

**Table 89** RFC-2408 ISAKMP Payload Types (continued)

<b>LOG DISPLAY</b>	<b>PAYLOAD TYPE</b>
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the NBG334W.

## 20.1 Firmware Upload Screen

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with a ".bin" extension, e.g., "NBG334W.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the Firmware and Configuration File Maintenance chapter for upgrading firmware using FTP/TFTP commands.

Click **Maintenance > Tools**. Follow the instructions in this screen to upload firmware to your NBG334W.

**Figure 106** Maintenance > Tools > Firmware

The following table describes the labels in this screen.

**Table 90** Maintenance > Tools > Firmware

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.



Do not turn off the NBG334W while firmware upload is in progress!

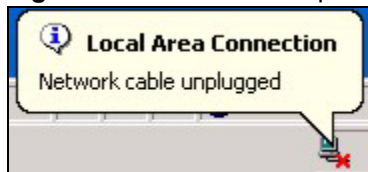
After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the NBG334W again.

**Figure 107** Upload Warning



The NBG334W automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 108** Network Temporarily Disconnected



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

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

**Figure 109** Upload Error Message



## 20.2 Configuration Screen

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

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

**Figure 110** Maintenance > Tools > Configuration

The screenshot shows the 'Configuration' tab in the Maintenance > Tools > Configuration section. It is divided into three main sections:

- Backup Configuration:** Contains the instruction 'Click **Backup** to save the current configuration of your system to your computer.' and a 'Backup' button.
- Restore Configuration:** Contains the instruction 'To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.' Below this is a 'File Path:' label, an input field, a 'Browse...' button, and an 'Upload' button.
- Back to Factory Defaults:** Contains the instruction 'Click **Reset** to clear all user-entered configuration information and return to factory defaults. After resetting, the' followed by a list:
  - Password will be 1234
  - LAN IP address will be 192.168.1.1
  - DHCP will be reset to server
 and a 'Reset' button.

## 20.2.1 Backup Configuration

Backup configuration allows you to back up (save) the NBG334W's current configuration to a file on your computer. Once your NBG334W is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the NBG334W's current configuration to your computer.

## 20.2.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG334W.

**Table 91** Maintenance Restore Configuration

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

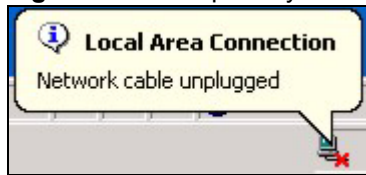


Do not turn off the NBG334W while configuration file upload is in progress

After you see a "configuration upload successful" screen, you must then wait one minute before logging into the NBG334W again.

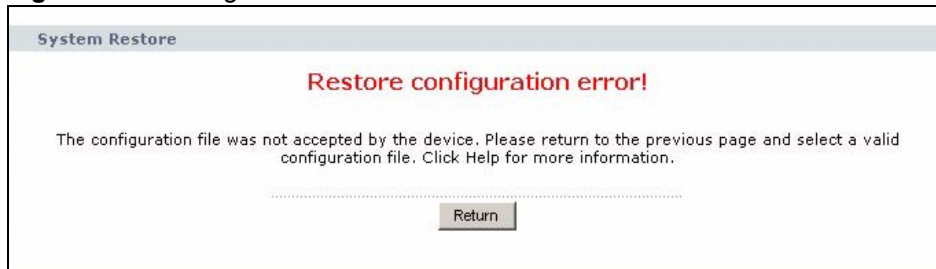
**Figure 111** Configuration Restore Successful

The NBG334W automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 112** Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default NBG334W IP address (192.168.1.1). See your Quick Start Guide for details on how to set up your computer's IP address.

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

**Figure 113** Configuration Restore Error

### 20.2.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the NBG334W to its factory defaults.

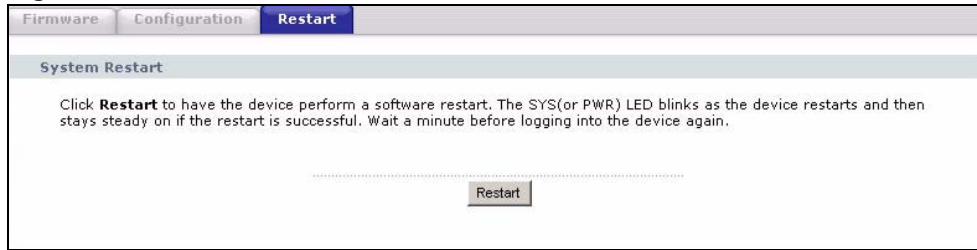
You can also press the **RESET** button on the rear panel to reset the factory defaults of your NBG334W. Refer to the chapter about introducing the web configurator for more information on the **RESET** button.

## 20.3 Restart Screen

System restart allows you to reboot the NBG334W without turning the power off.

Click **Maintenance > Tools > Restart**. Click **Restart** to have the NBG334W reboot. This does not affect the NBG334W's configuration.

**Figure 114** Maintenance > Tools > Restart





## Configuration Mode

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

**Figure 115** Maintenance > Config Mode > General

The screenshot shows a web interface for 'Configuration Mode' under the 'General' tab. It features two radio buttons: 'Basic' (which is selected) and 'Advanced'. Below the radio buttons, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in the screen.

**Table 92** Maintenance > Config Mode > General

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

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



**Table 93** Advanced Configuration Options

CATEGORY	LINK	TAB
Network	Wireless LAN	MAC Filter
		Advanced
		QoS
	WAN	Advanced
	LAN	IP Alias
		Advanced
	DHCP Server	Advanced
NAT	Advanced	
Security	Firewall	Services
	Content Filter	Schedule
Management	Static Route	IP Static Route
	Bandwidth MGMT	Advanced
		Monitor
	Remote MGMT	Telnet
		FTP
DNS		
Maintenance	Logs	Log Settings



In **AP Mode** many screens will not be available. See [Chapter 4 on page 61](#) for more information.

# Sys Op Mode

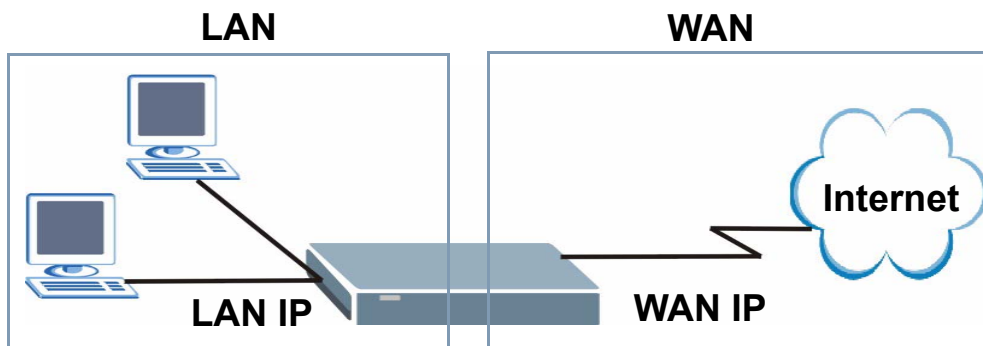
## 22.1 Overview

The **Sys Op Mode** (System Operation Mode) function lets you configure whether your NBG334W is a router or AP. You can choose between **Router Mode** and **AP Mode** depending on your network topology and the features you require from your device. See [Section 1.1 on page 29](#) for more information on which mode to choose.

### 22.1.1 Router

A router connects your local network with another network, such as the Internet. The router has two IP addresses, the LAN IP address and the WAN IP address.

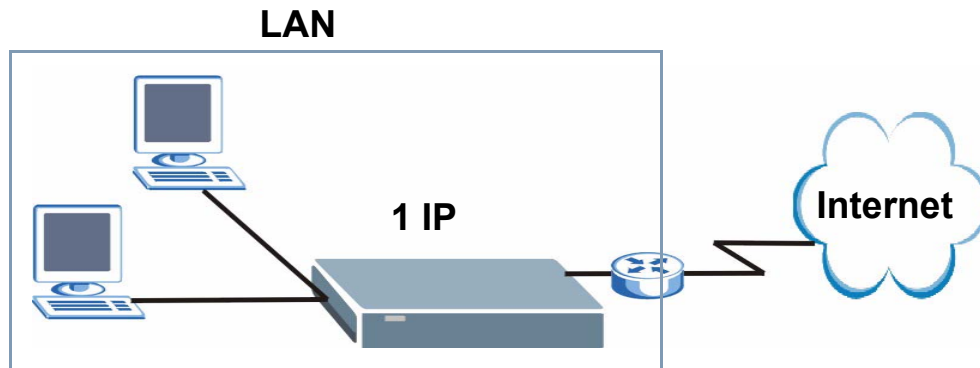
**Figure 116** LAN and WAN IP Addresses in Router Mode



### 22.1.2 AP

An AP extends one network and so has just one IP address. All Ethernet ports on the AP have the same IP address. To connect to the Internet, another device, such as a router, is required.

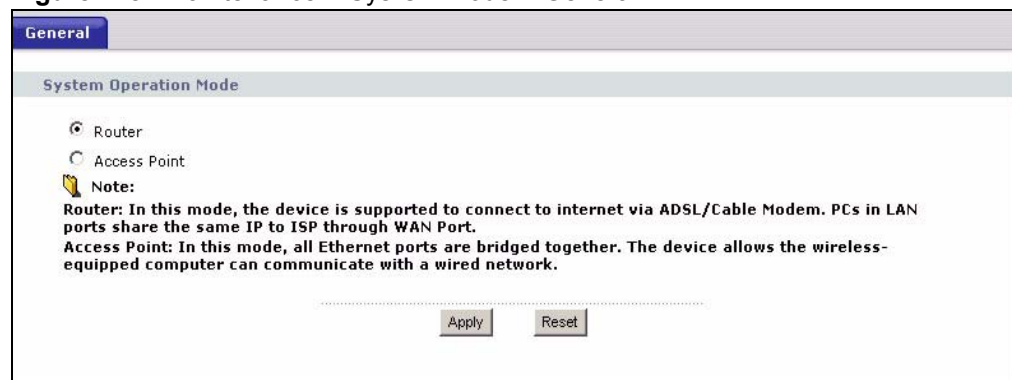
Figure 117 IP Address in AP Mode



## 22.2 Selecting System Operation Mode

Use this screen to select how you connect to the Internet.

Figure 118 Maintenance &gt; Sys OP Mode &gt; General



If you select Router Mode, the following pop-up message window appears.

Figure 119 Maintenance &gt; Sys Op Mode &gt; General: Router



- In this mode there are both LAN and WAN ports. The LAN Ethernet and WAN Ethernet ports have different IP addresses.
- The DHCP server on your device is enabled and allocates IP addresses to other devices on your local network.
- The LAN IP address of the device on the local network is set to 192.168.1.1.
- You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings.

If you select Access Point the following pop-up message window appears.

**Figure 120** Maintenance > Sys Op Mode > General: AP

- In **AP Mode** all Ethernet ports have the same IP address.
- All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port.
- The DHCP server on your device is disabled. In AP mode there must be a device with a DHCP server on your network such as a router or gateway which can allocate IP addresses.

The IP address of the device on the local network is set to 192.168.1.1.

