

# Maintenance

## 23.1 Overview

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

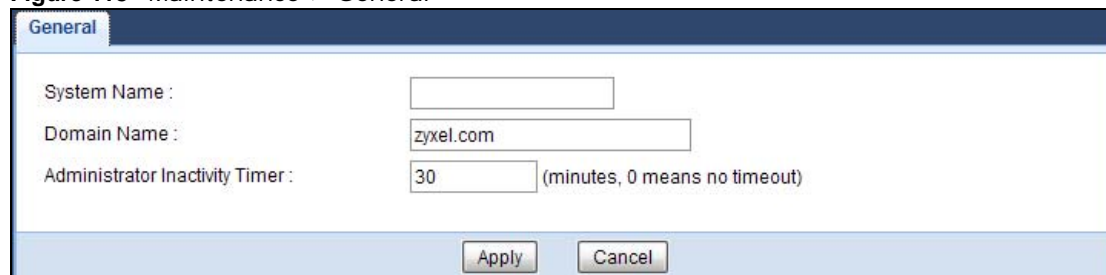
## 23.2 What You Can Do

- Use the **General** screen to set the timeout period of the management session ([Section 23.3 on page 166](#)).
- Use the **Password** screen to change your NBG6716's system password ([Section 23.4 on page 167](#)).
- Use the **Time** screen to change your NBG6716's time and date ([Section 23.5 on page 168](#)).
- Use the **Firmware Upgrade** screen to upload firmware to your NBG6716 ([Section 23.6 on page 169](#)).
- Use the **Backup/Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration ([Section 23.8 on page 172](#)).
- Use the **Restart** screen to reboot the NBG6716 without turning the power off ([Section 23.8 on page 172](#)).
- Use the **Language** screen to change the language for the Web Configurator ([Section 23.9 on page 172](#)).
- Use the **Sys OP Mode** screen to select how you want to use your NBG6716 ([Section 23.11 on page 174](#)).

## 23.3 General Screen

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

**Figure 118** Maintenance > General



The screenshot shows a web configuration interface for the 'General' screen. It features three input fields: 'System Name' (empty), 'Domain Name' (containing 'zyxel.com'), and 'Administrator Inactivity Timer' (containing '30'). A note next to the timer field states '(minutes, 0 means no timeout)'. At the bottom, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 68** Maintenance > General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the NBG6716 in an Ethernet network.
Domain Name	Enter the domain name you want to give to the NBG6716.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click <b>Apply</b> to save your changes back to the NBG6716.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 23.4 Password Screen

It is strongly recommended that you change your NBG6716's password.

If you forget your NBG6716's password (or IP address), you will need to reset the device. See [Section 23.8 on page 172](#) for details.

Click **Maintenance > Password**. The screen appears as shown.

**Figure 119** Maintenance > Password

The following table describes the labels in this screen.

**Table 69** Maintenance > Password

LABEL	DESCRIPTION
Password Setup	Change your NBG6716's password (recommended) using the fields as shown.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click <b>Apply</b> to save your changes back to the NBG6716.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 23.5 Time Setting Screen

Use this screen to configure the NBG6716's time based on your local time zone. To change your NBG6716's time and date, click **Maintenance > Time**. The screen appears as shown.

**Figure 120** Maintenance > Time

The following table describes the labels in this screen.

**Table 70** Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NBG6716. Each time you reload this page, the NBG6716 synchronizes the time with the time server.
Current Date	This field displays the date of your NBG6716. Each time you reload this page, the NBG6716 synchronizes the date with the time server.
Current Time and Date	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you select <b>Manual</b> , enter the new time in this field and then click <b>Apply</b> .

**Table 70** Maintenance > Time (continued)

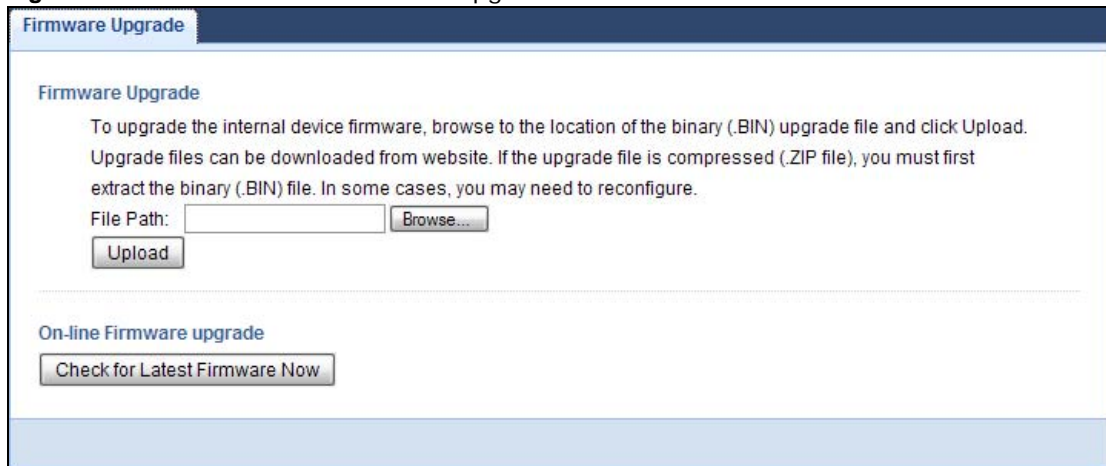
LABEL	DESCRIPTION
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually.  When you select <b>Manual</b> , enter the new date in this field and then click <b>Apply</b> .
Get from Time Server	Select this radio button to have the NBG6716 get the time and date from the time server you specified below.
User Defined Time Server Address	Select <b>User Defined Time Server Address</b> and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.  Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected <b>Daylight Savings</b> . The <b>at</b> field uses the 24 hour format. Here are a couple of examples:  Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Second, Sunday, March</b> and select <b>2</b> in the <b>at</b> field.  Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, March</b> . The time you select in the <b>at</b> field depends on your time zone. In Germany for instance, you would select 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected <b>Daylight Savings</b> . The <b>at</b> field uses the 24 hour format. Here are a couple of examples:  Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>First, Sunday, November</b> and select 2 in the <b>at</b> field.  Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, October</b> . The time you select in the <b>at</b> field depends on your time zone. In Germany for instance, you would select 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click <b>Apply</b> to save your changes back to the NBG6716.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 23.6 Firmware Upgrade Screen

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that uses the version number and project code with a `*.bin` extension, e.g., `V1.00(AAKG.0).bin`. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your NBG6716.

**Figure 121** Maintenance > Firmware Upgrade



The following table describes the labels in this screen.

**Table 71** Maintenance > Firmware Upgrade

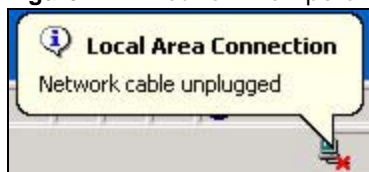
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click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

Note: Do not turn off the NBG6716 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the NBG6716 again.

The NBG6716 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 122** Network Temporarily Disconnected



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

If the upload was not successful, an error message appears. Click **Return** to go back to the **Firmware Upgrade** screen.

## 23.7 Configuration Backup/Restore Screen

Backup configuration allows you to back up (save) the NBG6716's current configuration to a file on your computer. Once your NBG6716 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG6716.

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

**Figure 123** Maintenance > Backup/Restore

**Backup/Restore**

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

---

**Restore Configuration**  
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.  
File Path:

---

**Back to Factory Defaults**  
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the  
- Password will be 1234  
- LAN IP address will be 192.168.1.1  
- DHCP will be reset to server

The following table describes the labels in this screen.

**Table 72** Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup	Click <b>Backup</b> to save the NBG6716's current configuration to your computer.
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.

**Table 72** Maintenance > Backup/Restore (continued)

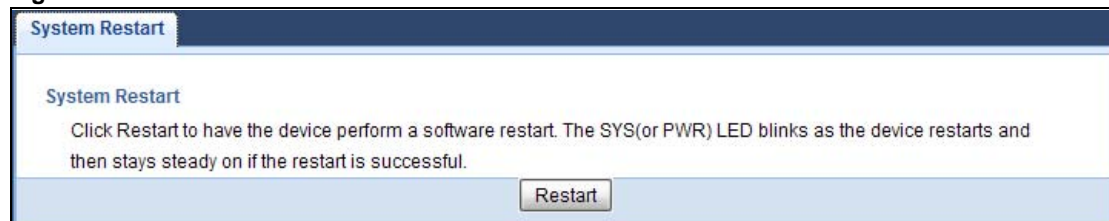
LABEL	DESCRIPTION
Upload	<p>Click <b>Upload</b> to begin the upload process.</p> <p><b>Note:</b> Do not turn off the NBG6716 while configuration file upload is in progress.</p> <p>After you see a "configuration upload successful" screen, you must then wait one minute before logging into the NBG6716 again. The NBG6716 automatically restarts in this time causing a temporary network disconnect.</p> <p>If you see an error screen, click Back to return to the Backup/Restore screen.</p>
Reset	<p>Pressing the <b>Reset</b> button in this section clears all user-entered configuration information and returns the NBG6716 to its factory defaults.</p> <p>You can also press the <b>RESET</b> button on the rear panel to reset the factory defaults of your NBG6716. Refer to the chapter about introducing the Web Configurator for more information on the <b>RESET</b> button.</p>

Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default NBG6716 IP address (192.168.1.1). See [Appendix B on page 193](#) for details on how to set up your computer's IP address.

## 23.8 Restart Screen

System restart allows you to reboot the NBG6716 without turning the power off.

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

**Figure 124** Maintenance > Restart

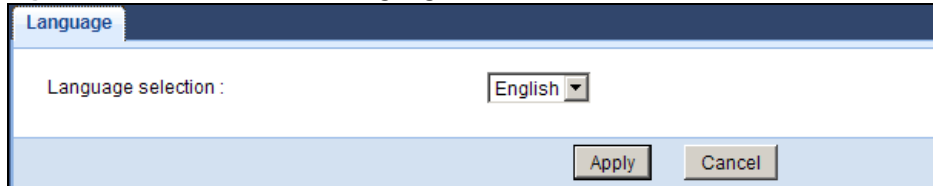
Click **Restart** to have the NBG6716 reboot. This does not affect the NBG6716's configuration.

## 23.9 Language Screen

Use this screen to change the language for the Web Configurator.

Select the language you prefer and click **Apply**. The Web Configurator language changes after a while without restarting the NBG6716.

Figure 125 Maintenance &gt; Language



## 23.10 System Operation Mode Overview

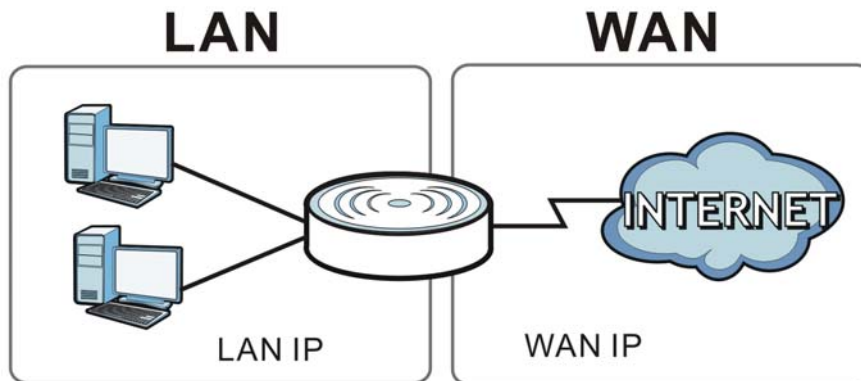
The **Sys OP Mode** (System Operation Mode) function lets you configure your NBG6716 as a router or access point. You can choose between **Router Mode**, and **Access Point Mode** depending on your network topology and the features you require from your device.

The following describes the device modes available in your NBG6716.

### 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 126 LAN and WAN IP Addresses in Router Mode

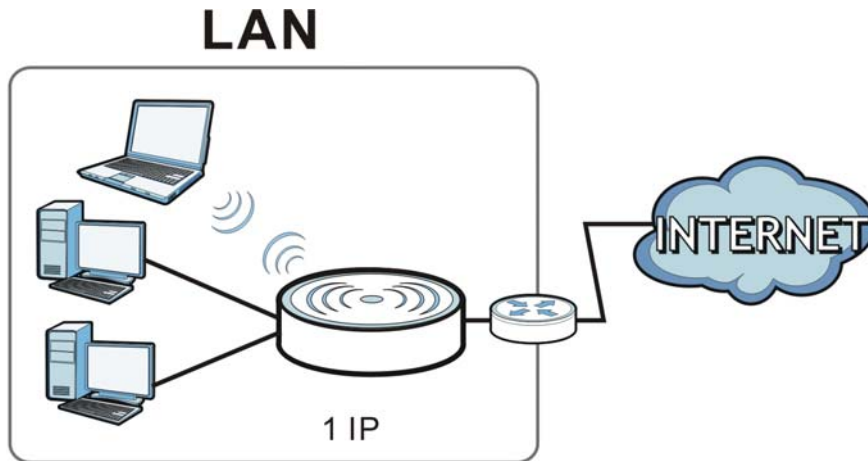


### Access Point

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



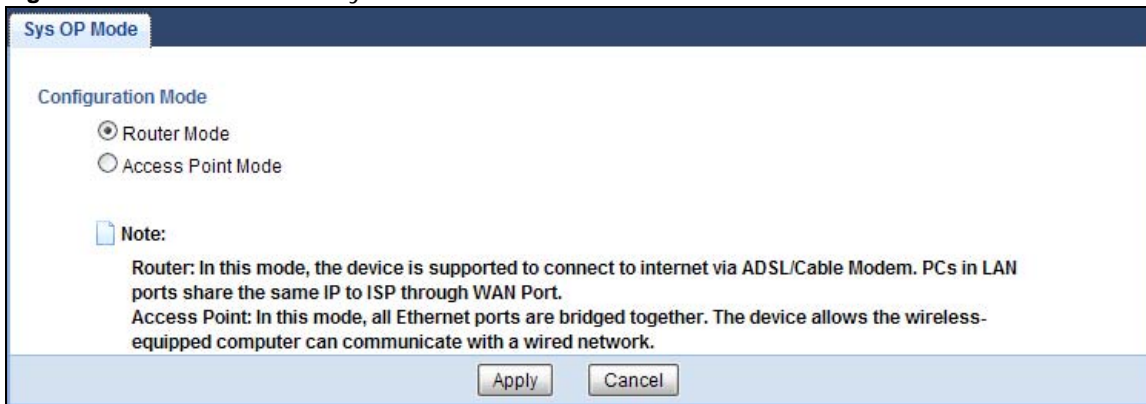
**Figure 127** Access Point Mode



## 23.11 Sys OP Mode Screen

Use this screen to select how you want to use your NBG6716.

