

# Remote Management

## 13.1 Overview

This chapter provides information on the **Remote Management** screens.

Remote management allows you to determine which services/protocols can access which NBG-418N interface (if any) from which computers.

You may manage your NBG-418N from a remote location via:

- LAN only
- LAN and WAN

**Note:** When you configure remote management to allow management from the LAN and WAN in the options above, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

## 13.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 You have disabled that service in one of the remote management screens.
- 2 The IP address in the **Secured Client WAN IP Address** field does not match the client IP address. If it does not match, the NBG-418N will disconnect the session immediately.
- 3 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- 4 There is a firewall rule that blocks it.

## 13.1.2 Remote Management and NAT

When NAT is enabled:

- Use the NBG-418N's WAN IP address when configuring from the WAN.
- Use the NBG-418N's LAN IP address when configuring from the LAN.

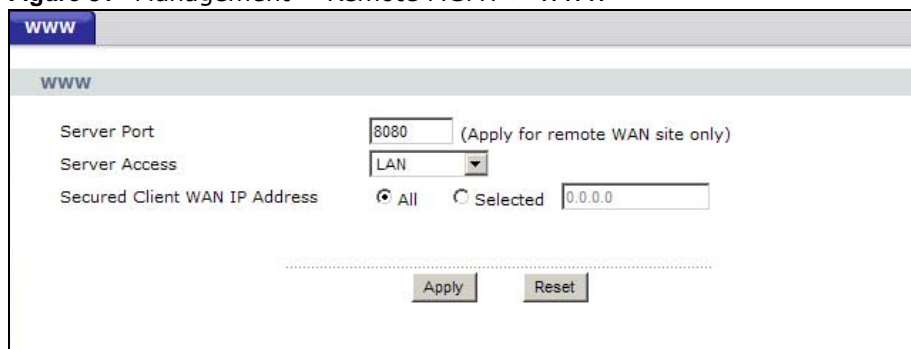
## 13.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The NBG-418N automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen.

## 13.2 WWW Screen

To change your NBG-418N's World Wide Web settings, click **Management > Remote MGMT** to display the **WWW** screen.

**Figure 81** Management > Remote MGMT > WWW



The screenshot shows the 'WWW' configuration screen. At the top, there is a blue header with 'WWW' in white. Below the header, the page title 'WWW' is displayed in a light blue bar. The main content area contains three configuration fields: 'Server Port' with a text input field containing '8080' and a note '(Apply for remote WAN site only)'; 'Server Access' with a dropdown menu currently set to 'LAN'; and 'Secured Client WAN IP Address' with radio buttons for 'All' (selected) and 'Selected', followed by a text input field containing '0.0.0.0'. At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

**Table 51** Management > Remote MGMT > WWW

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NBG-418N using this service.
Secured Client WAN IP Address	A secured client is a "trusted" computer that is allowed to communicate with the NBG-418N using this service.  Select <b>All</b> to allow any computer to access the NBG-418N using this service.  Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the NBG-418N using this service.  <b>Note: This only applies on WAN IP.</b>
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# Universal Plug-and-Play (UPnP)

## 14.1 Overview

This chapter introduces the UPnP feature in the Web Configurator.

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

## 14.2 What You Need to Know

### How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

### NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

### Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the NBG-418N allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

## 14.3 Configuring UPnP

Use this screen to enable UPnP. Click the **Management > UPnP** to open the following screen.

**Figure 82** Management > UPnP > General

The following table describes the labels in this screen.

**Table 52** Management > UPnP > General

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the NBG-418N's IP address (although you must still enter the password to access the Web Configurator).
Allow users to make port forwarding changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the NBG-418N so that they can communicate through the NBG-418N, for example, by using NAT traversal. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device. this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click <b>Apply</b> to save the setting to the NBG-418N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 14.3.1 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the NBG-418N.

Make sure the computer is connected to a LAN port of the NBG-418N. Turn on your computer and the NBG-418N.

#### 14.3.1.1 Auto-discover Your UPnP-enabled Network Device

- 1 Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

- 2 Right-click the icon and select **Properties**.

**Figure 83** Network Connections



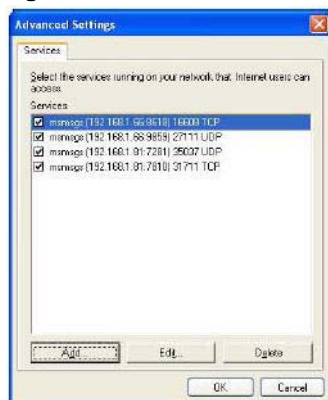
- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

**Figure 84** Internet Connection Properties

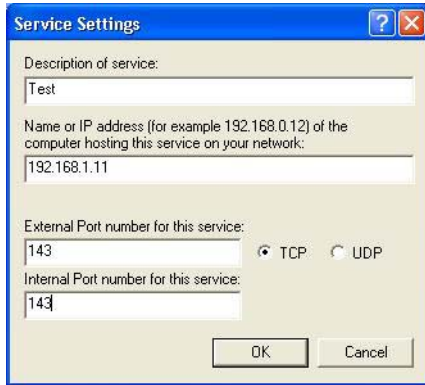


- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

**Figure 85** Internet Connection Properties: Advanced Settings



**Figure 86** Internet Connection Properties: Advanced Settings: Add



Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

- 5 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

**Figure 87** System Tray Icon



- 6 Double-click on the icon to display your current Internet connection status.

**Figure 88** Internet Connection Status



### 14.3.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the NBG-418N without finding out the IP address of the NBG-418N first. This comes helpful if you do not know the IP address of the NBG-418N.

Follow the steps below to access the Web Configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.



3 Select **My Network Places** under **Other Places**.

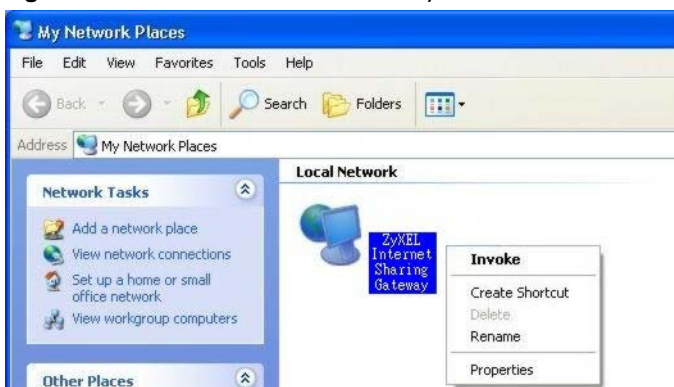
**Figure 89** Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your NBG-418N and select **Invoke**. The Web Configurator login screen displays.

**Figure 90** Network Connections: My Network Places





## 15.1 Overview

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

See the chapter about wizard setup for more information on the next few screens.

## 15.2 What You Can Do

- Use the **General** screen to enter a name to identify the NBG-418N in the network and set the password ([Section 15.3 on page 125](#)).
- Use the **Time Setting** screen to change your NBG-418N's time and date ([Section 15.4 on page 126](#)).

## 15.3 System General Screen

Use this screen to enter a name to identify the NBG-418N in the network and set the password. Click **Maintenance > System**. The following screen displays.

**Figure 91** Maintenance > System > General

The screenshot shows a web interface for system configuration. At the top, there are two tabs: 'General' (selected) and 'Time Setting'. Below the tabs is a 'System Setup' section with three input fields: 'System Name' (containing 'NBG-418N'), 'Domain Name' (containing 'zyxel.com'), and 'Administrator Inactivity Timer' (containing '30' with a note '(minutes, 0 means no timeout)'). Below this is a 'Password Setup' section with three password input fields: 'Old Password', 'New Password', and 'Retype to Confirm', each containing four dots. At the bottom of the form are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

**Table 53** Maintenance > System > General

LABEL	DESCRIPTION
System Setup	
System Name	System Name is a unique name to identify the NBG-418N in an Ethernet network. It is recommended you enter your computer's "Computer name" in this field (see the chapter about wizard setup for how to find your computer's name).  This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP.  The domain name entered by you is given priority over the ISP assigned domain name.
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).
Password Setup	Change your NBG-418N'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 NBG-418N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 15.4 Time Setting Screen

To change your NBG-418N's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown. Use this screen to configure the NBG-418N's time based on your local time zone.

**Figure 92** Maintenance > System > Time Setting

The following table describes the labels in this screen.

**Table 54** Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NBG-418N. Each time you reload this page, the NBG-418N synchronizes the time with the time server.
Current Date	This field displays the date of your NBG-418N. Each time you reload this page, the NBG-418N synchronizes the date with the time server.
Time and Date Setup	
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.
Copy Your Computer's Time Settings	Click this to copy the time settings of your computer into the NBG-418N's time and date setup.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new time in this field and then click <b>Apply</b> .

**Table 54** Maintenance > System > Time Setting (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 set <b>Time and Date Setup</b> to <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 NBG-418N get the time and date from the time server you specified below.
Auto	Select <b>Auto</b> to have the NBG-418N automatically search for an available time server and synchronize the date and time with the time server after you click <b>Apply</b> .
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>o'clock</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 first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>First, Sunday, April</b> and type 2 in the <b>o'clock</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 type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected <b>Daylight Savings</b> . The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:  Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Last, Sunday, October</b> and type 2 in the <b>o'clock</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 type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click <b>Apply</b> to save your changes back to the NBG-418N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.1 Overview

This chapter contains information about configuring general log settings and viewing the NBG-418N's logs.

The Web Configurator allows you to look at all of the NBG-418N's logs in one location.

## 16.2 What You Need to Know

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

## 16.3 View Log Screen

Use the **View Log** screen to see the logged messages for the NBG-418N. Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, Java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Click **Maintenance > Logs** to open the **View Log** screen.