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

**Table 94** Maintenance > Sys OP Mode > General

LABEL	DESCRIPTION
System Operation Mode	
Router	Select <b>Router</b> if your device routes traffic between a local network and another network such as the Internet. This mode offers services such as a firewall or bandwidth management.
Access Point	Select <b>Access Point</b> if your device bridges traffic between clients on the same network.
Apply	Click <b>Apply</b> to save your settings.
Reset	Click <b>Reset</b> to return your settings to the default ( <b>Router</b> )



If you select the incorrect System Operation Mode you cannot connect to the Internet.



# Troubleshooting

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

- [Power, Hardware Connections, and LEDs](#)
- [NBG334W Access and Login](#)
- [Internet Access](#)
- [Resetting the NBG334W to Its Factory Defaults](#)
- [Wireless Router/AP Troubleshooting](#)
- [Advanced Features](#)

## 23.1 Power, Hardware Connections, and LEDs



---

The NBG334W does not turn on. None of the LEDs turn on.

---

- 7 Make sure you are using the power adaptor or cord included with the NBG334W.
- 8 Make sure the power adaptor or cord is connected to the NBG334W and plugged in to an appropriate power source. Make sure the power source is turned on.
- 9 Disconnect and re-connect the power adaptor or cord to the NBG334W.
- 10 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 1.7 on page 31](#).
- 2 Check the hardware connections. See the Quick Start Guide.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Disconnect and re-connect the power adaptor to the NBG334W.
- 5 If the problem continues, contact the vendor.

## 23.2 NBG334W Access and Login



---

I don't know the IP address of my NBG334W.

---

- 1 The default IP address is **192.168.1.1**.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the NBG334W by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the NBG334W (it depends on the network), so enter this IP address in your Internet browser.
- 3 Set your device to **Router Mode**, login (see the Quick Start Guide for instructions) and go to the **Device Information** table in the **Status** screen. Your NBG334W's IP address is available in the **Device Information** table.
  - If the **DHCP** setting under **LAN information** is **None**, your device has a fixed IP address.
  - If the **DHCP** setting under **LAN information** is **Client**, then your device receives an IP address from a DHCP server on the network.
- 4 If your NBG334W is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.
- 5 Reset your NBG334W to change all settings back to their default. This means your current settings are lost. See [Section 23.4 on page 207](#) in the **Troubleshooting** for information on resetting your NBG334W.



---

I forgot the password.

---

- 1 The default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 23.4 on page 207](#).



---

I cannot see or access the **Login** screen in the web configurator.

---

- 1 Make sure you are using the correct IP address.
  - The default IP address is [192.168.1.1](#).
  - If you changed the IP address ([Section 7.3 on page 102](#)), use the new IP address.
  - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I don't know the IP address of my NBG334W](#).

- 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 217](#).
- 4 Make sure your computer is in the same subnet as the NBG334W. (If you know that there are routers between your computer and the NBG334W, skip this step.)
  - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Section 7.3 on page 102](#).
  - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG334W. See [Section 7.3 on page 102](#).
- 5 Reset the device to its factory defaults, and try to access the NBG334W with the default IP address. See [Section 7.3 on page 102](#).
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### Advanced Suggestions

- Try to access the NBG334W using another service, such as Telnet. If you can access the NBG334W, check the remote management settings and firewall rules to find out why the NBG334W does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN/ETHERNET** port.




---

I can see the **Login** screen, but I cannot log in to the NBG334W.

---

- 1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone is using Telnet to access the NBG334W. Log out of the NBG334W in the other session, or ask the person who is logged in to log out.
- 3 Disconnect and re-connect the power adaptor or cord to the NBG334W.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 23.4 on page 207](#).




---

I cannot Telnet to the NBG334W.

---

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




---

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

---



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

## 23.3 Internet Access



---

### I cannot access the Internet.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- 2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
- 4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 5 Go to Maintenance > Sys OP Mode > General. Check your System Operation Mode setting.
  - Select **Router** if your device routes traffic between a local network and another network such as the Internet.
  - Select **Access Point** if your device bridges traffic between clients on the same network.
- 6 If the problem continues, contact your ISP.



---

### I cannot access the Internet anymore. I had access to the Internet (with the NBG334W), 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 1.7 on page 31](#).
- 2 Reboot the NBG334W.
- 3 If the problem continues, contact your ISP.



---

### The Internet connection is slow or intermittent.

---

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.7 on page 31](#). If the NBG334W is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Check the signal strength. If the signal strength is low, try moving the NBG334W closer to the AP if possible, and look around to see if there are any devices that might be

interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

- 3 Reboot the NBG334W.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### Advanced Suggestions

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

## 23.4 Resetting the NBG334W to Its Factory Defaults

If you reset the NBG334W, you lose all of the changes you have made. The NBG334W reloads its default settings, and the password resets to **1234**. You have to make all of your changes again.



---

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

---

To reset the NBG334W,

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

If the NBG334W restarts automatically, wait for the NBG334W to finish restarting, and log in to the web configurator. The password is “1234”.

If the NBG334W does not restart automatically, disconnect and reconnect the NBG334W’s power. Then, follow the directions above again.

## 23.5 Wireless Router/AP Troubleshooting



---

I cannot access the NBG334W or ping any computer from the WLAN (wireless AP or router).

---

- 1 Make sure the wireless LAN is enabled on the NBG334W
- 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 NBG334W.

- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG334W.
  - 5 Check that both the NBG334W and your wireless station are using the same wireless and wireless security settings.
  - 6 Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the NBG334W.
  - 7 Make sure you allow the NBG334W to be remotely accessed through the WLAN interface. Check your remote management settings.
- See the chapter on Wireless LAN in the User's Guide for more information.

## 23.6 Advanced Features



---

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

---

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

You may be accessing the Web Configurator in AP Mode. Some screens and fields are available only in Router Mode. Use the **Maintenance > Sys OP Mode** screen to select Router Mode.



---

I set up URL keyword blocking, but I can still access a website that should be blocked.

---

Make sure that you select the **Enable URL Keyword Blocking** check box in the Content Filtering screen. Make sure that the keywords that you type are listed in the **Keyword List**.

If a keyword that is listed in the **Keyword List** is not blocked when it is found in a URL, customize the keyword blocking using commands. See the Customizing Keyword Blocking URL Checking section in the Content Filter chapter.

---

# PART VI

## Appendices and Index

---

Product Specifications and Wall-Mounting Instructions (211)

Pop-up Windows, JavaScripts and Java Permissions (217)

IP Addresses and Subnetting (223)

Setting up Your Computer's IP Address (231)

Wireless LANs (247)

Services (259)

Legal Information (263)

Customer Support (267)

Index (271)



# Product Specifications and Wall-Mounting Instructions

The following tables summarize the NBG334W's hardware and firmware features.

**Table 95** Hardware Features

Dimensions (W x D x H)	162 x 115 x 33 mm
Weight	237g
Power Specification	Input: 120~240 AC, 50~60 Hz Output: 12 V AC 1 A
Ethernet ports	Auto-negotiating: 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
4-5 Port Switch	A combination of switch and router makes your NBG334W a cost-effective and viable network solution. You can add up to four computers to the NBG334W without the cost of a hub when connecting to the Internet through the WAN port. You can add up to five computers to the NBG334W when you connect to the Internet in AP mode. Add more than four computers to your LAN by using a hub.
LEDs	PWR, LAN1-4, WAN, WLAN, WPS
Reset Button	The reset button is built into the rear panel. Use this button to restore the NBG334W 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 NBG334W is equipped with a 2dBi detachable antenna to provide clear radio transmission and reception on the wireless network.
Operation Environment	Temperature: 0° C ~ 40° C Humidity: 20% ~ 85% RH (Non-condensing)
Storage Environment	Temperature: -20° C ~ 60° C Humidity: 20% ~ 90% RH (Non-condensing)
Distance between the centers of the holes on the device's back.	125 mm
Screw size for wall-mounting	M3*10

**Table 96** Firmware Features

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)

**Table 96** Firmware Features

FEATURE	DESCRIPTION
Default Password	1234
DHCP Pool	192.168.1.33 to 192.168.1.64
Device Management	Use the web configurator to easily configure the rich range of features on the NBG334W.
Wireless Functionality	<p>Allows IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the NBG334W wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.</p> <p><b>Note:</b> The NBG334W may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.</p>
Firmware Upgrade	<p>Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the NBG334W.</p> <p><b>Note:</b> Only upload firmware for your specific model!</p>
Configuration Backup & Restoration	Make a copy of the NBG334W's configuration and put it back on the NBG334W later if you decide you want to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert a single public IP address to multiple private IP addresses for the computers on your network.
Firewall	You can configure firewall on the NBG334W for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.
Content Filter	<p>The NBG334W blocks or allows access to web sites that you specify and blocks access to web sites with URLs that contain keywords that you specify. You can define time periods and days during which content filtering is enabled. You can also include or exclude particular computers on your network from content filtering.</p> <p>You can also subscribe to category-based content filtering that allows your NBG334W to check web sites against an external database.</p>
Bandwidth Management	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Time and Date	Get the current time and date from an external server when you turn on your NBG334W. You can also set the time manually. These dates and times are then used in logs.
Port Forwarding	If you have a server (mail or web server for example) on your network, then use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the NBG334W assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.

**Table 96** Firmware Features

FEATURE	DESCRIPTION
IP Multicast	IP Multicast is used to send traffic to a specific group of computers. The NBG334W supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
IP Alias	IP Alias allows you to subdivide a physical network into logical networks over the same Ethernet interface with the NBG334W itself as the gateway for each subnet.
Logging and Tracing	Use packet tracing and logs for troubleshooting. You can send logs from the NBG334W to an external UNIX syslog server.
PPPoE	PPPoE mimics a dial-up over Ethernet Internet access connection.
PPTP Encapsulation	Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The NBG334W supports one PPTP connection at a time.
Universal Plug and Play (UPnP)	The NBG334W can communicate with other UPnP enabled devices in a network.

**Table 97** Feature Specifications

FEATURE	SPECIFICATION
Number of Static Routes	7
Number of Port Forwarding Rules	12
Number of NAT Sessions	2048
Number of Address Mapping Rules	10
Number of Bandwidth Management Classes	3
Number of DNS Name Server Record Entries	3

The following list, which is not exhaustive, illustrates the standards supported in the NBG334W.

**Table 98** Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol.
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1631	IP Network Address Translator (NAT)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2766	Network Address Translation - Protocol
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).



**Table 98** Standards Supported (continued)

STANDARD	DESCRIPTION
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
Microsoft PPTP	MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)
MBM v2	Media Bandwidth Management v2

## Wall-mounting Instructions

Do the following to hang your NBG334W on a wall.



See the [Figure 122 on page 215](#) for the size of screws to use and how far apart to place them.

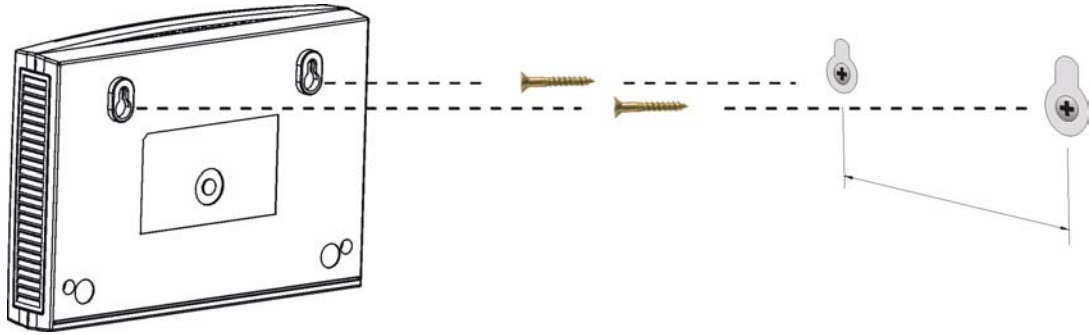
- 1 Locate a high position on a wall that is free of obstructions. Use a sturdy wall.
- 2 Drill two holes for the screws. Make sure the distance between the centers of the holes matches what is listed in the product specifications appendix.