**Figure 128** Maintenance > Sys OP Mode



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

**Table 73** Maintenance > Sys OP Mode

LABEL	DESCRIPTION
Configuration Mode	
Router Mode	Select <b>Router Mode</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.  You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings.

**Table 73** Maintenance > Sys OP Mode (continued)

LABEL	DESCRIPTION
Access Point Mode	Select <b>Access Point Mode</b> if your device bridges traffic between clients on the same network. <ul style="list-style-type: none"> <li>• In <b>Access Point Mode</b>, all Ethernet ports have the same IP address.</li> <li>• All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port.</li> <li>• The DHCP server on your device is disabled.</li> <li>• Router functions (such as NAT, bandwidth management, remote management, firewall and so on) are not available when the NBG6716 is in <b>Access Point Mode</b>.</li> <li>• The IP address of the device on the local network is set to 192.168.1.2.</li> </ul>
Apply	Click <b>Apply</b> to save your settings.
Cancel	Click <b>Cancel</b> to return your settings to the default ( <b>Router</b> ).

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

# Troubleshooting

## 24.1 Overview

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

- [Power, Hardware Connections, and LEDs](#)
- [NBG6716 Access and Login](#)
- [Internet Access](#)
- [Resetting the NBG6716 to Its Factory Defaults](#)
- [Wireless Connections](#)
- [USB Device Problems](#)
- [ZyXEL Share Center Utility Problems](#)

## 24.2 Power, Hardware Connections, and LEDs

---

The NBG6716 does not turn on. None of the LEDs turn on.

---

- 1 Make sure you are using the power adaptor or cord included with the NBG6716.
- 2 Make sure the power adaptor or cord is connected to the NBG6716 and plugged in to an appropriate power source. Make sure the power source is turned on.
- 3 Disconnect and re-connect the power adaptor or cord to the NBG6716.
- 4 If the problem continues, contact the vendor.

---

One of the LEDs does not behave as expected.

---

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.7 on page 16](#).
- 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 NBG6716.
- 5 If the problem continues, contact the vendor.

## 24.3 NBG6716 Access and Login

---

I don't know the IP address of my NBG6716.

---

- 1 The default IP address of the NBG6716 in **Router Mode** is **192.168.1.1**. The default IP address of the NBG6716 in **Access Point Mode** is **192.168.1.2**.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the NBG6716 in **Router Mode** 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 NBG6716 (it depends on the network), so enter this IP address in your Internet browser.
- 3 If your NBG6716 in **Access Point Mode** 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.
- 4 Reset your NBG6716 to change all settings back to their default. This means your current settings are lost. See [Section 24.5 on page 180](#) in the **Troubleshooting** for information on resetting your NBG6716.

---

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 24.5 on page 180](#).

---

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 of the NBG6716 in **Router Mode** is **192.168.1.1**. The default IP address of the NBG6716 in **Access Point Mode** is **192.168.1.2**.
  - If you changed the IP address ([Section 12.4 on page 108](#)), 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 NBG6716](#).

- 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 JavaScript and Java enabled. See [Appendix A on page 184](#).
- 4 Make sure your computer is in the same subnet as the NBG6716. (If you know that there are routers between your computer and the NBG6716, skip this step.)
  - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Section 12.4 on page 108](#).
  - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG6716. See [Section 12.4 on page 108](#).
- 5 Reset the device to its factory defaults, and try to access the NBG6716 with the default IP address. See [Section 1.5 on page 15](#).
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### Advanced Suggestions

- Try to access the NBG6716 using another service, such as Telnet. If you can access the NBG6716, check the remote management settings and firewall rules to find out why the NBG6716 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 NBG6716.

---

- 1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.
- 2 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
- 3 Disconnect and re-connect the power adaptor or cord to the NBG6716.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 24.5 on page 180](#).

## 24.4 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 Go to **Maintenance > Sys OP Mode**. Check your System Operation Mode setting.
  - If the NBG6716 is in **Router Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access. Your computer and the NBG6716 should be in the same subnet.
  - If the NBG6716 is in **Access Point Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access and your computer is set to obtain an dynamic IP address.
- 3 If the NBG6716 is in **Router Mode**, make sure you entered your ISP account information correctly in the wizard or the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 4 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.
- 5 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 6 If the problem continues, contact your ISP.

---

I cannot access the Internet anymore. I had access to the Internet (with the NBG6716), 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 16](#).
- 2 Reboot the NBG6716.
- 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 16](#). If the NBG6716 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 NBG6716 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 NBG6716.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### Advanced Suggestion

- Check the settings for QoS. If it is disabled, you might consider activating it.

## 24.5 Resetting the NBG6716 to Its Factory Defaults

If you reset the NBG6716, you lose all of the changes you have made. The NBG6716 re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

---

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

---

To reset the NBG6716:

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for one to four seconds to restart/reboot the NBG6716.
- 3 Press the **RESET** button for longer than five seconds to set the NBG6716 back to its factory-default configurations.

If the NBG6716 restarts automatically, wait for the NBG6716 to finish restarting, and log in to the Web Configurator. The password is "1234".

If the NBG6716 does not restart automatically, disconnect and reconnect the NBG6716's power. Then, follow the directions above again.

## 24.6 Wireless Connections

---

I cannot access the NBG6716 or ping any computer from the WLAN.

---

- 1 Make sure the wireless LAN is enabled on the NBG6716.
- 2 Make sure the wireless adapter on your computer 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 NBG6716.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG6716.
- 5 Check that both the NBG6716 and the wireless adapter on your computer 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 NBG6716.

- 7 Make sure you allow the NBG6716 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.

---

### 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 Filtering](#) chapter.

---

### I cannot access the Web Configurator after I switched to AP mode.

---

When you change from router mode to AP mode, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

Refer to [Appendix B on page 193](#) for instructions on how to change your computer's IP address.

---

### What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

---

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.



- Position the antennas for best reception. If the AP is placed on a table or floor, point the antennas upwards. If the AP is placed at a high position, point the antennas downwards. Try pointing the antennas in different directions and check which provides the strongest signal to the wireless clients.

## 24.7 USB Device Problems

---

I cannot access or see a USB device that is connected to the NBG6716.

---

- 1 Disconnect the problematic USB device, then reconnect it to the NBG6716.
- 2 Ensure that the USB device has power.
- 3 Check your cable connections.
- 4 Restart the NBG6716 by disconnecting the power and then reconnecting it.
- 5 If the USB device requires a special driver, install the driver from the installation disc that came with the device. After driver installation, reconnect the USB device to the NBG6716 and try to connect to it again with your computer.
- 6 If the problem persists, contact your vendor.

---

What kind of USB devices do the NBG6716 support?

---

- 1 It is strongly recommended to use version 2.0 or lower USB storage devices (such as memory sticks, USB hard drives) and/or USB devices (such as USB printers). Other USB products are not guaranteed to function properly with the NBG6716.

## 24.8 ZyXEL Share Center Utility Problems

---

I cannot access or see a USB device that is connected to the NBG6716.

---

- 1 Disconnect the problematic USB device, then reconnect it to the NBG6716.
- 2 Ensure that the USB device in question has power.
- 3 Check your cable connections.
- 4 Restart the NBG6716 by disconnecting the power and then reconnecting it.

- 5 If the USB device requires a special driver, install the driver from the installation disc that came with the device. After driver installation, reconnect the USB device to the NBG6716 and try to connect to it again with your computer.
- 6 If the problem persists, contact your vendor.

---

### I cannot install the ZyXEL Share Center Utility.

---

- 1 Make sure that the set up program is one required for your operating system.
- 2 Install the latest patches and updates for your operating system.
- 3 Check the [zyxel.com](http://zyxel.com) download site for a newer version of the utility.

# Pop-up Windows, JavaScript and Java Permissions

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

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

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

## Internet Explorer Pop-up Blockers

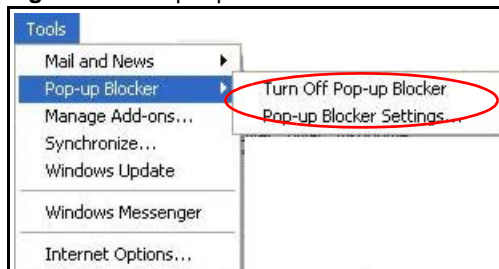
You may have to disable pop-up blocking to log into your device.

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

## Disable Pop-up Blockers

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

**Figure 129** 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 130** Internet Options: Privacy

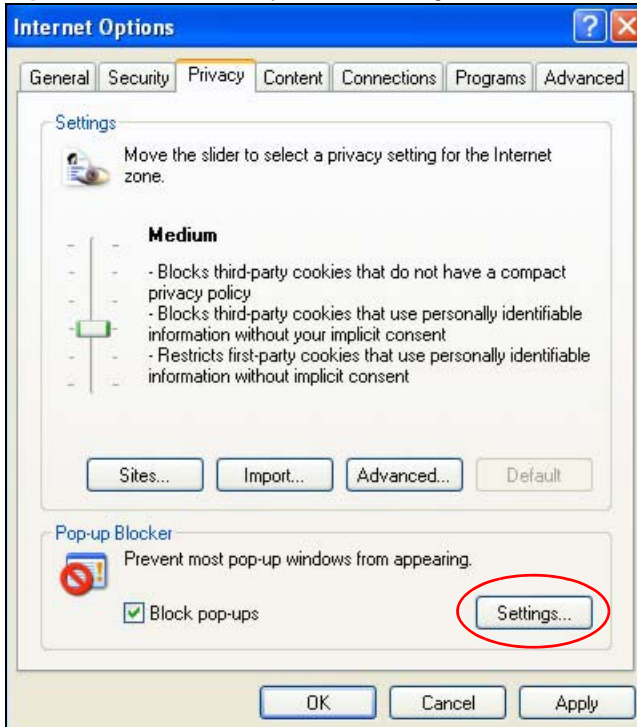
- 3 Click **Apply** to save this setting.

## Enable Pop-up Blockers with Exceptions

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

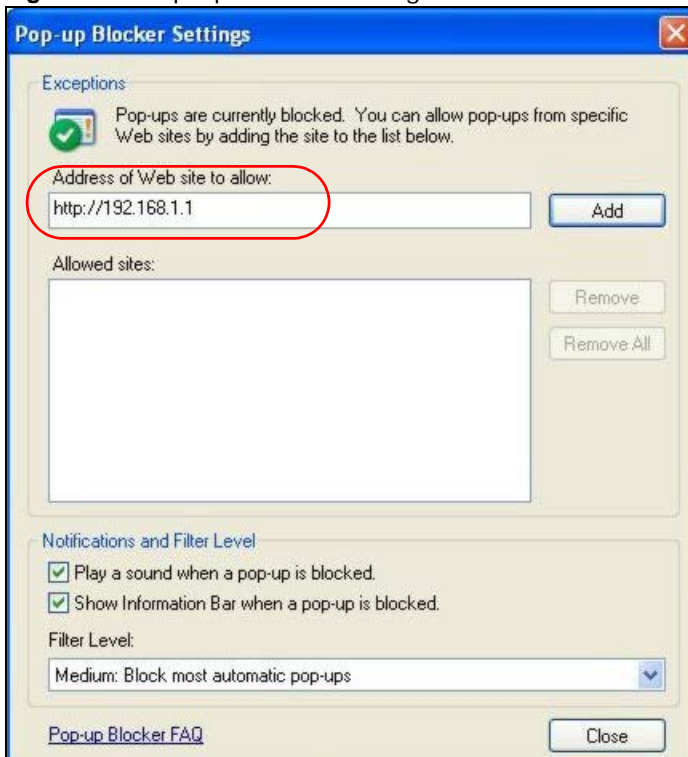
- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

**Figure 131** 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 132** Pop-up Blocker Settings



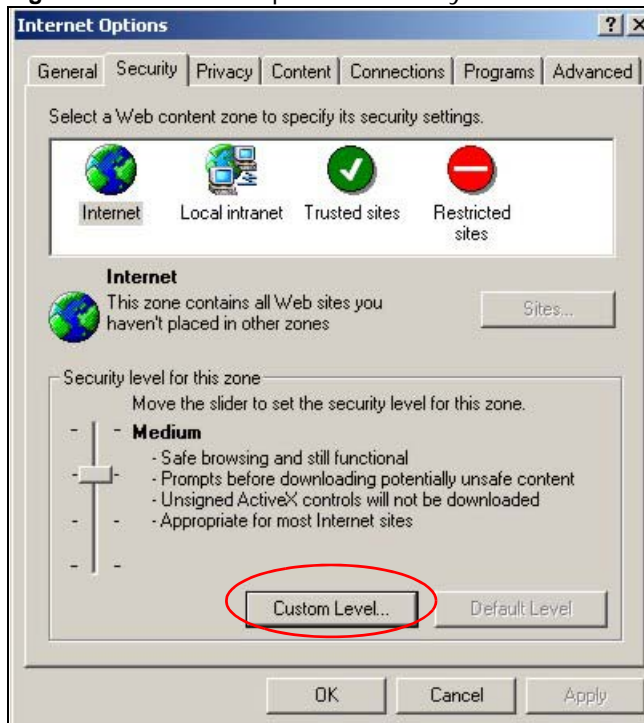
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