**Figure 93** Maintenance > Logs > View Log

View Log		
Logs		
<input type="button" value="Refresh"/> <input type="button" value="Clear Logs"/> <input type="button" value="First"/> <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Last"/> <span style="float: right;">1/7</span>		
#	Time	Message
1	Jan 1 00:00:04	started: BusyBox v1.17.3
2	Jan 1 00:00:04	Syslog daemon successfully started
3	Jan 1 00:00:07	Start WAN SETUP: wkmode=router wan_hwname=eth1 protocol=dhcp method=BOOT
4	Jan 1 00:00:07	Finish WAN SETUP: wkmode=router wan_hwname=eth1 protocol=dhcp method=BOOT
5	Jan 1 00:00:07	started, version 2.55 cachesize 150
6	Jan 1 00:00:07	compile time options: no-IPv6 GNU-getopt no-DBus no-I18N DHCP no-scripts no-TFTP
7	Jan 1 00:00:07	DHCP, IP range 192.168.1.33 -- 192.168.1.132, lease time 24m
8	Jan 1 00:00:07	reading /tmp/resolv.dnsmasq
9	Jan 1 00:00:07	using nameserver 4.2.2.4#53
10	Jan 1 00:00:07	using nameserver 156.154.70.1#53
11	Jan 1 00:00:07	using nameserver 168.126.63.1#53
12	Jan 1 00:00:07	read /etc/hosts - 0 addresses
13	Jan 1 00:00:07	read /tmp/hosts - 0 addresses
14	Jan 1 05:19:16	DHCPDISCOVER(br0) 172.23.26.4 00:24:21:7e:20:96
15	Jan 1 05:19:16	DHCPOFFER(br0) 192.168.1.83 00:24:21:7e:20:96
16	Jan 1 05:19:16	DHCPREQUEST(br0) 192.168.1.83 00:24:21:7e:20:96
17	Jan 1 05:19:16	DHCPACK(br0) 192.168.1.83 00:24:21:7e:20:96 twpc13774-02
18	Jan 1 05:19:16	Ignoring domain ZyXEL.com for DHCP host name twpc13774-02
19	Jan 1 05:33:50	DHCPREQUEST(br0) 172.23.26.4 00:24:21:7e:20:96
20	Jan 1 05:33:50	DHCPNAK(br0) 172.23.26.4 00:24:21:7e:20:96 lease not found

The following table describes the labels in this screen.

**Table 55** Maintenance > Logs > View Log

LABEL	DESCRIPTION
Refresh	Click <b>Refresh</b> to renew the log screen.
Clear Logs	Click <b>Clear Logs</b> to delete all the logs.
Next	Click <b>Next</b> to show the next page of log entries.
Last	Click <b>Last</b> to show the last page of log entries.
#	This is the index number of the log entry.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the NBG-418N's time and date.
Message	This field states the reason for the log.



## 17.1 Overview

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the NBG-418N.

## 17.2 What You Can Do

- Use the **Firmware** screen to upload firmware to your NBG-418N ([Section 17.3 on page 131](#)).
- Use the **Configuration** screen to view information related to factory defaults, backup configuration, and restoring configuration ([Section 17.4 on page 133](#)).
- Use the **Restart** screen to have the NBG-418N reboot ([Section 17.5 on page 134](#)).

## 17.3 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., “NBG-418N.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 > Tools**. Follow the instructions in this screen to upload firmware to your NBG-418N.

**Figure 94** Maintenance > Tools > Firmware

The screenshot shows a web interface with three tabs: **Firmware**, **Configuration**, and **Restart**. The **Firmware** tab is active. Below the tabs is a section titled **Firmware Upgrade**. The text in this section reads: "To upgrade the internal router firmware, browse to the location of the binary (.bin) upgrade file and click **Upload**. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.bin) file. In some cases, you may need to reconfigure." Below this text is a "File Path:" label followed by a text input field and a "Browse..." button. At the bottom of the form is an "Upload" button.

The following table describes the labels in this screen.

**Table 56** 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.

**Note:** Do not turn off the NBG-418N while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait for several minutes before logging into the NBG-418N again.

**Figure 95** Upload Warning



The NBG-418N automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 96** 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 97** Upload Error Message



## 17.4 Configuration Screen

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

**Figure 98** Maintenance > Tools > Configuration

The screenshot shows the 'Configuration' tab selected in a web interface. It is divided into three 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, a text 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 of defaults: '- Username is admin and password will be 1234', '- LAN IP address will be 192.168.1.1', and '- DHCP will be reset to server'. A 'Reset' button is located at the bottom.

### 17.4.1 Backup Configuration

Backup configuration allows you to back up (save) the NBG-418N's current configuration to a file on your computer. Once your NBG-418N 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 NBG-418N's current configuration to your computer.

### 17.4.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG-418N.

**Table 57** 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.

Note: Do not turn off the NBG-418N while configuration file upload is in progress.

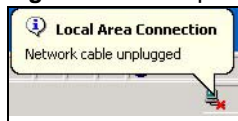
After you see a “configuration upload successful” screen, you must then wait one minute before logging into the NBG-418N again.

**Figure 99** Configuration Restore Successful



The NBG-418N automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 100** 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 NBG-418N IP address (192.168.1.1 in router mode). See [Appendix C on page 167](#) 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 101** Configuration Restore Error



### 17.4.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the NBG-418N to its factory defaults.

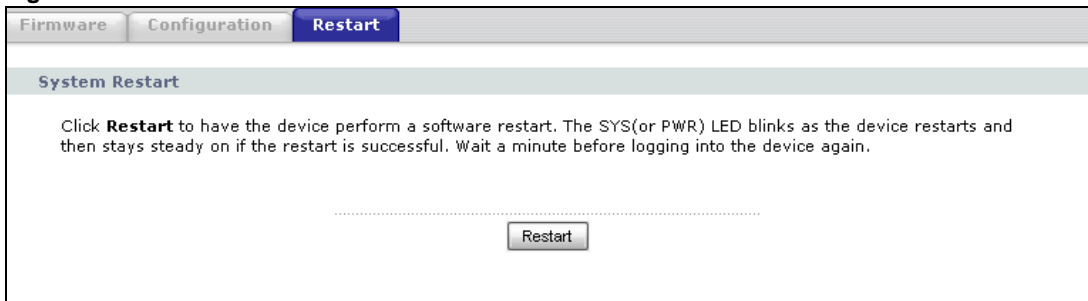
You can also press the **RESET** button on the rear panel to reset the factory defaults of your NBG-418N. Refer to [Section 2.3.1 on page 19](#) for more information on the **RESET** button.

## 17.5 Restart Screen

System restart allows you to reboot the NBG-418N without turning the power off.

Click **Maintenance > Tools > Restart**. Click **Restart** to have the NBG-418N reboot. This does not affect the NBG-418N's configuration.

**Figure 102** Maintenance > Tools > Restart





## Sys OP Mode

### 18.1 Overview

The **Sys OP Mode** (System Operation Mode) function lets you configure select the device operation mode: **Router**, **Access Point**, **Client Bridge** or **Universal Repeater**.

See [Chapter 4 on page 35](#) for more information on which mode to choose.

### 18.2 General Screen

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

**Figure 103** Maintenance > Sys OP Mode > General

**General**

**System Operation Mode**

Router  
 Access Point  
 Universal Repeater  
 Client Bridge

**Note :**

**Router :** In this mode, the device is supported to connect to internet via ADSL/Cable Modem. PCs in LAN ports share the same IP to ISP through WAN Port.

**Access Point :** In this mode, all Ethernet ports are bridged together. The device allows the wireless-equipped computer can communicate with a wired network.

**Universal Repeater :** In this mode, the device acts as both access point and wireless client. It can transmit wireless traffic between two wireless networks.

**Client Bridge :** In this mode, the device acts as a wireless client. It can connect to an existing network via an access point. Also bridge functions are added between the wireless LAN and the LAN.

Apply    Reset

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

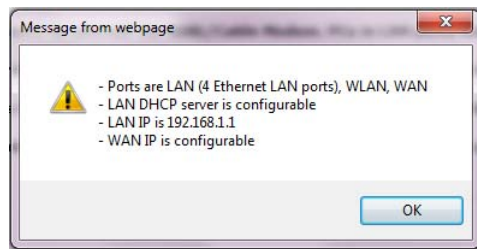
**Table 58** Maintenance > Sys Op Mode > General

LABEL	DESCRIPTION
System Operation Mode	
Router	Use this mode if you want to use routing functions such as LAN DHCP, NAT, firewall and so on on the NBG-418N (N). The NBG-418N has separate LAN and WAN network IP addresses.
Access Point	Use this mode if you already have a Router (R) in your network and you want to bridge all wired and wireless network connections.

**Table 58** Maintenance > Sys Op Mode > General (continued)

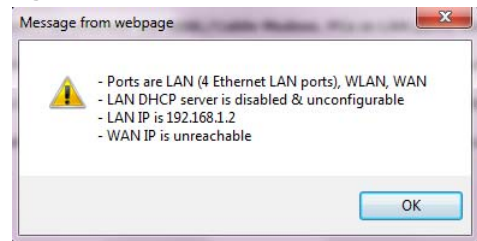
LABEL	DESCRIPTION
Universal Repeater	Use this mode if there is an existing wireless router or access point in your network and you want the NBG-418N to wirelessly relay communications from its wireless clients to it.
Client Bridge	Use this mode if there is an existing wireless router or access point (AP) in the network to which you want to connect your NBG-418N wirelessly. You should know the SSID and wireless security details of the wireless router or access point to which you want to connect.
Apply	Click <b>Apply</b> to save your settings.
Reset	Click <b>Reset</b> to return to the previous screen settings.

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

**Figure 104** Maintenance > Sys Op Mode > 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 NBG-418N 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 a non-router mode (**Access Point**, **Client Bridge** or **Universal Repeater**) the following pop-up message window appears.

**Figure 105** Maintenance > Sys Op Mode > General: Non-Router

- In non-router 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 this mode there must be a device with a DHCP server on your network such as a router which can allocate IP addresses or else you need to manually assign IP addresses to devices on your network.
- The LAN IP address of the NBG-418N is set to 192.168.1.2.



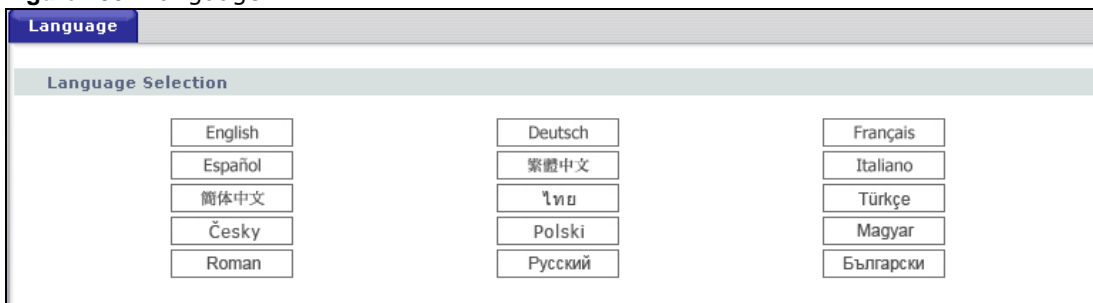
# Language

## 19.1 Language Screen

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

Click the language you prefer. The Web Configurator language changes after a while without restarting the NBG-418N.

