if you select Use NTP (Network Time Protocol) Time Server.
Get from NTP Server	Click this button to set the NWA1300-NJ to get time and date information from a specified NTP (Network Time Protocol) time server. This button is available only if you select Use NTP (Network Time Protocol) Time Server.
Use NTP (Network Time Protocol) Time Server	Select this check box to allow the NWA1300-NJ to get time and date information from an NTP (Network Time Protocol) time server.
Server IP/ Domain Name	Enter the IP address or URL (up to 100 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Update Time	Enter a number to determine how often the NWA1300-NJ uses the NTP server to update the time and date.
Daylight Saving Time	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.

Table 9 ADMINISTRATION > MANAGEMENT (continued)

LABEL	DESCRIPTION
Start Date	Select the month and day that your daylight-savings time starts on if you selected Daylight Saving Time .
End Date	Select the month and day that your daylight-savings time ends on if you selected Daylight Saving Time .
LED Setting	Select Enable to have the LEDs on the front panel operate as long as the NWA1300-NJ is powered on. Select Disable to have the LEDs on the front panel operate during start-up and turn off once the NWA1300-NJ is ready.
Secure Administrator IP Address	Select Any to use any computer to access the web configurator on the NWA1300-NJ. Select Specify and then enter the IP address(es) or ranges of IP addresses of the computer(s) that are allowed to log in to configure the NWA1300-NJ. The addresses can be on the LAN or the WAN.
Allow remote user to ping the device	Ping (Packet Internet Groper) is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. Select Enable to have the NWA1300-NJ respond to incoming Ping requests from the WAN. This is less secure since someone on the Internet can see that the NWA1300-NJ is there by pinging it. Select Disable to have the NWA1300-NJ not respond to incoming Ping requests from the WAN. This is more secure since someone on the Internet cannot see that the NWA1300-NJ is there by pinging it.
Apply	Click Apply to save your changes back to the NWA1300-NJ.

6.3 FTP

You can use FTP (File Transfer Protocol) to upload and download the NWA1300-NJ's firmware and configuration files, see [Section 6.4 on page 49](#) and [Section 6.5 on page 53](#) for details. To use this feature, your computer must have an FTP client.

To change your NWA1300-NJ's FTP settings, click **ADMINISTRATION > FTP**. The screen appears as shown. Use this screen to specify from which IP address the access can come.

Figure 12 ADMINISTRATION > FTP

The following table describes the labels in this screen.

Table 10 ADMINISTRATION > FTP

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use FTP to access the NWA1300-NJ.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the NWA1300-NJ using this service. Select All to allow any computer to access the NWA1300-NJ using FTP. Choose Selected to just allow the computer with the IP address that you specify to access the NWA1300-NJ using FTP.
Reset	Click Reset to reload the default configuration for this screen.
Apply	Click Apply to save your changes back to the NWA1300-NJ.

6.4 FIRMWARE

There are two ways to upgrade firmware to the NWA1300-NJ: manually or scheduled.

To manually upgrade the firmware, you have to download the latest firmware first from www.zyxel.com and then upload it to the NWA1300-NJ. You can upload it to the NWA1300-NJ using the Web Configurator or using a TFTP server.

With scheduled firmware upgrade, you need to set up a TFTP server where the NWA1300-NJ can automatically download the latest firmware at the specified time.

6.4.1 Manual Firmware Upgrade Using the Web Configurator

Follow the instructions in this screen to upload firmware to your NWA1300-NJ using the web configurator.

- 1 Click **ADMINISTRATION > FIRMWARE**.

Figure 13 ADMINISTRATION > FIRMWARE > Manual Firmware Upgrade: Using the Web Configurator

- 2 Specify the name of the firmware file in the **Local PC File Path** field or click **Browse** to locate the file and click **Apply** to start the file transfer process. The firmware must be a binary file and should have a .bin extension.
- 3 When the file transfer is completed successfully, the NWA1300-NJ automatically restarts.

WARNING!

Do not interrupt the file upload process as this may PERMANENTLY damage the device.

- 4 After the NWA1300-NJ finishes restarting, access the web configurator again. Check the firmware version number in the **SYSTEM STATUS** screen.

Note: When the NWA1300-NJ restarts, all connections terminate. Subscribers need to log in again.

6.4.2 Manual Firmware Upgrade via TFTP Server

Use the following procedure to use TFTP to upload the firmware from a TFTP server to the NWA1300-NJ.

- 1 Download the latest firmware from www.zyxel.com and store it in a TFTP server. Unzip the file if it is zipped.

- 2 Run a TFTP server program and specify the location of the firmware file and the communication mode. Refer to the documentation that comes with your TFTP server program for instructions.
- 3 Access the web configurator. Refer to the section on accessing the web configurator for instructions.
- 4 Click **ADMINISTRATION > FIRMWARE**.

Figure 14 ADMINISTRATION > FIRMWARE > Manual Firmware Upgrade: via TFTP Server

The screenshot shows the 'FIRMWARE' section of a web configurator. There are two tabs: 'Manual Firmware Upgrade' (selected) and 'Scheduled Firmware Upgrade'. Under the 'Manual Firmware Upgrade' tab, there is a 'Firmware' section with three input fields: 'Local PC File Path' (with a 'Browse...' button), 'Remote TFTP Server IP Address', and 'File Name'. Each field has an 'Apply' button to its right. A red circle is drawn around the 'Remote TFTP Server IP Address' and 'File Name' fields and their respective 'Apply' buttons.

- 5 Specify the IP address of the TFTP server in the **Remote TFTP Server IP Address** field.
- 6 Specify the name of the firmware file in the **File Name** field.
- 7 Click **Apply** to start the file transfer process.
- 8 When the file transfer is completed successfully, the NWA1300-NJ automatically restarts.

WARNING!

Do not interrupt the file upload process as this may PERMANENTLY damage the device.

- 9 After the NWA1300-NJ finishes restarting, access the web configurator again. Check the firmware version number in the **SYSTEM STATUS** screen.

6.4.3 Scheduled Firmware Upgrade

Click **ADMINISTRATION > FIRMWARE > Scheduled Firmware Upgrade**.

Configure the screen to automatically download the latest firmware from a TFTP server.

Note: Make sure that the TFTP server has the firmware and synchronization check file before you configure for scheduled firmware upgrades.

Make sure that you check new features or functionality enhancements in new firmware releases before you put the firmware on the TFTP server.

WARNING!

Do not interrupt the file upload process as this may PERMANENTLY damage the device.

Figure 15 ADMINISTRATION > FIRMWARE > Scheduled Firmware Upgrade

The screenshot shows the 'FIRMWARE' configuration page with the 'Scheduled Firmware Upgrade' tab selected. It includes radio buttons for 'Disable' (selected) and 'Enable'. Below these are input fields for 'TFTP Server IP' and 'File Synchronization', with a 'View Sample Code' link next to the latter. The 'Frequency' section has radio buttons for 'Weekly' (selected), 'Daily', and 'Hourly', followed by dropdown menus for 'Sunday', '00', 'Hour', '00', and 'Minute'. An 'Apply' button is located at the bottom of the form.

The following table describes the labels in this screen.

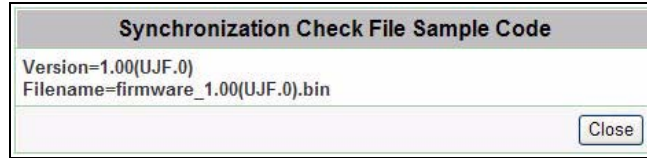
Table 11 ADMINISTRATION > FIRMWARE > Scheduled Firmware Upgrade

LABEL	DESCRIPTION
Enable Disable	Select Disable or Enable to turn the scheduled firmware upgrade function on or off (disabled by default).
TFTP Server IP	Type the IP address of the TFTP server from which the NWA1300-NJ can download new firmware files.
File Synchronization	A synchronization check file is a .txt file containing the latest firmware filename and version number on the TFTP server. Enter the name of the check file.
View Sample File	Click View Sample File to see an example synchronization check file.
Frequency	Set how often (Weekly , Daily or Hourly) you want to have the NWA1300-NJ check for new firmware and upgrade to new firmware if available (default Weekly). Then select the day (applies only when you select Weekly), the hour (applies when you select Daily or Hourly) and the minute that you want the NWA1300-NJ to do the check and upload.
Apply	Click Apply to save your changes back to the NWA1300-NJ.

Note: When the NWA1300-NJ restarts, all connections terminate. Subscribers need to log in again.

The following figure shows an example of a check file's content.

Figure 16 Synchronization Check File Example



6.5 CONFIGURATION

You can use the web configurator to perform configuration file backup and restore. Backing up the configuration allows you to back up (save) the device's current configuration to a file. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

WARNING!
DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS
MAY PERMANENTLY DAMAGE YOUR DEVICE.

6.5.1 Backup Configuration Using HTTP

Use the following procedure to use HTTP to back up the device's current configuration to a file on your computer.

- 1 Click **ADMINISTRATION > CONFIGURATION**. A screen displays as shown next. Click **Backup**.

Figure 17 ADMINISTRATION > CONFIGURATION: Backup Using HTTP

The screenshot shows the CONFIGURATION page with three main sections: Backup, Restore, and Reset. The Backup section is highlighted with a red circle around the 'Backup' button. The Restore section has a 'Browse...' button next to the Local PC File Path field. The Reset section has an 'Apply' button.

CONFIGURATION

Backup

Click Backup to backup the system configuration from this device to your computer or to the remote TFTP server.

Remote TFTP Server IP Address: File Name:

Restore

To restore your stored system configuration to this device.

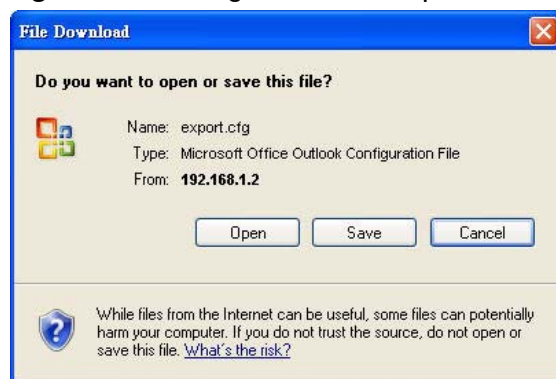
Local PC File Path:

Remote TFTP Server IP Address: File Name:

Reset the system back to factory defaults

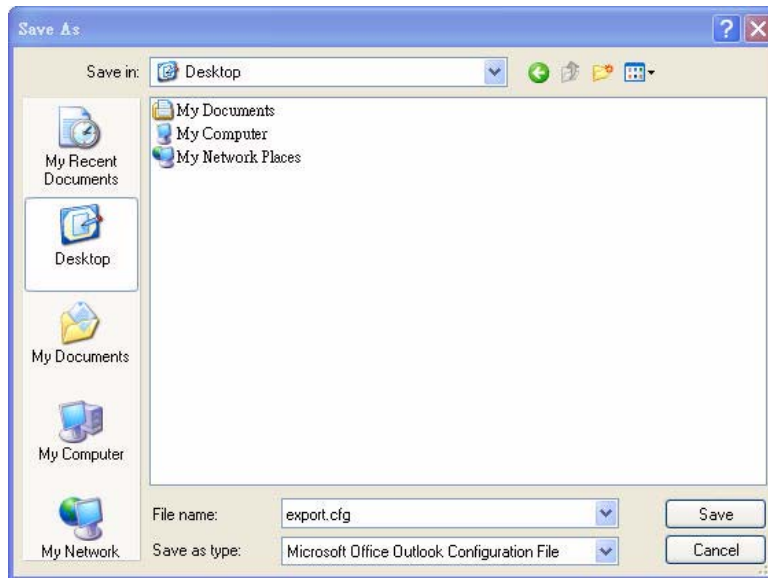
- 2 A **File Download** window displays as shown next. Click **Save**.

Figure 18 Configuration Backup: File Download



- 3 A **Save As** window displays.

Figure 19 Configuration Backup: Save As



- 4 Specify the file name and/or location and click **Save** to start the backup process.

6.5.2 Backup Configuration Using TFTP

Use the following procedure to use TFTP to back up the device's current configuration to a file on a TFTP server.

- 1 Click **ADMINISTRATION > CONFIGURATION**. A screen displays as shown next.

Figure 20 ADMINISTRATION > CONFIGURATION: Backup Using TFTP

CONFIGURATION

Backup

Click Backup to backup the system configuration from this device to your computer or to the remote TFTP server.

Remote TFTP Server IP Address: File Name:

Restore

To restore your stored system configuration to this device.

Local PC File Path:

Remote TFTP Server IP Address: File Name:

Reset the system back to factory defaults

- 2 Enter the IP address of the TFTP server in dotted decimal notation in the **Remote TFTP Server IP Address** field.
- 3 Specify a file name for the configuration backup in the **File Name** field.
- 4 Click **Apply**. When the file transfer process is complete, a screen displays as follows.

Figure 21 Configuration Backup: Using TFTP Successful

Success!

The Export Configuration has been transferred.

6.5.3 Restore Configuration Using HTTP

This section shows you how to upload a new or previously saved configuration file from your computer to your NWA1300-NJ.

Note: This function erases the current configuration before restoring a previous backup configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

- 1 Click **ADMINISTRATION > CONFIGURATION**. A screen displays as shown next.

Figure 22 ADMINISTRATION > CONFIGURATION: Restore Using HTTP

CONFIGURATION

Backup
Click Backup to backup the system configuration from this device to your computer or to the remote TFTP server.
Remote TFTP Server IP Address: File Name:

Restore
To restore your stored system configuration to this device.
Local PC File Path:
Remote TFTP Server IP Address: File Name:
Reset the system back to factory defaults

- 2 Specify the location and filename of a configuration file in the **Local PC File Path** field or click **Browse**.
- 3 Click **Apply** to start the configuration restore process. The NWA1300-NJ automatically restarts after the restoration process is complete.

6.5.4 Restore Configuration Using TFTP

This section shows you how to upload a new or previously saved configuration file from a TFTP server to your NWA1300-NJ.

Note: This function erases the current configuration before restoring a previous backup configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

- 1 Click **ADMINISTRATION > CONFIGURATION**. A screen displays as shown next.

Figure 23 ADMINISTRATION > CONFIGURATION: Restore Using TFTP

The screenshot shows the CONFIGURATION page with three main sections: Backup, Restore, and Reset the system back to factory defaults. The Restore section is active, showing fields for Local PC File Path, Remote TFTP Server IP Address, and File Name. The Remote TFTP Server IP Address and File Name fields are highlighted with a red circle. The Apply button is visible next to the File Name field.

- 2 Enter the IP address of the TFTP server in dotted decimal notation in the **Remote TFTP Server IP Address** field.
- 3 Specify the file name of the configuration file in the **File Name** field.
- 4 Click **Apply** to start the configuration restore process. The NWA1300-NJ automatically restarts after the restoration process is complete.

6.5.5 Back to Factory Defaults

Pressing the **Apply** button in this section clears all user-entered configuration information and returns the NWA1300-NJ to its factory defaults.

You can also press the reset button on the front panel to reset the factory defaults of your NWA1300-NJ. Refer to the chapter about introducing the Web Configurator for more information on the reset button.

6.6 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. Your NWA1300-NJ supports

SNMP agent functionality, which allows a manager station to manage and monitor the NWA1300-NJ through the network.

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the NWA1300-NJ). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include number of packets received, node port status and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 12 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

Click **ADMINISTRATION > SNMP** to open the following screen. Use this screen to configure the NWA1300-NJ SNMP settings.

Figure 24 ADMINISTRATION > SNMP

The screenshot shows the 'SNMP Agent Configuration' screen. It has a title bar 'SNMP Agent Configuration' and a sub-header 'SNMP Setup'. Under 'SNMP Setup', there are radio buttons for 'Enable' (selected) and 'Disable'. Below this are input fields for 'SNMP Port' (with a hint '(161 or 16100 ~16199)') and 'Trap Port' (with a hint '(162 or 16200 ~16299)'). A 'Time interval' field is set to '60' with a hint '(1-60 Second)'. There is a checkbox for 'SNMPv3' with a link 'Configure SNMPv3 User Profile'. Below this is a table labeled 'Configuration' with 5 rows. The table has columns: 'No', 'Community Name', 'NMS Address', 'Privileges', and 'Status'. The first row is pre-filled with '1', 'public', 'ANY', 'Read', and 'Valid'. The other rows have empty input fields. At the bottom right is an 'Apply' button.

No	Community Name	NMS Address	Privileges	Status
1	public	ANY	Read	Valid
2			Write	Valid
3			Read	Valid
4			Read	Valid
5			Read	Valid

The following table describes the fields in this screen.

Table 13 ADMINISTRATION > SNMP

LABEL	DESCRIPTION
SNMP Setup	Select Enable to allow a manager station to manage and monitor the NWA1300-NJ through the network via SNMP. Otherwise, select Disable .
Port	
SNMP Port	Enter the NWA1300-NJ's port number to which the manager station sends requests.
Trap Port	Enter the port number on which the manager station listens for SNMP traps and information from the NWA1300-NJ.
Time interval	Specify how long (in seconds) the NWA1300-NJ waits before sending SNMP traps to the ENC server after start-up.
SNMPv3	Select this to enable SNMPv3 on the NWA1300-NJ.
Configure SNMPv3 User Profile	Click Configure SNMPv3 User Profile to open a screen where you can configure SNMPv3 users.
Configuration	
No	This is the index number of the entry.

Table 13 ADMINISTRATION > SNMP (continued)

LABEL	DESCRIPTION
Community Name	Enter the password for the incoming Get, GetNext or Set requests from the management station. The default community for read-only access is public and the default community for read-write access is private .
NMS Address	Enter the IP address of the Network Management System (NMS) that controls and monitors the managed device (NWA1300-NJ). If the NWA1300-NJ is connected to a DHCP server that supports option 224, the NWA1300-NJ can obtain the ENC server's IP address automatically from the DHCP server. ANY means any computer that connects to the NWA1300-NJ can request SNMP information and/or receive traps from the NWA1300-NJ.
Privileges	Select the privilege level of the password. Read means the password is for read-only (Get or GetNext) access. Write means the password is for read-write (Get/GetNext and Set) access. Trap Recipient means the password is for accepting SNMP traps from the NWA1300-NJ. All means the password has all the above permissions.
Status	Select whether this password is valid or not.
Apply	Click Apply to save your changes back to the NWA1300-NJ.