## JavaScript

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

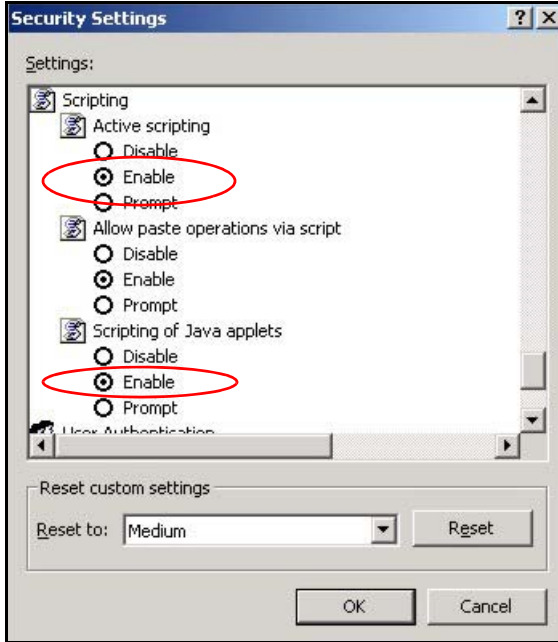
- 1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

**Figure 133** 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.

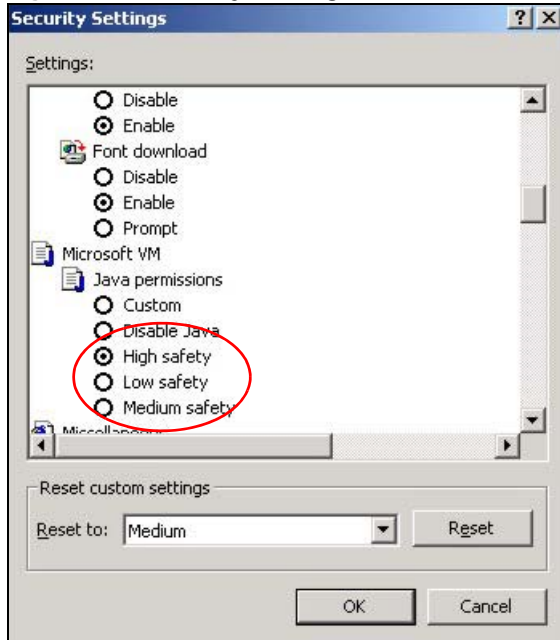
**Figure 134** Security Settings - Java Scripting



## 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.

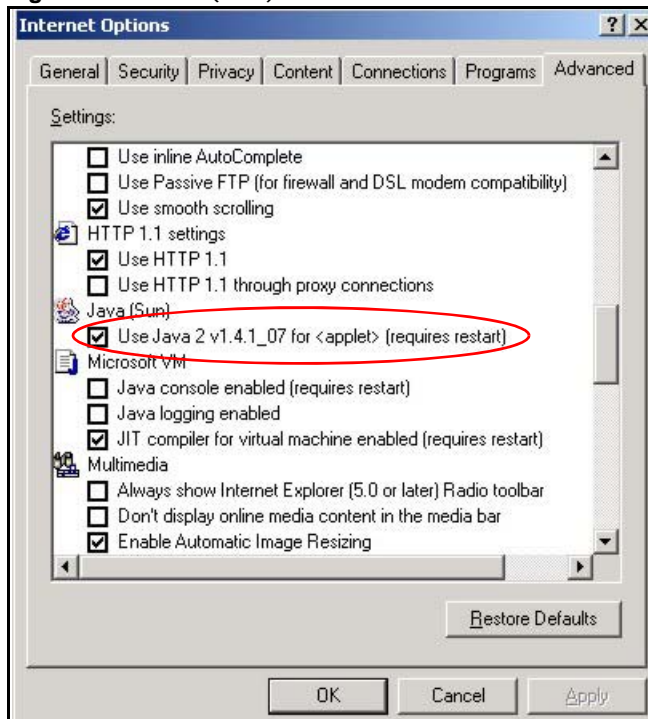
Figure 135 Security Settings - Java



## 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 136 Java (Sun)



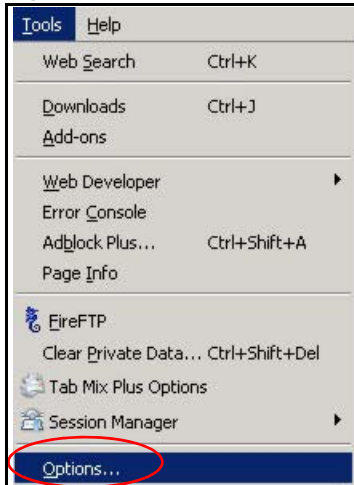


## Mozilla Firefox

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

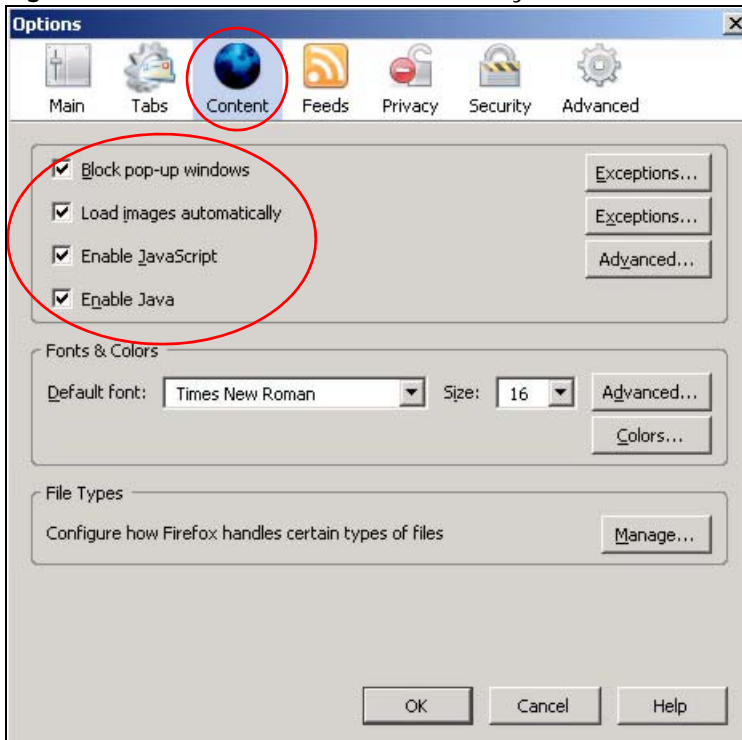
You can enable Java, Javascript and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

**Figure 137** Mozilla Firefox: TOOLS > Options



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

**Figure 138** Mozilla Firefox Content Security



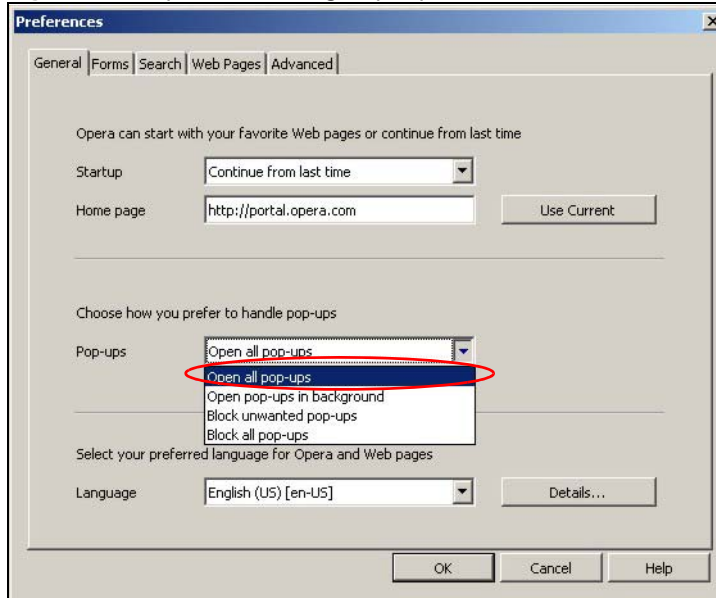
## Opera

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

### Allowing Pop-Ups

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

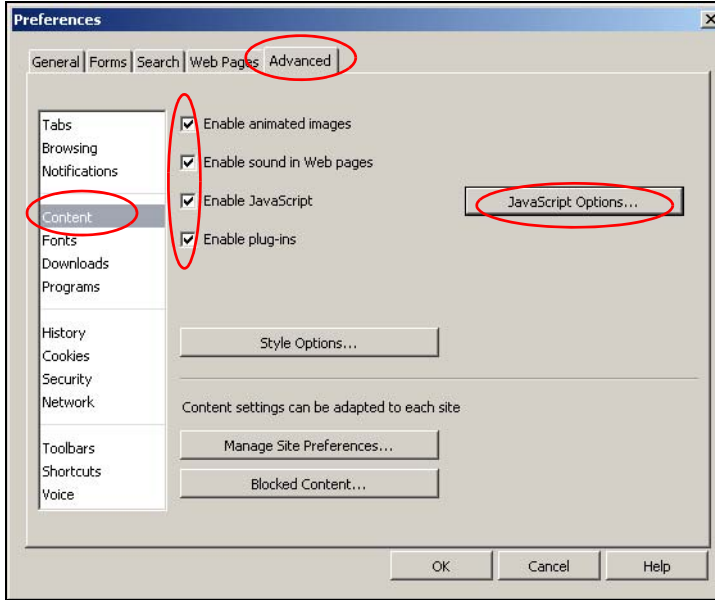
**Figure 139** Opera: Allowing Pop-Ups



### Enabling Java

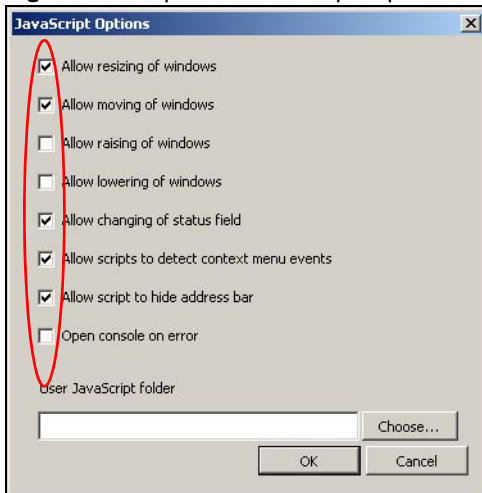
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 140 Opera: Enabling Java



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

Figure 141 Opera: JavaScript Options



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

# Setting Up Your Computer's IP Address

Note: Your specific NBG6716 may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

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

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

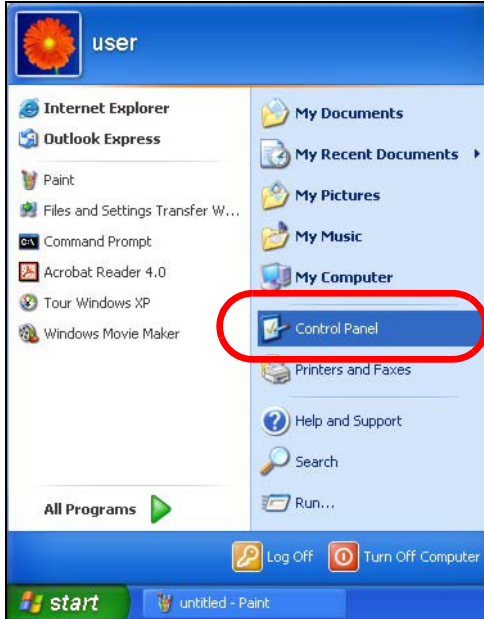
In this appendix, you can set up an IP address for:

- [Windows XP/NT/2000](#) on [page 193](#)
- [Windows Vista](#) on [page 197](#)
- [Windows 7](#) on [page 201](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 205](#)
- [Mac OS X: 10.5 and 10.6](#) on [page 208](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 211](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 215](#)

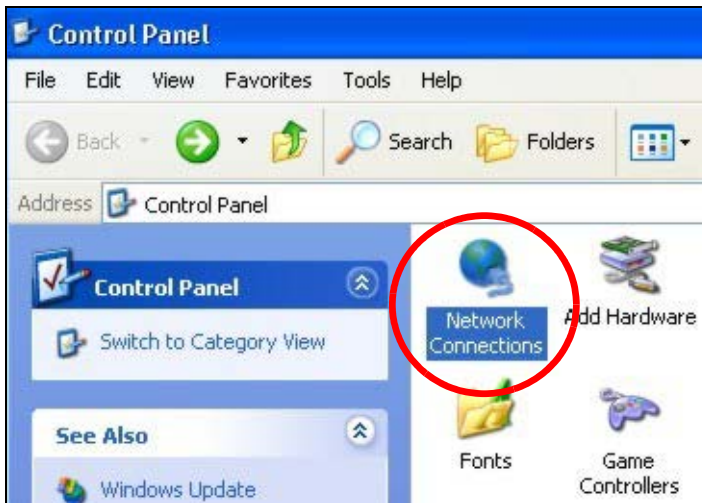
## Windows XP/NT/2000

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

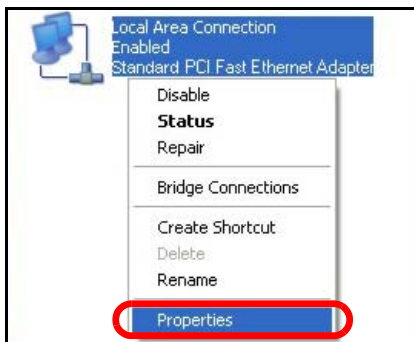
- 1 Click **Start** > **Control Panel**.



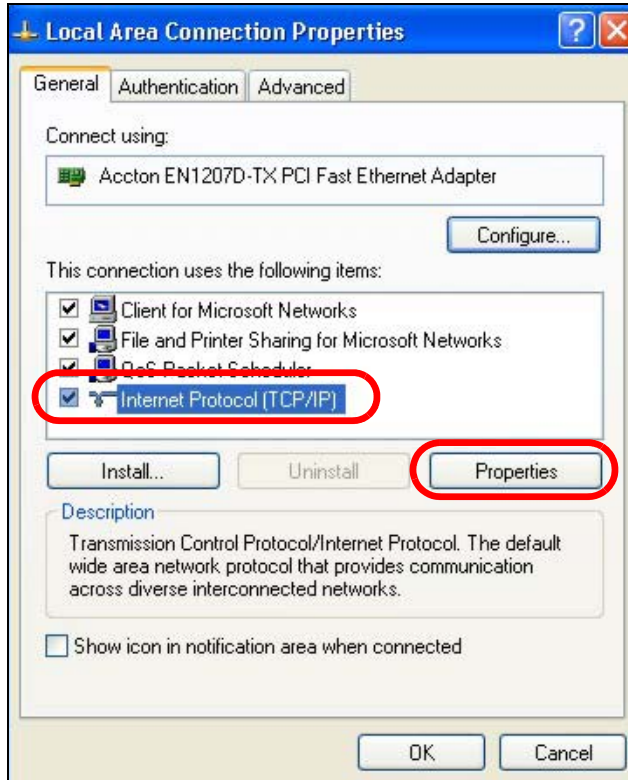
- 2 In the **Control Panel**, click the **Network Connections** icon.