**Figure 106** Language



**Figure 107** Language Change Example





# 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](#)
- [NBG-418N Access and Login](#)
- [Internet Access](#)
- [Resetting the NBG-418N to Its Factory Defaults](#)
- [Wireless Problems](#)

## 20.1 Power, Hardware Connections, and LEDs

---

The NBG-418N does not turn on. None of the LEDs turn on.

---

- 1 Make sure you are using the power adaptor or cord included with the NBG-418N.
- 2 Make sure the power adaptor or cord is connected to the NBG-418N 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 NBG-418N.
- 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 1.3 on page 15](#).
- 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 NBG-418N.
- 5 If the problem continues, contact the vendor.

## 20.2 NBG-418N Access and Login

---

I don't know the IP address of my NBG-418N.

---

- 1 The default IP address in router mode is **192.168.1.1** and in non-router 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 NBG-418N 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 NBG-418N (it depends on the network), so enter this IP address in your Internet browser. 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 NBG-418N'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.
- 3 If your NBG-418N 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 NBG-418N to change all settings back to their default. This means your current settings are lost. See [Section 20.4 on page 144](#) in the **Troubleshooting** for information on resetting your NBG-418N.

---

I forgot the username and password.

---

- 1 The default username is **admin** and default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 20.4 on page 144](#).

---

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 (router mode).
  - If you changed the IP address, 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 NBG-418N](#).

- 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 B on page 157](#).
- 4 Make sure your computer is in the same subnet as the NBG-418N. (If you know that there are routers between your computer and the NBG-418N, skip this step.)
  - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address.
  - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG-418N.
- 5 Reset the device to its factory defaults, and try to access the NBG-418N with the default IP address.
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### Advanced Suggestions

- 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 NBG-418N.

---

- 1 Make sure you have entered the password correctly. The default username is **admin** and 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 NBG-418N.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 20.4 on page 144](#).

## 20.3 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.
- 6 If the problem continues, contact your ISP.

---

I cannot access the Internet anymore. I had access to the Internet (with the NBG-418N), 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 1.3 on page 15](#).
- 2 Reboot the NBG-418N.
- 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 1.3 on page 15](#). If the NBG-418N 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 NBG-418N 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 NBG-418N.
- 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.

## 20.4 Resetting the NBG-418N to Its Factory Defaults

If you reset the NBG-418N, you lose all of the changes you have made. The NBG-418N re-loads its default settings, and the username/password resets to **admin/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 NBG-418N,

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for longer than 1 second to restart/reboot the NBG-418N.
- 3 Press the **RESET** button for longer than five seconds to set the NBG-418N back to its factory-default configurations.

If the NBG-418N restarts automatically, wait for the NBG-418N to finish restarting, and log in to the Web Configurator. The username is **admin** and password is **1234**.

If the NBG-418N does not restart automatically, disconnect and reconnect the NBG-418N's power. Then, follow the directions above again.

## 20.5 Wireless Problems

---

I cannot access the NBG-418N or ping any computer from the WLAN.

---

- 1 Make sure the wireless LAN is enabled on the NBG-418N.
- 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 NBG-418N.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG-418N.
- 5 Check that both the NBG-418N 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 NBG-418N.
- 7 Make sure you allow the NBG-418N to be remotely accessed through the WLAN interface. Check your remote management settings.
  - See [Chapter 6 Wireless LAN](#) for more information.

---

I cannot access the Web Configurator after I switched to a non-router mode.

---

When you change from router mode to a non-router mode, you must manually give your computer an IP address in the range between 192.168.1.3 and 192.168.1.254 as non-router mode has no LAN DHCP server.

Refer to [Appendix C on page 167](#) for instructions on how to change your computer's IP address.



# 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.

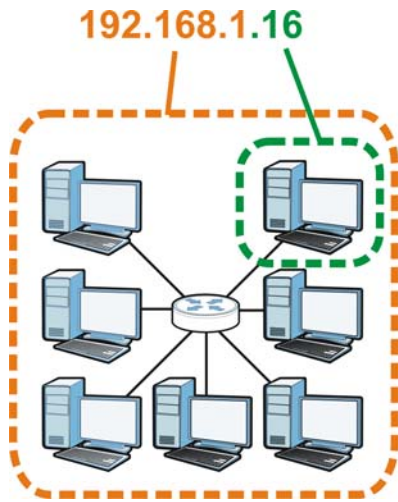
## Structure

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 108** 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 59** IP Address Network Number and Host ID Example

	<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 60** 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 61** 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 62** Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192

**Table 62** Alternative Subnet Mask Notation (continued)

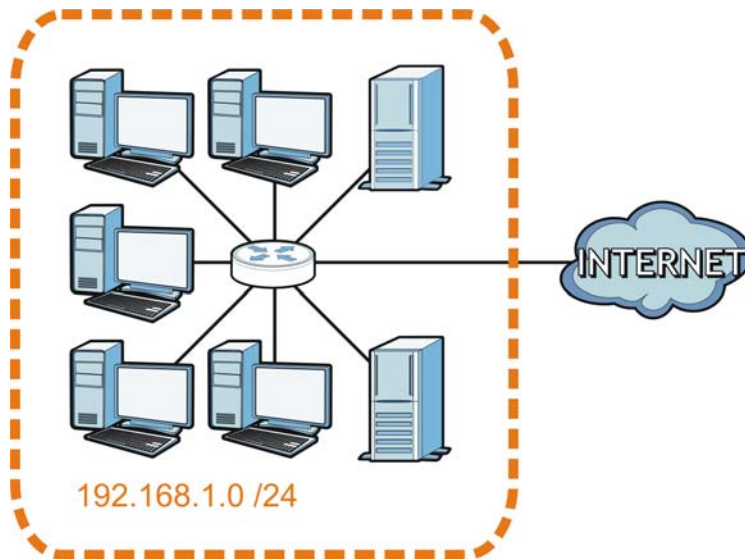
SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

## 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.

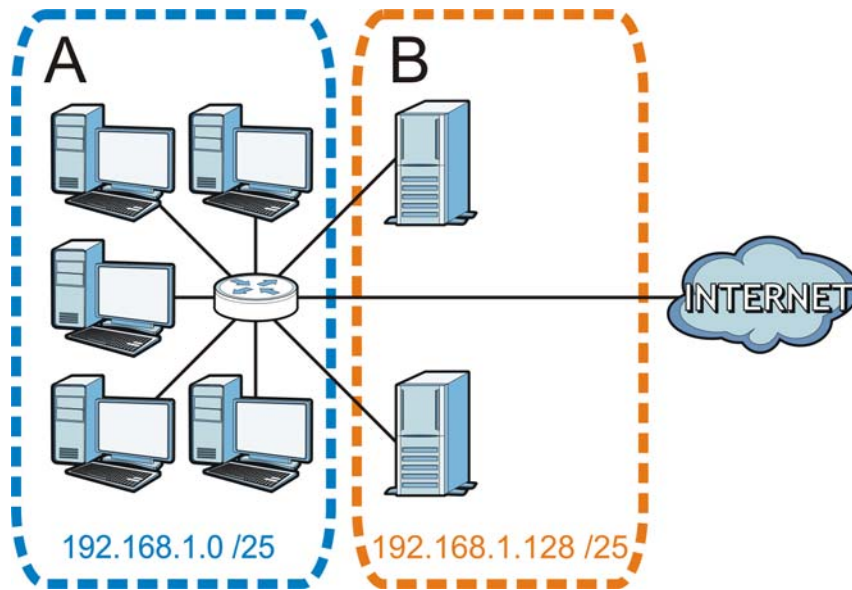
The following figure shows the company network before subnetting.

**Figure 109** 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 110** 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 63** 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 64** 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 65** 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 66** 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 67** Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191

**Table 67** Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
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 68** 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 69** 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

## Configuring IP Addresses

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the NBG-418N.

Once you have decided on the network number, pick an IP address for your NBG-418N 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 NBG-418N 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 NBG-418N 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.

## IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

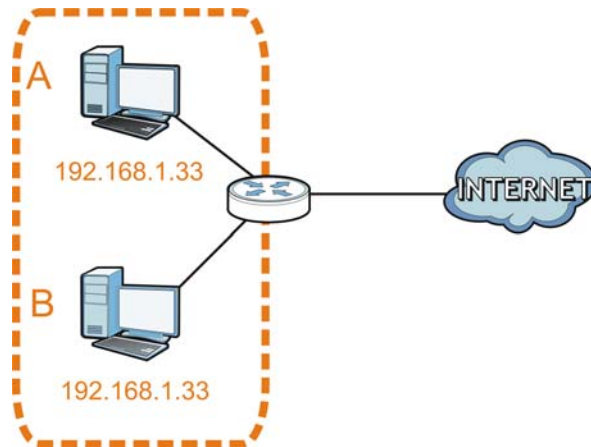
## Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to



computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

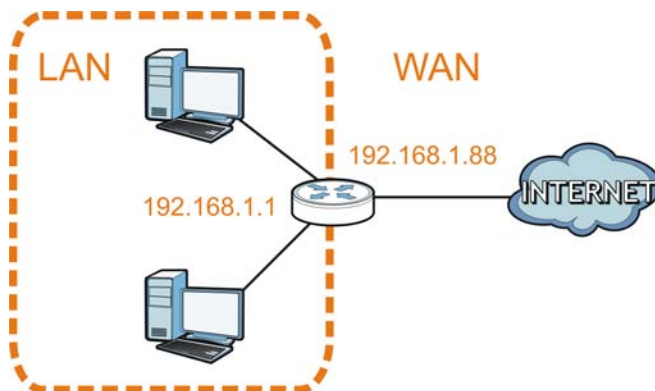
**Figure 111** Conflicting Computer IP Addresses Example



### Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

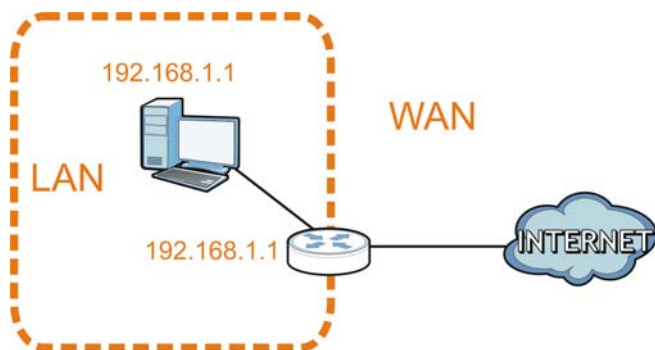
**Figure 112** Conflicting Router IP Addresses Example



### Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

**Figure 113** Conflicting Computer and Router IP Addresses Example



# Pop-up Windows, JavaScripts and Java Permissions

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

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

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

## Internet Explorer Pop-up Blockers

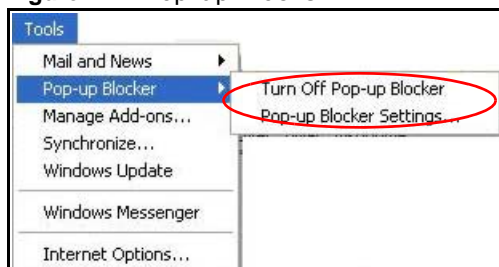
You may have to disable pop-up blocking to log into your device.