6.6.1 SNMPv3 User Profile

From the **ADMINISTRATION > SNMP** screen, click the **Configure SNMPv3 User Profile** link to view the screen as shown. Use this screen to create SNMP

users for authentication with managers using SNMP v3. An SNMP user is an SNMP manager.

Figure 25 ADMINISTRATION > SNMP > Configure SNMPv3 User Profile

SNMPv3 User Profile

SNMPv3 Admin

☐ Enable SNMPv3 Admin

User Name: (8~20 characters)

Password: (8~20 characters)

Confirm Password: (8~20 characters)

Access Type: read-only ▼

Authentication Protocol: MD5 ▼

Privacy Protocol: None ▼

SNMPv3 User

☐ Enable SNMPv3 User

User Name: (8~20 characters)

Password: (8~20 characters)

Confirm Password: (8~20 characters)

Access Type: read-only ▼

Authentication Protocol: MD5 ▼

Privacy Protocol: None ▼

Reset Apply

The following table describes the labels in this screen.

Table 14 ADMINISTRATION > SNMP > Configure SNMPv3 User Profile

LABEL	DESCRIPTION
SNMPv3 Admin/ SNMPv3 User	
Enable SNMPv3 Admin/Enable SNMPv3 User	Select the checkbox to activate the SNMPv3 login account.
Username	Specify the username of a login account on the NWA1300-NJ.
Password	Enter the password from 8 to 20 ASCII characters for the login account.
Confirm Password	Enter the password again for confirmation.

Table 14 ADMINISTRATION > SNMP > Configure SNMPv3 User Profile (continued)

LABEL	DESCRIPTION
Access Type	Specify the access right for the admin login account. The user account has read right only. readwrite - the account has read and write rights, meaning that the user can create and edit the MIBs on the NWA1300-NJ, except the user account and AAA configuration. readonly - the account has read right only, meaning the user can collect information from the NWA1300-NJ.
Authentication Protocol	Select an authentication algorithm. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Privacy Protocol	Specify the encryption method for SNMP communication with this user. You can choose one of the following: • None - Do not implement encryption for encrypting SNMP packets. • DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Reset	Click Reset to reload the default configuration for this screen.
Apply	Click Apply to save your changes back to the NWA1300-NJ.

6.7 SYSTEM STATUS

Click **ADMINISTRATION > SYSTEM STATUS** or **QUICK VIEW** to open this screen.

Figure 26 ADMINISTRATION > SYSTEM STATUS

The screenshot shows a web interface titled "SYSTEM". Below the title is a section labeled "Detailed system information" with a "refresh" button. The main content is a table with system status details.

Service	Internet Connection	OK
	Wireless Service	OK
System	Firmware Version	v1.00(UJF.0)b01_alpha6
	Wireless Firmware Version	2.2.0.0
	BootROM Version	1.00.01.b01
	LAN MAC Address	50:67:F0:00:96:39
	WLAN MAC Address	50:67:F0:00:97:14
	System Time	2000/01/01 00:08:48
	System Up Time	00D:00H:08M:48S
WAN IP	WAN Port Mode	DHCP Client
	IP Address	192.168.1.2
	Subnet Mask	255.255.255.0
	Default IP Gateway	192.168.1.254
DNS	Primary DNS Server	192.168.1.254
	Secondary DNS Server	
Wireless	ESSID	Zyxel
	Channel	6
	Encryption	
Network Traffic	WAN Traffic	Tx Data:66657 Rx Data:19867 Tx Error: 0 Rx Error: 0
	Wireless Traffic	Tx Data:118974 Rx Data:7820350 Tx Error: 0 Rx Error: 0

The following table describes the labels in this screen.

Table 15 ADMINISTRATION > SYSTEM STATUS

LABEL	DESCRIPTION
Service	
Internet Connection	This field displays the status of the NWA1300-NJ's connection to the Internet.
Wireless Service	This field displays the status of the NWA1300-NJ's wireless LAN.

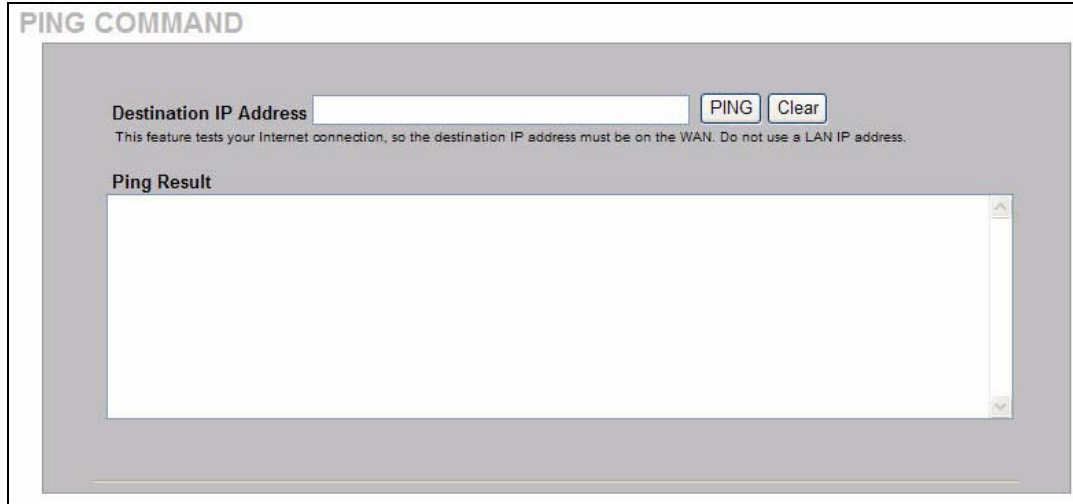
Table 15 ADMINISTRATION > SYSTEM STATUS (continued)

LABEL	DESCRIPTION
System	
Firmware Version	This field displays the version of the firmware on the NWA1300-NJ.
Wireless Firmware Version	This field displays the version of the wireless features on the NWA1300-NJ.
BootROM Version	This field displays the version of the bootbase in the NWA1300-NJ.
LAN MAC Address	This field displays the MAC address of the NWA1300-NJ on the LAN.
WLAN MAC Address	This field displays the MAC address of the NWA1300-NJ on the WLAN.
System Time	This field displays the NWA1300-NJ's current time.
System Up Time	This field displays the how long the NWA1300-NJ has been operating since it was last started.
WAN IP	
WAN Port Mode	This field displays the DHCP mode of the NWA1300-NJ. It displays DHCP Client or Static IP .
IP Address	This field displays the IP address of the NWA1300-NJ.
Subnet Mask	This field displays the subnet mask of the NWA1300-NJ.
Gateway IP address	This field displays the IP address of the default gateway of the WAN port on the NWA1300-NJ.
DNS	
Primary DNS Server	This field displays the IP address of the primary DNS server.
Secondary DNS Server	This field displays the IP address of the secondary DNS server.
Wireless	
ESSID	This field displays the NWA1300-NJ's Extended Service Set IDentity.
Channel	This field displays the channel that the NWA1300-NJ is using.
Encryption	This field displays the type of data encryption that the NWA1300-NJ is using. WEP displays if the NWA1300-NJ is using WEP data encryption. WPA displays if NWA1300-NJ is using WPA data encryption. WPA2 displays if NWA1300-NJ is using WPA2 data encryption. Disable displays if the NWA1300-NJ is not using data encryption.
Network Traffic	
WAN Traffic	This field displays traffic statistics for the NWA1300-NJ's WAN connection.
Wireless Traffic	This field displays traffic statistics for the NWA1300-NJ's wireless LAN connection.

6.8 PING COMMAND

Click **Maintenance > Diagnostic** to open the screen shown next.

Figure 27 ADMINISTRATION > PING COMMAND



The following table describes the fields in this screen.

Table 16 ADMINISTRATION > PING COMMAND

LABEL	DESCRIPTION
Destination IP Address	Type the IP address or the URL of a device on the WAN that you want to ping in order to test the Internet connection. This feature tests your Internet connection, so the destination IP address must be on the WAN. Do not use a LAN IP address.
Ping	Click this button to have the device ping the IP address.
Clear	Click this button to clear the ping results in the multi-line text box.
Ping Result	This multi-line text box displays the results of the ping.

System Tools

7.1 Overview

This chapter covers how to use the **RESTART** screen.

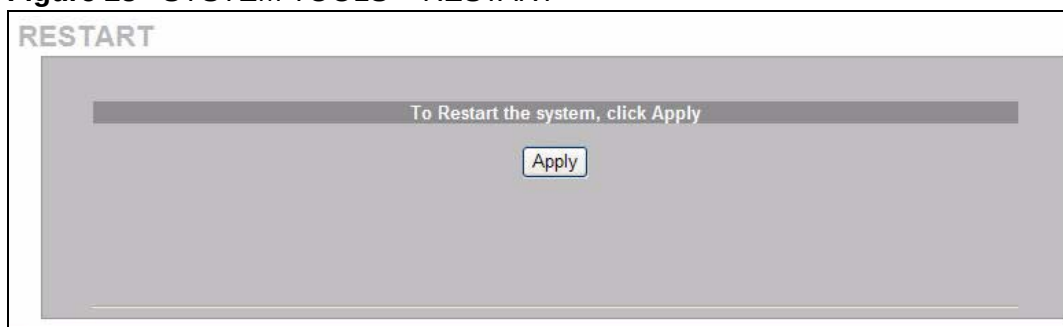
7.1.1 What You Can Do in this Chapter

Use the **RESTART** screen ([Section 7.2 on page 67](#)) to reboot the NWA1300-NJ.

7.2 RESTART

Click **SYSTEM TOOLS > RESTART** to open the screen shown next. Click **Apply** to have the NWA1300-NJ reboot. This does not affect the NWA1300-NJ's configuration.

Figure 28 SYSTEM TOOLS > RESTART



Troubleshooting

8.1 Overview

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](#)
- [NWA1300-NJ Access and Login](#)
- [Internet Access](#)
- [Wireless LAN Troubleshooting](#)

8.2 Power, Hardware Connections, and LEDs

The NWA1300-NJ does not turn on. None of the LEDs turn on.

- 1 Make sure the NWA1300-NJ is connected to a PoE switch.
- 2 Make sure the PoE switch is connected to an appropriate power source and the power source is turned on.
- 3 Disconnect and re-connect the Ethernet cable between the NWA1300-NJ and the PoE switch.
- 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 1.6 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 Ethernet cable between the NWA1300-NJ and the PoE switch to turn the NWA1300-NJ off and on.
- 5 If the problem continues, contact the vendor.

8.3 NWA1300-NJ Access and Login

[I forgot the IP address for the NWA1300-NJ.](#)

- 1 The NWA1300-NJ's Ethernet port is in DHCP client mode by default. If the NWA1300-NJ is working as a DHCP client and receives an IP address from a DHCP server, check the DHCP server for the NWA1300-NJ's IP address.
- 2 If you configured a static IP address and have forgotten it, you have to reset the device to its factory defaults. See [Section 1.5 on page 19](#).

[I cannot see or access the **Login** screen in the web configurator.](#)

- 1 Make sure you are using the correct IP address.
 - See the troubleshooting suggestions for [I forgot the IP address for the NWA1300-NJ](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See [Appendix B on page 75](#).
- 4 Reset the device to its factory defaults, and try to access the NWA1300-NJ with the default IP address. See [Section 1.5 on page 19](#).
- 5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

I can see the **Login** screen, but I cannot log in to the NWA1300-NJ.

- 1 Make sure you have entered the user name and password correctly. The default user name is **admin** and default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 Disconnect and re-connect the Ethernet cable between the NWA1300-NJ and the PoE switch to turn the NWA1300-NJ off and on.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 8.2 on page 69](#).

8.4 Internet Access

I cannot access the Internet through the NWA1300-NJ.

- 1 Make sure you can access the NWA1300-NJ through either wireless or wired connections.
- 2 Make sure the NWA1300-NJ is connected to a network with Internet access.
- 3 Make sure your computer is set to obtain a dynamic IP address or has an IP address which is in the same subnet as the broadband modem or router.
- 4 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NWA1300-NJ), 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 1.6 on page 20](#).
- 2 Disconnect and re-connect the Ethernet cable between the NWA1300-NJ and the PoE switch to turn the NWA1300-NJ off and on.
- 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. If the NWA1300-NJ is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 If you are accessing the Internet wirelessly, check the signal strength. If the signal strength is low, try moving your computer closer to the NWA1300-NJ 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 Disconnect and re-connect the Ethernet cable between the NWA1300-NJ and the PoE switch to turn the NWA1300-NJ off and on.
- 4 If the problem continues, contact the network administrator or vendor.

8.5 Wireless LAN Troubleshooting

I cannot access the NWA1300-NJ or ping any computer from the WLAN.

- 1 Make sure the wireless LAN is enabled on the NWA1300-NJ.
- 2 Make sure the wireless adapter on the wireless station is working properly.
- 3 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the NWA1300-NJ.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NWA1300-NJ.
- 5 Check that both the NWA1300-NJ and your wireless client are using the same wireless and wireless security settings.

Product Specifications

The following tables summarize the NWA1300-NJ's hardware and firmware features.

Table 17 Hardware Features

Dimensions	39.3 mm (W) x 71.6 mm (D) x 55 mm (H)
Device Weight	84 g
DRAM	32 MB
Flash Memory	8 MB
Power Specification	PoE IEEE 802.3af support
Power Consumption	7.2 Watt
Ethernet Ports	One RJ-45 port on the front panel One IEEE 802.3af compliant RJ-45 port on the rear panel Auto-negotiating: 10 Mbps, 100 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
Phone Ports	One RJ-11 FXS POTS port on the front panel One RJ-11 FXO POTS port on the rear panel for POTS pass-through
LEDs	PWR/SYS, ETHN
Reset Button	The reset button is built into the front panel. Use this button to restore the NWA1300-NJ to its factory default settings. Press for 1 second to restart the device. Press for 5 seconds to restore to factory default settings.
Antenna	The NWA1300-NJ is embedded with two transmitter antennas and two receiver antennas to provide clear radio transmission and reception on the wireless network.
Operation Environment	Temperature: 0° C ~ 50° C Humidity: 20% ~ 95%
Storage Environment	Temperature: -30° C ~ 60° C Humidity: 10% ~ 90%

Table 18 Firmware Features

FEATURE	DESCRIPTION
Default User Name	admin
Default Password	1234
Default Wireless SSID	ZyXEL
Device Management	Use the Web Configurator to easily configure the rich range of features on the NWA1300-NJ.
Wireless Functionality	Allows IEEE 802.11b, IEEE 802.11g and/or IEEE 802.11n wireless clients to connect to the NWA1300-NJ wirelessly. Enable wireless security (WPA(2)-PSK) and/or MAC filtering to protect your wireless network. Note: The NWA1300-NJ 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 NWA1300-NJ. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the NWA1300-NJ's configuration and put it back on the NWA1300-NJ later if you decide you want to revert back to an earlier configuration.
Time and Date	Get the current time and date from an external server when you turn on your NWA1300-NJ. You can also set the time manually. These dates and times are then used in logs.

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: The screens used below belong to Internet Explorer version 6, 7 and 8. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

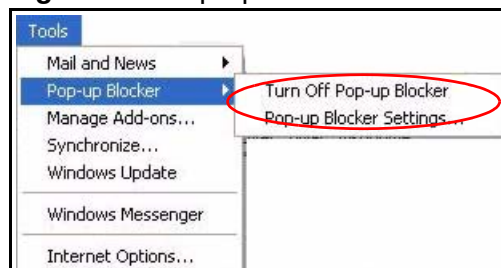
You may have to disable pop-up blocking to log into your device.

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 29 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 30 Internet Options: Privacy



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

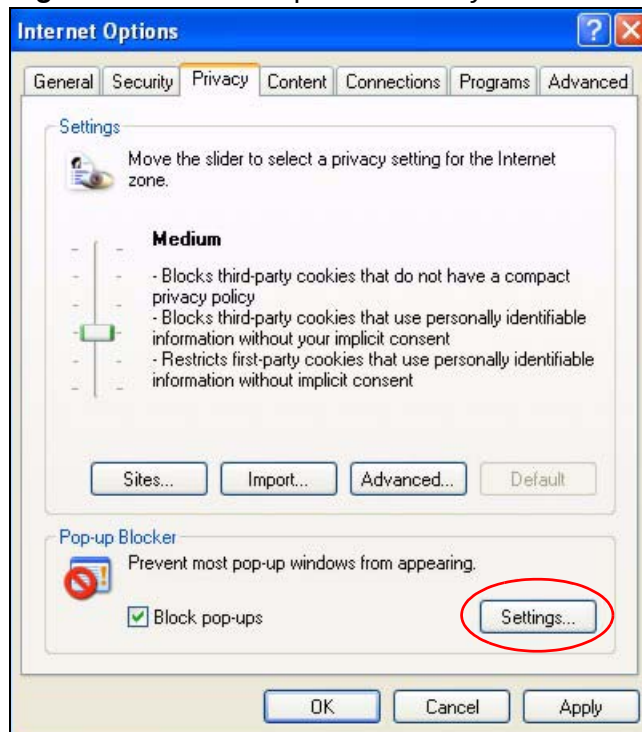
Enable Pop-up Blockers with Exceptions

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.