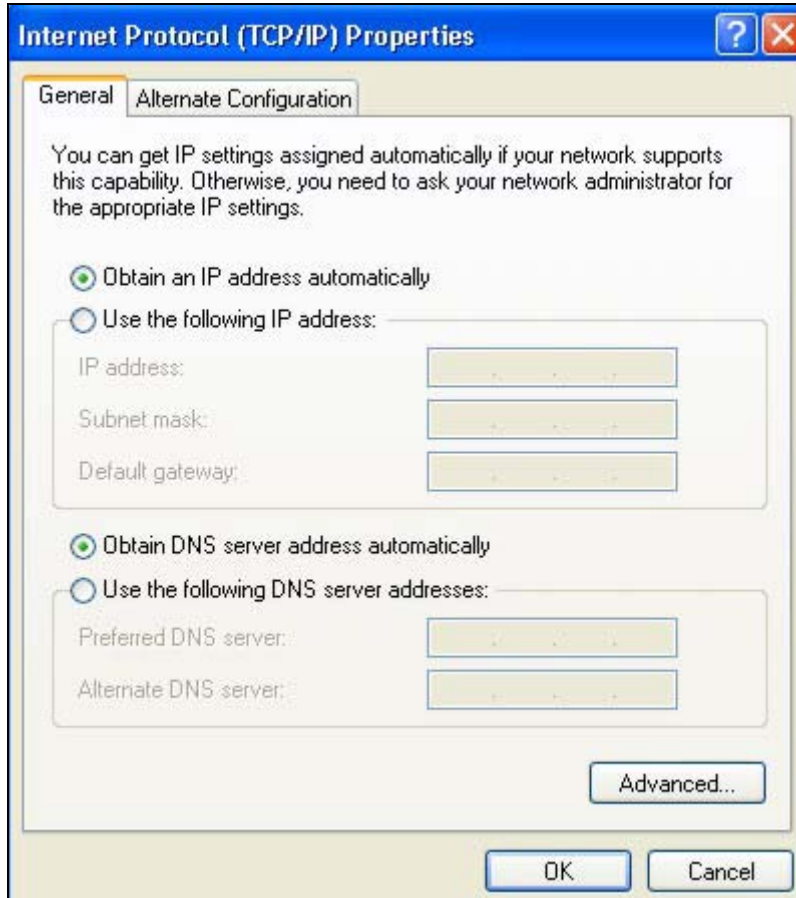
- 3 Right-click **Local Area Connection** and then select **Properties**.



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



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



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

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

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

## Verifying Settings

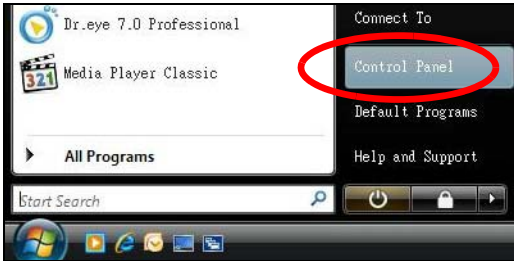
- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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

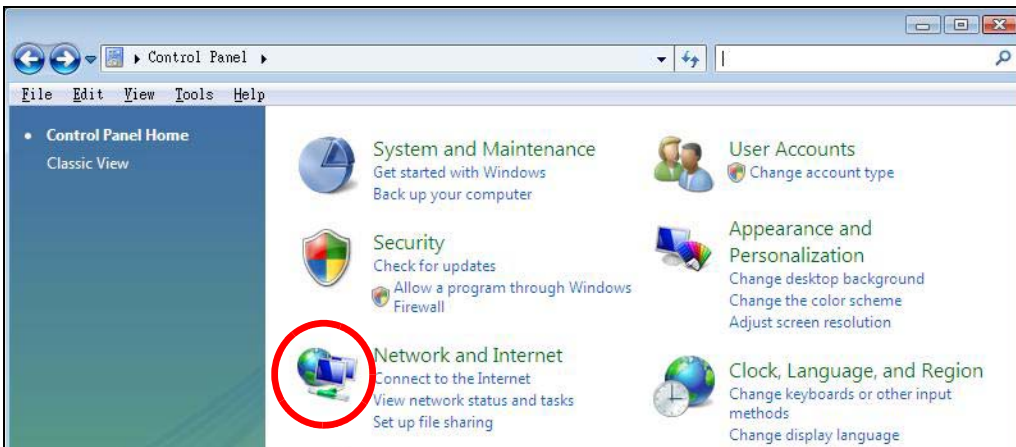
## Windows Vista

This section shows screens from Windows Vista Professional.

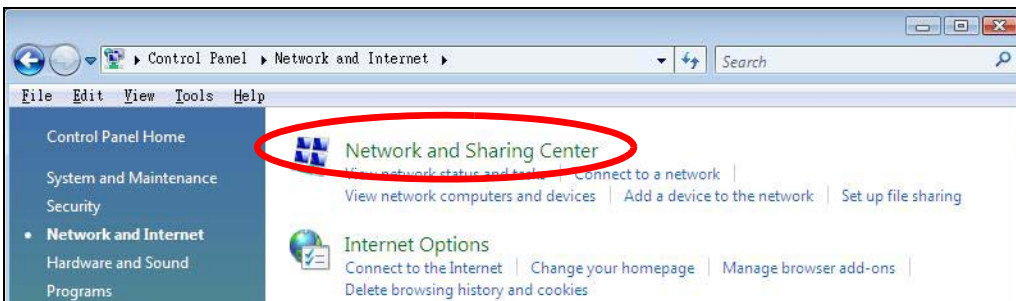
- 1 Click **Start > Control Panel**.



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

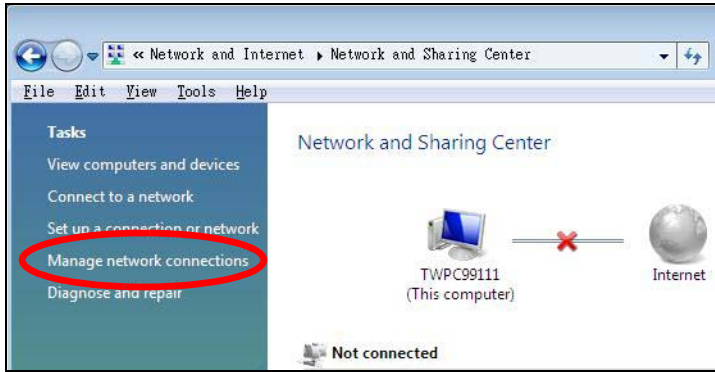


- 3 Click the **Network and Sharing Center** icon.



- 4 Click **Manage network connections**.



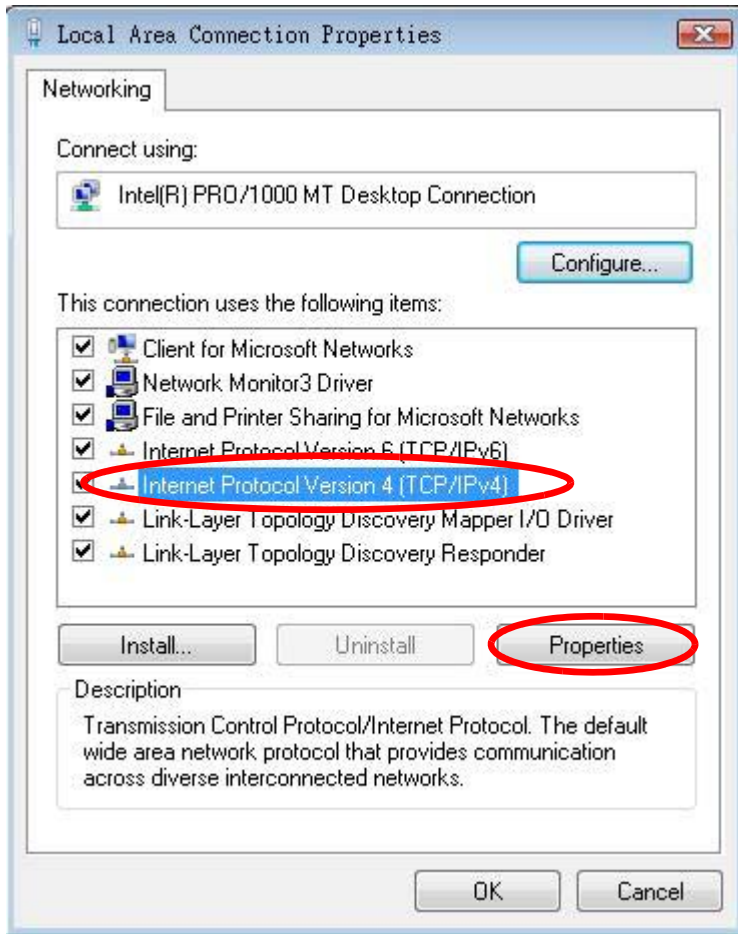


- 5 Right-click **Local Area Connection** and then select **Properties**.

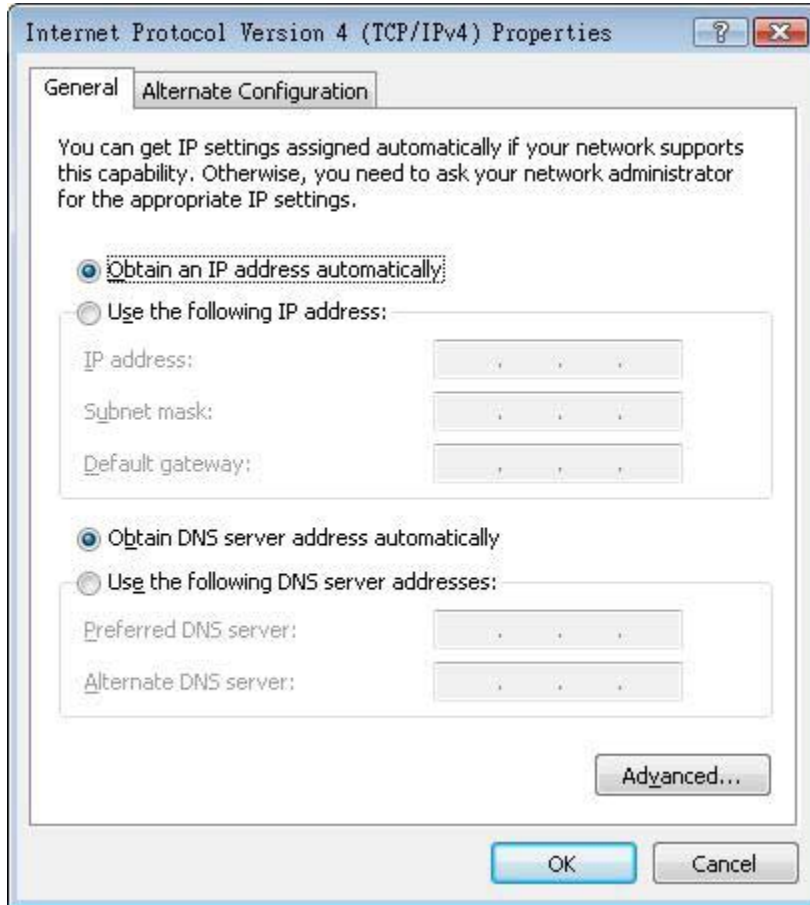


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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



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



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

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

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

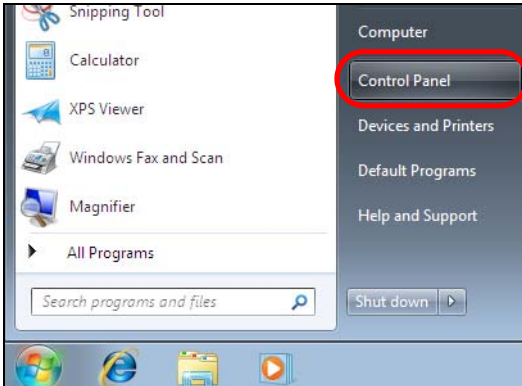
## Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].  
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

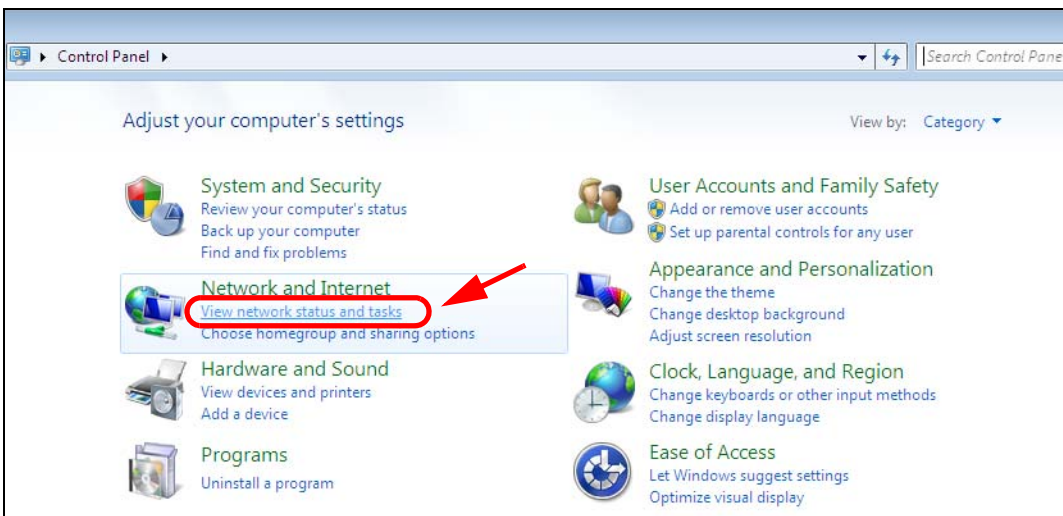
## Windows 7

This section shows screens from Windows 7 Enterprise.