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

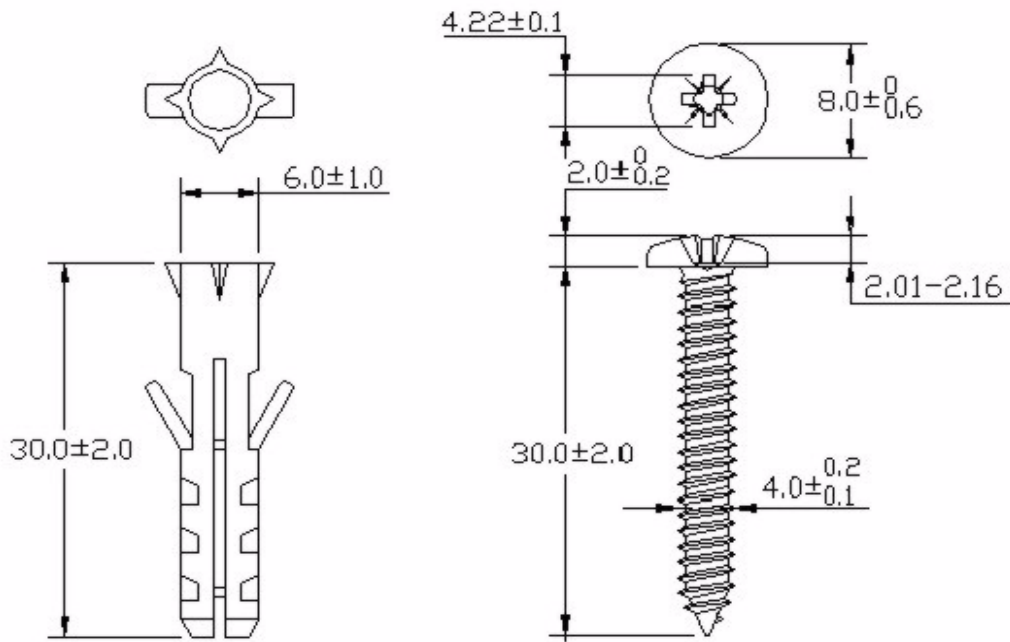
- 3 Do not screw the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.
- 4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the NBG334W with the connection cables.
- 5 Align the holes on the back of the NBG334W with the screws on the wall. Hang the NBG334W on the screws.

**Figure 121** Wall-mounting Example



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

**Figure 122** Masonry Plug and M4 Tap Screw





# Pop-up Windows, JavaScripts and Java Permissions

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

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



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

## Internet Explorer Pop-up Blockers

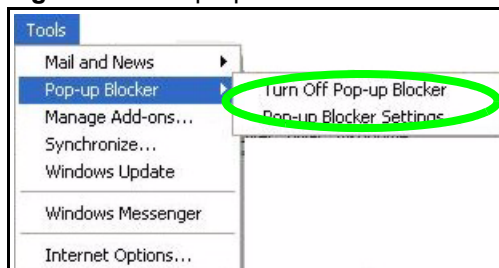
You may have to disable pop-up blocking to log into your device.

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

### Disable pop-up Blockers

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

**Figure 123** Pop-up Blocker

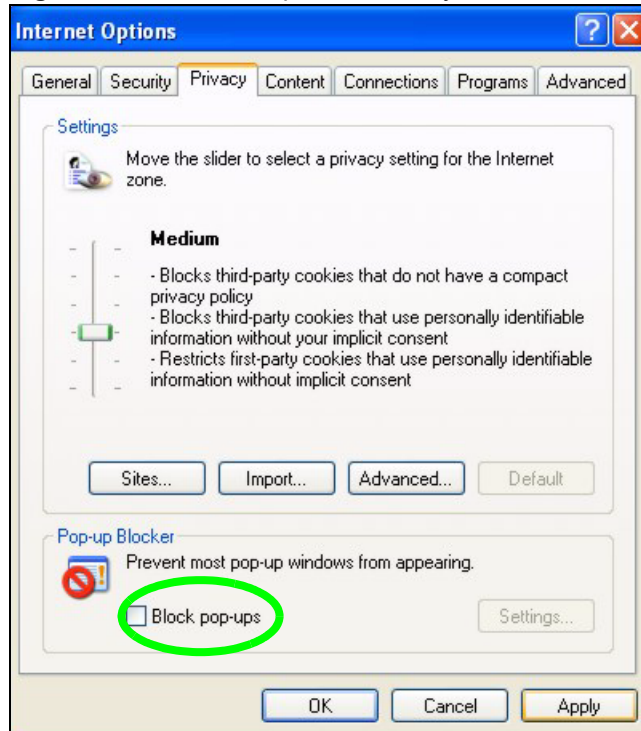


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 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 124** Internet Options: Privacy

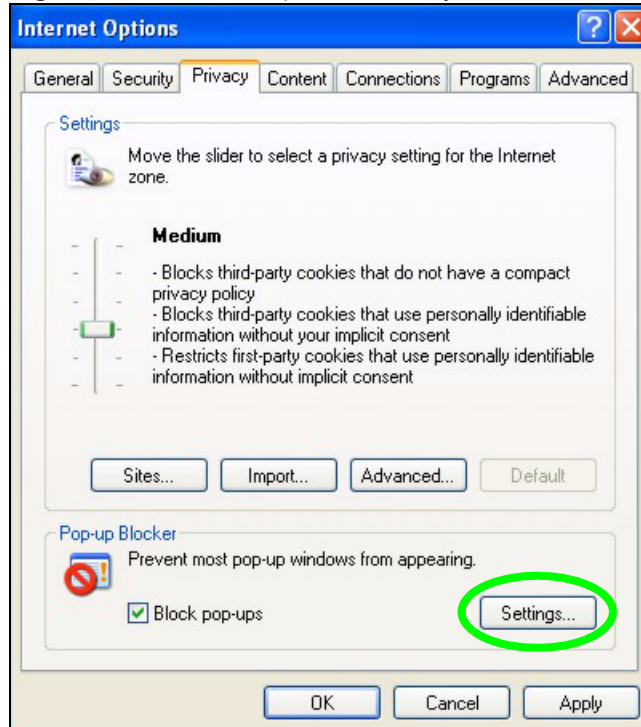


- 3 Click **Apply** to save this setting.

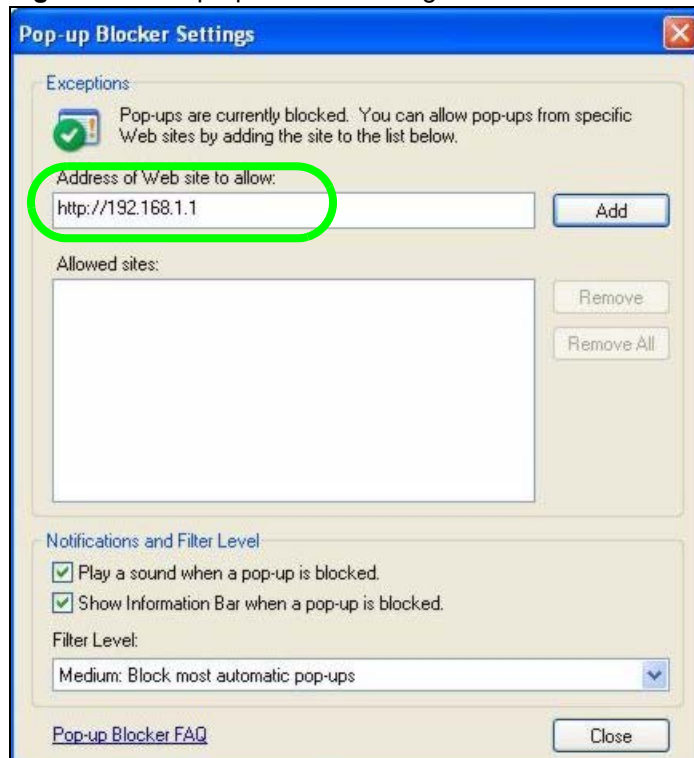
### Enable pop-up Blockers with Exceptions

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 125** 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 126** Pop-up Blocker Settings

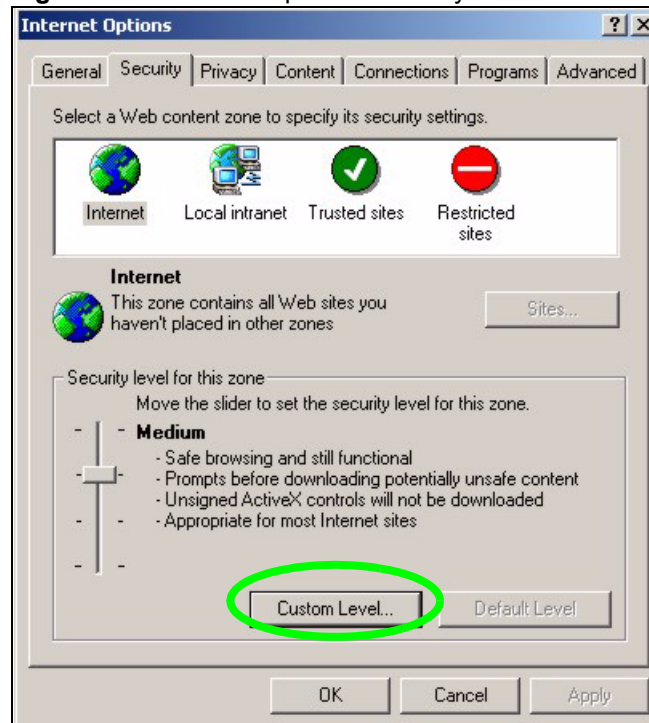
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

## JavaScripts

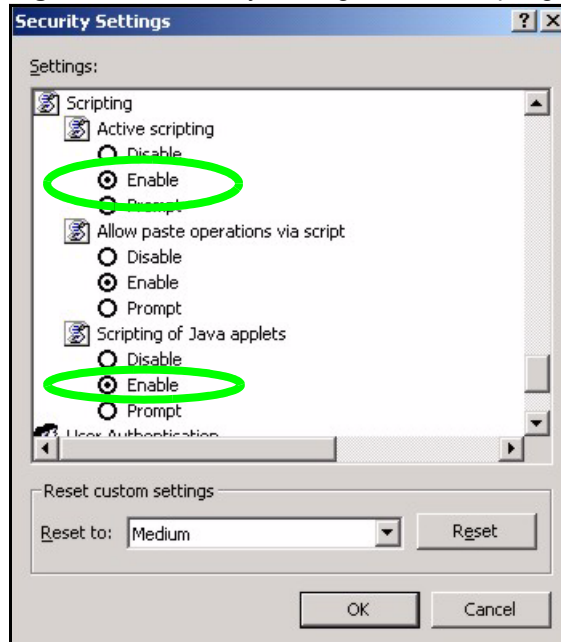
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

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

**Figure 127** Internet Options: Security

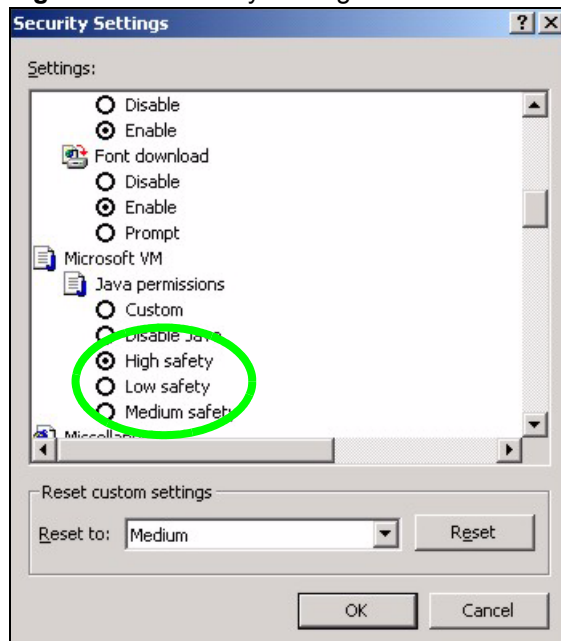


- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6 Click **OK** to close the window.