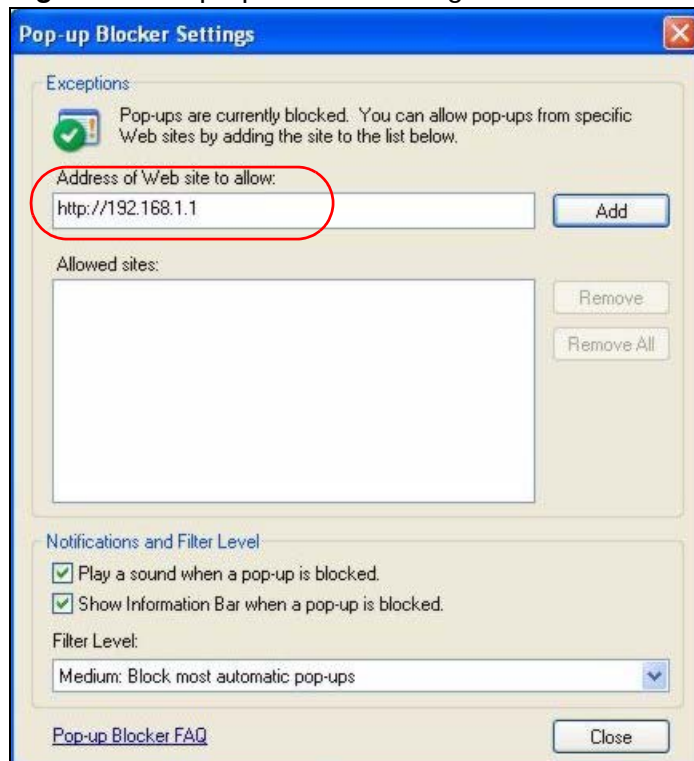
Figure 31 Internet Options: Privacy



- 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 32 Pop-up Blocker Settings



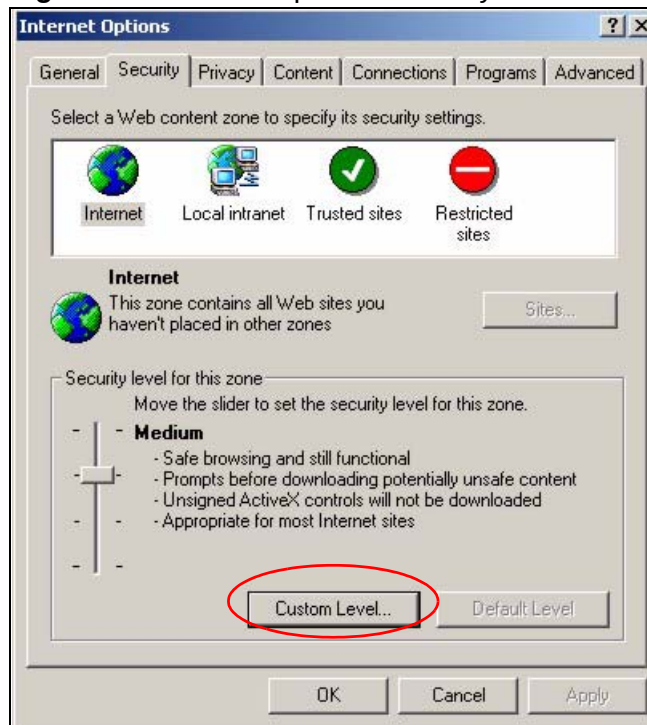
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

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.

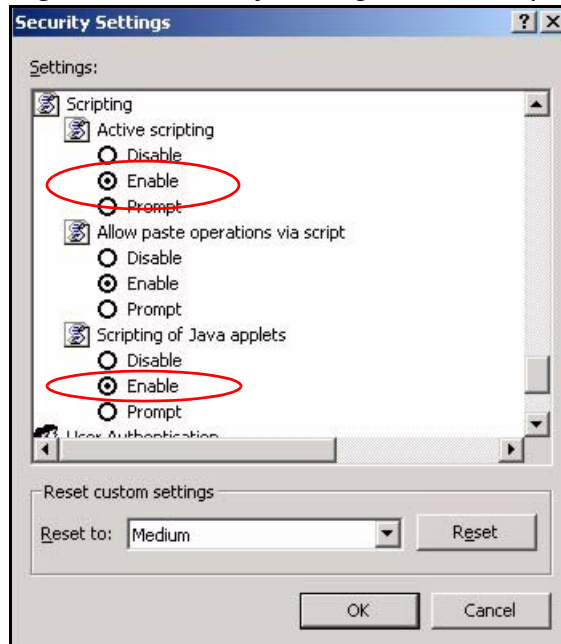
Figure 33 Internet Options: Security



- 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 34 Security Settings - Java Scripting

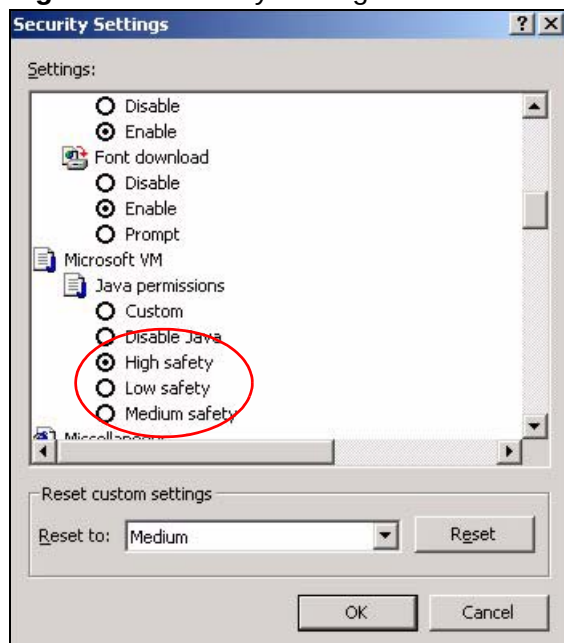


Java Permissions

- 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 35 Security Settings - Java

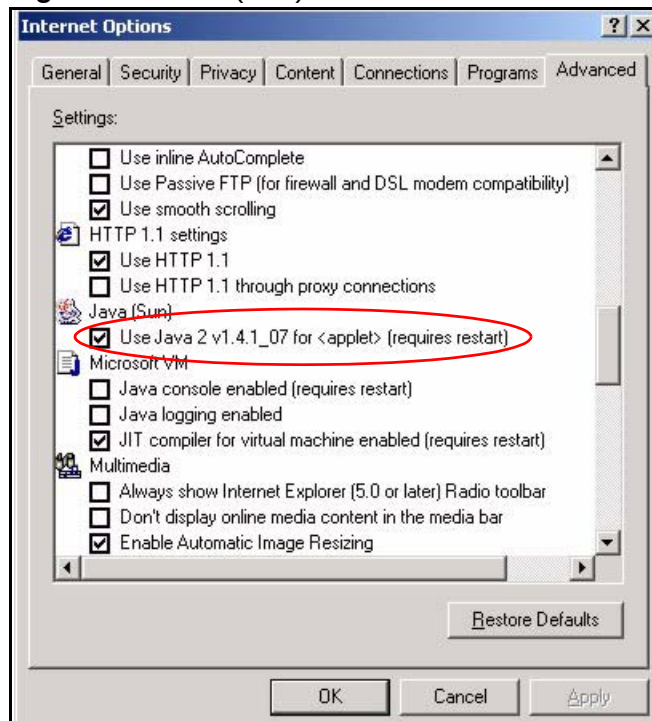


JAVA (Sun)

- 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 36 Java (Sun)

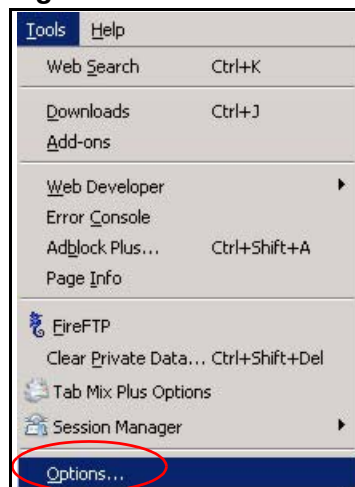


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

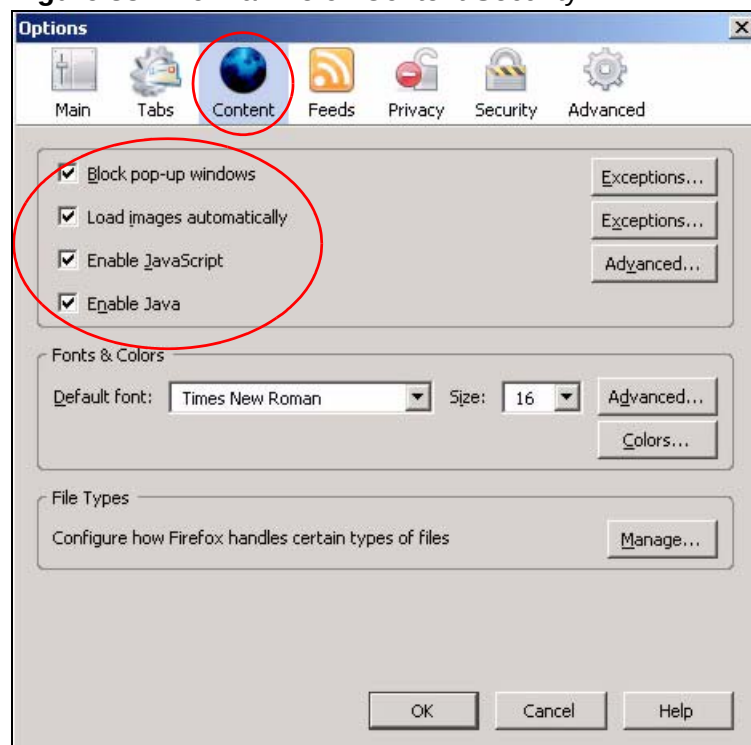
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

Figure 37 Mozilla Firefox: TOOLS > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 38 Mozilla Firefox Content Security



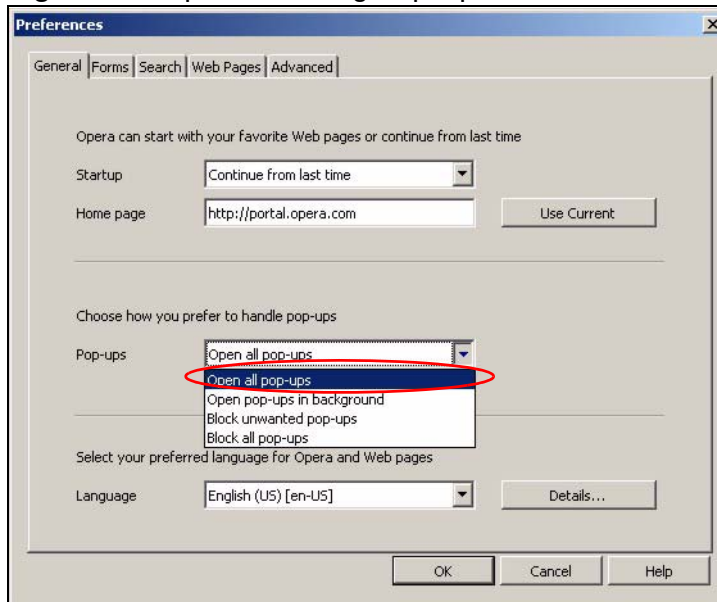
Opera

Opera 10 screens are used here. Screens for other versions may vary slightly.

Allowing Pop-Ups

From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

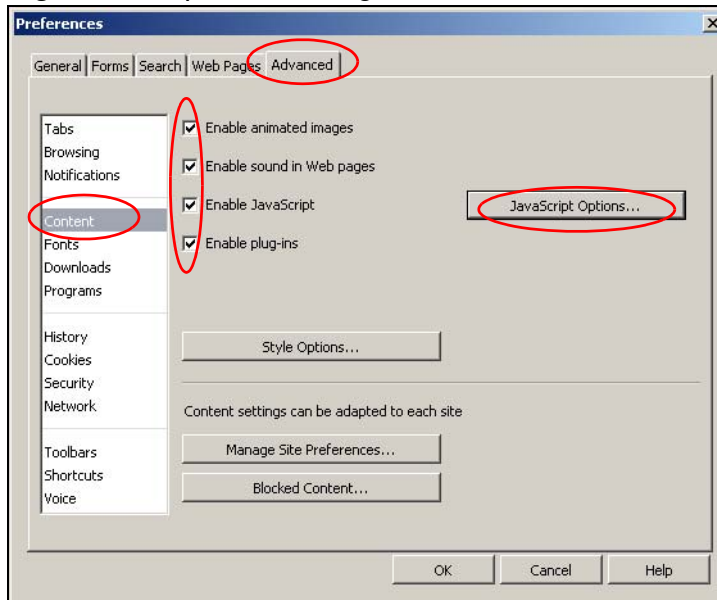
Figure 39 Opera: Allowing Pop-Ups



Enabling Java

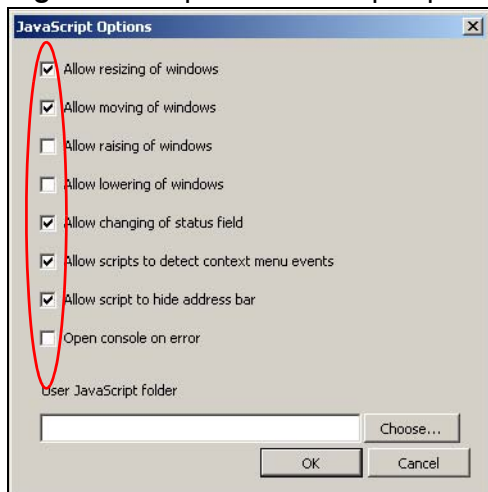
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 40 Opera: Enabling Java



To customize JavaScript behavior in the Opera browser, click **JavaScript Options**.

Figure 41 Opera: JavaScript Options



Select the items you want Opera's JavaScript to apply.

Setting Up Your Computer's IP Address

Note: Your specific NWA1300-NJ may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

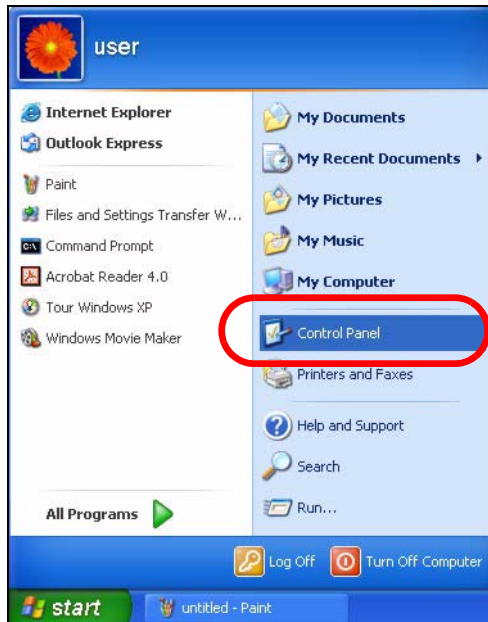
In this appendix, you can set up an IP address for:

- [Windows XP/NT/2000](#) on [page 88](#)
- [Windows Vista](#) on [page 91](#)
- [Windows 7](#) on [page 95](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 99](#)
- [Mac OS X: 10.5 and 10.6](#) on [page 102](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 105](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 110](#)

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

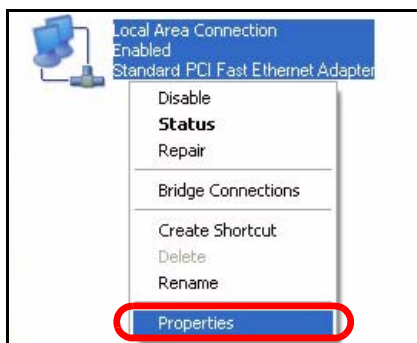
- 1 Click **Start > Control Panel**.



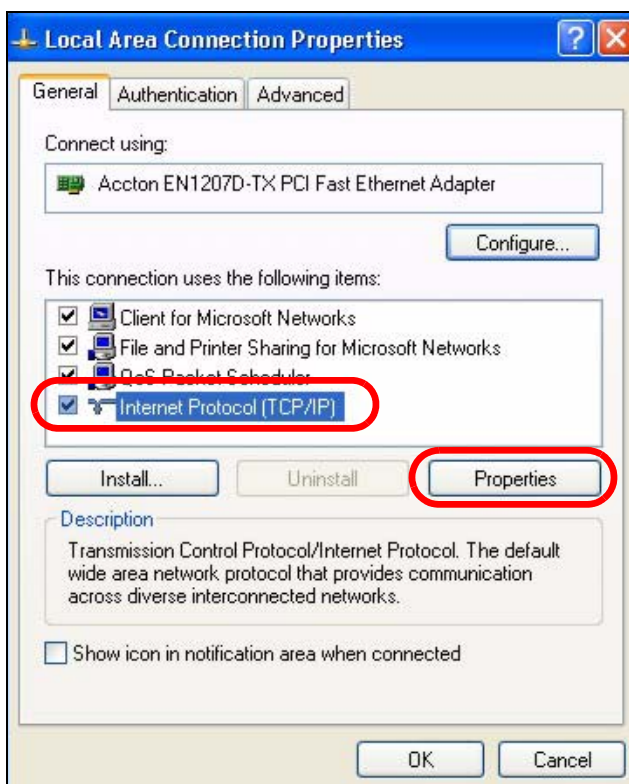
- 2 In the **Control Panel**, click the **Network Connections** icon.



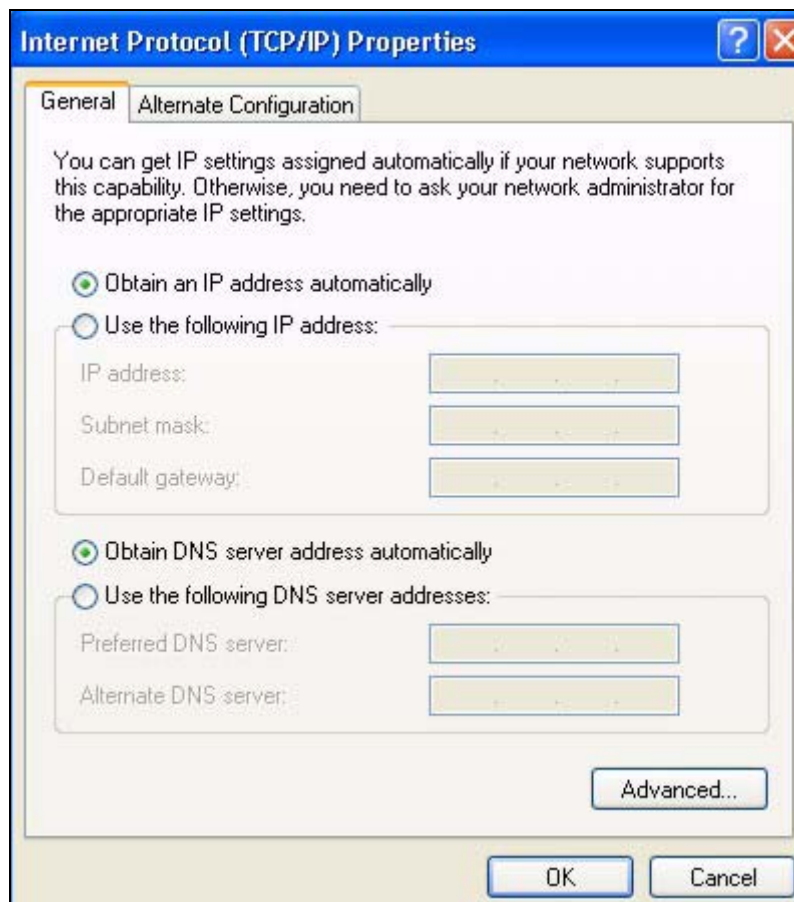
- 3 Right-click **Local Area Connection** and then select **Properties**.