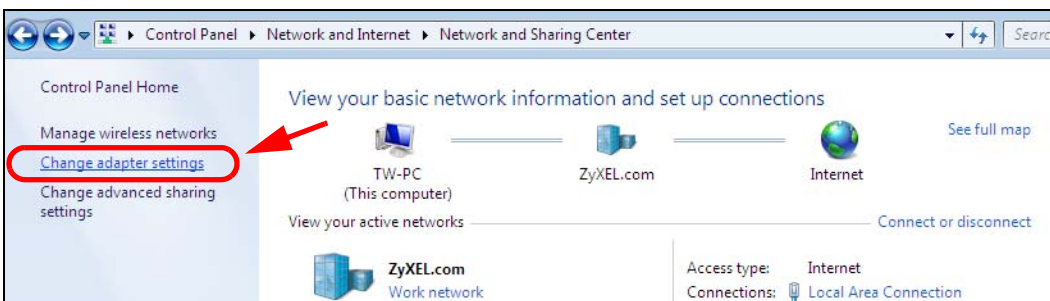
- 1 Click **Start > Control Panel**.



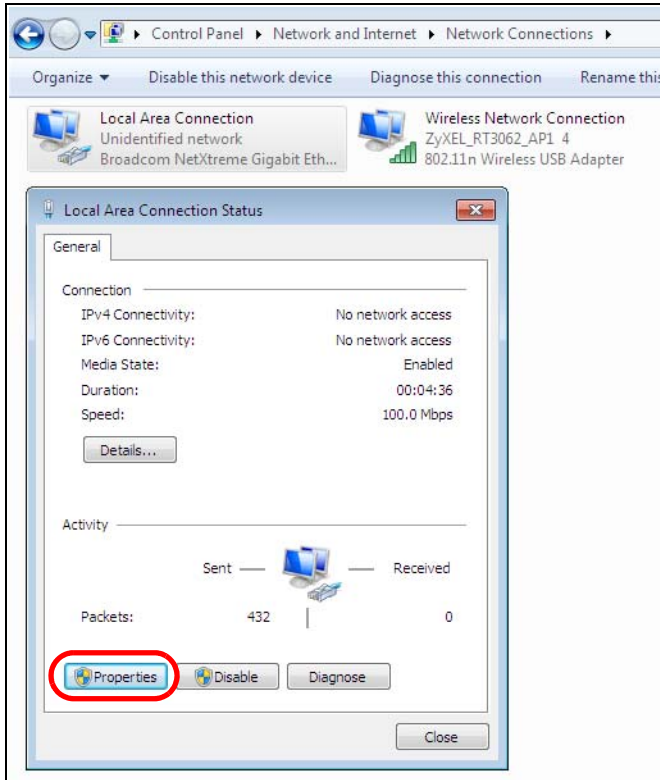
- 2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.



- 3 Click **Change adapter settings**.

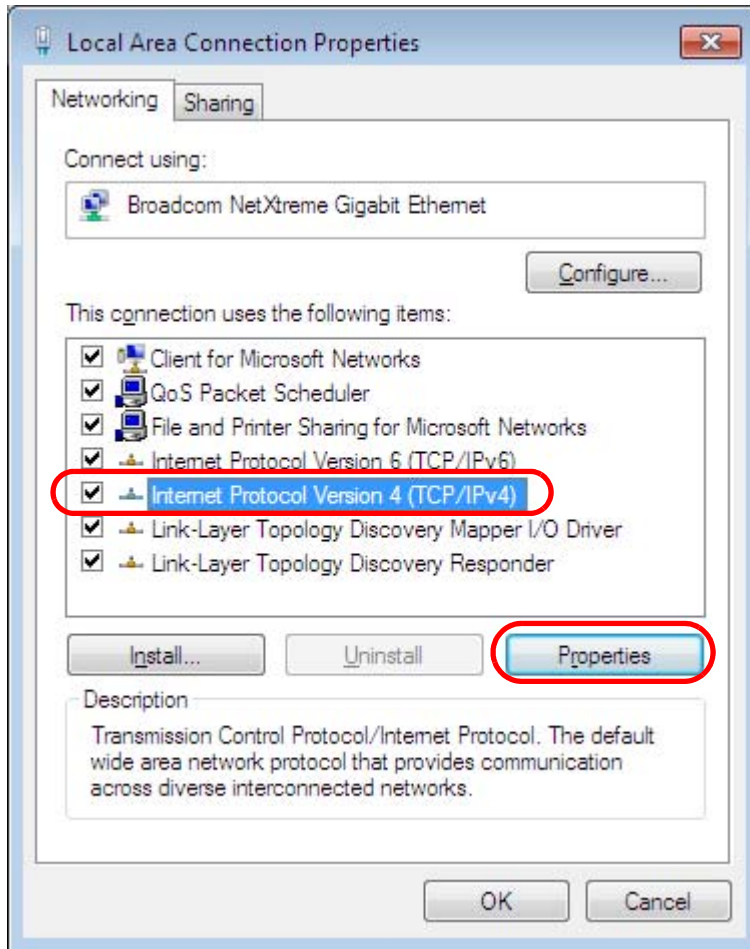


- 4 Double click **Local Area Connection** and then select **Properties**.

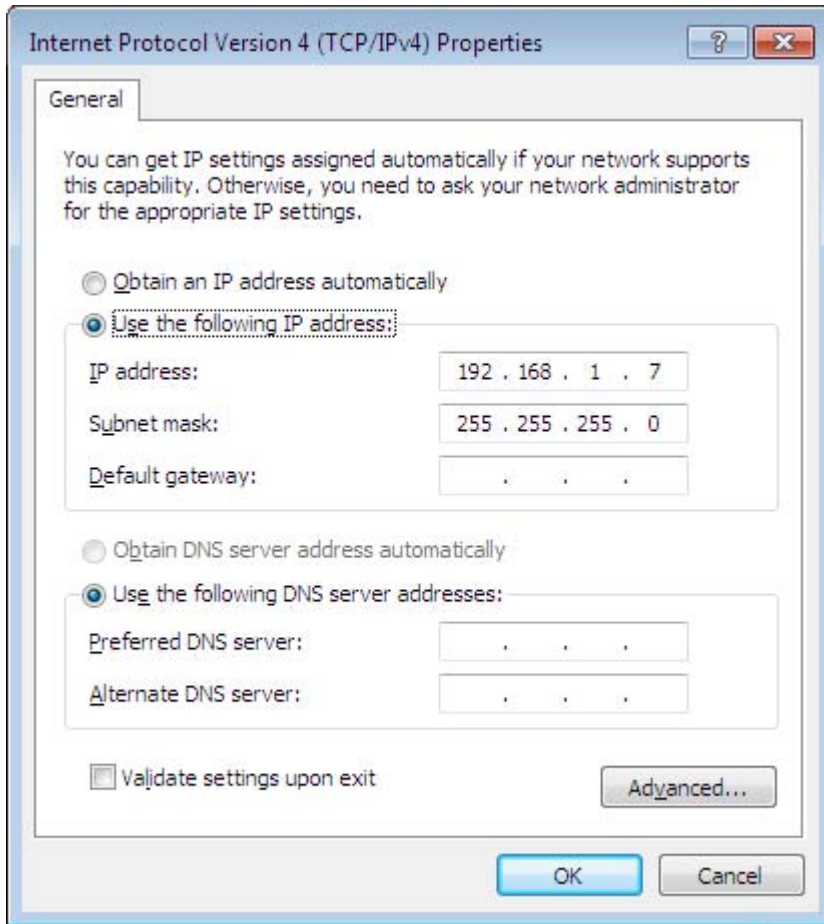


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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



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



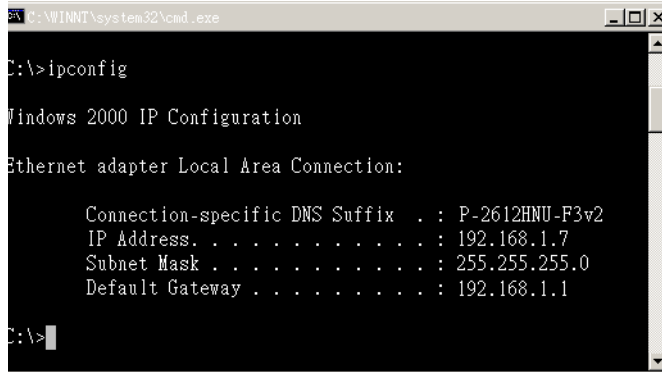
- 7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