**Figure 128** 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.

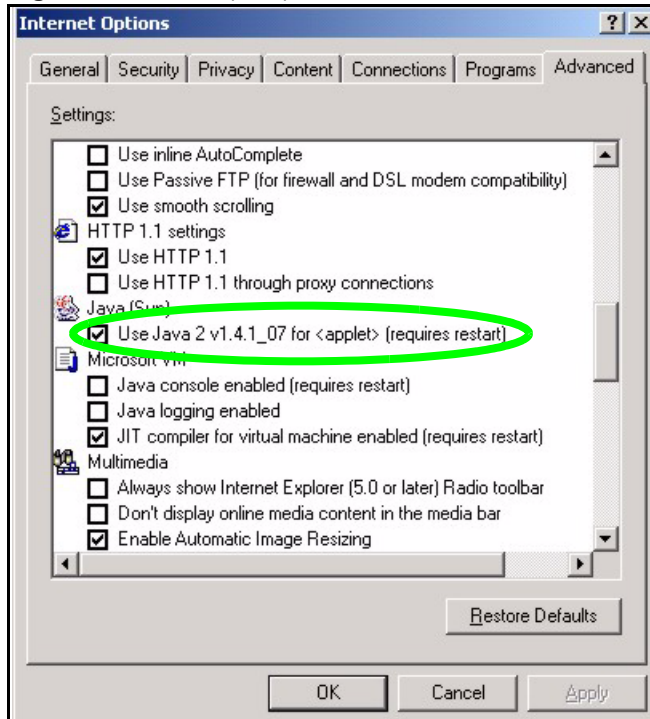
**Figure 129** Security Settings - Java



## 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 130 Java (Sun)



# IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

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

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

## Introduction to IP Addresses

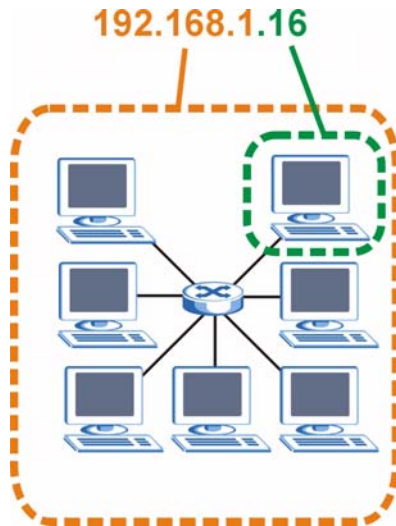
One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique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

## Structure

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

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

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

**Figure 131** Network Number and Host ID

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

## Subnet Masks

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

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

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

**Table 99** Subnet Mask - Identifying Network Number

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

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

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

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

**Table 100** Subnet Masks

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

## Network Size

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

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

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

**Table 101** Maximum Host Numbers

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

## Notation

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

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

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

**Table 102** Alternative Subnet Mask Notation

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

**Table 102** Alternative Subnet Mask Notation (continued)

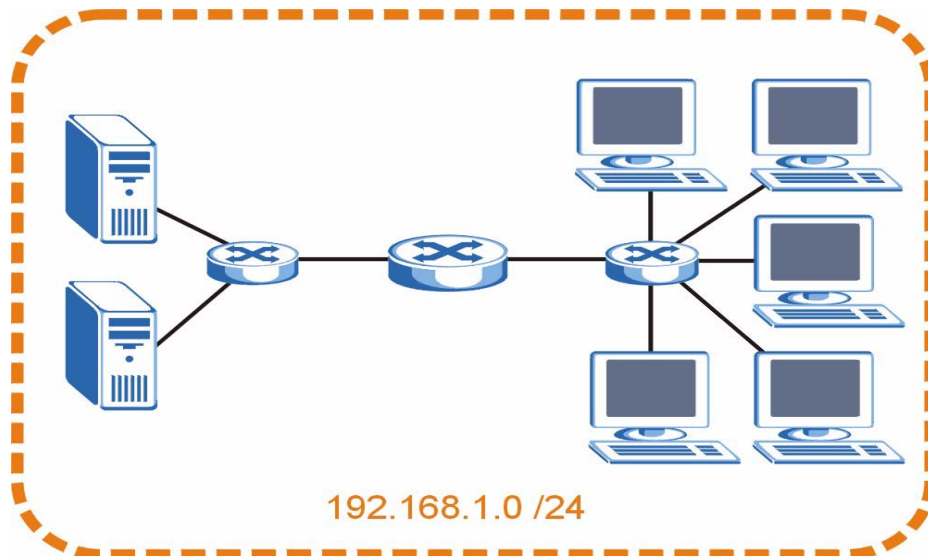
SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

## Subnetting

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

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

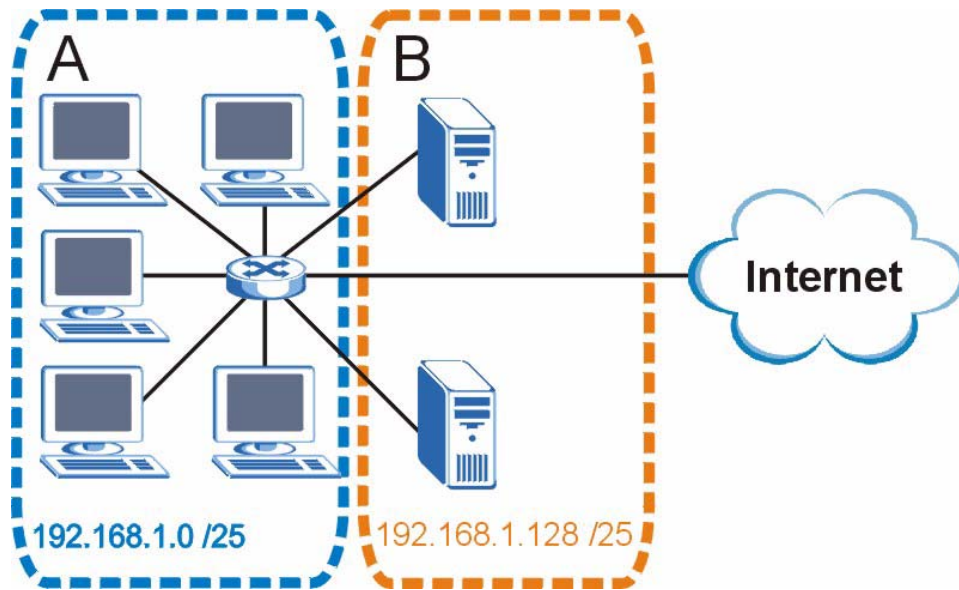
The following figure shows the company network before subnetting.

**Figure 132** Subnetting Example: Before Subnetting

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

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

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

**Figure 133** Subnetting Example: After Subnetting

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

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

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

## Example: Four Subnets

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

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

**Table 103** Subnet 1

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

**Table 104** Subnet 2

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

**Table 105** Subnet 3

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

**Table 106** Subnet 4

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

## Example: Eight Subnets

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

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

**Table 107** Eight Subnets

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

**Table 107** Eight Subnets (continued)

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

## Subnet Planning

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

**Table 108** 24-bit Network Number Subnet Planning

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

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

**Table 109** 16-bit Network Number Subnet Planning

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



**Table 109** 16-bit Network Number Subnet Planning (continued)

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

## Configuring IP Addresses

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the NBG334W.

Once you have decided on the network number, pick an IP address for your NBG334W that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your NBG334W will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the NBG334W unless you are instructed to do otherwise.

### Private IP Addresses

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

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

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

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

# Setting up Your Computer's IP Address

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

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

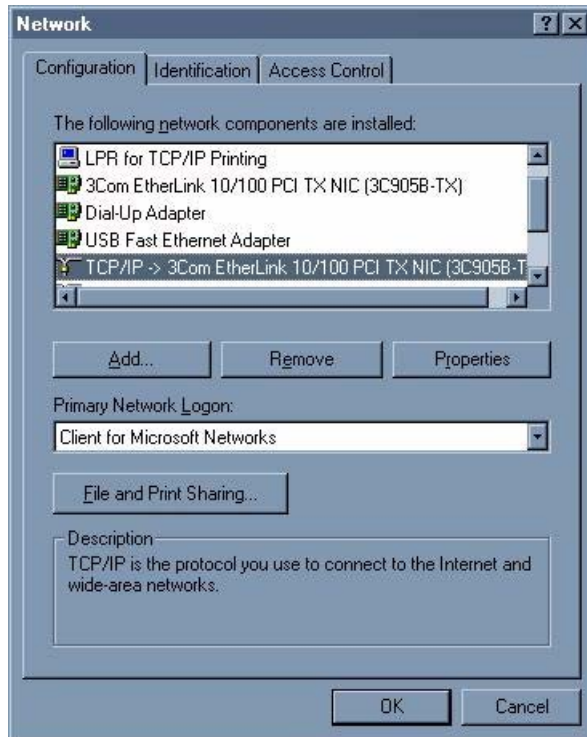
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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

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

## Windows 95/98/Me

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

**Figure 134** Windows 95/98/Me: Network: Configuration

## Installing Components

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

If you need the adapter:

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

If you need TCP/IP:

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

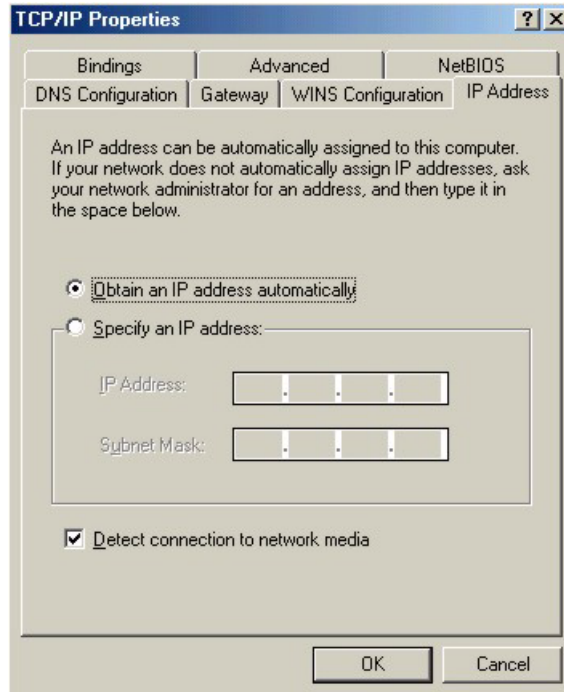
If you need Client for Microsoft Networks:

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

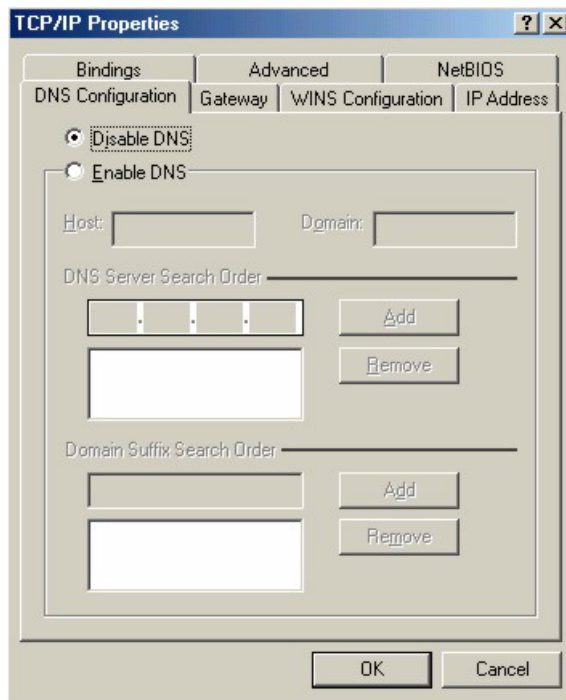
## Configuring

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

**Figure 135** Windows 95/98/Me: TCP/IP Properties: IP Address



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

**Figure 136** Windows 95/98/Me: TCP/IP Properties: DNS Configuration

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

## Verifying Settings

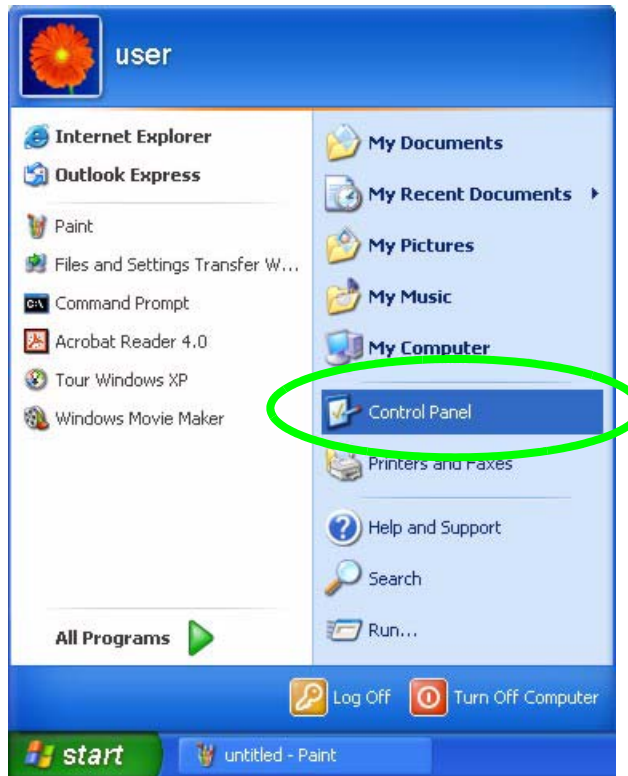
- 1 Click **Start** and then **Run**.
- 2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

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

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

Figure 137 Windows XP: Start Menu



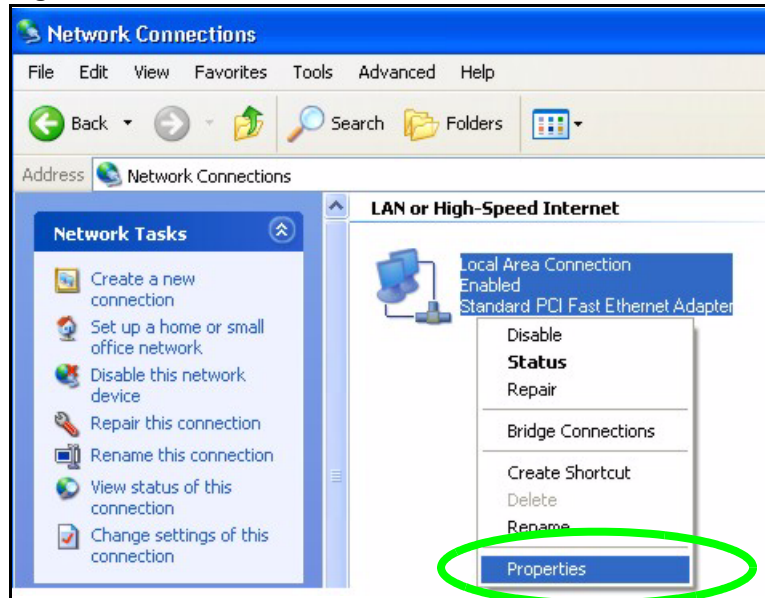
- 2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 138 Windows XP: Control Panel



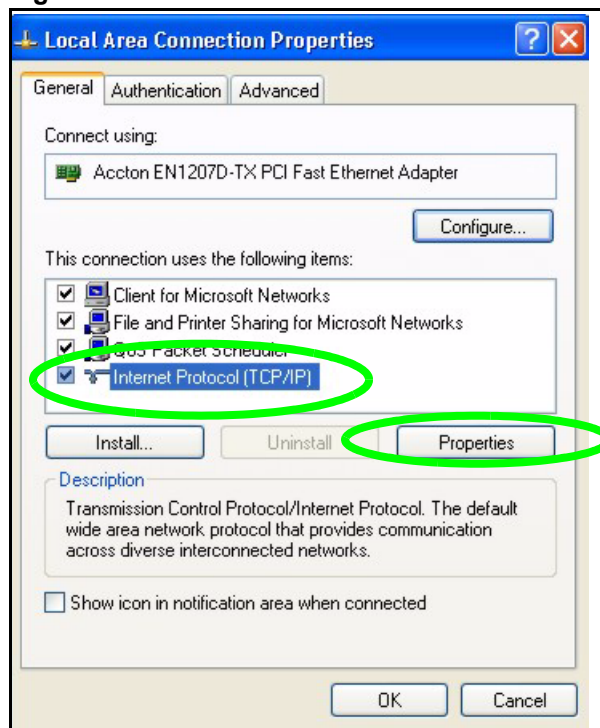
- 3 Right-click **Local Area Connection** and then click **Properties**.

**Figure 139** Windows XP: Control Panel: Network Connections: Properties



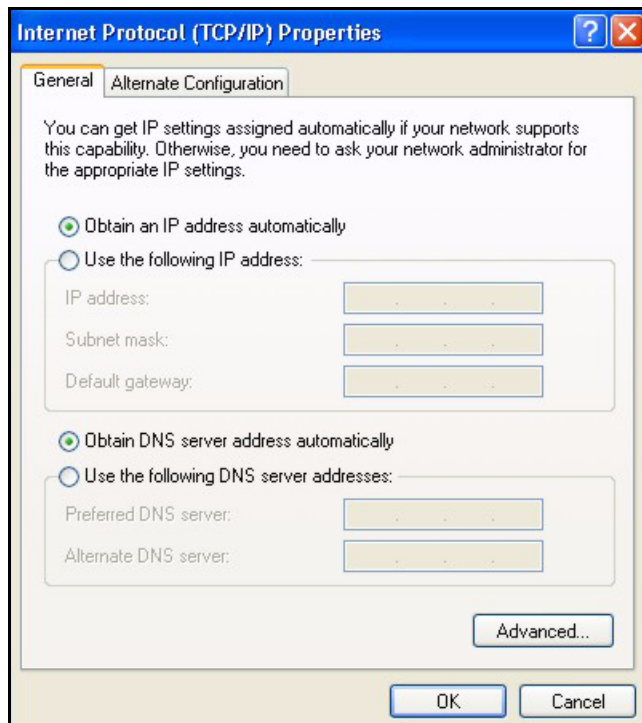
**4** Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

**Figure 140** Windows XP: Local Area Connection Properties



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

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

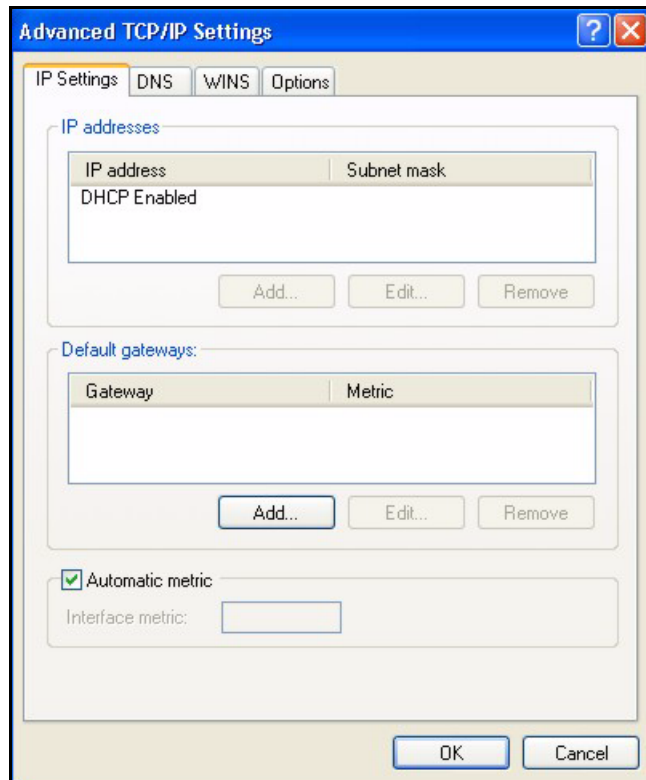
**Figure 141** Windows XP: Internet Protocol (TCP/IP) Properties

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

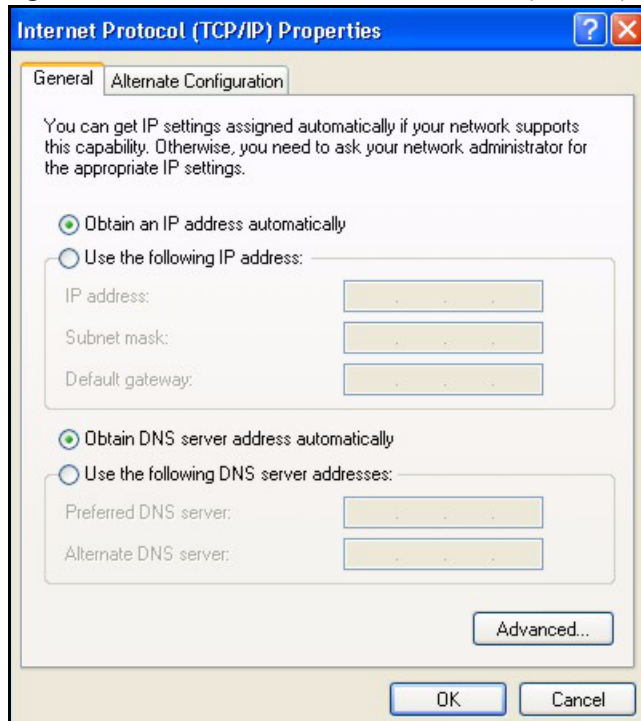
Do one or more of the following if you want to configure additional IP addresses:

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



**Figure 142** Windows XP: Advanced TCP/IP Properties

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

**Figure 143** Windows XP: Internet Protocol (TCP/IP) Properties

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

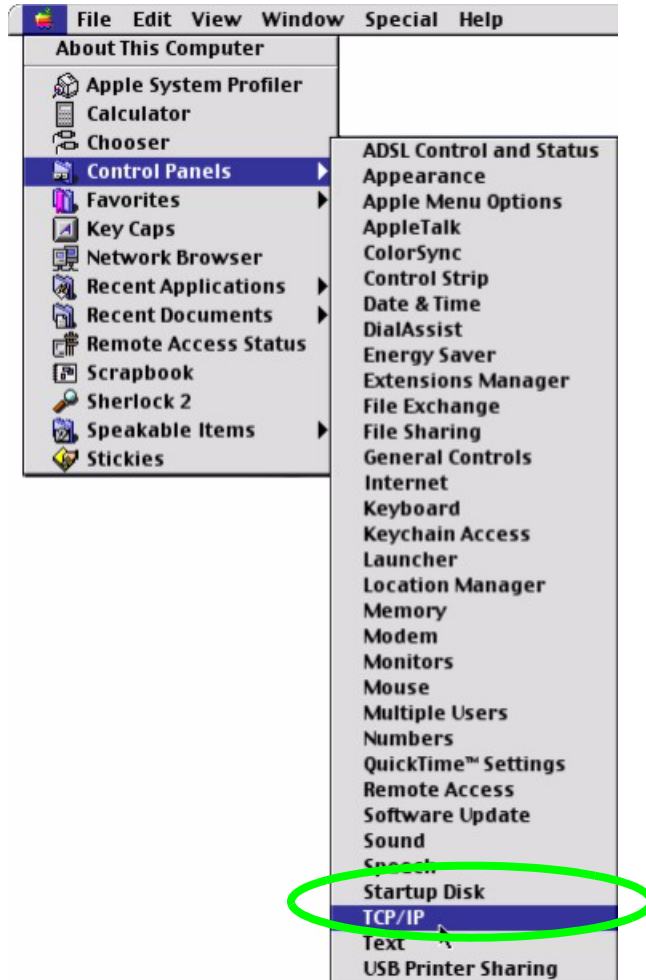
## Verifying Settings

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

## Macintosh OS 8/9

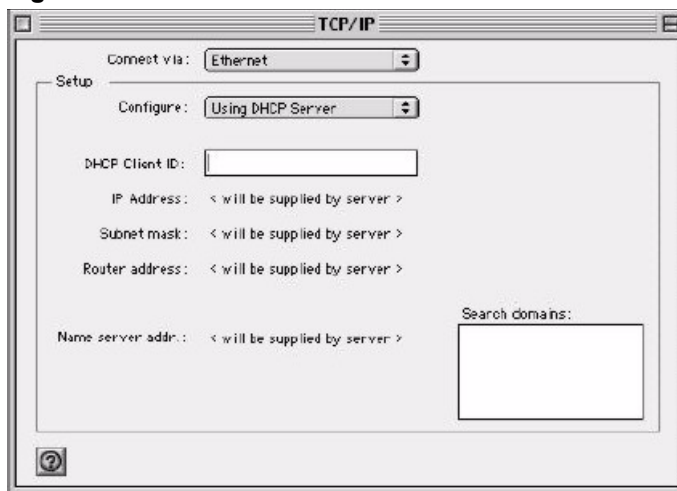
- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 144 Macintosh OS 8/9: Apple Menu



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

Figure 145 Macintosh OS 8/9: TCP/IP



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

4 For statically assigned settings, do the following:

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

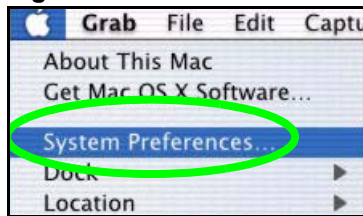
## Verifying Settings

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

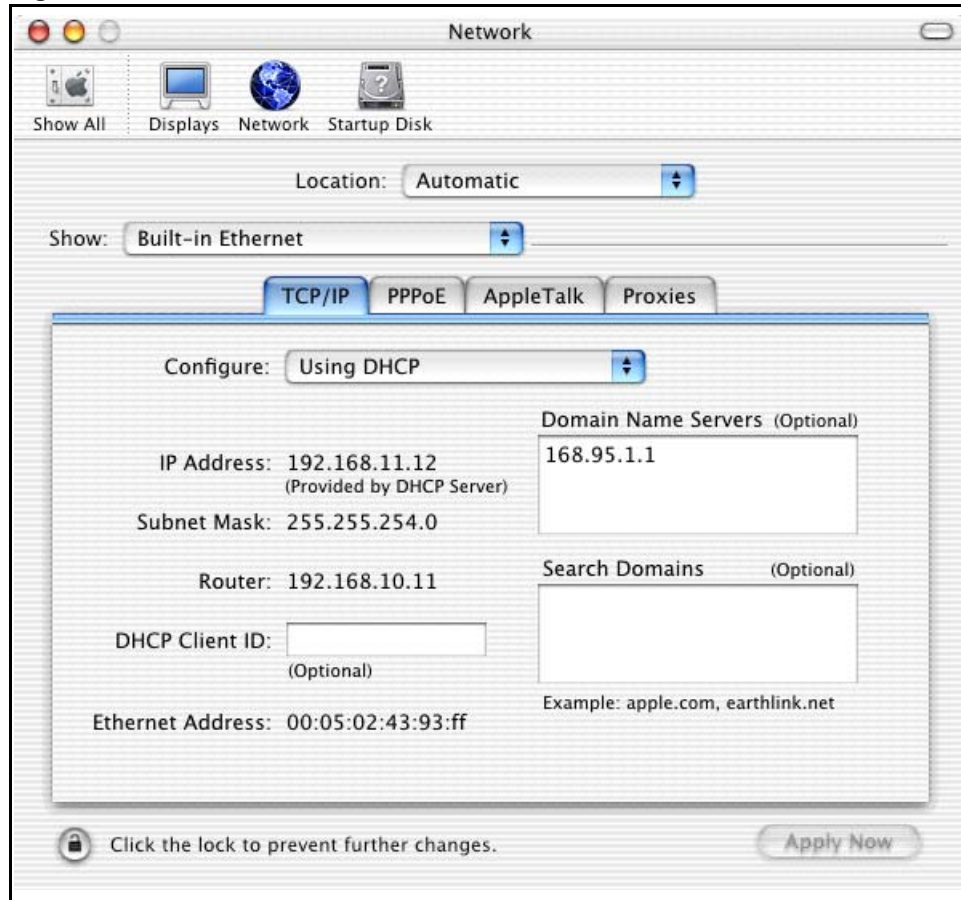
## Macintosh OS X

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

**Figure 146** Macintosh OS X: Apple Menu



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

**Figure 147** Macintosh OS X: Network

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

## Verifying Settings

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

## Linux

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



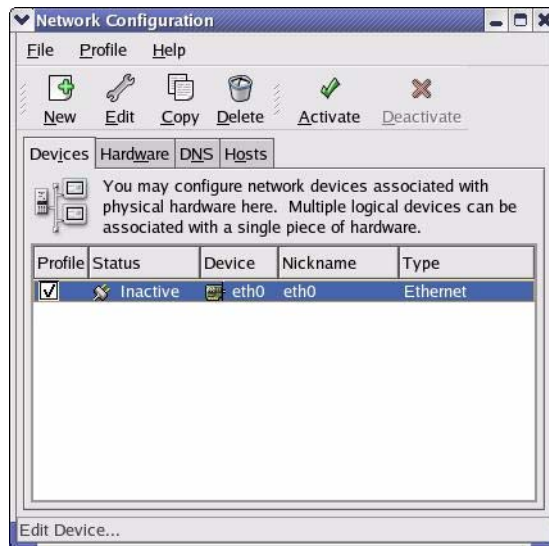
Make sure you are logged in as the root administrator.

## Using the K Desktop Environment (KDE)

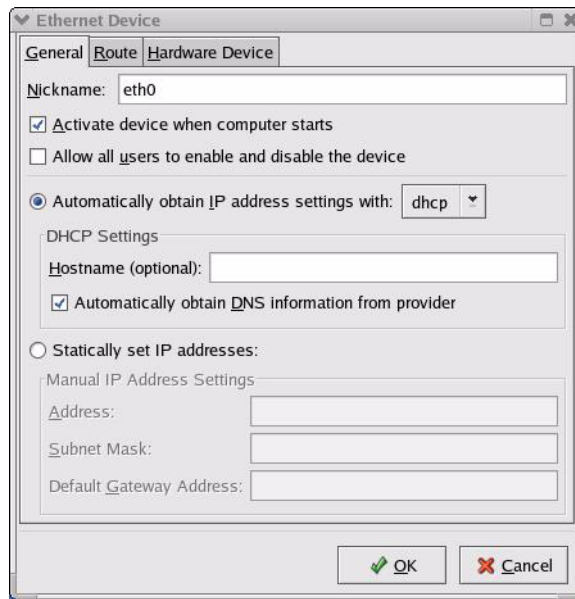
Follow the steps below to configure your computer IP address using the KDE.

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

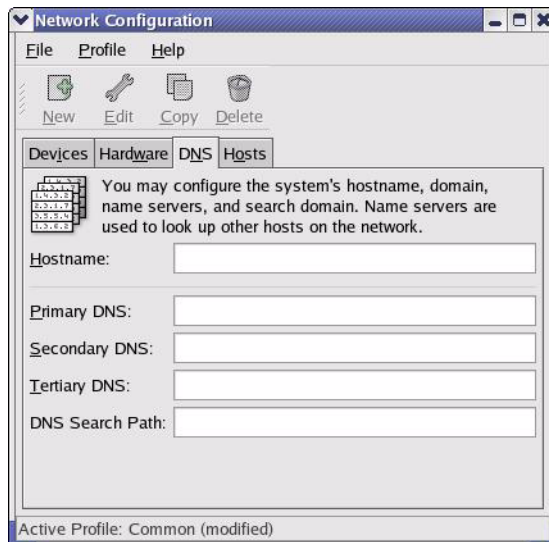
**Figure 148** Red Hat 9.0: KDE: Network Configuration: Devices



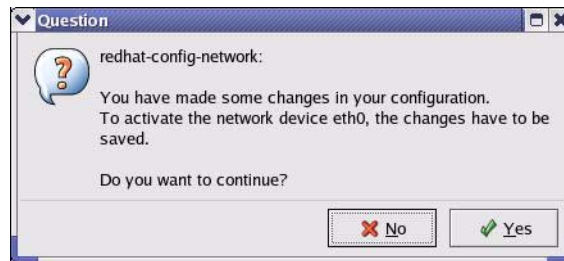
- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