- 4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.



- 5 The **Internet Protocol TCP / IP Properties** window opens.



- 6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided.

- 7 Click **OK** to close the **Internet Protocol (TCP / IP) Properties** window.
- 8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

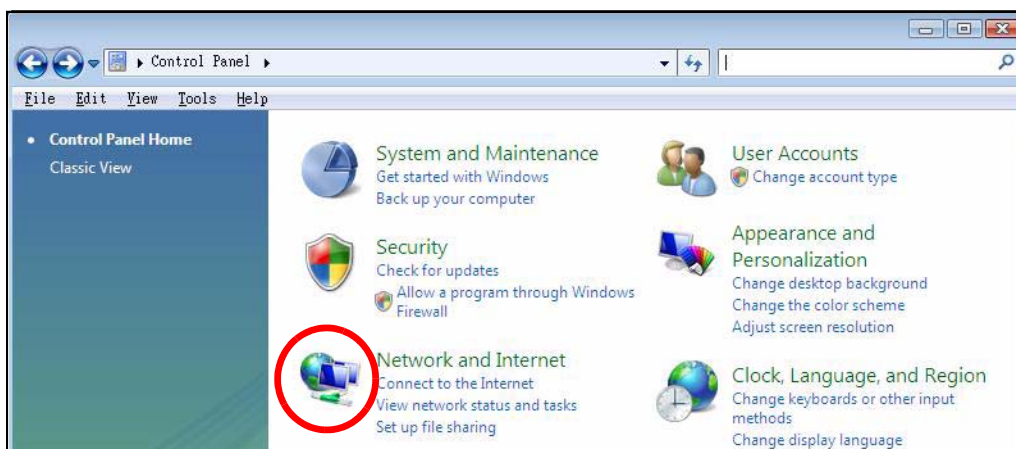
Windows Vista

This section shows screens from Windows Vista Professional.

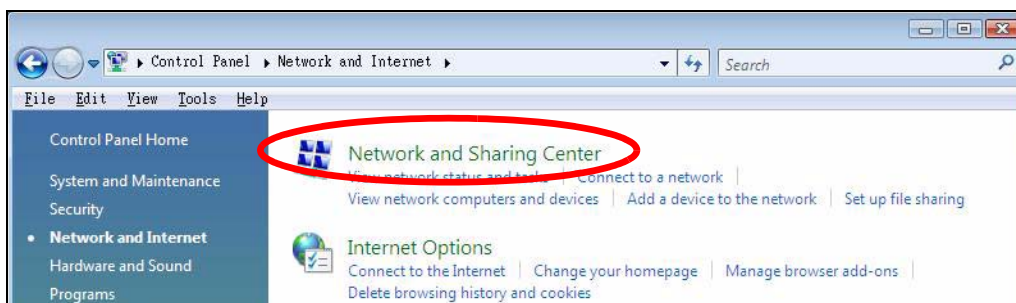
- 1 Click **Start > Control Panel**.



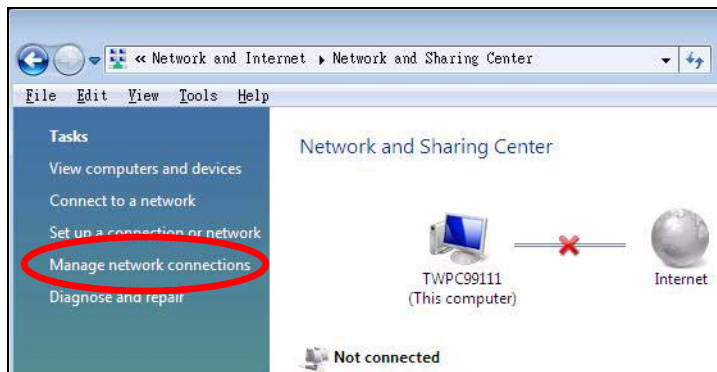
- 2 In the **Control Panel**, click the **Network and Internet** icon.



- 3 Click the **Network and Sharing Center** icon.



4 Click **Manage network connections**.

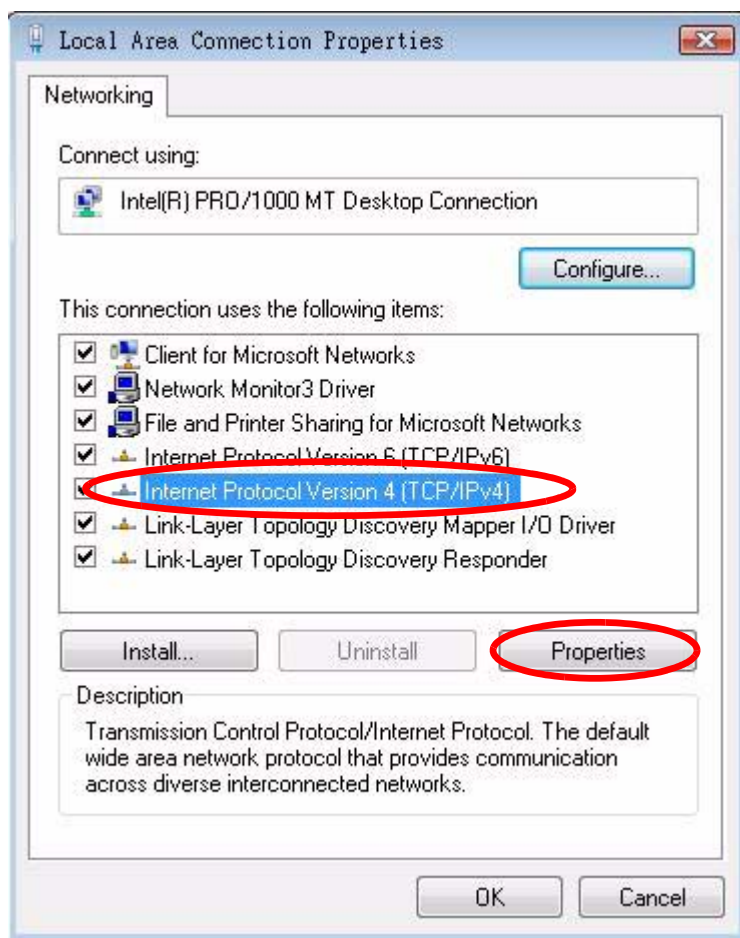


5 Right-click **Local Area Connection** and then select **Properties**.

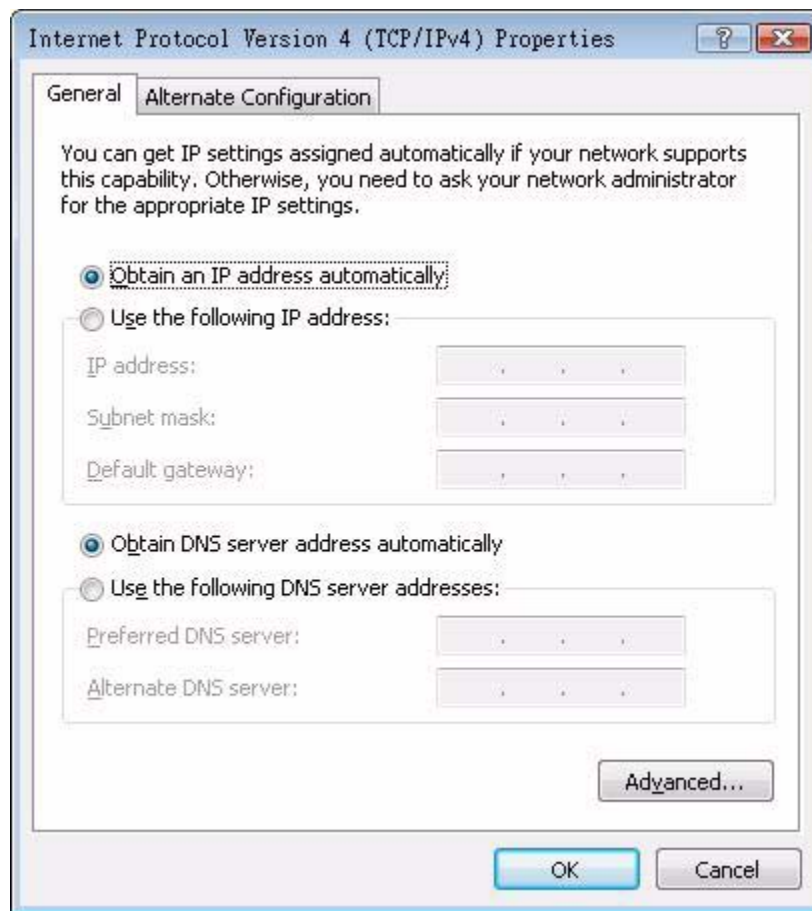


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

- 6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



- 7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



- 8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided. Click **Advanced**.

- 9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

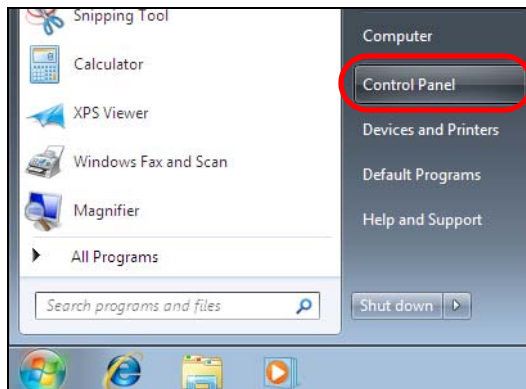
- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

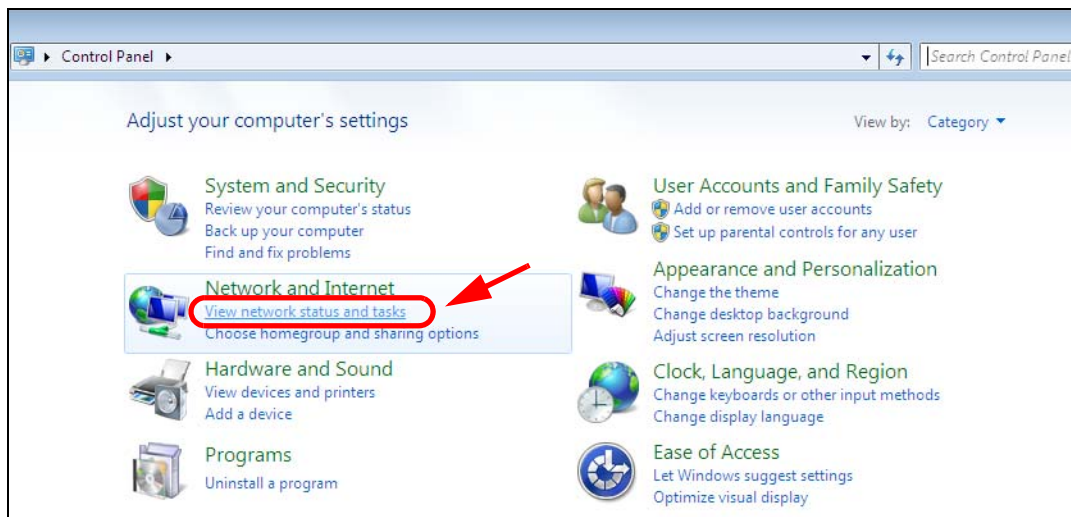
Windows 7

This section shows screens from Windows 7 Enterprise.

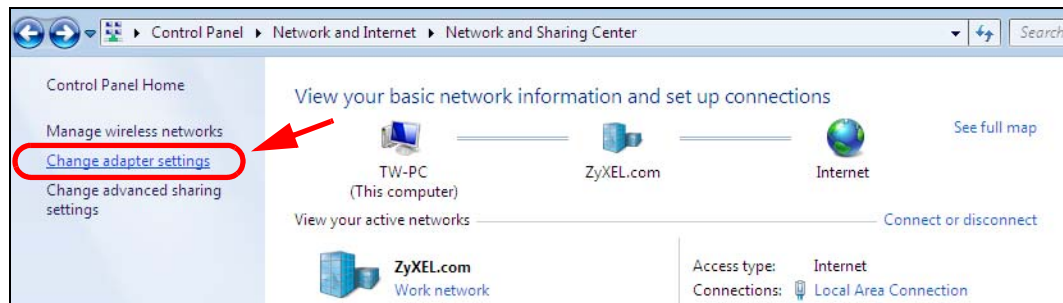
- 1 Click **Start > Control Panel**.



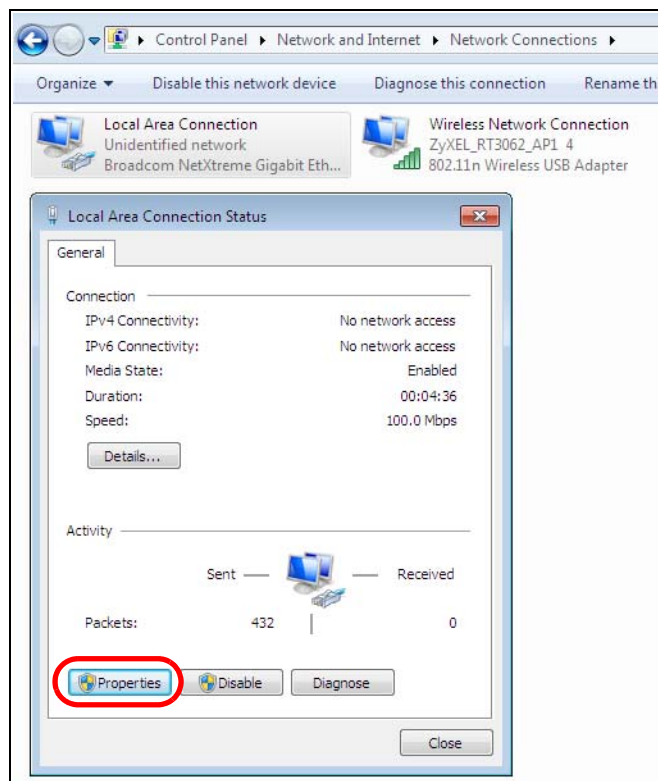
- 2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.



3 Click **Change adapter settings**.

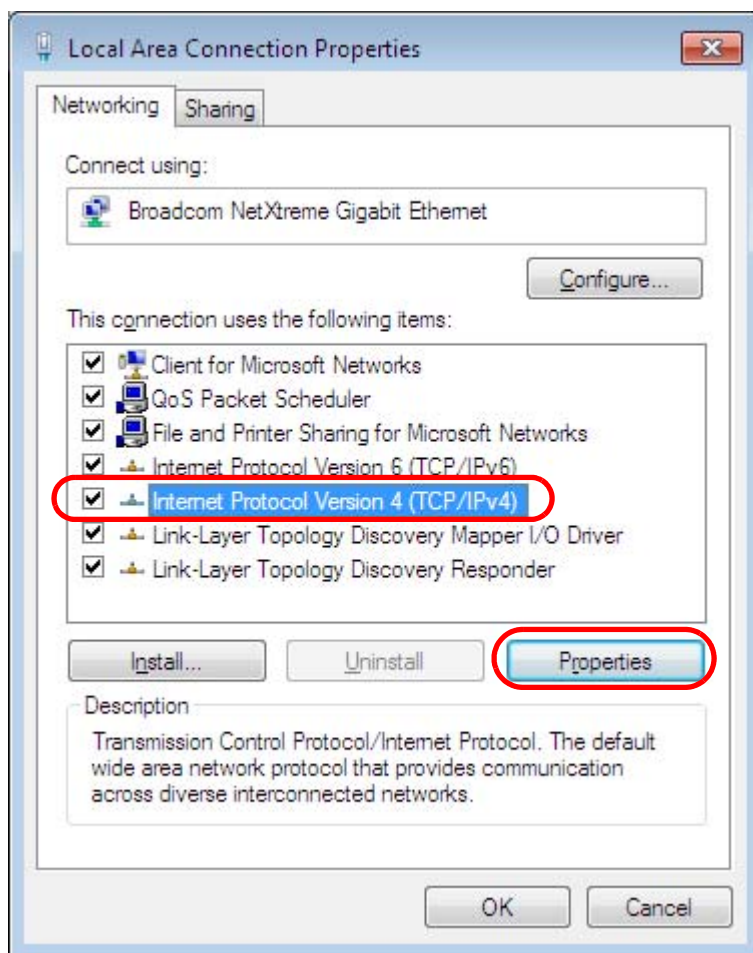


4 Double click **Local Area Connection** and then select **Properties**.

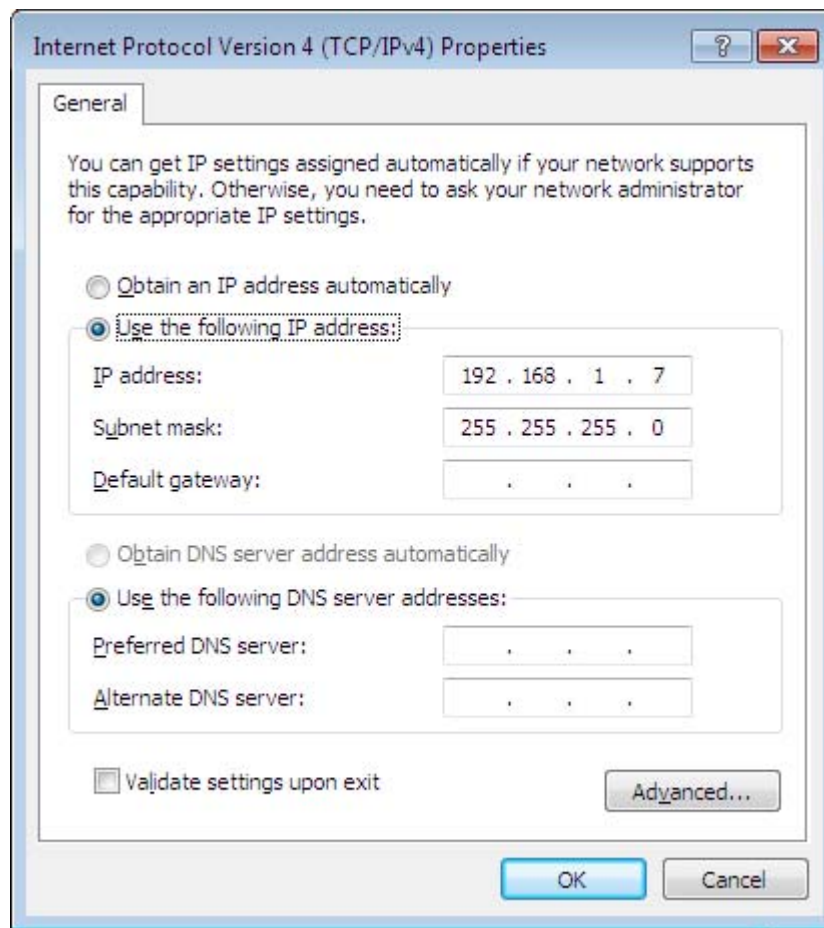


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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