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

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

## Verifying Settings

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



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

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

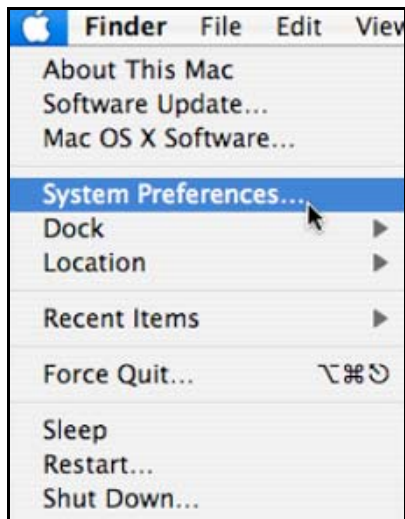
    Connection-specific DNS Suffix  . : P-2612HNU-F3v2
    IP Address. . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\>
```

## Mac OS X: 10.3 and 10.4

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

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

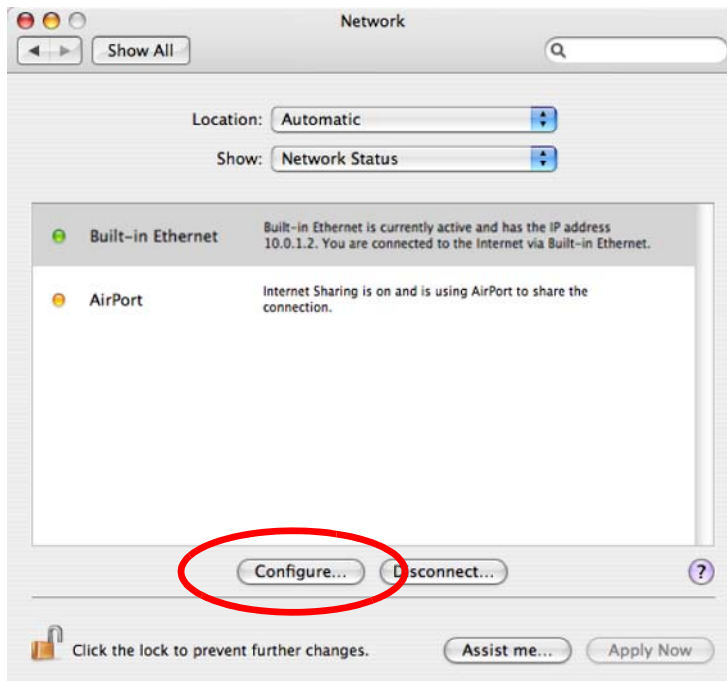


- 2 In the **System Preferences** window, click the **Network** icon.

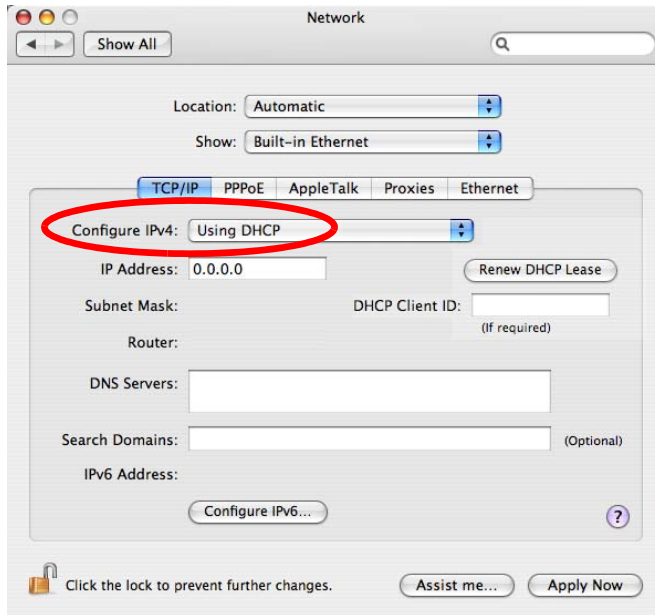




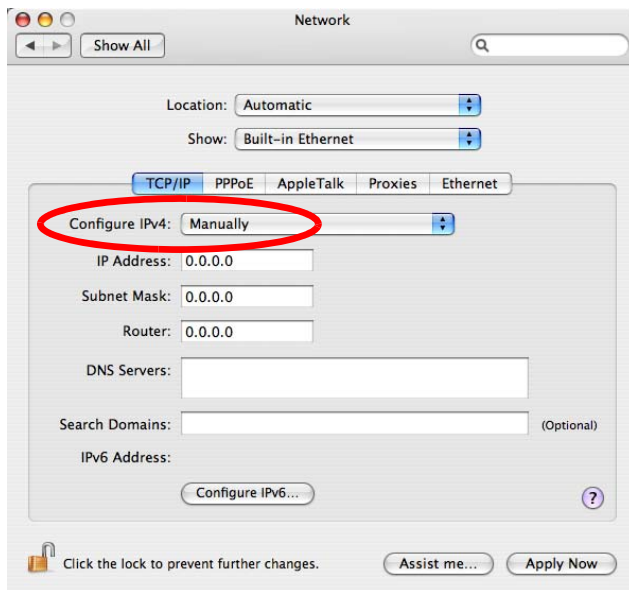
- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.



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



- 5 For statically assigned settings, do the following:
- From the **Configure IPv4** list, select **Manually**.
  - In the **IP Address** field, type your IP address.
  - In the **Subnet Mask** field, type your subnet mask.
  - In the **Router** field, type the IP address of your device.

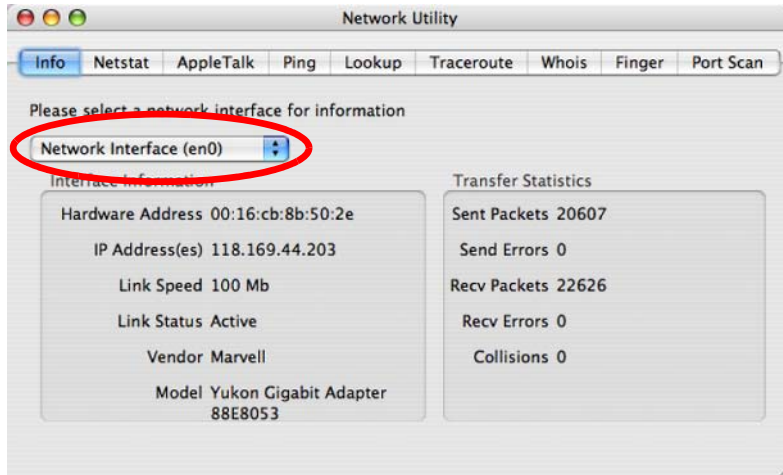


- 6 Click **Apply Now** and close the window.

## Verifying Settings

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

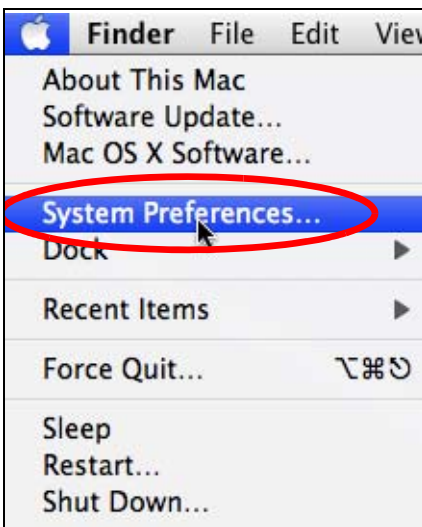
**Figure 142** Mac OS X 10.4: Network Utility



## Mac OS X: 10.5 and 10.6

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

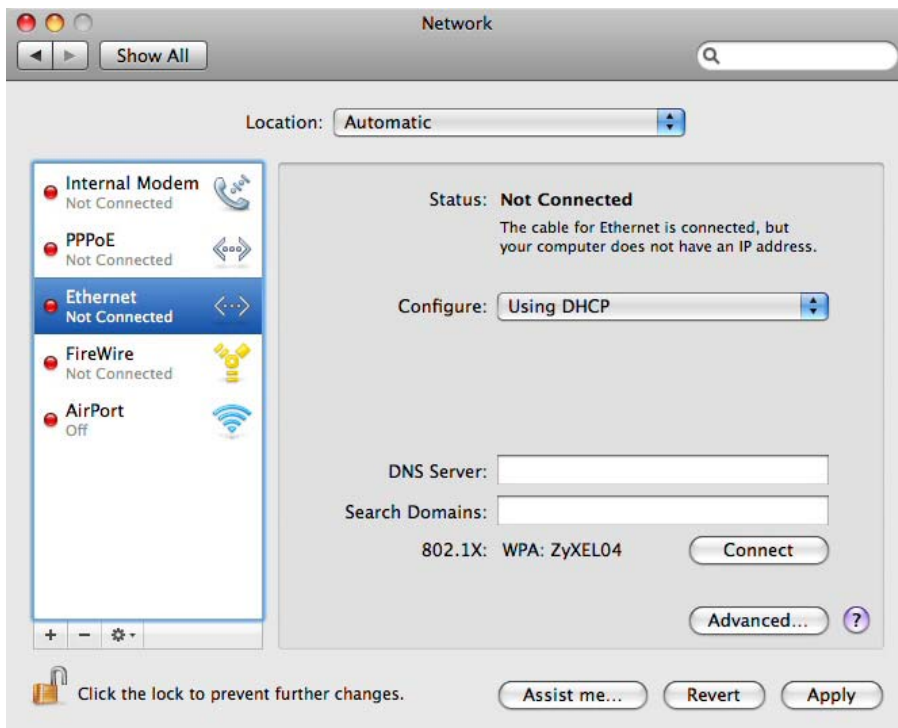
- 1 Click **Apple > System Preferences**.



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

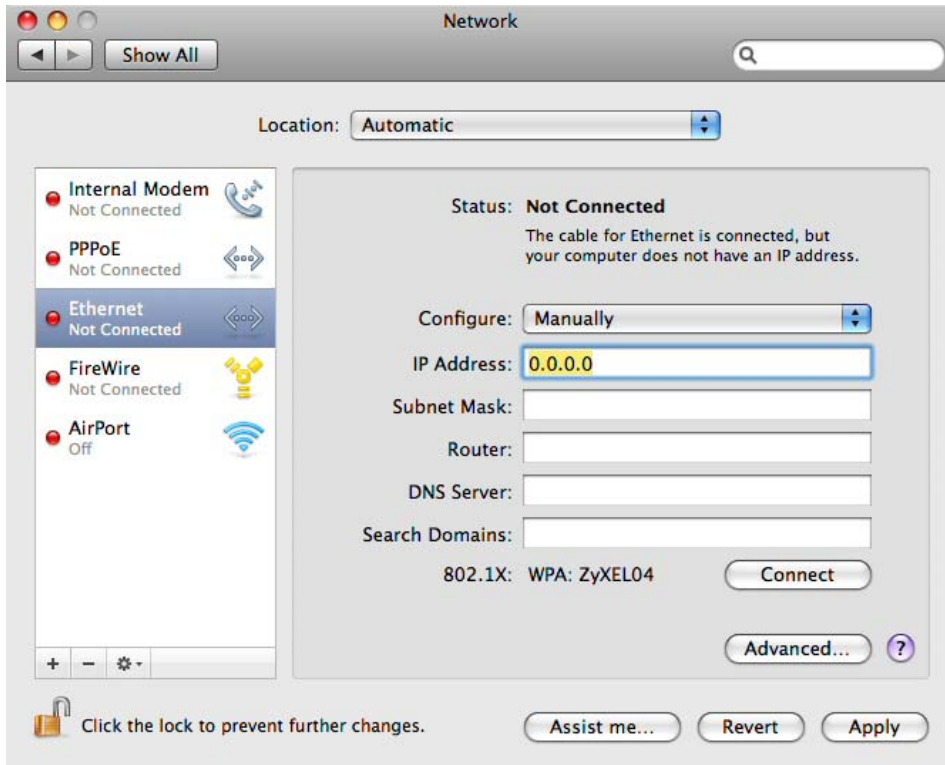


- 3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.



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

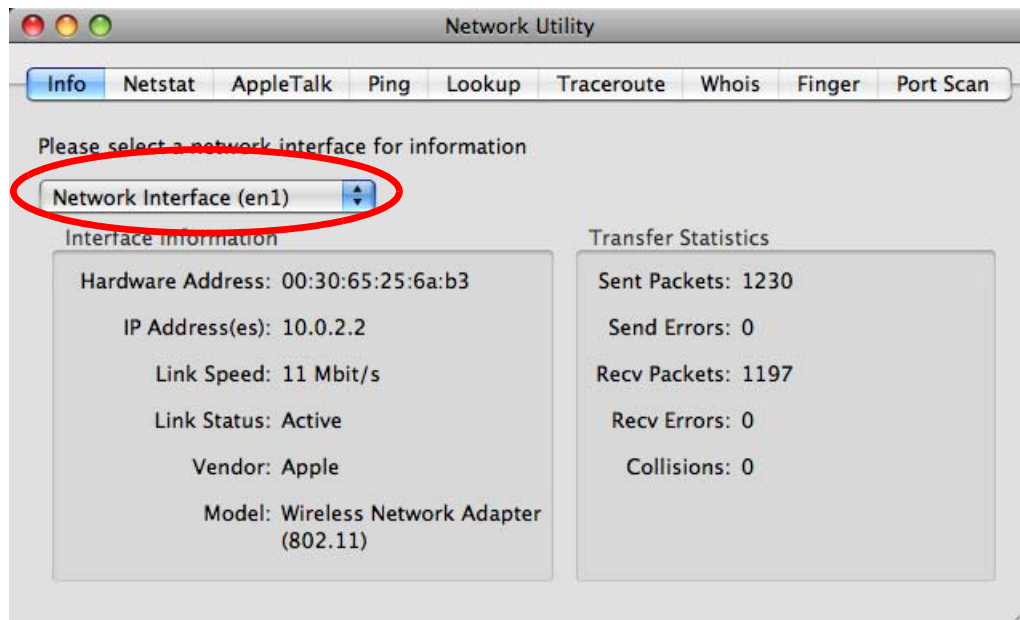
- 5 For statically assigned settings, do the following:
  - From the **Configure** list, select **Manually**.
  - In the **IP Address** field, enter your IP address.
  - In the **Subnet Mask** field, enter your subnet mask.
  - In the **Router** field, enter the IP address of your NBG6716.



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

## Verifying Settings

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

**Figure 143** Mac OS X 10.5: Network Utility

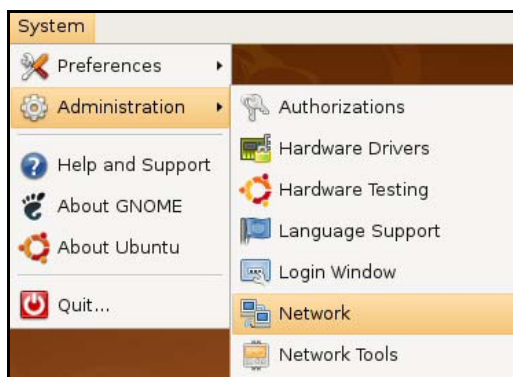
## Linux: Ubuntu 8 (GNOME)

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

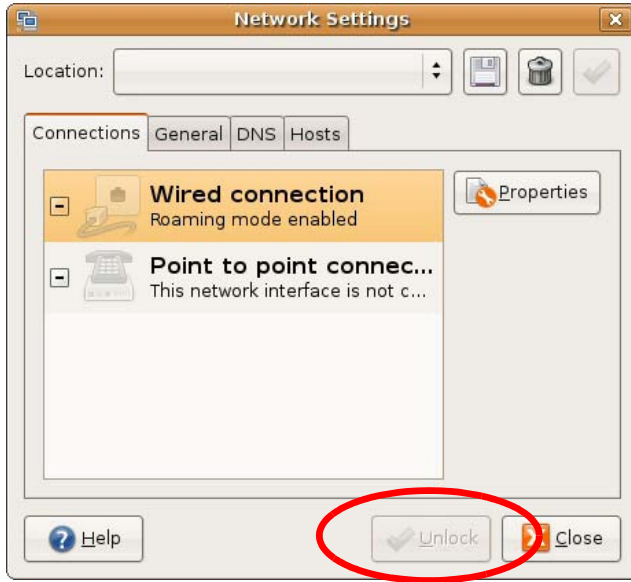
Note: Make sure you are logged in as the root administrator.

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

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



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

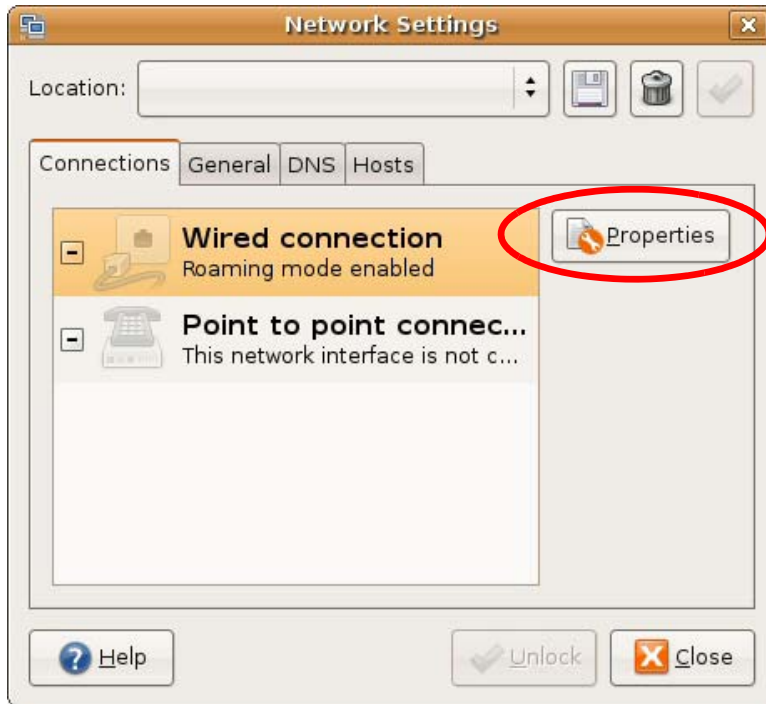


- 3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.



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





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



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

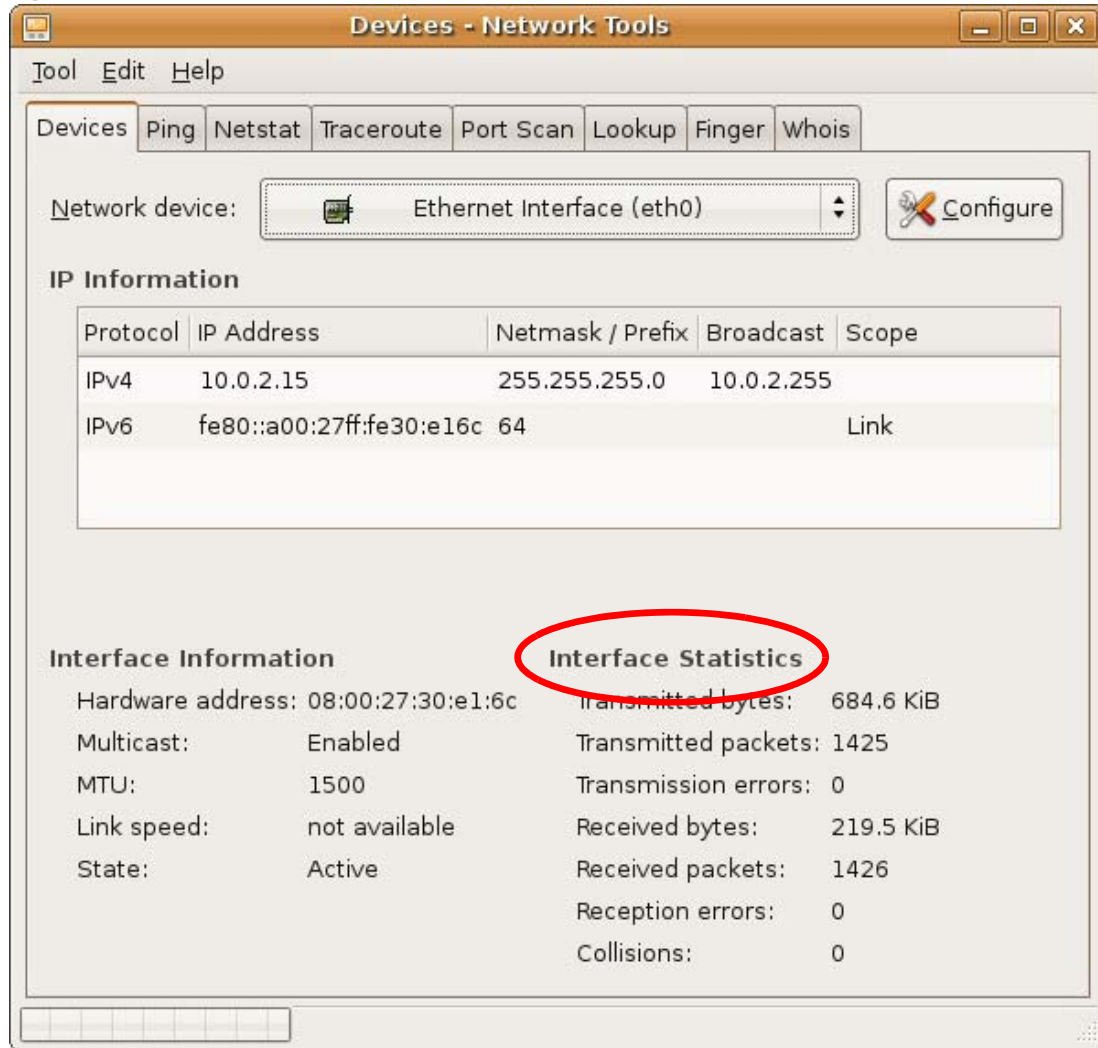




- 8 Click the **Close** button to apply the changes.

## Verifying Settings

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

**Figure 144** Ubuntu 8: Network Tools

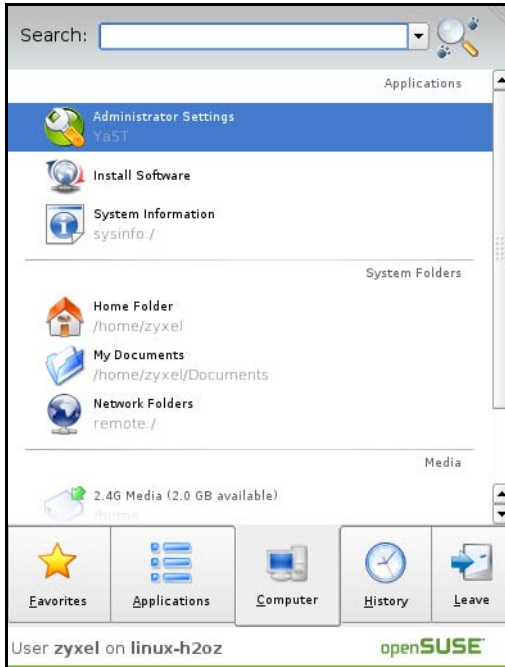
## Linux: openSUSE 10.3 (KDE)

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

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

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

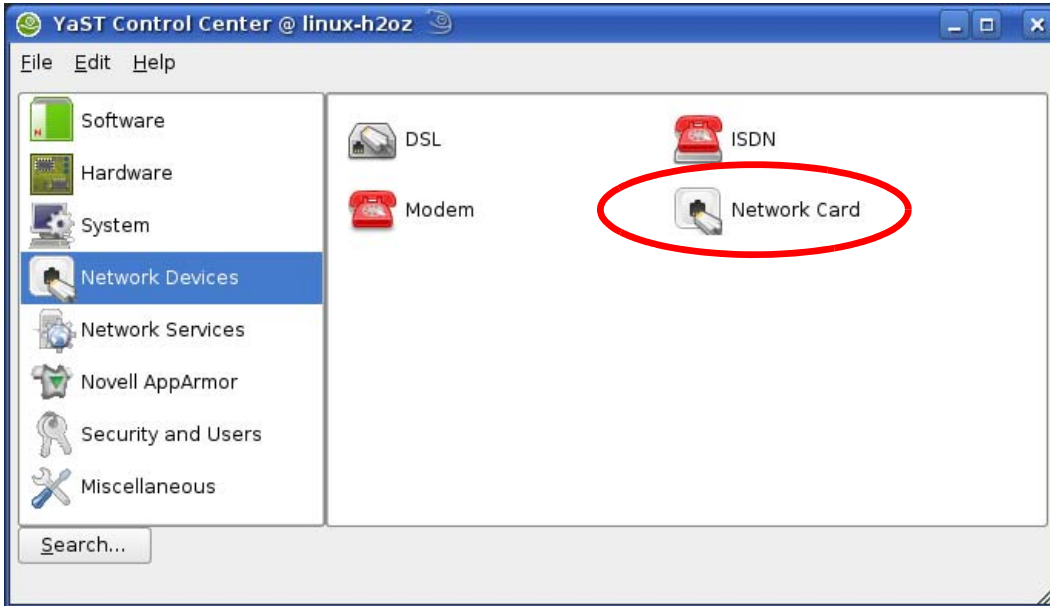
- 1 Click **K Menu > Computer > Administrator Settings (YaST)**.



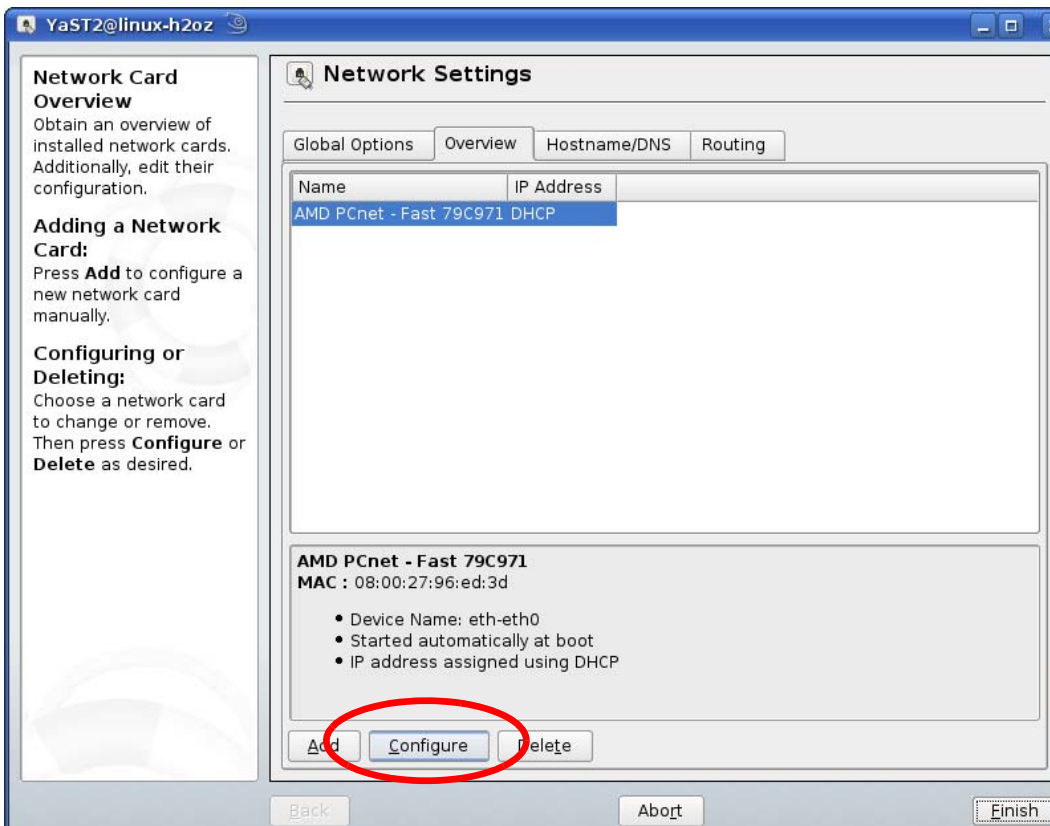
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.



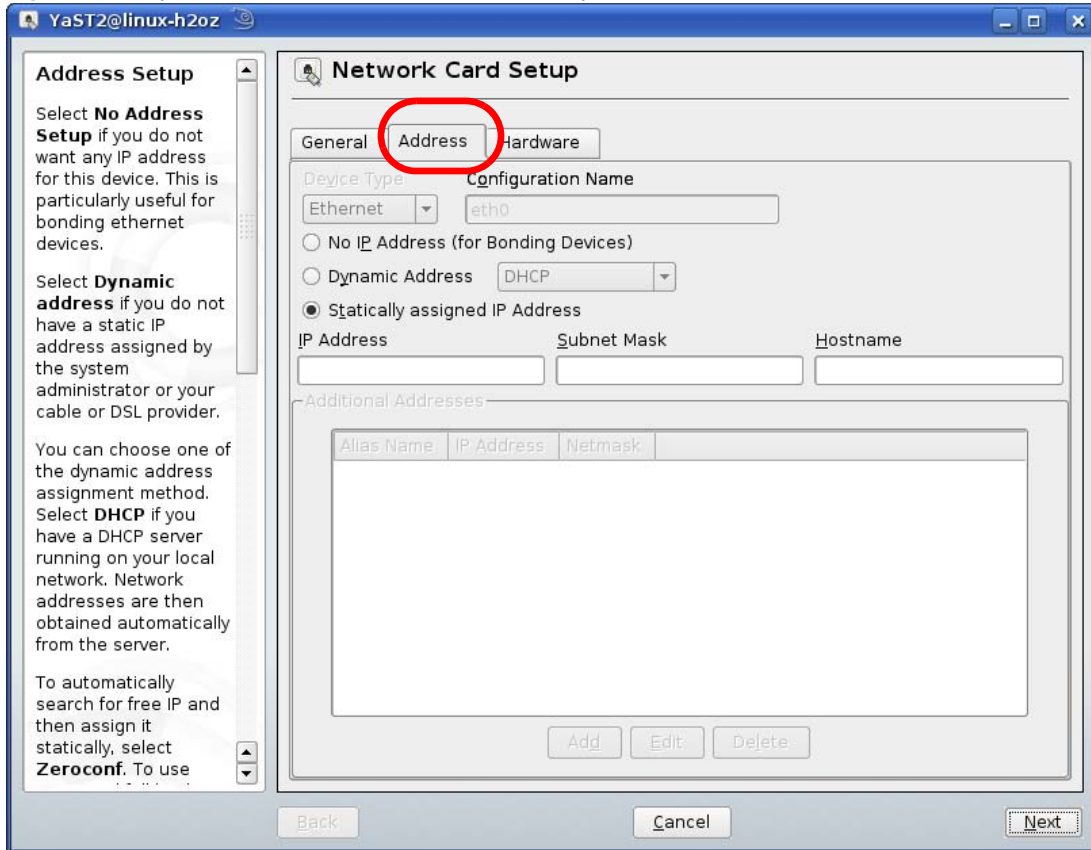
- 3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.



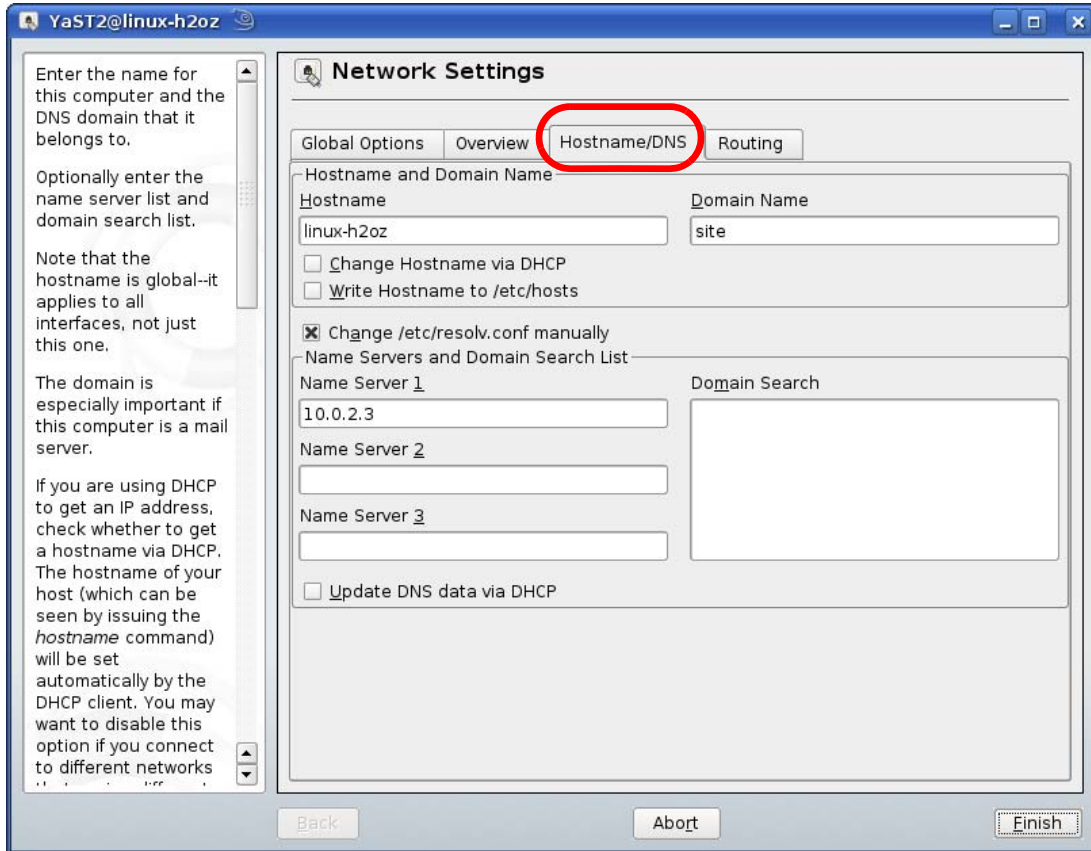
- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



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

**Figure 145** openSUSE 10.3: Network Card Setup

- 6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address. Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.
- 7 Click **Next** to save the changes and close the **Network Card Setup** window.
- 8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

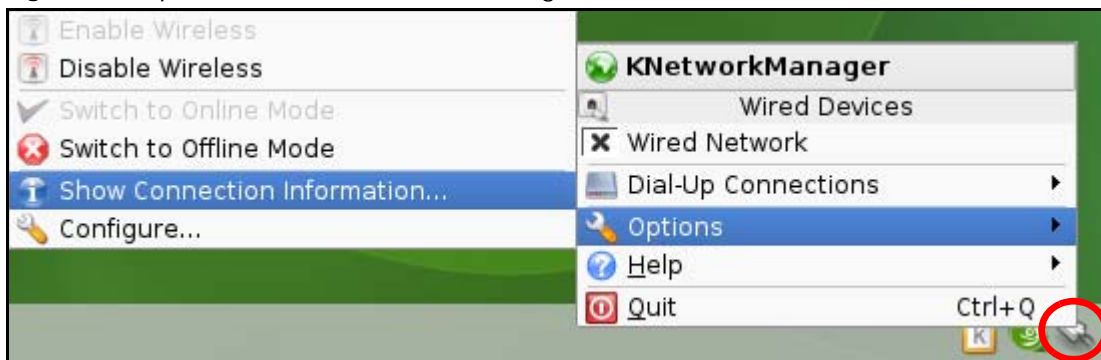


- 9 Click **Finish** to save your settings and close the window.

## Verifying Settings

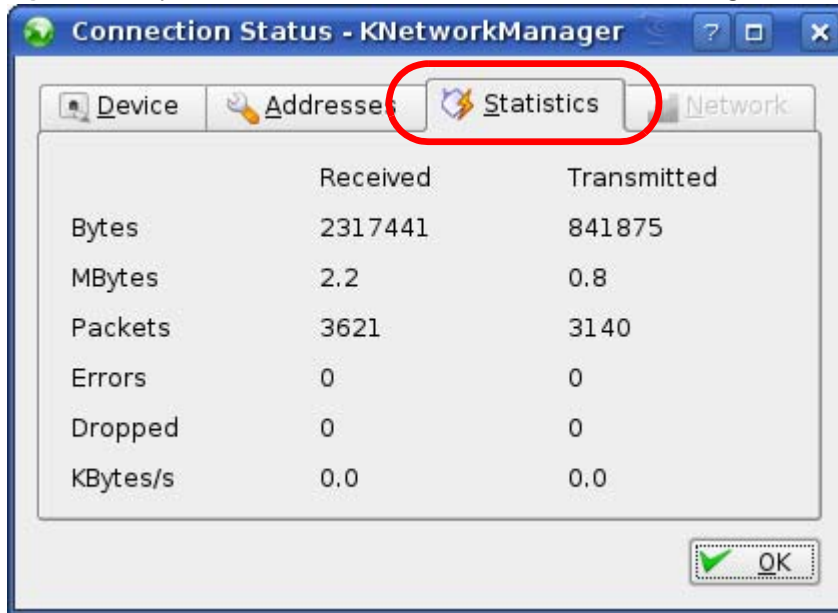
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

**Figure 146** openSUSE 10.3: KNetwork Manager



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

**Figure 147** openSUSE: Connection Status - KNetwork Manager



## Common Services

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

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

**Table 74** Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example <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.
H.323	TCP	1720	NetMeeting uses this protocol.



**Table 74** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.

**Table 74** Commonly Used Services (continued)

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

# Legal Information

## Copyright

Copyright © 2013 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

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 Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.



### FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b, 802.11g or 802.11n (20MHz) operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. IEEE 802.11n (40MHz) operation of this product in the U.S.A. is firmware-limited to channels 3 through 9.
- 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.
- Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.
- Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

### Industry Canada Statement

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

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

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

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

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

### IC Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

**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。

在 5.25 - 5.35 GHz 頻帶內操作之無線資訊傳輸設備，限於室內使用。

**Notices**

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

This 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**

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

**ZyXEL Limited Warranty**

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

**Note**

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

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at [http://www.zyxel.com/web/support\\_warranty\\_info.php](http://www.zyxel.com/web/support_warranty_info.php).

**Registration**

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

**Open Source Licenses**

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at [www.zyxel.com](http://www.zyxel.com). To obtain the source code covered under those Licenses, please contact [support@zyxel.com.tw](mailto:support@zyxel.com.tw) to get it.

**Regulatory Information****European Union**

The following information applies if you use the product within the European Union.

**Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)**

Compliance Information for 2.4GHz and 5GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

[Czech]	ZyXEL tímto prohlašuje, že tento zařízen je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[German]	Hiermit erkläre ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΖΥΧΕΛ ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕC.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv egyéb előírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/EC.
[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 1999/5/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 1999/5/EC.



### National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesi menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Ausnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2, 4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "Overview of Regulatory Requirements for Wireless LANs":

Overview of Regulatory Requirements for Wireless LANs			
Frequency Band (MHz)	Max Power Level (EIRP) <sup>1</sup> (mW)	Indoor ONLY	Indoor and Outdoor
2400-2483.5	100		✓
5150-5350	200	✓	
5470-5725	1000		✓

**Belgium**

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check <http://www.bipt.be> for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie <http://www.bipt.be> voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez <http://www.ibpt.be> pour de plus amples détails.

**Denmark**

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

**Italy**

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check <http://www.sviluppoeconomico.gov.it/> for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare <http://www.sviluppoeconomico.gov.it/> per maggiori dettagli.

**Latvia**

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check <http://www.esd.lv> for more details.

2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: <http://www.esd.lv>.

**Notes:**

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.
2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

**List of national codes**

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Malta	MT
Belgium	BE	Netherlands	NL
Cyprus	CY	Poland	PL
Czech Republic	CR	Portugal	PT
Denmark	DK	Slovakia	SK
Estonia	EE	Slovenia	SI
Finland	FI	Spain	ES
France	FR	Sweden	SE
Germany	DE	United Kingdom	GB
Greece	GR	Iceland	IS
Hungary	HU	Liechtenstein	LI
Ireland	IE	Norway	NO
Italy	IT	Switzerland	CH
Latvia	LV	Bulgaria	BG
Lithuania	LT	Romania	RO
Luxembourg	LU	Turkey	TR

**Safety Warnings**

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.

- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

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



# Index

## A

ActiveX [136](#)  
 Address Assignment [77](#)  
 AP [13](#)  
 AP Mode  
   menu [54](#)  
   status screen [52](#)  
 AP+Bridge [13](#)

## B

Bridge/Repeater [13](#)

## C

certifications [224](#)  
   notices [225](#)  
   viewing [225](#)  
 Channel [45, 53](#)  
 channel [85](#)  
 CIFS [158](#)  
 Common Internet File System, see CIFS  
 Configuration  
   restore [171](#)  
 content filtering [135](#)  
   by keyword (in URL) [135](#)  
 Cookies [136](#)  
 copyright [224](#)  
 CPU usage [46, 53](#)

## D

Daylight saving [169](#)  
 DDNS [125](#)  
   see also Dynamic DNS

  service providers [125](#)  
 DHCP [72, 110](#)  
   DHCP server  
     see also Dynamic Host Configuration Protocol  
 DHCP server [108, 110](#)  
 Digital Living Network Alliance [157](#)  
 disclaimer [224](#)  
 DLNA [156, 157](#)  
   indexing [159](#)  
   overview [156](#)  
   rescan [159](#)  
 DLNA-compliant client [157](#)  
 DNS [112](#)  
 DNS Server [77](#)  
 DNS server [112](#)  
 documentation  
   related [2](#)  
 Domain Name System [112](#)  
 Domain Name System. See DNS.  
 duplex setting [46, 54](#)  