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

## Disable Pop-up Blockers

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

**Figure 114** 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 115** Internet Options: Privacy

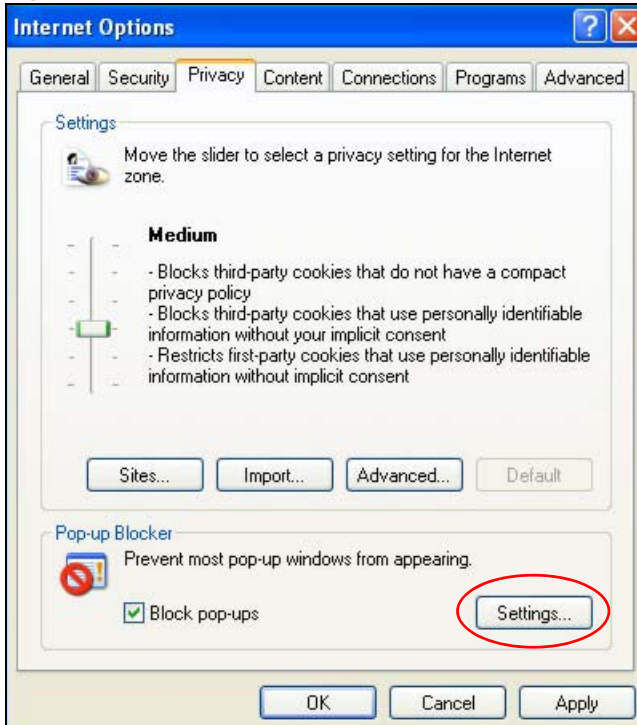


- 3 Click **Apply** to save this setting.

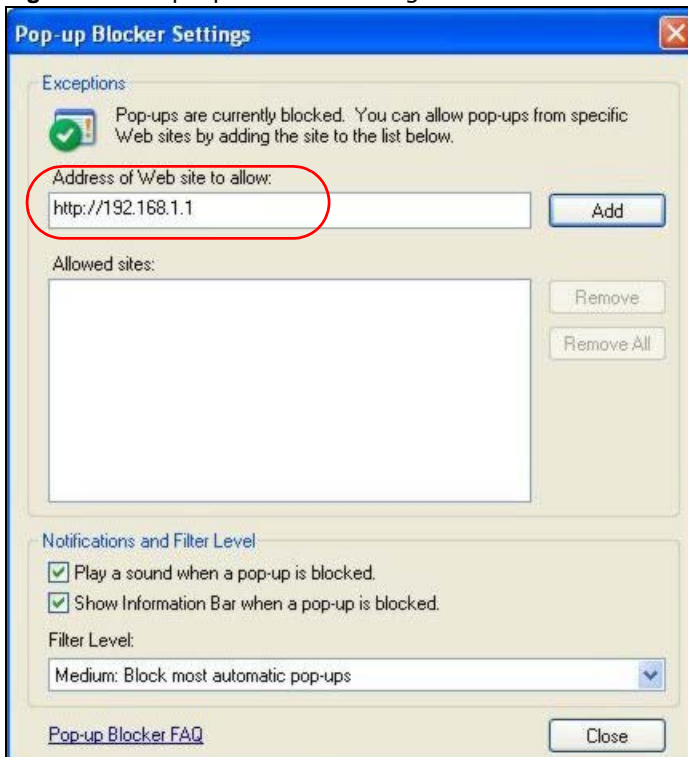
## Enable Pop-up Blockers with Exceptions

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 116** 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 117** Pop-up Blocker Settings

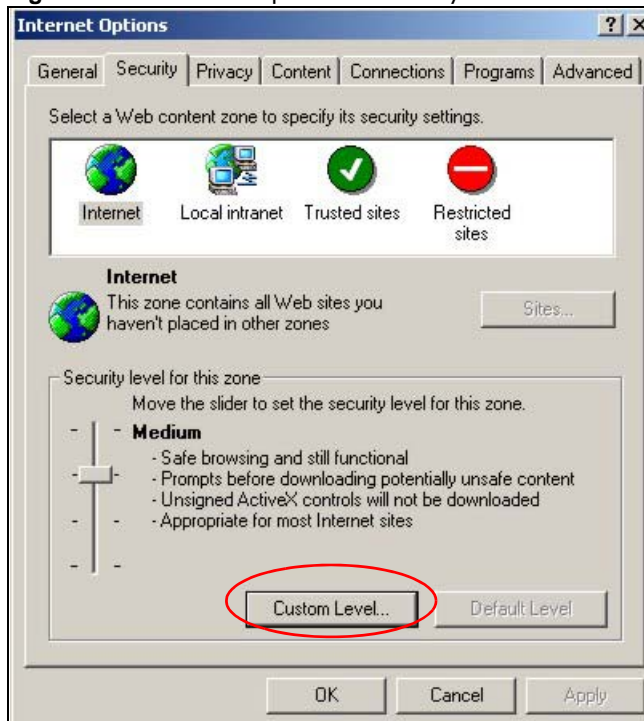
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

## JavaScripts

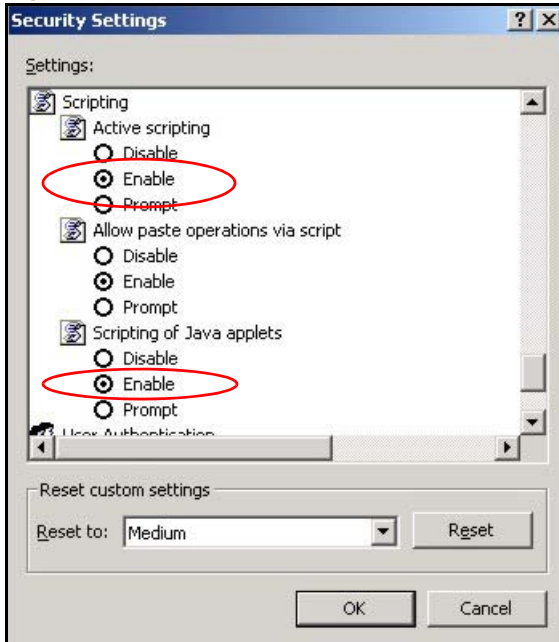
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

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

**Figure 118** Internet Options: Security



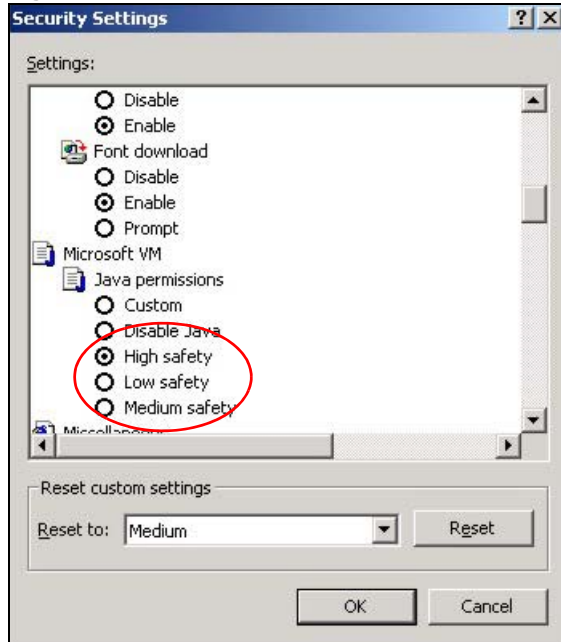
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6 Click **OK** to close the window.