- 6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



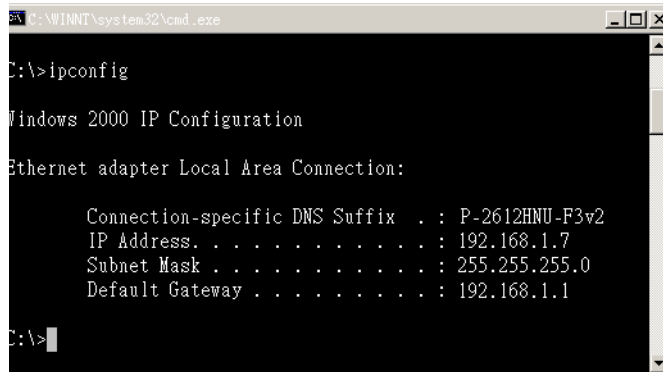
- 7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].
- 3 The IP settings are displayed as follows.



```
C:\WINNT\system32\cmd.exe

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

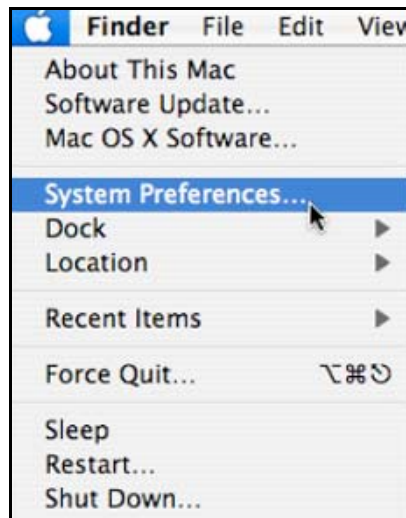
    Connection-specific DNS Suffix  . : P-2612HNU-F3v2
    IP Address. . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\>
```

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

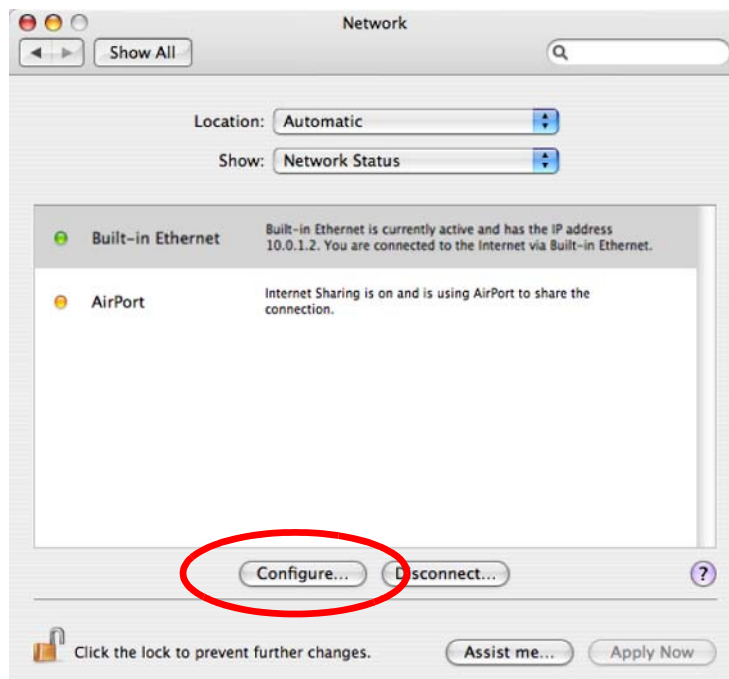
- 1 Click **Apple > System Preferences**.



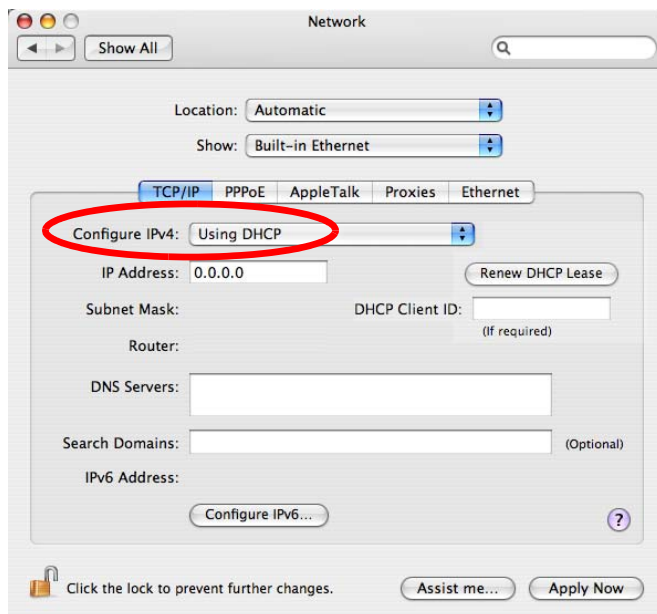
- 2 In the **System Preferences** window, click the **Network** icon.



- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.

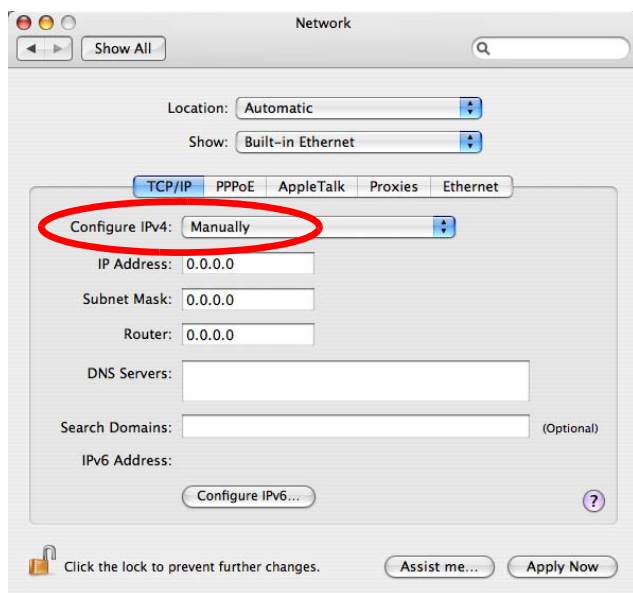


- 4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP / IP** tab.



- 5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.

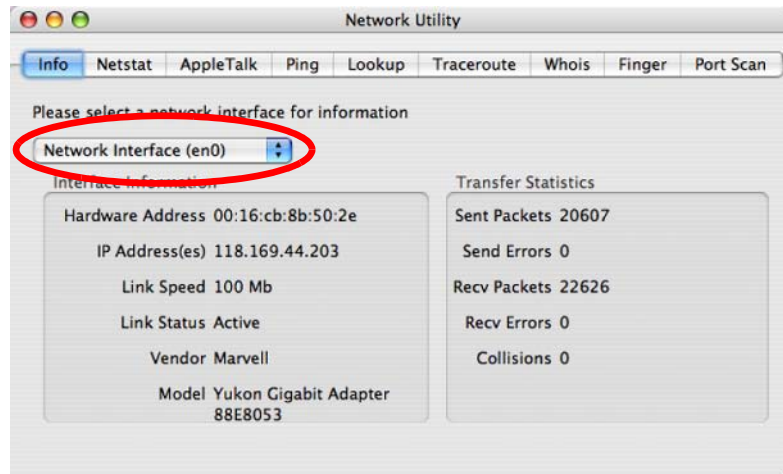


- 6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 42 Mac OS X 10.4: Network Utility



Mac OS X: 10.5 and 10.6

The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

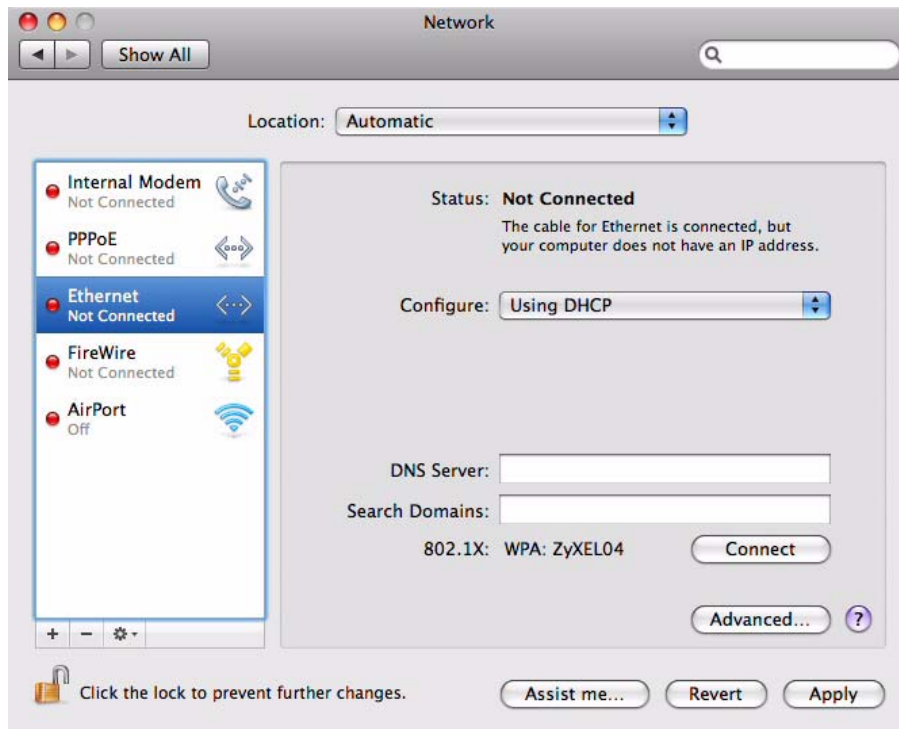
- 1 Click **Apple > System Preferences**.



- 2 In **System Preferences**, click the **Network** icon.



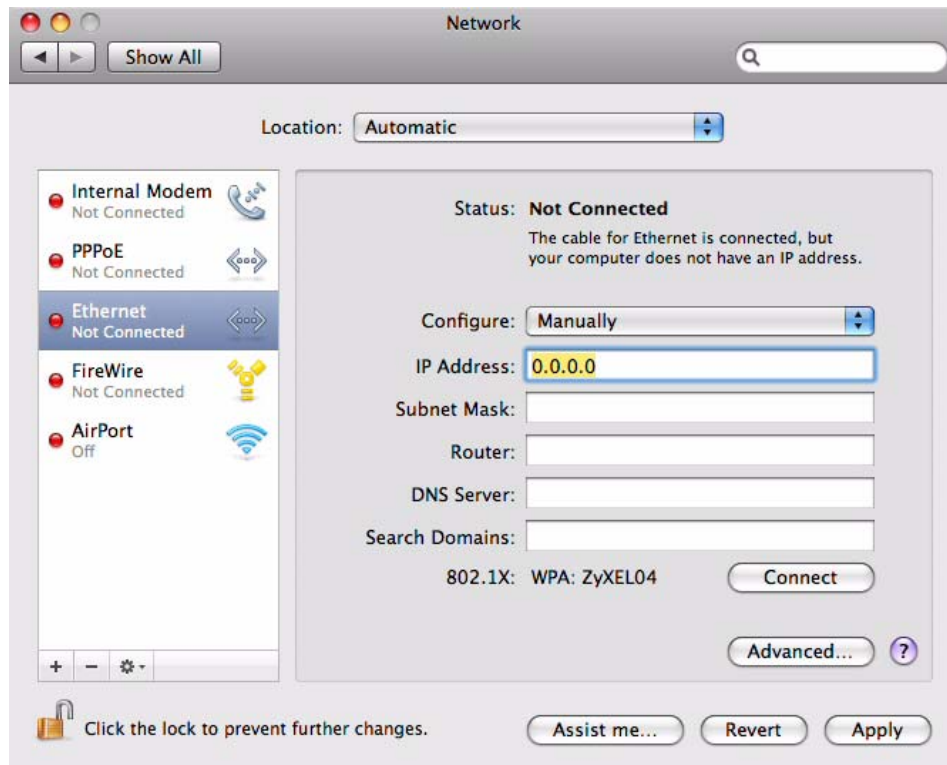
- 3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.



- 4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your NWA1300-NJ.

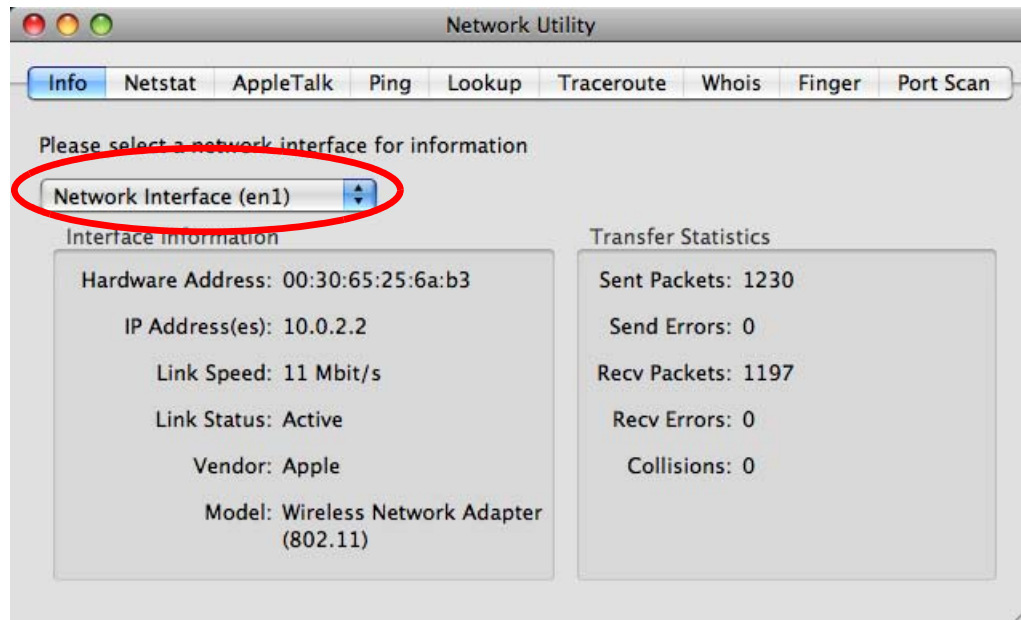


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 43 Mac OS X 10.5: Network Utility



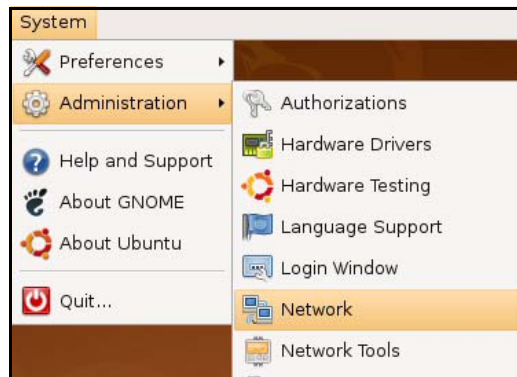
Linux: Ubuntu 8 (GNOME)

This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

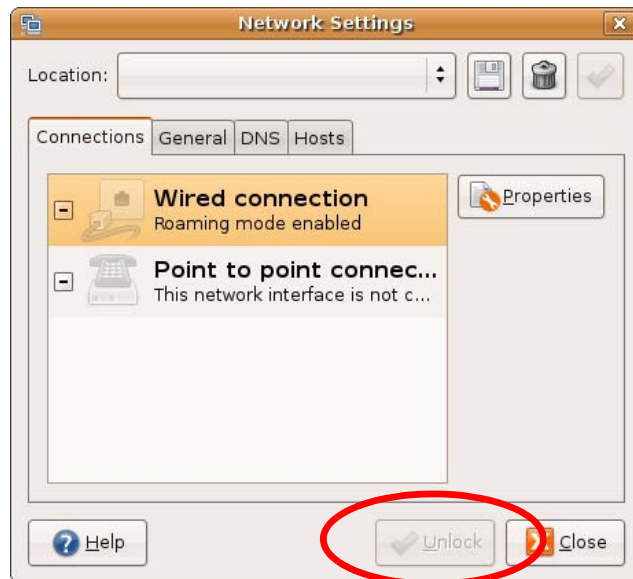
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

- 1 Click **System > Administration > Network**.



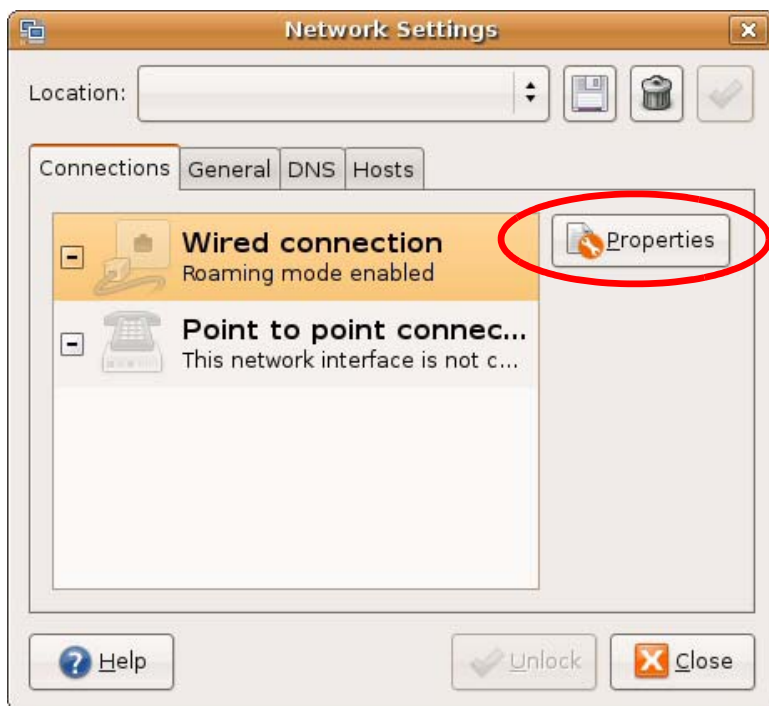
- 2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.



- 3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.