**Figure 149** Red Hat 9.0: KDE: Ethernet Device: General

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

**Figure 150** Red Hat 9.0: KDE: Network Configuration: DNS

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

**Figure 151** Red Hat 9.0: KDE: Network Configuration: Activate

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

## Using Configuration Files

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

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

**Figure 152** Red Hat 9.0: Dynamic IP Address Setting in `ifconfig-eth0`

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

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

**Figure 153** Red Hat 9.0: Static IP Address Setting in `ifconfig-eth0`

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



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

**Figure 154** Red Hat 9.0: DNS Settings in `resolv.conf`

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

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

**Figure 155** Red Hat 9.0: Restart Ethernet Card

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

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

### 23.6.1 Verifying Settings

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

**Figure 156** Red Hat 9.0: Checking TCP/IP Properties

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

# Wireless LANs

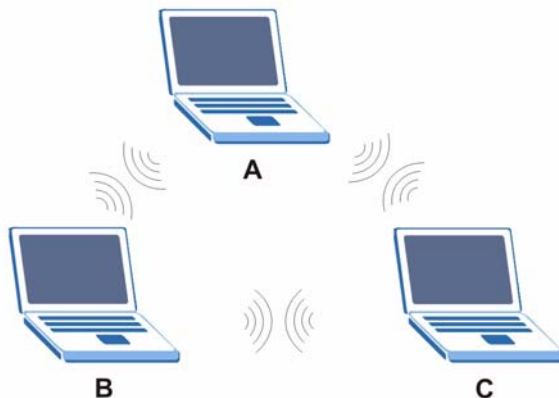
## Wireless LAN Topologies

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

### Ad-hoc Wireless LAN Configuration

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

**Figure 157** Peer-to-Peer Communication in an Ad-hoc Network

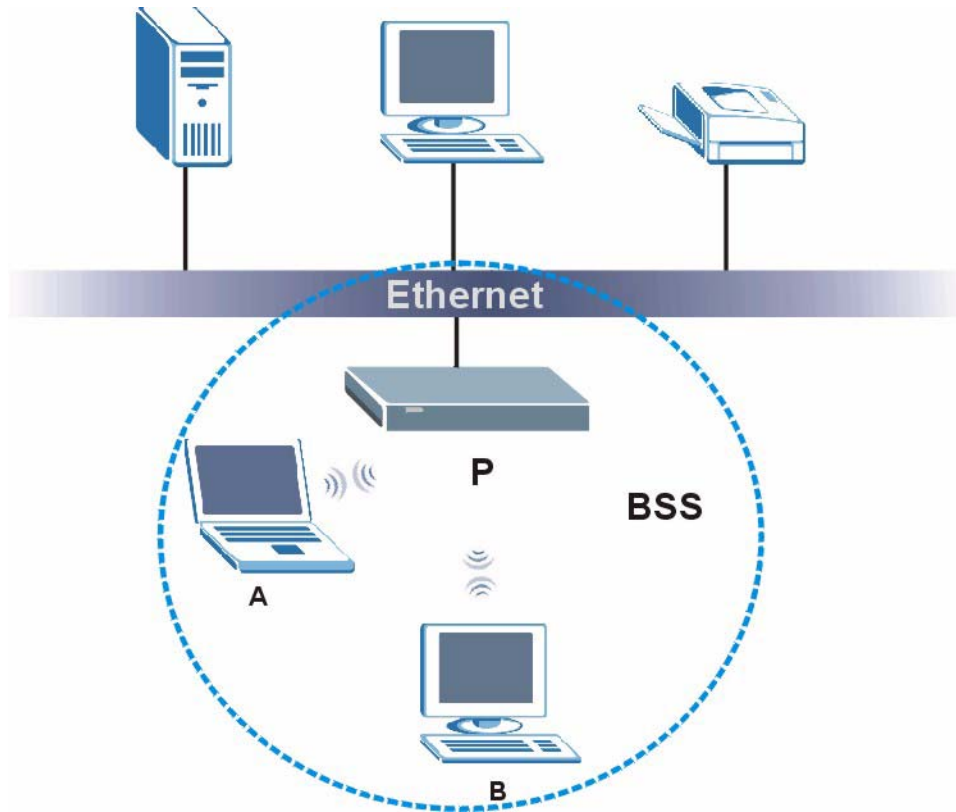


### BSS

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

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

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

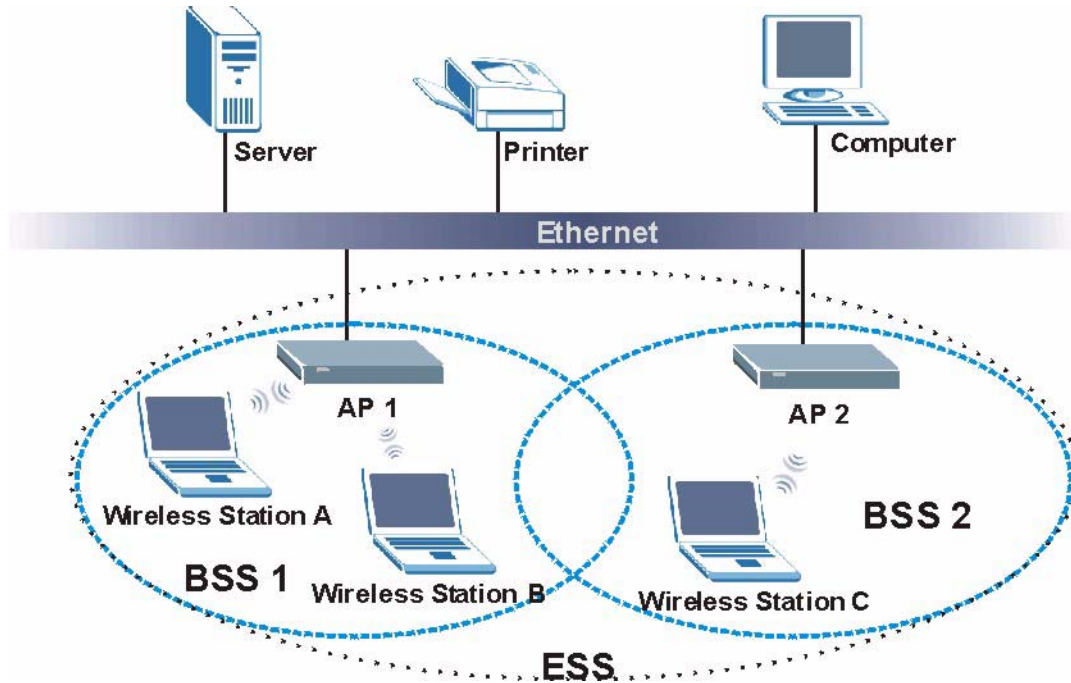
**Figure 158** Basic Service Set

## ESS

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

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

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

**Figure 159** Infrastructure WLAN

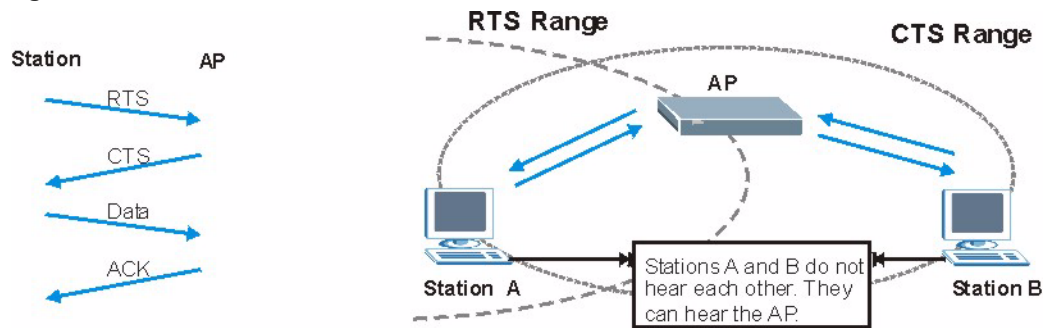
## Channel

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

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

## RTS/CTS

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

**Figure 160** RTS/CTS

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

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

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

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

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

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



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

## Fragmentation Threshold

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

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

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

## Preamble Type

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

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

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

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



The AP and the wireless stations **MUST** use the same preamble mode in order to communicate.

### IEEE 802.11g Wireless LAN

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

**Table 110** IEEE 802.11g

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

## IEEE 802.1x

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

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

## RADIUS

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

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

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

### Types of RADIUS Messages

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

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

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

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

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

## Types of Authentication

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

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

### EAP-MD5 (Message-Digest Algorithm 5)

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

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

### EAP-TLS (Transport Layer Security)

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

### EAP-TTLS (Tunneled Transport Layer Service)

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



## PEAP (Protected EAP)

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

## LEAP

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

## Dynamic WEP Key Exchange

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

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



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 111** Comparison of EAP Authentication Types

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

## WPA(2)

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

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

## Encryption

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

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

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

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

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

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

## User Authentication

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

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

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

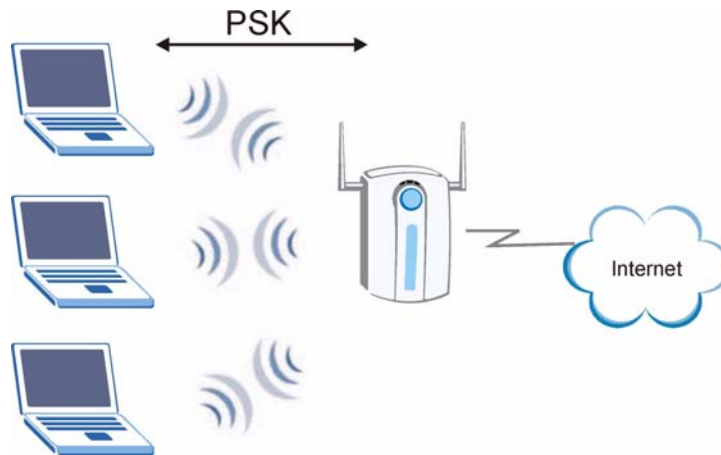
Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## 23.6.2 WPA(2)-PSK Application Example

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

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
- 3 The AP derives and distributes keys to the wireless clients.
- 4 The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

**Figure 161** WPA(2)-PSK Authentication



## 23.6.3 WPA(2) with RADIUS Application Example

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

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

## Security Parameters Summary

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

**Table 112** Wireless Security Relational Matrix

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



## Services

The following table lists some commonly-used services and their associated protocols and port numbers.

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

**Table 113** Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (e.g. <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.

**Table 113** Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.

**Table 113** Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.



**Table 113** Examples of Services (continued)

<b>NAME</b>	<b>PROTOCOL</b>	<b>PORT(S)</b>	<b>DESCRIPTION</b>
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP UDP	7000 user- defined	A videoconferencing solution. The UDP port number is specified in the application.

# Legal Information

## Copyright

Copyright © 2007 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

## Disclaimer

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

## Trademarks

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

## Certifications

### Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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



### FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

### 注意！

依據 低功率電波輻射性電機管理辦法

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

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

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。

### Notices

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

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

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

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

### Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.

- 3 Select the certification you wish to view from this page.