**Figure 119** 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.

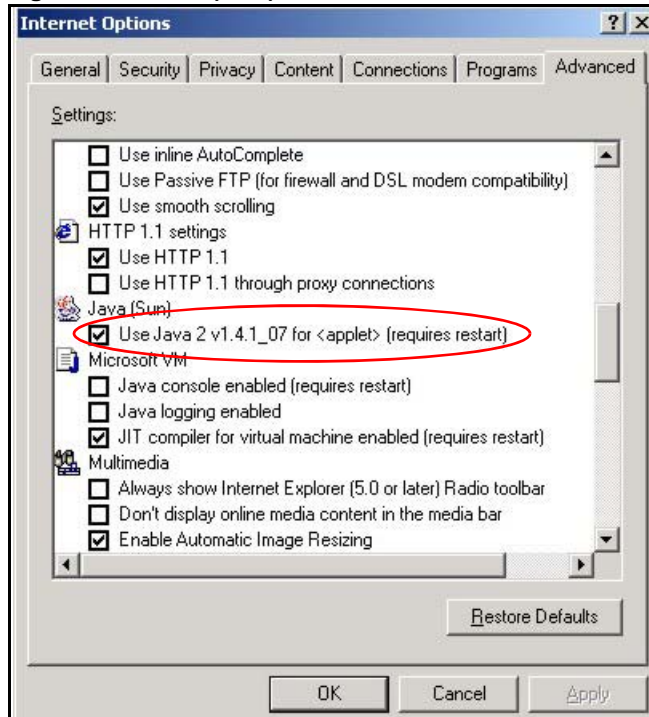
**Figure 120** Security Settings - Java



## 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 121** Java (Sun)



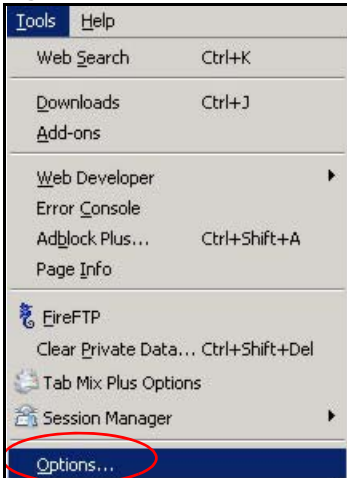


## Mozilla Firefox

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

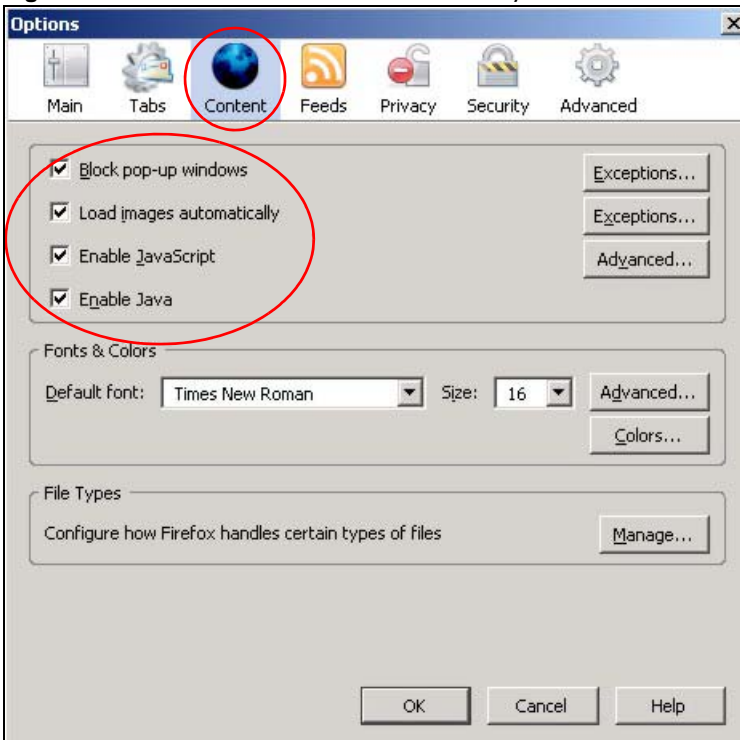
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

**Figure 122** Mozilla Firefox: TOOLS > Options



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

**Figure 123** Mozilla Firefox Content Security



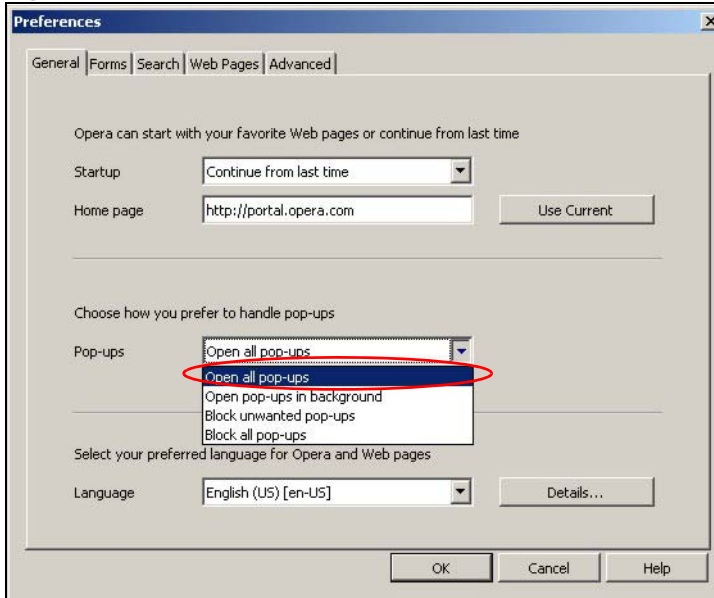
## Opera

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

### Allowing Pop-Ups

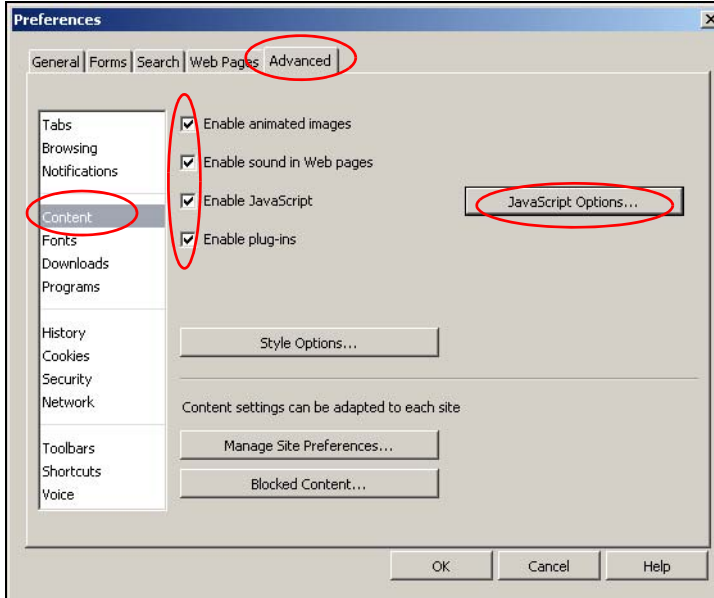
From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

**Figure 124** Opera: Allowing Pop-Ups

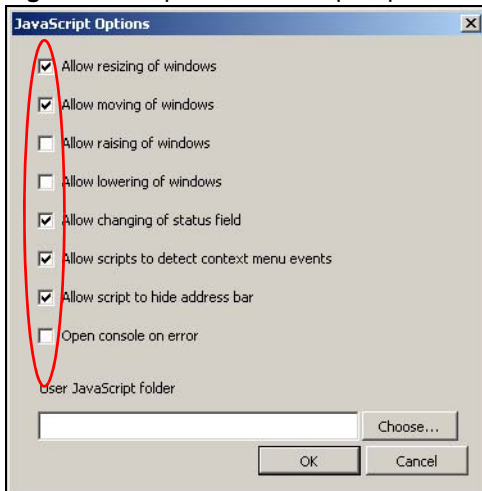


### Enabling Java

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 125** Opera: Enabling Java

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

**Figure 126** Opera: JavaScript Options

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



# Setting Up Your Computer's IP Address

Note: Your specific NBG-418N 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.

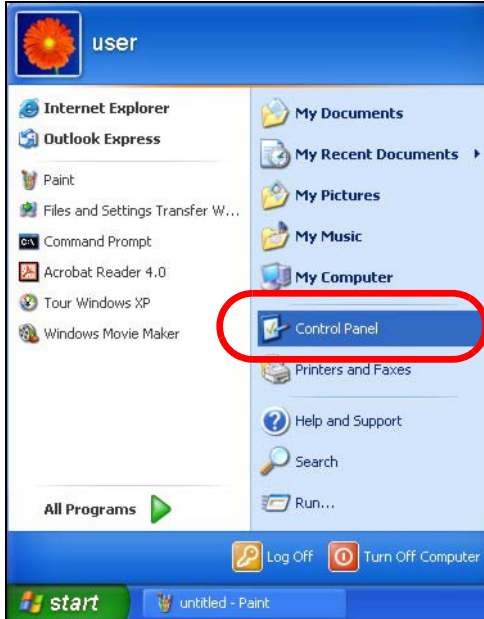
In this appendix, you can set up an IP address for:

- [Windows XP/NT/2000](#) on [page 167](#)
- [Windows Vista](#) on [page 171](#)
- [Windows 7](#) on [page 175](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 179](#)
- [Mac OS X: 10.5 and 10.6](#) on [page 182](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 185](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 189](#)

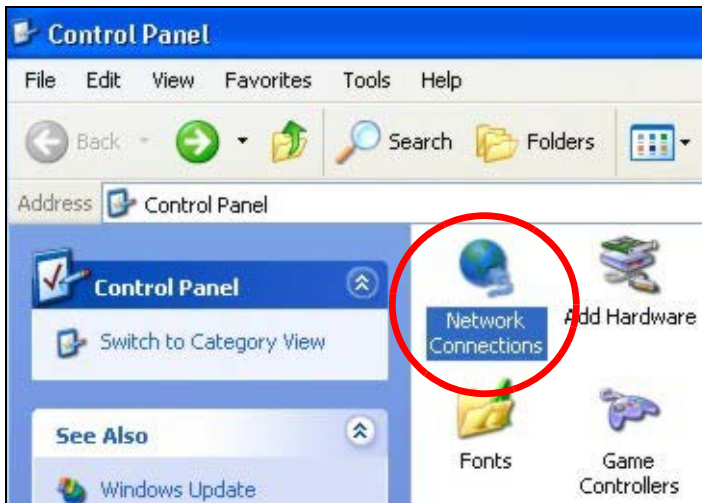
## Windows XP/NT/2000

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

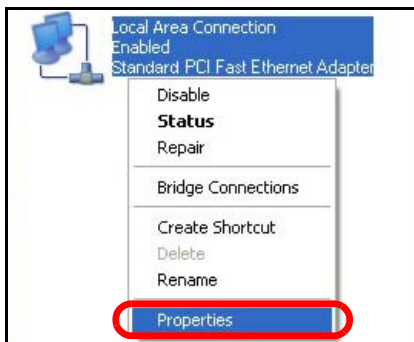
- 1 Click **Start > Control Panel**.



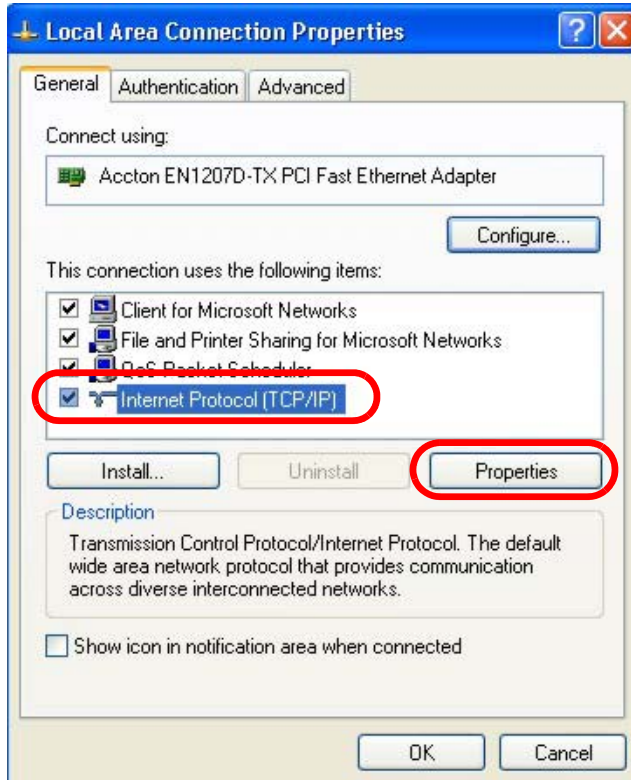
2 In the **Control Panel**, click the **Network Connections** icon.