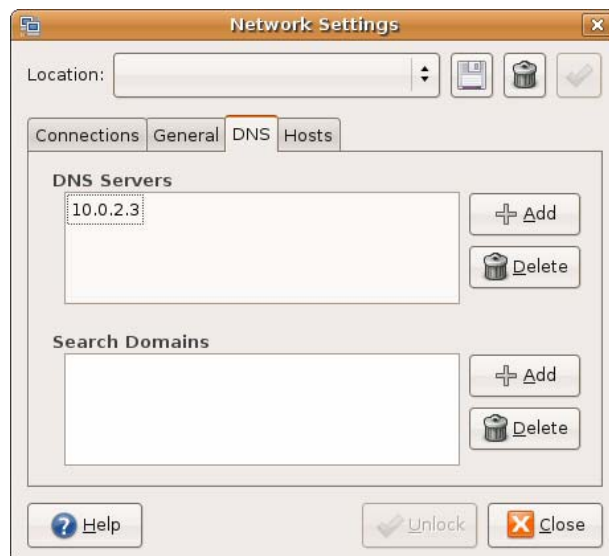
- 4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.



- 5 The **Properties** dialog box opens.



- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
 - In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.
- 6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.
- 7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

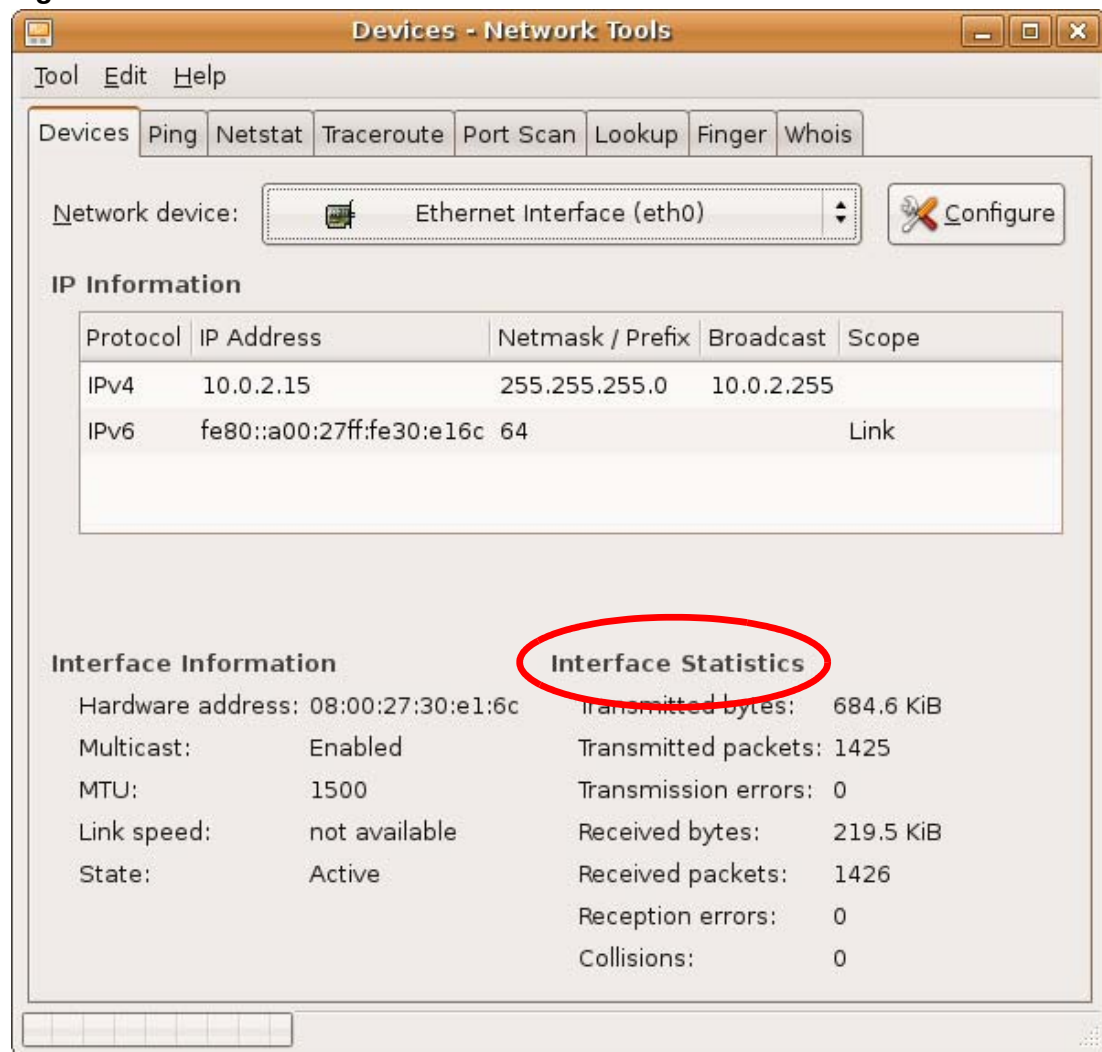


- 8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 44 Ubuntu 8: Network Tools



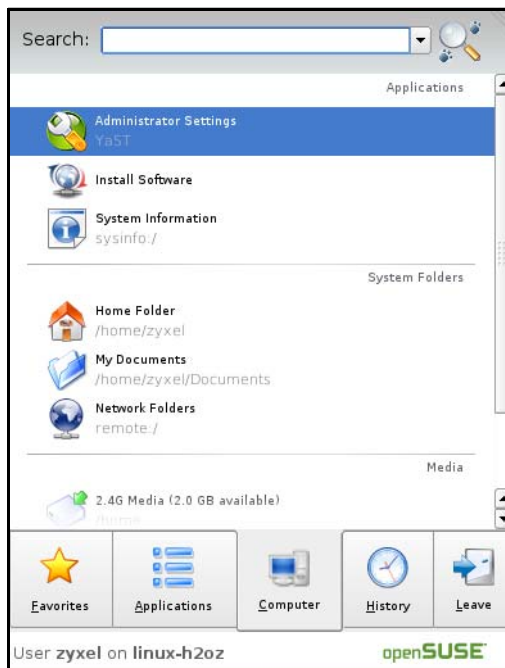
Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

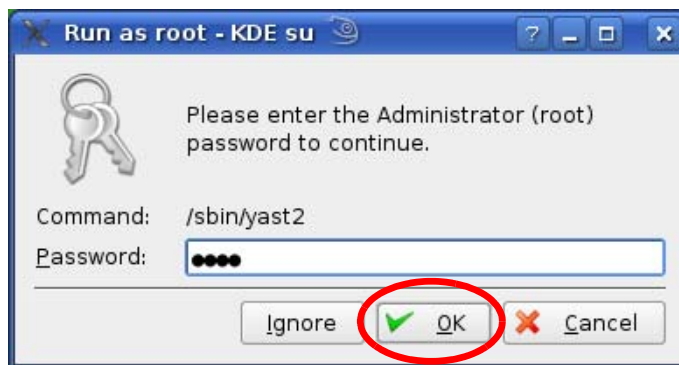
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

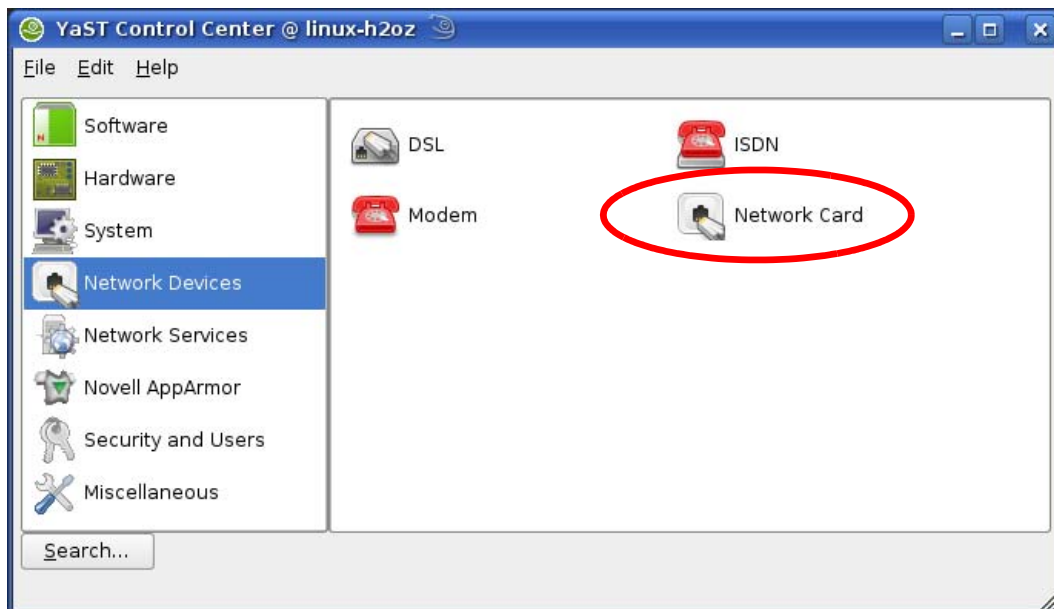
- 1 Click **K Menu > Computer > Administrator Settings (YaST)**.



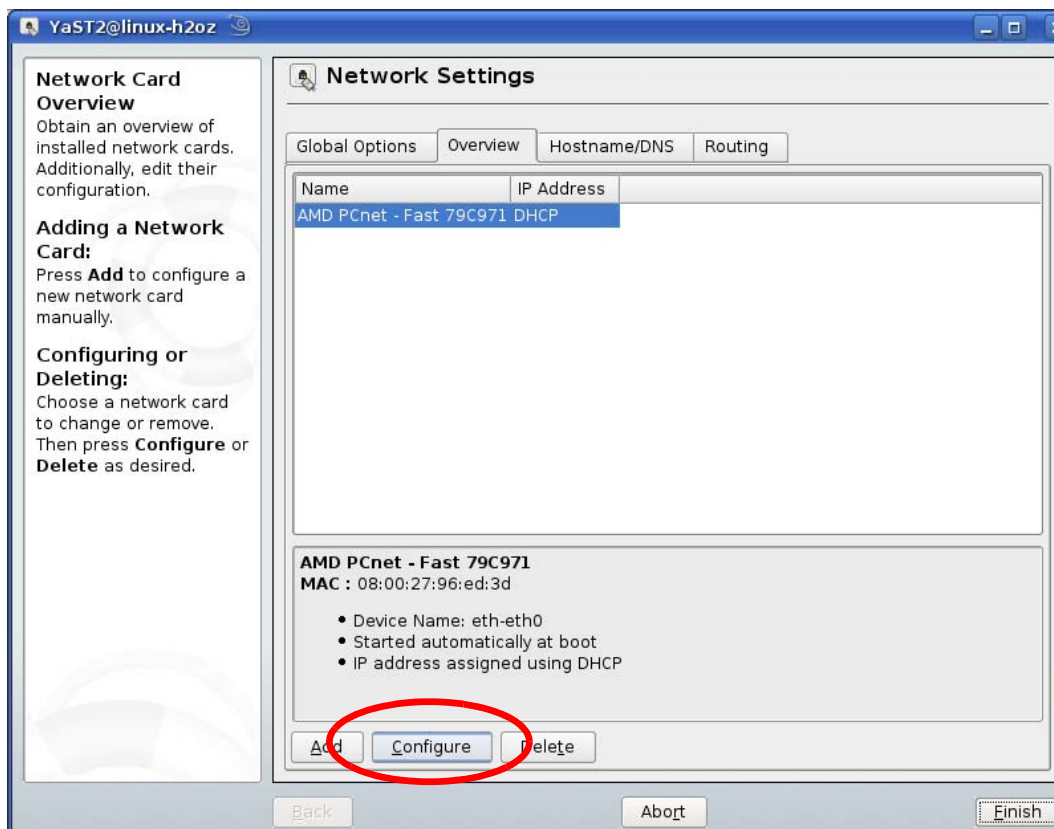
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.



- 3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

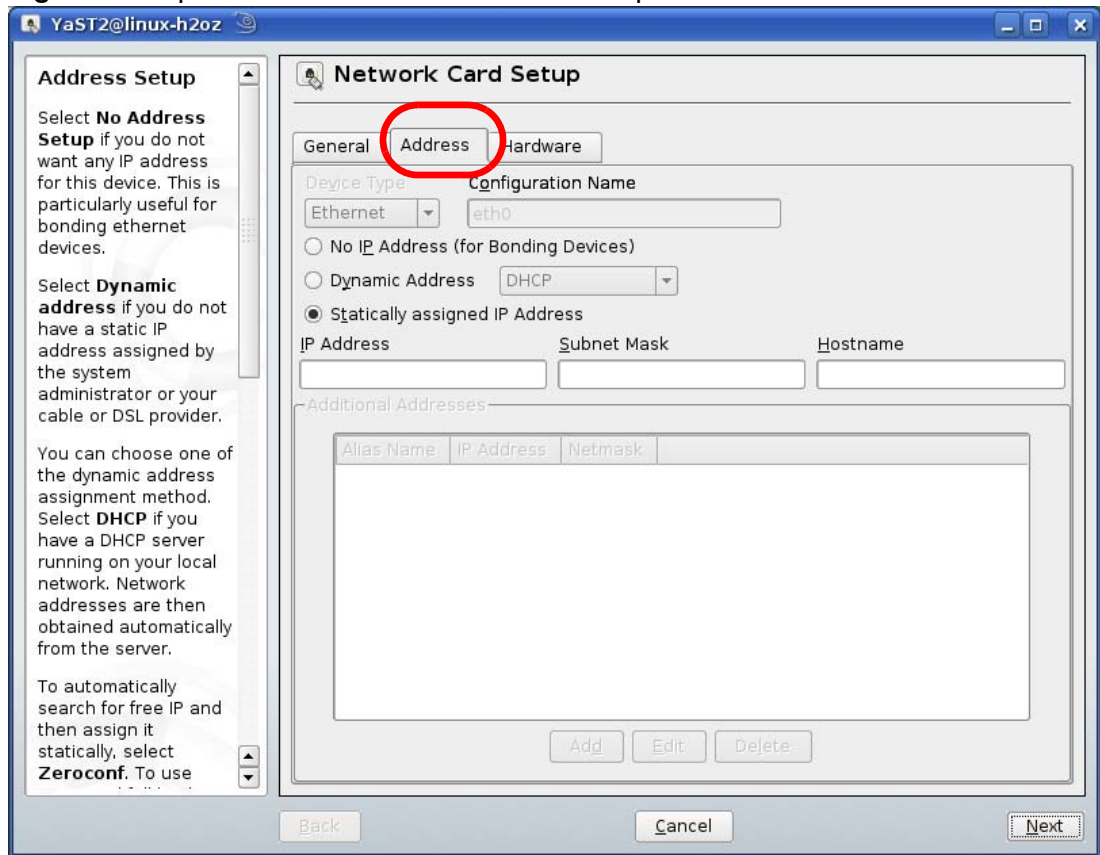


- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



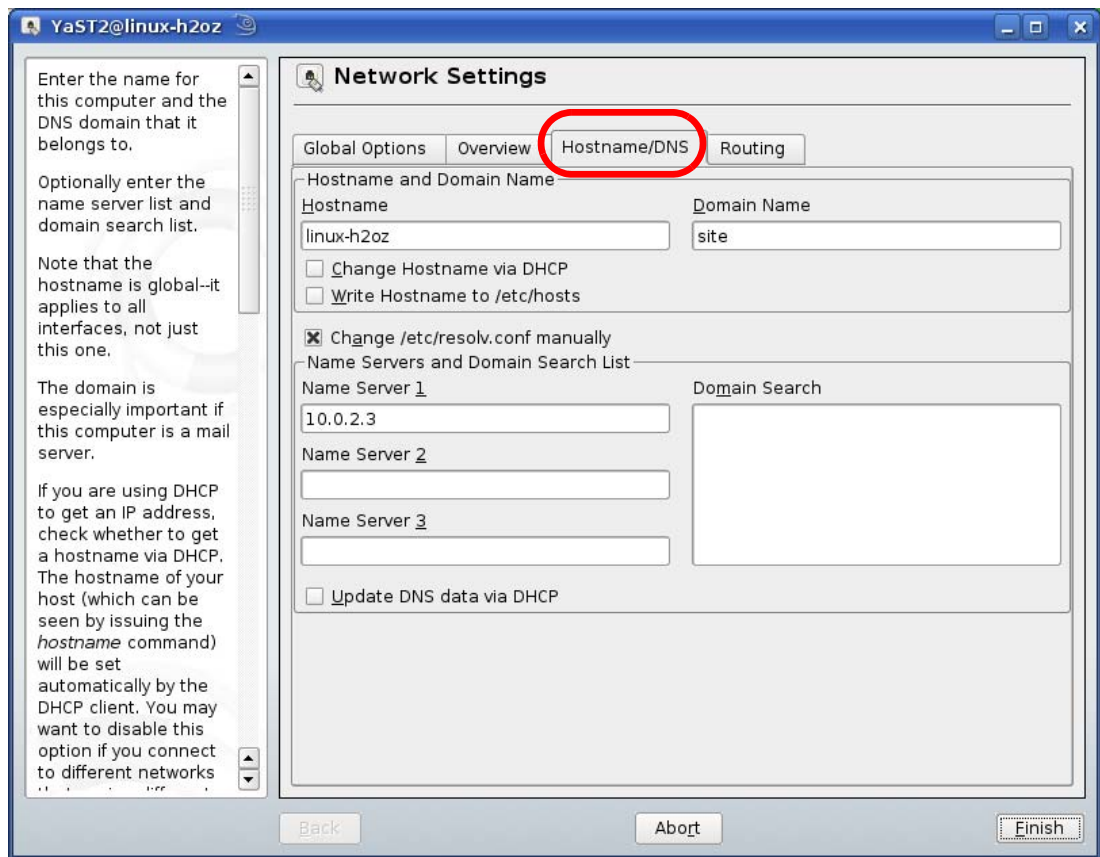
- 5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 45 openSUSE 10.3: Network Card Setup



- 6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.
- Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.
- 7 Click **Next** to save the changes and close the **Network Card Setup** window.