## ZyXEL Limited Warranty

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

### Note

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

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

### Registration

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



# Customer Support

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

## Required Information

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

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

## Corporate Headquarters (Worldwide)

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

## Costa Rica

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

## Czech Republic

- E-mail: [info@cz.zyxel.com](mailto:info@cz.zyxel.com)
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: [www.zyxel.cz](http://www.zyxel.cz)

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

### **Denmark**

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

### **Finland**

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

### **France**

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

### **Germany**

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

### **Hungary**

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

**India**

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

**Japan**

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

**Kazakhstan**

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

**Malaysia**

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

**North America**

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



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

### **Norway**

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

### **Poland**

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

### **Russia**

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

### **Singapore**

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

### **Spain**

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

**Sweden**

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

**Thailand**

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

**Ukraine**

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

**United Kingdom**

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



# Index

## Numerics

802.11 Mode [84](#)

## A

ActiveX [134](#)

address resolution protocol (ARP) [105](#)

Alert [178](#)

alternative subnet mask notation [225](#)

any IP

note [105](#)

AP [199](#)

AP (Access Point) [249](#)

AP Mode [199](#)

menu [64](#)

overview [61](#)

status screen [62](#)

AP network [199](#)

Asymmetrical routes [128](#)

and IP alias [128](#)

see also triangle routes [128](#)

## B

Backup configuration [193](#)

Bandwidth management [58](#)

application-based [143](#)

classes and priorities [148](#)

monitor [152](#)

overview [143](#)

priority [144](#)

services [145](#)

subnet-based [143](#)

Bandwidth management monitor [40](#)

Basic wireless security [49](#)

BitTorrent [145](#)

BSS [247](#)

## C

CA [253](#)

Certificate Authority [253](#)

certifications [263](#)

notices [264](#)

viewing [264](#)

Channel [37](#), [63](#), [249](#)

Interference [249](#)

channel [69](#)

command interface [31](#)

Configuration [192](#)

backup [193](#)

reset the factory defaults [194](#)

restore [193](#)

contact information [267](#)

Content Filtering

Days and Times [133](#)

Restrict Web Features [133](#)

Cookies [134](#)

copyright [263](#)

CPU usage [37](#), [63](#)

CTS (Clear to Send) [250](#)

customer support [267](#)

## D

Daylight saving [175](#)

DDNS [123](#)

see also Dynamic DNS

DHCP [41](#), [109](#)

DHCP server

see also Dynamic Host Configuration Protocol

DHCP client information [111](#)

DHCP client list [111](#)

DHCP server [103](#), [109](#)

DHCP table [41](#), [111](#)

DHCP client information

DHCP status

Dimensions [211](#)

disclaimer [263](#)

DNS [55](#), [110](#)

DNS server

see also Domain name system

DNS (Domain Name System) [157](#)  
DNS server [110](#)  
Domain name [47](#)  
    vs host name. see also system name  
Domain Name System [110](#)  
duplex setting [38](#), [64](#)  
Dynamic DNS [123](#)  
Dynamic Host Configuration Protocol [109](#)  
Dynamic WEP Key Exchange [254](#)  
DynDNS Wildcard [123](#)

## E

EAP Authentication [253](#)  
e-mail [87](#)  
Encryption [255](#)  
encryption [72](#)  
    and local (user) database [73](#)  
    key [73](#)  
    WPA compatible [73](#)  
ESS [248](#)  
ESSID [207](#)  
Extended Service Set [248](#)  
Extended wireless security [50](#)

## F

Factory LAN defaults [103](#)  
FCC interference statement [263](#)  
feature specifications [213](#)  
File Transfer Program [145](#)  
Firewall [127](#)  
    Firewall overview  
    guidelines [128](#)  
    ICMP packets [130](#)  
    network security  
    Stateful inspection [127](#)  
    ZyXEL device firewall [127](#)  
Firmware upload [191](#)  
    file extension  
    using HTTP  
firmware version [37](#), [63](#)  
Fragmentation Threshold [83](#), [250](#)  
FTP [31](#), [156](#)  
FTP. see also File Transfer Program [145](#)

## G

gateway [140](#)  
General wireless LAN screen [75](#)

## H

Hidden Node [249](#)  
HTTP [145](#)  
Hyper Text Transfer Protocol [145](#)

## I

IANA [230](#)  
IBSS [247](#)  
IEEE 802.11g [251](#)  
IGMP [93](#), [104](#)  
    see also Internet Group Multicast Protocol  
    version  
IGMP version [93](#), [104](#)  
Independent Basic Service Set [247](#)  
Install UPnP [161](#)  
    Windows Me [161](#)  
    Windows XP [162](#)  
Internet Assigned Numbers Authority  
    See IANA  
Internet connection  
    Ethernet  
    PPPoE. see also PPP over Ethernet  
    PPTP  
    WAN connection  
Internet connection wizard [50](#)  
Internet Group Multicast Protocol [93](#), [104](#)  
IP Address [106](#), [115](#)  
IP address [55](#)  
    dynamic  
IP alias [106](#)  
IP packet transmission [104](#)  
    Broadcast  
    Multicast  
    Unicast  
IP Pool [109](#)

## J

Java [134](#)

**L**

LAN **103**  
  IP pool setup **103**  
LAN overview **103**  
LAN Setup **93**  
LAN setup **103**  
LAN TCP/IP **103**  
Link type **38, 63**  
local (user) database **72**  
  and encryption **73**  
Local Area Network **103**  
Log **177**

**M**

MAC **82**  
MAC address **71, 93**  
  cloning **57, 93**  
MAC address filter **71**  
MAC address filtering **82**  
MAC filter **82**  
managing the device  
  good habits **31**  
  using FTP. See FTP.  
  using Telnet. See command interface.  
  using the command interface. See command interface.  
  using the web configurator. See web configurator.  
Media access control **82**  
Memory usage **37, 63**  
Metric **141**  
MSN messenger **145**  
MSN Webcam **145**  
Multicast **93, 104**  
  IGMP **93, 104**

**N**

NAT **113, 115, 230**  
  overview **113**  
  port forwarding **113**  
  see also Network Address Translation  
  server sets **113**  
NAT session **120**  
NAT Traversal **159**  
Navigation Panel **38, 64**  
navigation panel **38, 64**

NetBIOS **102, 108**  
  see also Network Basic Input/Output System **102**  
Network Address Translation **113, 115**  
Network Basic Input/Output System **108**

**O**

Operating Channel **37, 63**  
Output Power **84**

**P**

P2P **145**  
  peer-to-peer **145**  
Point-to-Point Protocol over Ethernet **51, 95**  
Point-to-Point Tunneling Protocol **52, 98**  
Pool Size **109**  
Port forwarding **113, 115**  
  default server **113**  
  example **114**  
  local server **115**  
  port numbers  
  services  
port speed **38, 64**  
Power Specification **211**  
PPPoE **51, 95**  
  benefits **52**  
  dial-up connection  
  see also Point-to-Point Protocol over Ethernet **51**  
PPTP **52, 98**  
  see also Point-to-Point Tunneling Protocol **52**  
Preamble Mode **251**  
priorities **75**  
Private **141**  
product registration **265**

**Q**

QoS **75**  
QoS priorities **75**  
Quality of Service (QoS) **84**

**R**

RADIUS [252](#)  
  Shared Secret Key [253](#)  
RADIUS Message Types [252](#)  
RADIUS Messages [252](#)  
RADIUS server [72](#)  
registration  
  product [265](#)  
related documentation [3](#)  
Remote management [153](#)  
  and NAT [154](#)  
  and the firewall [153](#)  
  FTP [156](#)  
  limitations [153](#)  
  remote management session [153](#)  
  system timeout [154](#)  
Reset button [35](#), [194](#)  
Reset the device [35](#)  
Restore configuration [193](#)  
Restrict Web Features [134](#)  
RF (Radio Frequency) [212](#)  
RoadRunner [95](#)  
Roaming [83](#)  
roaming [73](#)  
  requirements [74](#)  
router [199](#)  
Router Mode [199](#)  
RTS (Request To Send) [250](#)  
RTS Threshold [249](#), [250](#)  
RTS/CTS Threshold [83](#)

**S**

safety warnings [6](#)  
Security Parameters [257](#)  
Service and port numbers [146](#)  
Service Set [76](#)  
Service Set IDentification [76](#)  
Service Set IDentity. See SSID.  
services  
  and port numbers [259](#)  
  and protocols [259](#)  
Session Initiated Protocol [145](#)  
Simple Mail Transfer Protocol [180](#)  
SIP [145](#)  
SMTP [180](#)  
SNMP [128](#)  
SSID [37](#), [63](#), [69](#), [76](#)

Static DHCP [110](#)  
Static Route [139](#)  
Static route  
  and remote node  
  overview  
Status [35](#)  
subnet [223](#)  
Subnet Mask [106](#)  
subnet mask [55](#), [224](#)  
subnetting [226](#)  
Summary [40](#)  
  Bandwidth management monitor [40](#)  
  DHCP table [41](#)  
  Packet statistics [41](#)  
  Wireless station status [42](#)  
syntax conventions [4](#)  
Sys Op Mode [199](#)  
  selecting [200](#)  
System General Setup [173](#)  
System Name [173](#)  
System name [46](#)  
  vs computer name  
System restart [194](#)

**T**

TCP/IP configuration [109](#)  
Telnet [155](#)  
Temperature [211](#)  
Time setting [174](#)  
trademarks [263](#)  
Triangle routes  
  and IP alias [128](#)  
  see also asymmetrical routes [128](#)  
trigger port [118](#)  
Trigger port forwarding [118](#)  
  example [118](#)  
  process [118](#)

**U**

Universal Plug and Play [159](#)  
  Application [159](#)  
UPnP [159](#)  
  Forum [160](#)  
  security issues [159](#)  
URL Keyword Blocking [134](#)  
Use Authentication [255](#)

user authentication [72](#)  
  local (user) database [72](#)  
  RADIUS server [72](#)  
User Name [124](#)

## V

VoIP [145](#)  
VPN [98](#)

## W

WAN  
  IP address assignment [54](#)  
WAN advanced [101](#)  
WAN IP address [54](#)  
WAN IP address assignment [56](#)  
WAN MAC address [93](#)  
warranty [265](#)  
  note [265](#)  
Web Configurator  
  how to access [33](#)  
  Overview [33](#)  
Web configurator  
  navigating [35](#)  
web configurator [31](#)  
Web Proxy [134](#)  
WEP Encryption [78](#)  
WEP encryption [77](#)  
WEP key [77](#)  
Wi-Fi Multimedia QoS [75](#)  
Wildcard [123](#)  
Windows Networking [108](#)  
Wireless association list [42](#)  
wireless channel [207](#)  
wireless LAN [207](#)  
Wireless LAN wizard [47](#)  
Wireless network  
  basic guidelines [69](#)  
  channel [69](#)  
  encryption [72](#)  
  example [69](#)  
  MAC address filter [71](#)  
  overview [69](#)  
  security [70](#)  
  SSID [69](#)  
Wireless security [70](#)  
  overview [71](#)  
  type [71](#)

wireless security [207](#)  
Wireless tutorial [61](#), [89](#)  
Wizard setup [45](#)  
  Bandwidth management [58](#)  
  complete [59](#)  
  Internet connection [50](#)  
  system information [46](#)  
  wireless LAN [47](#)  
WLAN  
  Interference [249](#)  
  Security Parameters [257](#)  
WMM [75](#)  
WMM priorities [75](#)  
World Wide Web [145](#)  
WPA compatible [73](#)  
WPA, WPA2 [254](#)  
WWW [87](#), [145](#)

## X

Xbox Live [145](#)

## Z

ZyNOS [37](#), [63](#)