 Dynamic DNS [125](#)  
 Dynamic Host Configuration Protocol [110](#)  
 DynDNS [125](#)  
 DynDNS see also DDNS [125](#)

## E

encryption [86](#)  
   and local (user) database [87](#)  
   key [87](#)  
   WPA compatible [87](#)  
 ESSID [180](#)

## F

FCC interference statement [224](#)  
 file sharing [157](#)  
   access right [160, 162](#)



- bandwidth [162](#)
- example [162](#)
- FTP [161](#)
- overview [157](#)
- Samba [159](#)
- user account [160](#), [161](#)
- Windows Explorer [159](#)
- work group [159](#)

Firewall [131](#)

- Firewall overview
- guidelines [131](#)
- ICMP packets [132](#)
- network security
- Stateful inspection [131](#)
- ZyXEL device firewall [131](#)

firewall

- stateful inspection [130](#)

Firmware upload [169](#)

- file extension
- using HTTP

firmware version [45](#), [53](#)

## G

- General wireless LAN screen [89](#)
- Guest WLAN [87](#)
- Guest WLAN Bandwidth [88](#)
- Guide
  - Quick Start [2](#)

## I

- IGMP [78](#)
  - see also Internet Group Multicast Protocol
  - version
- IGMP version [78](#)
- Internet Group Multicast Protocol [78](#)
- IP Address [109](#), [118](#)
- IP alias [108](#)
- IP Pool [111](#)

## J

- Java [136](#)

## L

- LAN [107](#)
  - IP pool setup [110](#)
- LAN overview [107](#)
- LAN setup [107](#)
- LAN TCP/IP [110](#)
- Language [172](#)
- Link type [46](#), [54](#)
- local (user) database [86](#)
  - and encryption [87](#)
- Local Area Network [107](#)

## M

- MAC [100](#)
- MAC address [77](#), [86](#)
  - cloning [77](#)
- MAC address filter [86](#)
- MAC address filtering [100](#)
- MAC filter [100](#)
- managing the device
  - good habits [15](#)
  - using the web configurator. See web configurator.
  - using the WPS. See WPS.
- MBSSID [13](#)
- Media access control [100](#)
- media client [156](#)
- media file [156](#), [159](#)
  - type [159](#)
- media server [156](#)
  - overview [156](#)
- media file play [156](#)
- Memory usage [46](#), [53](#)
- mode [13](#)
- Multicast [78](#)
  - IGMP [78](#)

## N

- NAT [115, 118](#)
  - global [116](#)
  - how it works [117](#)
  - inside [116](#)
  - local [116](#)
  - outside [116](#)
  - overview [115](#)
  - port forwarding [122](#)
  - see also Network Address Translation
  - server [116](#)
  - server sets [122](#)
- NAT Traversal [150](#)
- Navigation Panel [46, 54](#)
- navigation panel [46, 54](#)
- Network Address Translation [115, 118](#)

## O

- operating mode [13](#)
- other documentation [2](#)

## P

- Point-to-Point Protocol over Ethernet [80](#)
- Pool Size [111](#)
- Port forwarding [118, 122](#)
  - default server [118, 122](#)
  - example [122](#)
  - local server [118](#)
  - port numbers
  - services
- port speed [46, 54](#)
- PPPoE [80](#)
  - dial-up connection
- product registration [225](#)

## Q

- Quality of Service (QoS) [102](#)
- Quick Start Guide [2](#)

## R

- RADIUS server [86](#)
- registration
  - product [225](#)
- related documentation [2](#)
- Remote management
  - and NAT [147](#)
  - limitations [146](#)
  - system timeout [147](#)
- Reset button [15](#)
- Reset the device [15](#)
- Restore configuration [171](#)
- Roaming [102](#)
- Router Mode
  - status screen [43](#)
- RTS/CTS Threshold [85, 102](#)

## S

- Samba [158](#)
- Scheduling [105](#)
- Server Message Block, see SMB
- Service and port numbers [134](#)
- Service Set [40, 89, 99](#)
- Service Set IDentification [40, 89, 99](#)
- Service Set IDentity. See SSID.
- SMB [158](#)
- SSID [40, 45, 53, 85, 89, 99](#)
- stateful inspection firewall [130](#)
- Static DHCP [111](#)
- Static Route [127](#)
- Status [43](#)
- StreamBoost [139](#)
  - automatic update [140](#)
  - bandwidth [139](#)
  - bandwidth and performance [144](#)
  - data rate [140](#)
  - device priority [142](#)
  - download traffic [143](#)
  - example [139](#)
  - maximum bandwidth [140](#)
  - overview [139](#)
  - QoS [139](#)

- top traffic flows [142](#)
- Subnet Mask [109](#)
- Summary
  - DHCP table [72](#)
  - Packet statistics [73](#)
  - Wireless station status [74](#)
- System General Setup [166](#)
- System restart [172](#)

## T

- TCP/IP configuration [110](#)
- Time setting [168](#)
- trademarks [224](#)
- trigger port [123](#)
- Trigger port forwarding [123](#)
  - example [123](#)
  - process [123](#)

## U

- Universal Plug and Play [150](#)
  - Application [150](#)
  - Security issues [150](#)
- UPnP [150](#)
- URL Keyword Blocking [136](#)
- USB media sharing [156](#)
- user authentication [86](#)
  - local (user) database [86](#)
  - RADIUS server [86](#)
- User Name [126](#)

## W

- Wake On LAN [148](#)
- WAN (Wide Area Network) [76](#)
- WAN MAC address [77](#)
- warranty [225](#)
  - note [225](#)
- Web Configurator
  - how to access [28](#)
  - Overview [28](#)

- web configurator [14](#)
- Web Proxy [136](#)
- WEP Encryption [93, 95](#)
- WEP encryption [92](#)
- WEP key [92](#)
- windows media player [156](#)
- Wireless association list [74](#)
- wireless channel [180](#)
- wireless LAN [180](#)
- wireless LAN scheduling [105](#)
- Wireless network
  - basic guidelines [85](#)
  - channel [85](#)
  - encryption [86](#)
  - example [84](#)
  - MAC address filter [86](#)
  - overview [84](#)
  - security [85](#)
  - SSID [85](#)
- Wireless security [85](#)
  - overview [85](#)
  - type [85](#)
- wireless security [180](#)
- Wireless tutorial [57](#)
- Wizard setup [19](#)
- WLAN button [15](#)
- WoL [148](#)
- work group [158](#)
  - name [158](#)
  - Windows [158](#)
- WPA compatible [87](#)
- WPS [14](#)