- 8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

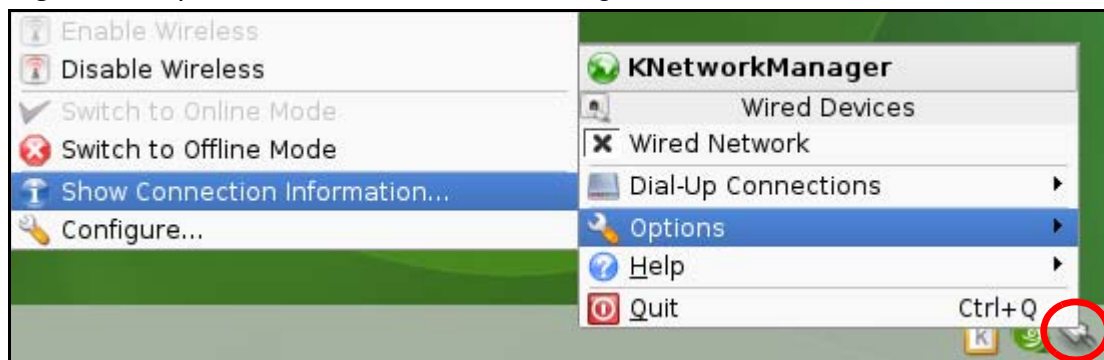


- 9 Click **Finish** to save your settings and close the window.

Verifying Settings

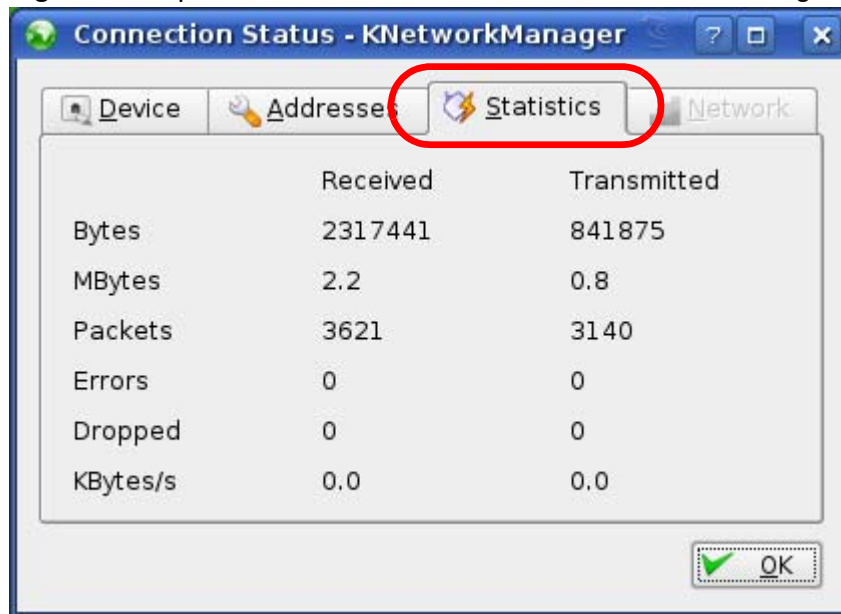
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 46 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics** tab to see if your connection is working properly.

Figure 47 openSUSE: Connection Status - KNetwork Manager



Wireless LANs

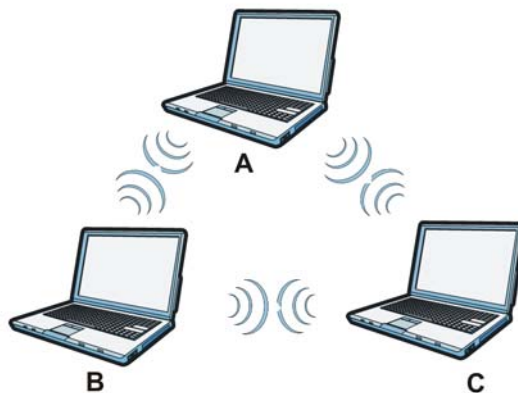
Wireless LAN Topologies

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

Ad-hoc Wireless LAN Configuration

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

Figure 48 Peer-to-Peer Communication in an Ad-hoc Network



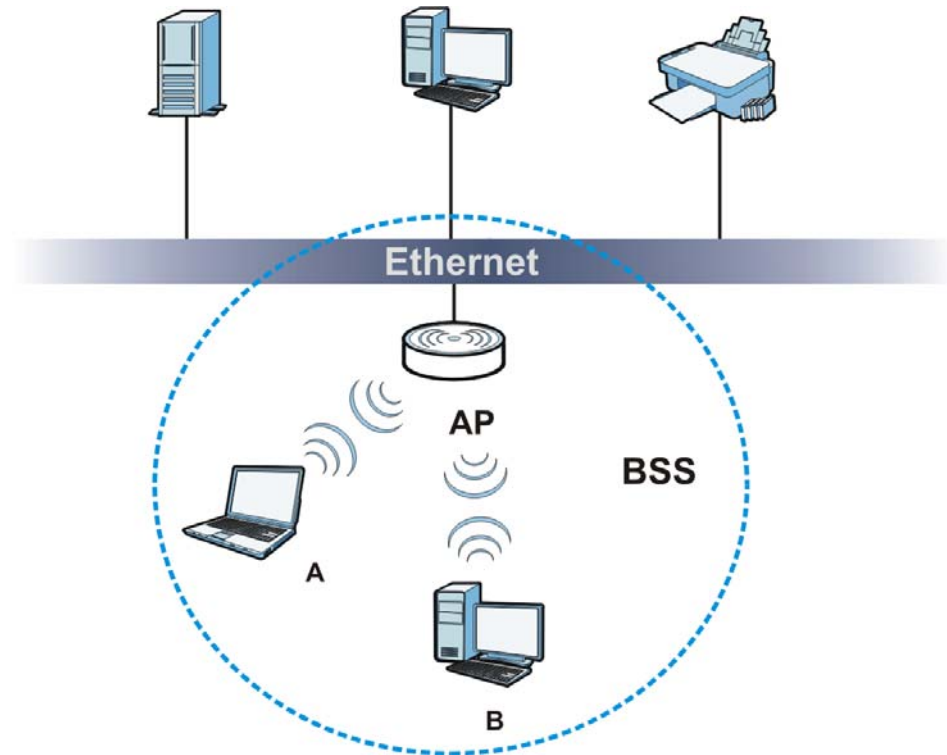
BSS

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

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

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

Figure 49 Basic Service Set



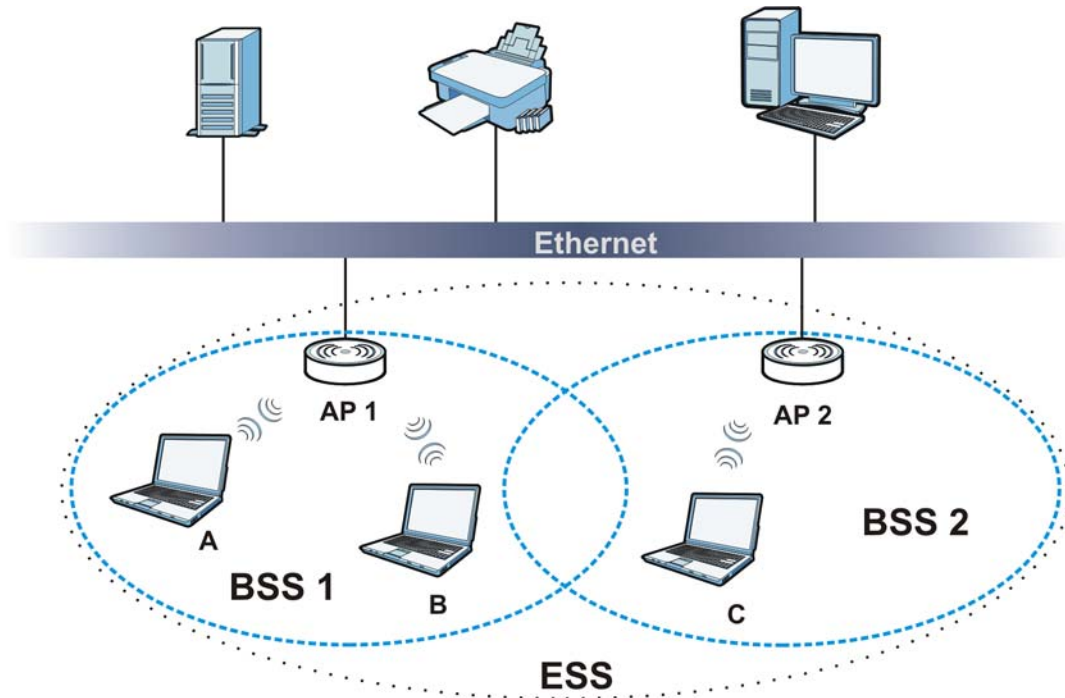
ESS

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

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

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

Figure 50 Infrastructure WLAN



Channel

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

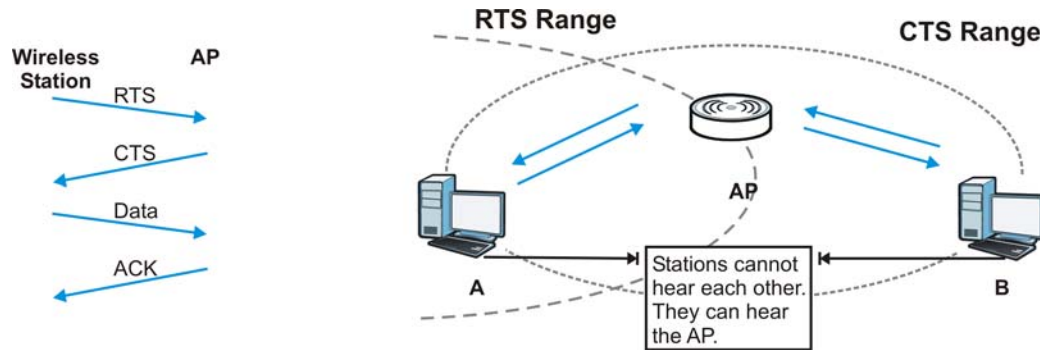
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel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

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or

wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 51 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

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

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

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

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

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the NWA1300-NJ uses long preamble.

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

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has

several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 19 IEEE 802.11g

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

Wireless Security Overview

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

Wireless security methods available on the NWA1300-NJ are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NWA1300-NJ identity.

The following figure shows the relative effectiveness of these wireless security methods available on your NWA1300-NJ.

Table 20 Wireless Security Levels

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

Note: You must enable the same wireless security settings on the NWA1300-NJ and on all wireless clients that you want to associate with it.

IEEE 802.1x

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

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

RADIUS

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

- Authentication
Determines the identity of the users.
- Authorization
Determines the network services available to authenticated users once they are connected to the network.
- Accounting
Keeps track of the client's network activity.

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

Types of RADIUS Messages

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

- Access-Request
Sent by an access point requesting authentication.
- Access-Reject
Sent by a RADIUS server rejecting access.
- Access-Accept
Sent by a RADIUS server allowing access.

- Access-Challenge

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

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

- Accounting-Request

Sent by the access point requesting accounting.

- Accounting-Response

Sent by the RADIUS server to indicate that it has started or stopped accounting.

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

Types of EAP Authentication

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

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

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

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

EAP-MD5 (Message-Digest Algorithm 5)

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

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

EAP-TLS (Transport Layer Security)

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

EAP-TTLS (Tunneled Transport Layer Service)

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

PEAP (Protected EAP)

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

LEAP

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

Dynamic WEP Key Exchange

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

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

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 21 Comparison of EAP Authentication Types

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

WPA and WPA2

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

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

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

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

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

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

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

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

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

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

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

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

keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

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

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

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

Wireless Client WPA Supplicants

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

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

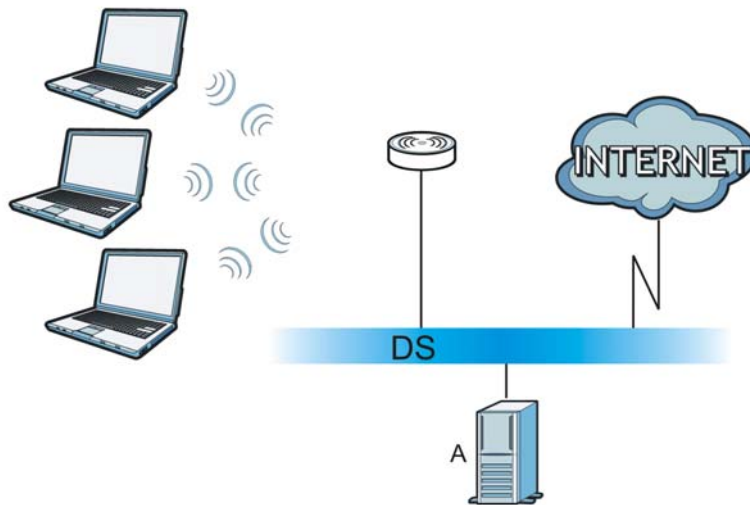
WPA(2) with RADIUS Application Example

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

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

- 4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 52 WPA(2) with RADIUS Application Example



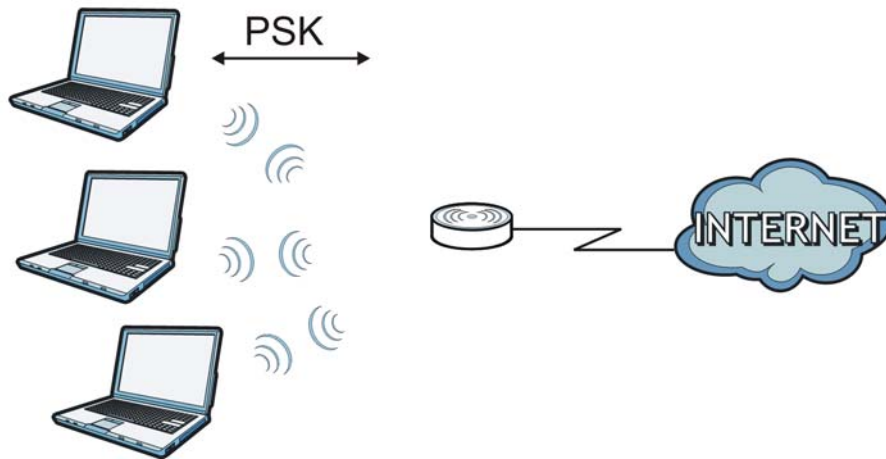
WPA(2)-PSK Application Example

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

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and allows it to join the network only if the password matches.
- 3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

- 4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 53 WPA(2)-PSK Authentication



Security Parameters Summary

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

Table 22 Wireless Security Relational Matrix

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

Antenna Overview

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

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

Antenna Characteristics

Frequency

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

Radiation Pattern

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

Antenna Gain

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

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

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

Types of Antennas for WLAN

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

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

Positioning Antennas

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

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

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

Open Software Announcements

End-User License Agreement for "NWA1300-NJ"

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE 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 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 OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED. HOWEVER, CERTAIN ZYXEL'S PRODUCTS MAY CONTAIN-IN PART-SOME THIRD PARTY'S FREE AND OPEN SOFTWARE PROGRAMS WHICH ALLOW YOU TO FREELY COPY, RUN, DISTRIBUTE, MODIFY AND IMPROVE THE SOFTWARE UNDER THE APPLICABLE TERMS OF SUCH THRID PARTY'S LICENSES ("OPEN-SOURCED COMPONENTS"). THE OPEN-SOURCED COMPONENTS ARE LISTED IN THE NOTICE OR APPENDIX BELOW. ZYXEL MAY HAVE DISTRIBUTED TO YOU HARDWARE AND/OR SOFTWARE, OR MADE AVAILABLE FOR ELECTRONIC DOWNLOADS THESE FREE SOFTWARE PROGRAMS OF THRID PARTIES AND YOU ARE LICENSED TO FREELY COPY, MODIFY AND REDISTIBUTE THAT SOFTWARE UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY. NONE OF THE STATEMENTS OR DOCUMENTATION FROM ZYXEL INCLUDING ANY RESTRICTIONS OR CONDITIONS STATED IN THIS END USER LICENSE AGREEMENT SHALL RESTRICT ANY RIGHTS AND LICENSES YOU MAY HAVE WITH RESPECT TO THE OPEN-SOURCED COMPONENTS UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY.

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 international copyright law, trade secret law, international treaty provisions, and the applicable national laws of each respective country. 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. 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, you may not market, co-brand, and 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 License Notice as below for the third party software, and your use of such material is exclusively 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 other than compliance with the applicable license terms of such third party, and makes no warranty (express, implied or statutory) whatsoever with respect thereto. 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, AND NON-INFRINGEMENT. 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 SOFTWARE OR PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's

TOTAL 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 if the parties agree to a binding arbitration. 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: Some components of this product incorporate free software programs covered under the open source code licenses which allows you to freely copy, modify and redistribute the software. For at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyXEL Technical Support (support@zyxel.com.tw), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes bridge-utils, Busybox, Iptables, ntpclient, Ethtool and Iwpriv-Wireless Tools software under GPL 2.0 license.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by

the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output

from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes GoAhead WebServer software under below license.

Licensing

GoAhead WebServer is available under two licenses:

1.) GoAhead provides WebServer as an open source product under the linked royalty free licensing terms. GoAhead has four main requirements in order to use GoAhead WebServer in your product. They are:

- 1.You must notify GoAhead prior or upon shipment of any product.
- 2.You must display the GoAhead Logo on the initial page of your Web site.
- 3.GoAhead may identify your company as a user of GoAhead WebServer in conjunction with its own marketing efforts. You also agree that GoAhead may identify your company as a user of the GoAhead WebServer by placing your company logo on its Web site.
- 4.You agree to license back to GoAhead all modifications you make to the WebServer.

By downloading the software you are agreeing to the terms of this license.

2.) For those customers who do not wish to comply with the above requirements, GoAhead offers a license without a requirement to show the logo or license back modifications under the linked commercial license. This agreement is modified from the above agreement as follows:

- 1.Deletes requirements for promotion and licensing back modifications You must notify GoAhead prior or upon shipment of any product.
- 2.Changes terms for Prices and Payments and requires a one-time fee.
- 3.Is numbered differently.

If you wish to license the software under these terms Contact Us

The above explanation was provided for your reference as a layperson's overview to the license, but it is not a substitute for the actual license. Please review the full license carefully prior to downloading the software. If you have any questions or need additional information, "Contact Us".

License Agreement

THIS LICENSE ALLOWS ONLY THE LIMITED USE OF GO AHEAD SOFTWARE, INC. PROPRIETARY CODE. PLEASE CAREFULLY READ THIS AGREEMENT AS IT PERTAINS TO THIS LICENSE, YOU CERTIFY THAT YOU WILL USE THE SOFTWARE ONLY IN THE MANNER PERMITTED HEREIN.

1. Definitions.

1.1 "Documentation" means any documentation GoAhead includes with the Original Code.

1.2 "GoAhead" means Go Ahead Software, Inc.