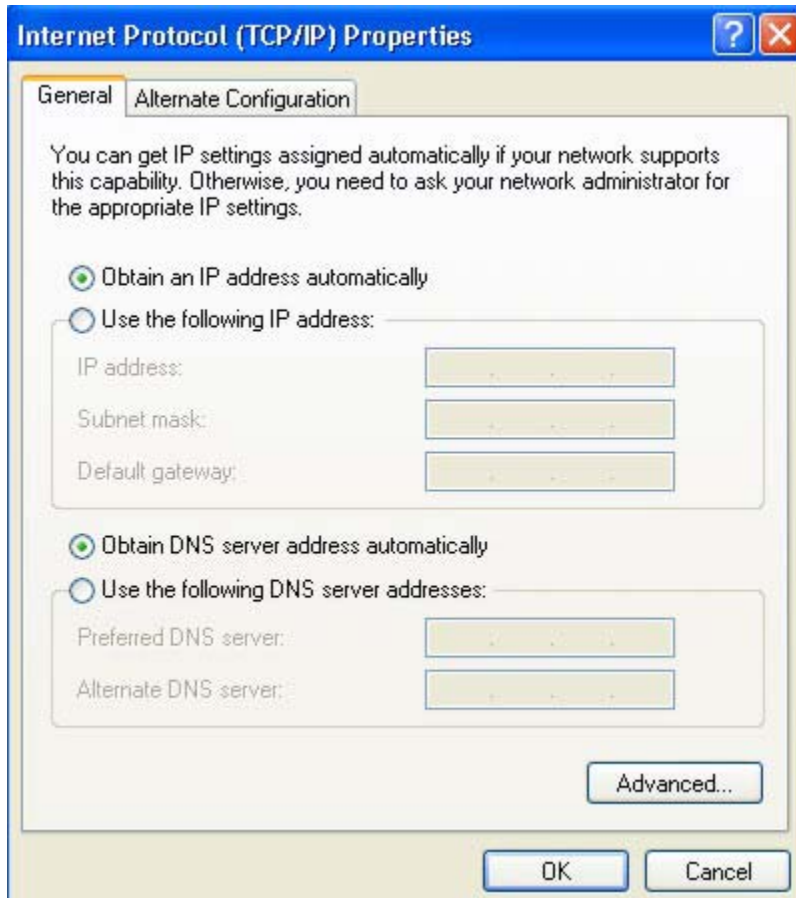
3 Right-click **Local Area Connection** and then select **Properties**.



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

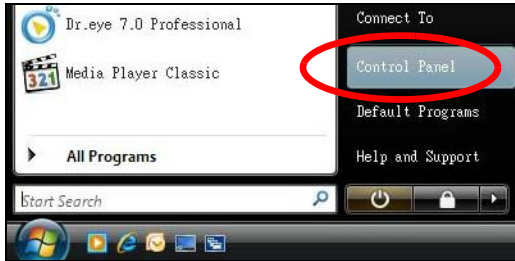
- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].  
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab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



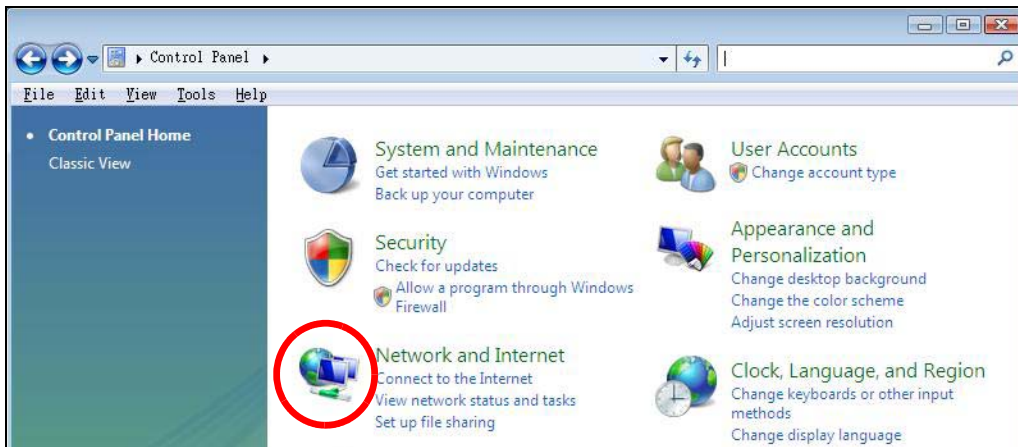
## Windows Vista

This section shows screens from Windows Vista Professional.

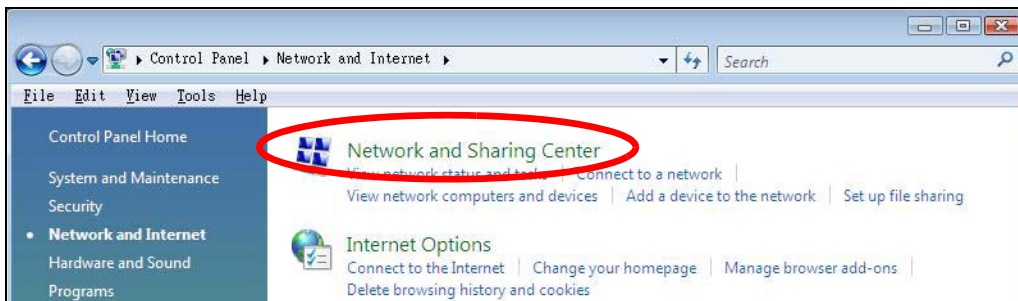
- 1 Click **Start > Control Panel**.



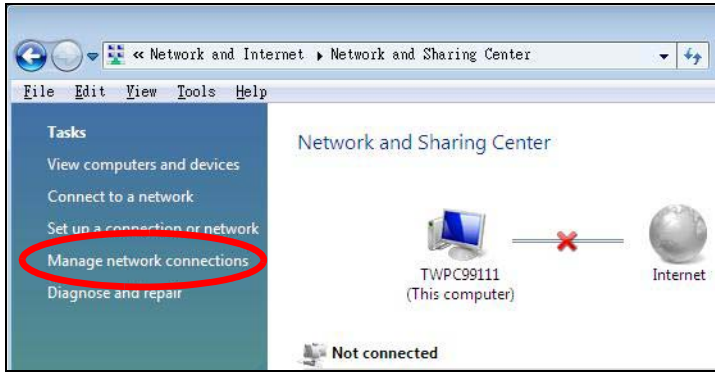
- 2 In the **Control Panel**, click the **Network and Internet** icon.



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



- 4 Click **Manage network connections**.

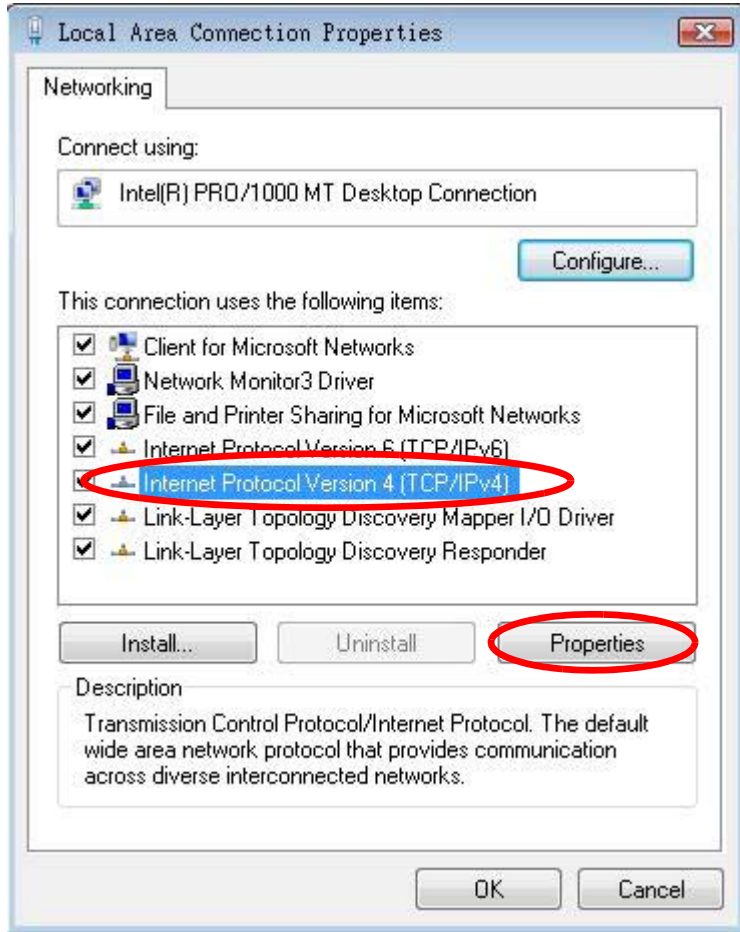


- 5 Right-click **Local Area Connection** and then select **Properties**.