1.3 "Intellectual Property Rights" means all rights, whether now existing or hereinafter acquired, in and to trade secrets, patents, copyrights, trademarks, know-how, as well as moral rights and similar rights of any type under the laws of any governmental authority, domestic or foreign, including rights in and to all applications and registrations relating to any of the foregoing.

1.4 "License" or "Agreement" means this document.

1.5 "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications.

1.6 "Original Code" means the Source Code to GoAhead? proprietary computer software entitled GoAhead WebServer.

1.7 "Response Header" means the first portion of the response message output by the GoAhead WebServer, containing but not limited to, header fields for date, content-type, server identification and cache control.

1.8 "Server Identification Field" means the field in the Response Header which contains the text "Server: GoAhead-Webs".

1.9 "You" means an individual or a legal entity exercising rights under, and complying with all of the terms of, this license or a future version of this license. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of fifty percent (50%) or more of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1 Limited Source Code Grant.

GoAhead hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims, to use, reproduce, modify, copy and distribute the Original Code.

2.2 Binary Code.

GoAhead hereby grants You a world-wide, royalty-free, non-exclusive license to copy and distribute the binary code versions of the Original Code together with Your Modifications.

2.3 License Back to GoAhead.

You hereby grant in both source code and binary code to GoAhead a world-wide, royalty-free, non-exclusive license to copy, modify, display, use and sublicense any Modifications You make that are distributed or planned for distribution. Within 30

days of either such event, You agree to ship to GoAhead a file containing the Modifications (in a media to be determined by the parties), including any programmers' notes and other programmers' materials. Additionally, You will provide to GoAhead a complete description of the product, the product code or model number, the date on which the product is initially shipped, and a contact name, phone number and e-mail address for future correspondence. GoAhead will keep confidential all data specifically marked as such.

2.4 Restrictions on Use.

You may sublicense Modifications to third parties such as subcontractors or OEM's provided that You enter into license agreements with such third parties that bind such third parties to all the obligations under this Agreement applicable to you and that are otherwise substantially similar in scope and application to this Agreement.

3. Term.

This Agreement and license are effective from the time You accept the terms of this Agreement until this Agreement is terminated. You may terminate this Agreement at any time by uninstalling or destroying all copies of the Original Code including any and all binary versions and removing any Modifications to the Original Code existing in any products. This Agreement will terminate immediately and without further notice if You fail to comply with any provision of this Agreement. All restrictions on use, and all other provisions that may reasonably be interpreted to survive termination of this Agreement, will survive termination of this Agreement for any reason. Upon termination, You agree to uninstall or destroy all copies of the Original Code, Modifications, and Documentation.

4. Trademarks and Brand.

4.1 License and Use.

GoAhead hereby grants to You a limited world-wide, royalty-free, non-exclusive license to use the GoAhead trade names, trademarks, logos, service marks and product designations posted in Exhibit A (collectively, the "GoAhead Marks") in connection with the activities by You under this Agreement. Additionally, GoAhead grants You a license under the terms above to such GoAhead trademarks as shall be identified at a URL (the "URL") provided by GoAhead. The use by You of GoAhead Marks shall be in accordance with GoAhead trademark policies regarding trademark usage as established at the web site designated by the URL, or as otherwise communicated to You by GoAhead at its sole discretion. You understand and agree that any use of GoAhead Marks in connection with this Agreement shall not create any right, title or interest in or to such GoAhead Marks and that all such use and goodwill associated with GoAhead Marks will inure to the benefit of GoAhead.

4.2 Promotion by You of GoAhead WebServer Mark.

In consideration for the licenses granted by GoAhead to You herein, You agree to notify GoAhead when You incorporate the GoAhead WebServer in Your product and to inform GoAhead when such product begins to ship. You agree to promote the Original Code by prominently and visibly displaying a graphic of the GoAhead WebServer mark on the initial web page of Your product that is displayed each time a user connects to it. You also agree that GoAhead may identify your company as a user of the GoAhead WebServer in conjunction with its own marketing efforts. You may further promote the Original Code by displaying the GoAhead WebServer mark in marketing and promotional materials such as the home page of your web site or web pages promoting the product.

4.3 Placement of Copyright Notice by You.

You agree to include copies of the following notice (the "Notice") regarding proprietary rights in all copies of the products that You distribute, as follows: (i) embedded in the object code; and (ii) on the title pages of all documentation. Furthermore, You agree to use commercially reasonable efforts to cause any licensees of your products to embed the Notice in object code and on the title pages or relevant documentation. The Notice is as follows: Copyright (c) 20xx GoAhead Software, Inc. All Rights Reserved. Unless GoAhead otherwise instructs, the year 20xx is to be replaced with the year during which the release of the Original Code containing the notice is issued by GoAhead. If this year is not supplied with Documentation, GoAhead will supply it upon request.

4.4 No Modifications to Server Identification Field.

You agree not to remove or modify the Server identification Field contained in the Response Header as defined in Section 1.6 and 1.7.

5. Warranty Disclaimers.

THE ORIGINAL CODE, THE DOCUMENTATION AND THE MEDIA UPON WHICH THE ORIGINAL CODE IS RECORDED (IF ANY) ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, EXPRESS, STATUTORY OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The entire risk as to the quality and performance of the Original Code (including any Modifications You make) and the Documentation is with You. Should the Original Code or the Documentation prove defective, You (and not GoAhead or its distributors, licensors or dealers) assume the entire cost of all necessary servicing or repair. GoAhead does not warrant that the functions contained in the Original Code will meet your requirements or operate in the combination that You may select for use, that the operation of the Original Code will be uninterrupted or error free, or that defects in the Original Code will be corrected. No oral

or written statement by GoAhead or by a representative of GoAhead shall create a warranty or increase the scope of this warranty.

GOAHEAD DOES NOT WARRANT THE ORIGINAL CODE AGAINST INFRINGEMENT OR THE LIKE WITH RESPECT TO ANY COPYRIGHT, PATENT, TRADE SECRET, TRADEMARK OR OTHER PROPRIETARY RIGHT OF ANY THIRD PARTY AND DOES NOT WARRANT THAT THE ORIGINAL CODE DOES NOT INCLUDE ANY VIRUS, SOFTWARE ROUTINE OR OTHER SOFTWARE DESIGNED TO PERMIT UNAUTHORIZED ACCESS, TO DISABLE, ERASE OR OTHERWISE HARM SOFTWARE, HARDWARE OR DATA, OR TO PERFORM ANY OTHER SUCH ACTIONS.

Any warranties that by law survive the foregoing disclaimers shall terminate ninety (90) days from the date You received the Original Code.

6. Limitation of Liability.

YOUR SOLE REMEDIES AND GOAHEAD'S ENTIRE LIABILITY ARE SET FORTH ABOVE. IN NO EVENT WILL GOAHEAD OR ITS DISTRIBUTORS OR DEALERS BE LIABLE FOR DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE ORIGINAL CODE, THE INABILITY TO USE THE ORIGINAL CODE, OR ANY DEFECT IN THE ORIGINAL CODE, INCLUDING ANY LOST PROFITS, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

You agree that GoAhead and its distributors and dealers will not be LIABLE for defense or indemnity with respect to any claim against You by any third party arising from your possession or use of the Original Code or the Documentation.

In no event will GoAhead's total liability to You for all damages, losses, and causes of action (whether in contract, tort, including negligence, or otherwise) exceed the amount You paid for this product.

SOME STATES DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, AND SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

7. Indemnification by You.

You agree to indemnify and hold GoAhead harmless against any and all claims, losses, damages and costs (including legal expenses and reasonable counsel fees) arising out of any claim of a third party with respect to the contents of the Your products, and any intellectual property rights or other rights or interests related thereto.

8. High Risk Activities.

The Original Code is not fault-tolerant and is not designed , manufactured or intended for use or resale as online control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines or weapons systems, in which the failure of the Original Code could lead directly to death, personal injury, or severe physical or environmental damage. GoAhead and its suppliers specifically disclaim any express or implied warranty of fitness for any high risk uses listed above.

9. Government Restricted Rights.

For units of the Department of Defense, use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013. Contractor/manufacturer is GoAhead Software, Inc., 10900 N.E. 8th Street, Suite 750, Bellevue, Washington 98004.

If the Commercial Computer Software Restricted rights clause at FAR 52.227-19 or its successors apply, the Software and Documentation constitute restricted computer software as defined in that clause and the Government shall not have the license for published software set forth in subparagraph (c)(3) of that clause.

The Original Code (i) was developed at private expense, and no part of it was developed with governmental funds; (ii) is a trade secret of GoAhead (or its licensor(s)) for all purposes of the Freedom of Information Act; (iii) is "restricted computer software" subject to limited utilization as provided in the contract between the vendor and the governmental entity; and (iv) in all respects is proprietary data belonging solely to GoAhead (or its licensor(s)).

10. Governing Law and Interpretation.

This Agreement shall be interpreted under and governed by the laws of the State of Washington, without regard to its rules governing the conflict of laws. If any provision of this Agreement is held illegal or unenforceable by a court or tribunal of competent jurisdiction, the remaining provisions of this Agreement shall remain in effect and the invalid provision deemed modified to the least degree necessary to remedy such invalidity.

11. Entire Agreement.

This Agreement is the complete agreement between GoAhead and You and supersedes all prior agreements, oral or written, with respect to the subject matter hereof.

If You have any questions concerning this Agreement, You may write to GoAhead Software, Inc., 10900 N.E. 8th Street, Suite 750, Bellevue, Washington 98004 or send e-mail to info@goahead.com.

BY CLICKING ON THE "Register" BUTTON ON THE REGISTRATION FORM, YOU ACCEPT AND AGREE TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS SET FORTH IN THIS AGREEMENT. IF YOU DO NOT WISH TO ACCEPT THIS LICENSE OR YOU DO NOT QUALIFY FOR A LICENSE BASED ON THE TERMS SET FORTH ABOVE, YOU MUST NOT CLICK THE "Register" BUTTON.

Exhibit A

GoAhead Trademarks, Logos, and Product Designation Information

01/28/00

This Product includes Ntpclient software under below license.

```
/*
 * ntpclient.c - NTP client
 *
 * Copyright 1997, 1999, 2000 Larry Doolittle <larry@doolittle.boa.org>
 * Last hack: 2 December, 2000
 *
 * This program is free software; you can redistribute it and/or modify
 * it under the terms of the GNU General Public License (Version 2,
 * June 1991) as published by the Free Software Foundation. At the
 * time of writing, that license was published by the FSF with the URL
 * http://www.gnu.org/copyleft/gpl.html, and is incorporated herein by
 * reference.
 *
 * This program is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
 * GNU General Public License for more details.
 *
 *
```

This Product includes Ethtool software under below license.

This is the Debian GNU/Linux prepackaged version of "ethtool".

This package is currently maintained by Anibal Monsalve Salazar
<anibal@debian.org>

Sources obtained from: <http://sourceforge.net/projects/gkernel/>

Copyright Notices

amd8111e.c

Copyright (C) 2003 Advanced Micro Devices Inc.

de2104x.c

Copyright 2001 Sun Microsystems (thockin@sun.com)

e100.c

e1000.c

Copyright (c) 2002 Intel Corporation

ethtool-copy.h

Copyright (C) 1998 David S. Miller (davem@redhat.com)

Copyright 2001 Jeff Garzik <jgarzik@pobox.com>

Portions Copyright 2001 Sun Microsystems (thockin@sun.com)

Portions Copyright 2002 Intel (eli.kupermann@intel.com,

Portions Copyright 2001 Sun Microsystems (thockin@sun.com)

Portions Copyright 2002 Intel (scott.feldman@intel.com)

ethtool.8:

Copyright 1999 by David S. Miller. All Rights Reserved.

ethtool.8:

Portions Copyright 2001 Sun Microsystems

ethtool.c

Copyright (C) 1998 David S. Miller (davem@dm.cobaltmicro.com)

Portions Copyright 2001 Sun Microsystems

Copyright 2001 Jeff Garzik <jgarzik@mandrakesoft.com>

Portions Copyright 2002 Intel

fec_8xx.c

Copyright (C) 2004 Intracom S.A.

ibm_emac.c

Copyright (c) 2004, 2005 Zultys Technologies

igb.c

Copyright (c) 2007 Intel Corporation

ixgb.c

Copyright (c) 2006 Intel Corporation

ixgbe.c

Copyright (c) 2007 Intel Corporation

marvell.c
Copyright (C) 2004, 2006

natsemi.c
Copyright 2001 Sun Microsystems (thockin@sun.com)

pcnet32.c
Copyright 2004 IBM Corporation (jklewis@us.ibm.com)

realtek.c
Copyright 2001 Sun Microsystems (thockin@sun.com)

vioc.c
Copyright 2006 Fabric7 Systems, Inc

ethtool is licensed under the GNU General Public License version 2.

On Debian GNU/Linux systems, the complete text of the GNU General Public License version 2 can be found in `/usr/share/common-licenses/GPL-2'.

This Product includes Net-snmp software under below license

Various copyrights apply to this package, listed in various separate parts below.
Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) ----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) ----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) ----

Copyright ?2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- * Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

----- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- * Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES,

INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) ----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) ----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) ----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) ----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- * Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR

CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Legal Information

Copyright

Copyright © 2011 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

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

Trademarks

NetUSB is a trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

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

- This device may not cause harmful interference.

- This device must accept any interference received, including interference that may cause undesired operations.

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

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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



FCC Radiation Exposure Statement

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

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.

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.

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 is designed for the WLAN 2.4 GHz and/or 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz et/ou 5 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

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

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

Viewing Certifications

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

ZyXEL Limited Warranty

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

Note

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

To obtain the services of this warranty, contact 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.

Index

A

Advanced Encryption Standard
See AES.

AES [125](#)

antenna

directional [130](#)

gain [129](#)

omni-directional [130](#)

AP [17](#)

AP (access point) [117](#)

AP+Bridge [17](#)

B

Basic Service Set, See BSS [115](#)

bootrom version [65](#)

Bridge/Repeater [17](#)

BSS [115](#)

C

CA [123](#)

Certificate Authority
See CA.

certifications [157](#)

notices [159](#)

viewing [160](#)

channel [36](#), [65](#), [117](#)

interference [117](#)

Configuration

reset the factory defaults [58](#)

configuration file

backup [53](#), [55](#)

restore [56](#), [57](#)

copyright [157](#)

CTS (Clear to Send) [118](#)

D

Daylight saving [47](#)

diagnostic [66](#)

Dimensions [73](#)

disclaimer [157](#)

DNS [32](#), [65](#)

DNS server

see also Domain name system

dynamic WEP key exchange [124](#)

E

EAP Authentication [122](#)

encryption [37](#), [65](#), [125](#)

and local (user) database [38](#)

key [38](#)

WPA compatible [38](#)

ESS [116](#)

ESSID [65](#)

Extended Service Set, See ESS [116](#)

F

FCC interference statement [157](#)

firmware version [65](#)

fragmentation threshold [119](#)

FTP [48](#)

G

General wireless LAN screen [38](#)

H

hidden node [117](#)

I

IBSS [115](#)

IEEE 802.11g [119](#)

Independent Basic Service Set
See IBSS [115](#)

initialization vector (IV) [125](#)

IP address [32](#)
WAN [65](#)

L

LAN
MAC address [65](#)

LAN setup [31](#)

local (user) database [37](#)
and encryption [38](#)

M

Management Information Base (MIB) [59](#)

managing the device
good habits [18](#)
using the web configurator. See web
configurator.

manual firmware upgrade
using TFTP [50](#)

MBSSID [17](#)

Message Integrity Check (MIC) [125](#)

MIB
and SNMP [59](#)

MIB (Management Information Base) [59](#)
mode [17](#)

N

Navigation Panel [23](#)
navigation panel [23](#)

O

operating mode [17](#)

P

Pairwise Master Key (PMK) [125](#), [127](#)
Power Specification [73](#)
preamble mode [119](#)
private IP address [31](#)
product registration [160](#)
PSK [125](#)

R

RADIUS [121](#)
message types [121](#)
messages [121](#)
shared secret key [122](#)

RADIUS server [37](#)

registration
product [160](#)

related documentation [3](#)

remote management
FTP [48](#)

Reset button [19](#), [58](#)

Reset the device [19](#)

RF (Radio Frequency) [74](#)

Roaming [40](#), [42](#)

RTS (Request To Send) [118](#)
threshold [117](#), [118](#)

RTS/CTS Threshold [36](#), [40](#)

S

safety warnings [8](#)

Service Set [39](#)

Service Set IDentification [39](#)

Service Set IDentity. See SSID.

Simple Network Management Protocol, see SNMP

SNMP [58](#)

- agent [59](#)
- and MIB [59](#)
- authentication [63](#)
- manager [59](#)
- network components [59](#)
- object variables [59](#)
- protocol operations [59](#)
- users [61](#)

SSID [36](#), [39](#)

Subnet Mask [33](#)

subnet mask

- WAN [65](#)

syntax conventions [6](#)

System General Setup [46](#)

T

Temperature [73](#)

Temporal Key Integrity Protocol (TKIP) [125](#)

U

user authentication [36](#)

- local (user) database [37](#)
- RADIUS server [37](#)

W

WAN

- IP address [65](#)
- subnet mask [65](#)

WAN port mode [65](#)

warranty [160](#)

note [160](#)

Web Configurator

- how to access [21](#)
- Overview [21](#)

web configurator [18](#)

WEP [65](#)

Wi-Fi Protected Access [124](#)

wireless [65](#)

wireless client WPA supplicants [126](#)

wireless firmware version [65](#)

Wireless network

- basic guidelines [36](#)
- channel [36](#)
- encryption [37](#)
- example [35](#)
- overview [35](#)
- security [36](#)
- SSID [36](#)

Wireless security [36](#)

- overview [36](#)
- type [36](#)

wireless security [120](#)

WLAN

- interference [117](#)
- security parameters [128](#)

WPA [65](#), [124](#)

- key caching [126](#)
- pre-authentication [126](#)
- user authentication [126](#)
- vs WPA-PSK [125](#)
- wireless client supplicant [126](#)
- with RADIUS application example [126](#)

WPA compatible [38](#)

WPA2 [65](#), [124](#)

- user authentication [126](#)
- vs WPA2-PSK [125](#)
- wireless client supplicant [126](#)
- with RADIUS application example [126](#)

WPA2-Pre-Shared Key [124](#)

WPA2-PSK [124](#), [125](#)

- application example [127](#)

WPA-PSK [125](#)

- application example [127](#)