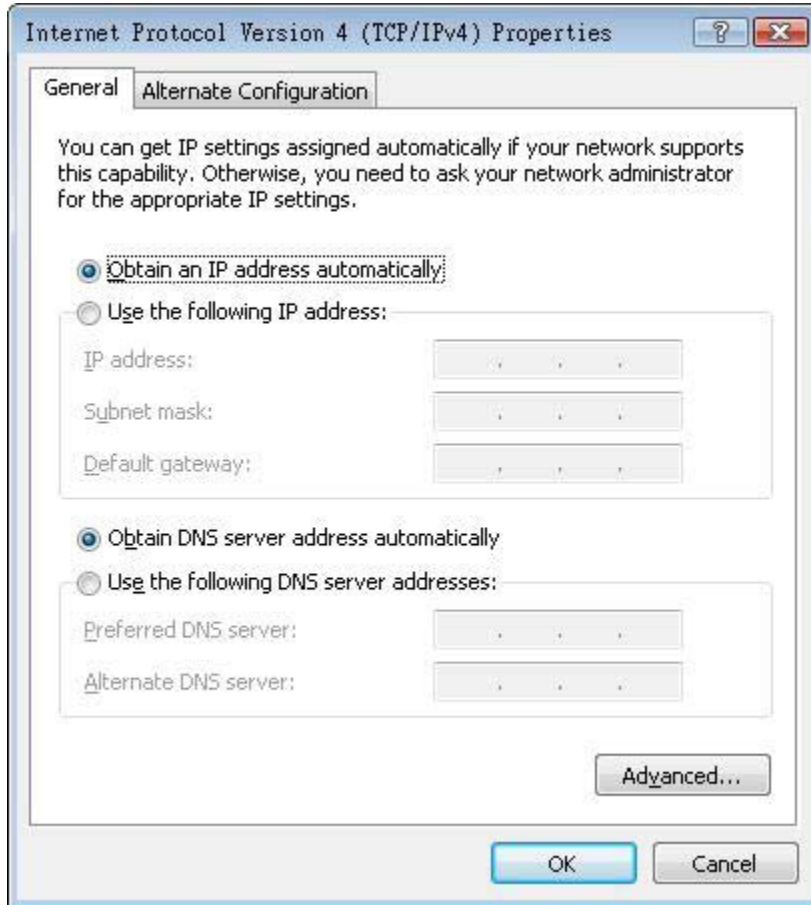


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

- 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.

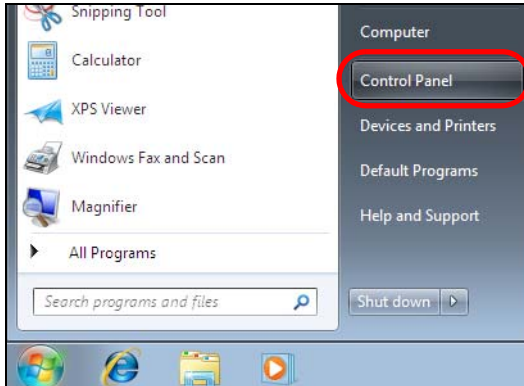
## Verifying Settings

- 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.

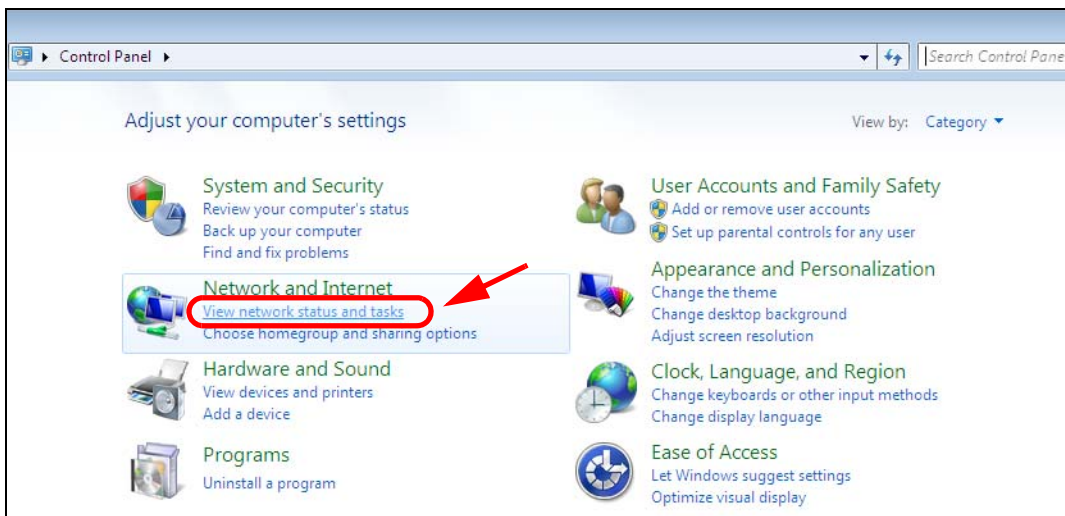
## Windows 7

This section shows screens from Windows 7 Enterprise.

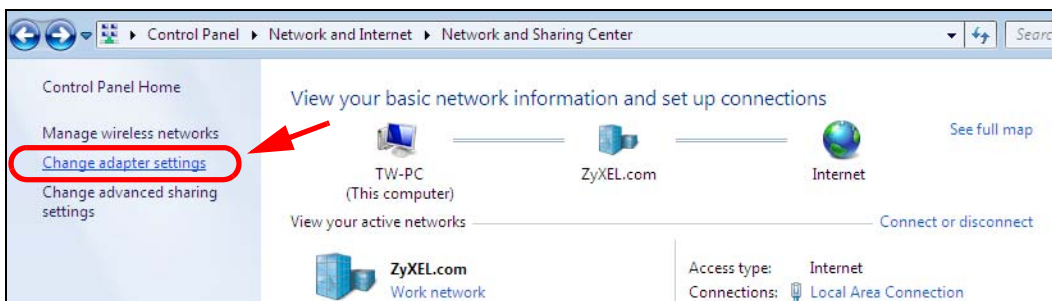
- 1 Click **Start > Control Panel**.



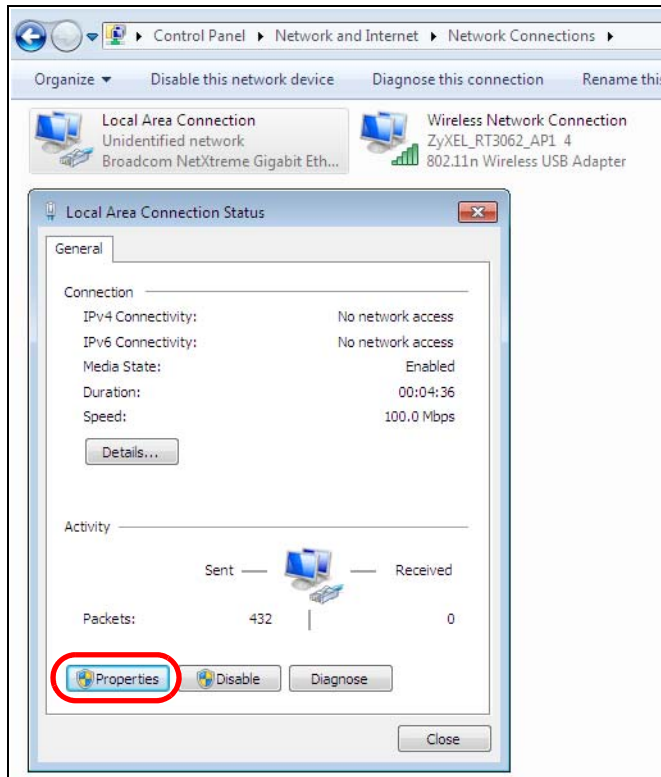
- 2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.



- 3 Click **Change adapter settings**.

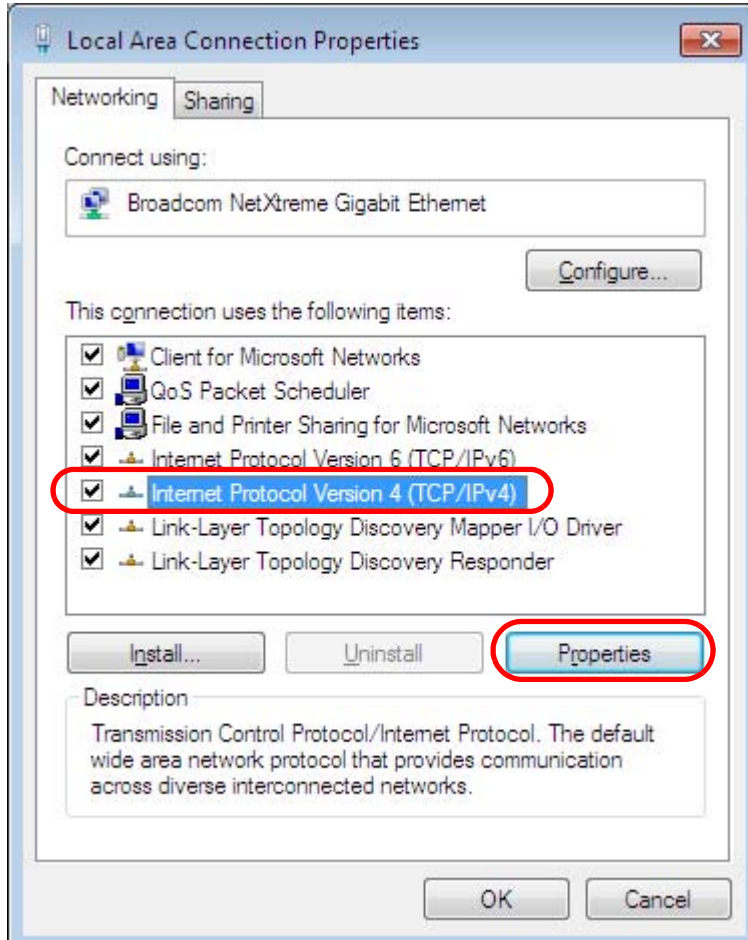


- 4 Double click **Local Area Connection** and then select **Properties**.



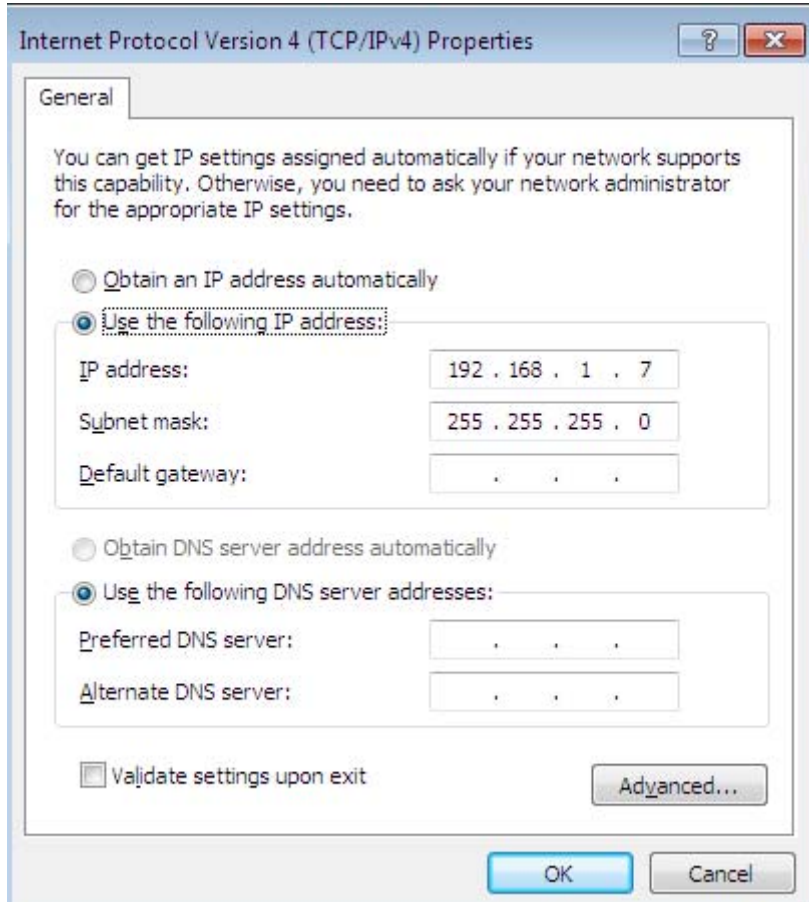
Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

- 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:

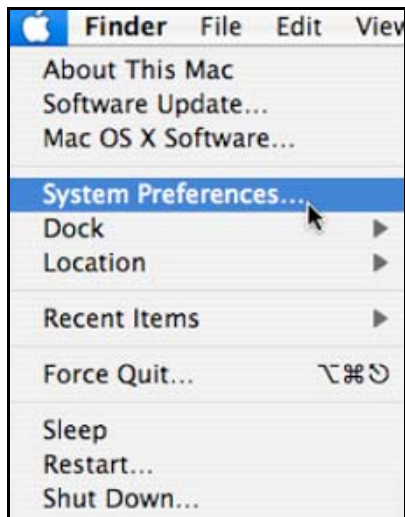
    Connection-specific DNS Suffix  . : P-2612HNU-F3v2
    IP Address. . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

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.

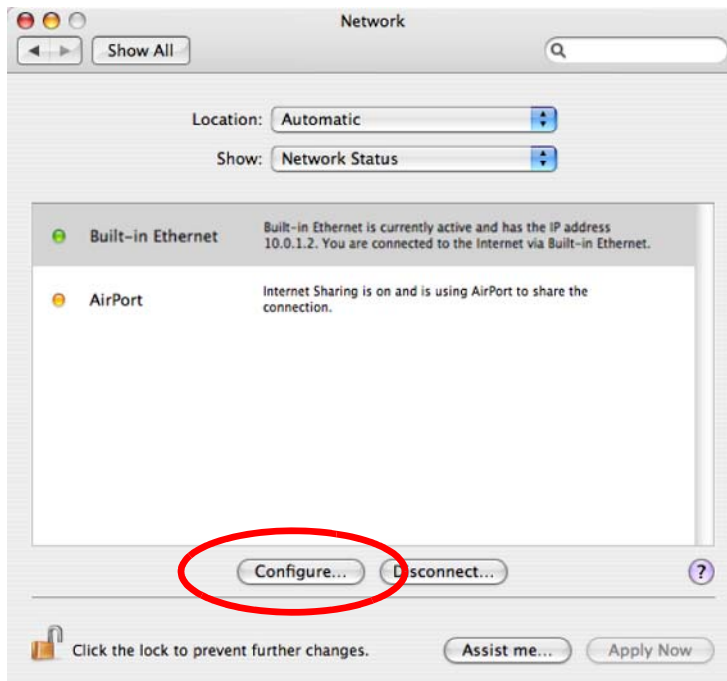
- 1 Click **Apple** > **System Preferences**.



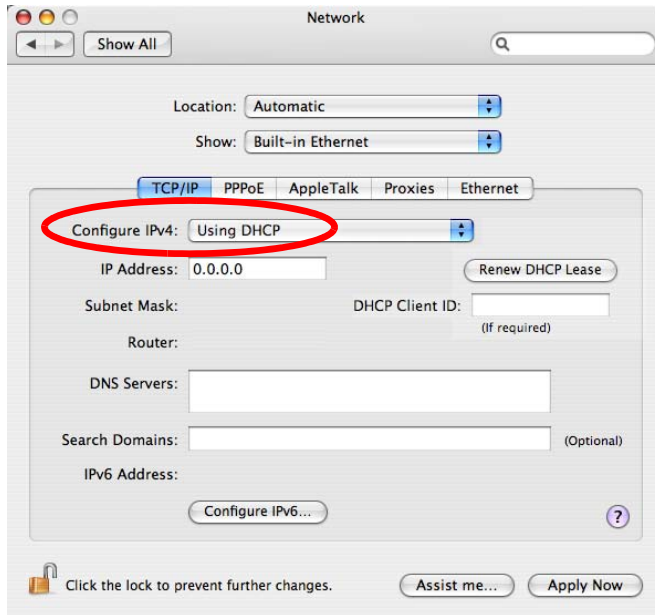
- 2 In the **System Preferences** window, click the **Network** icon.



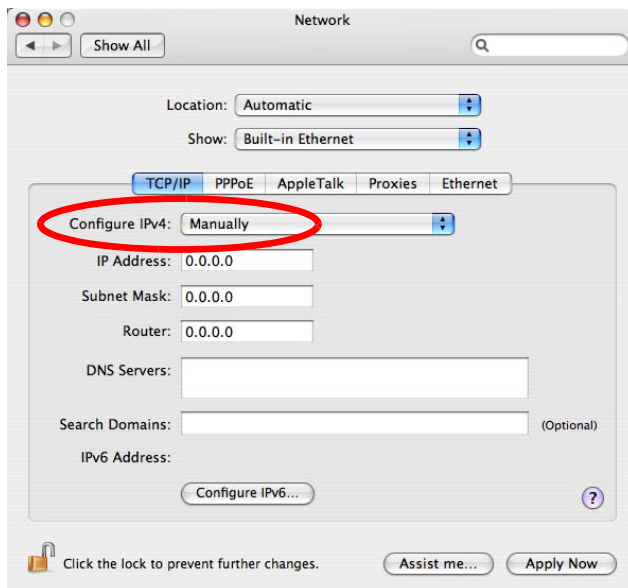
- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.



- 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.

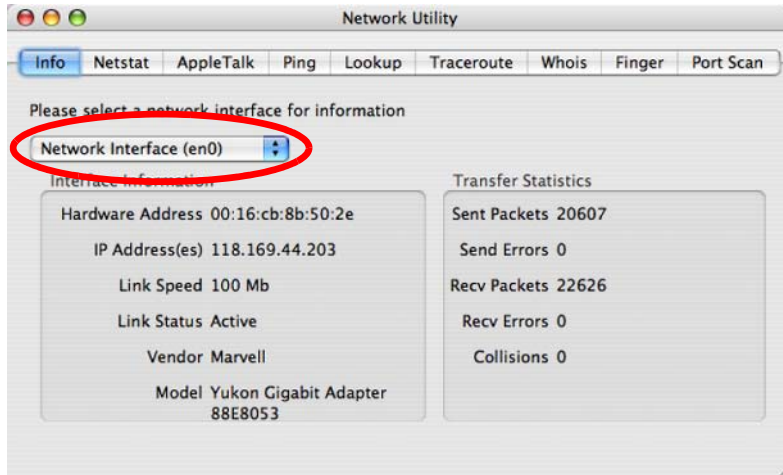


- 6 Click **Apply Now** and close the window.

## Verifying Settings

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

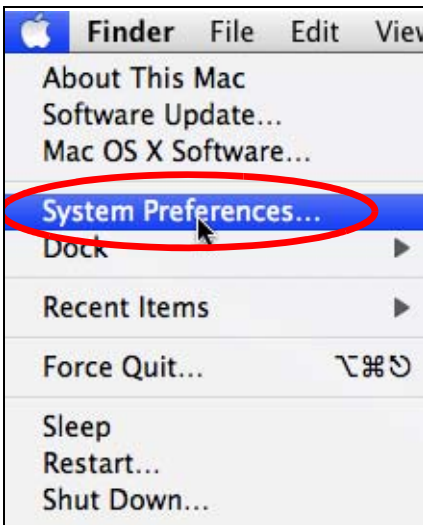
Figure 127 Mac OS X 10.4: Network Utility



## 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.

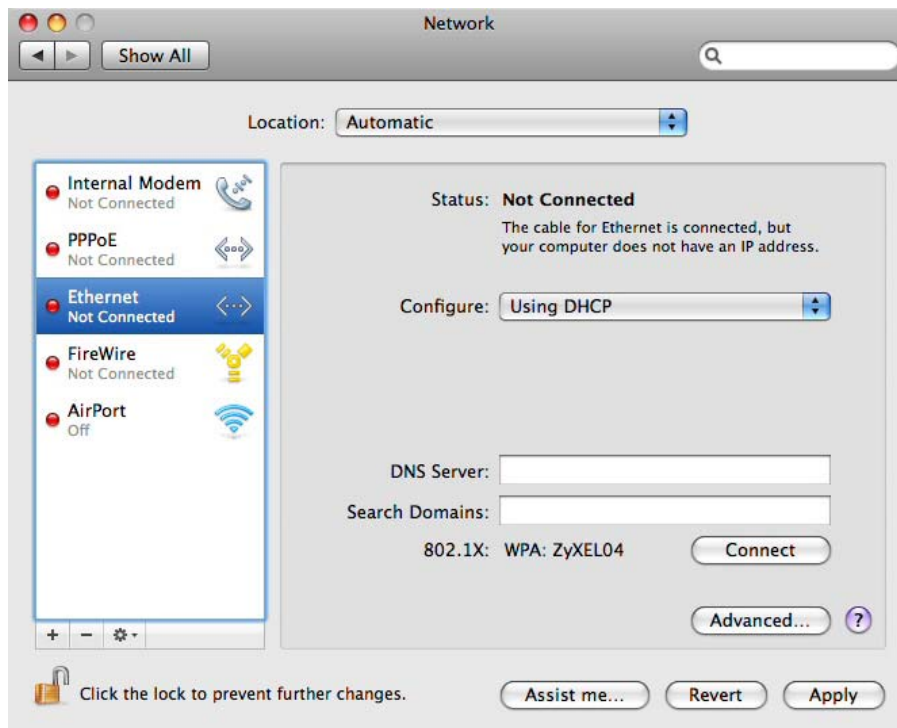
- 1 Click **Apple** > **System Preferences**.



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

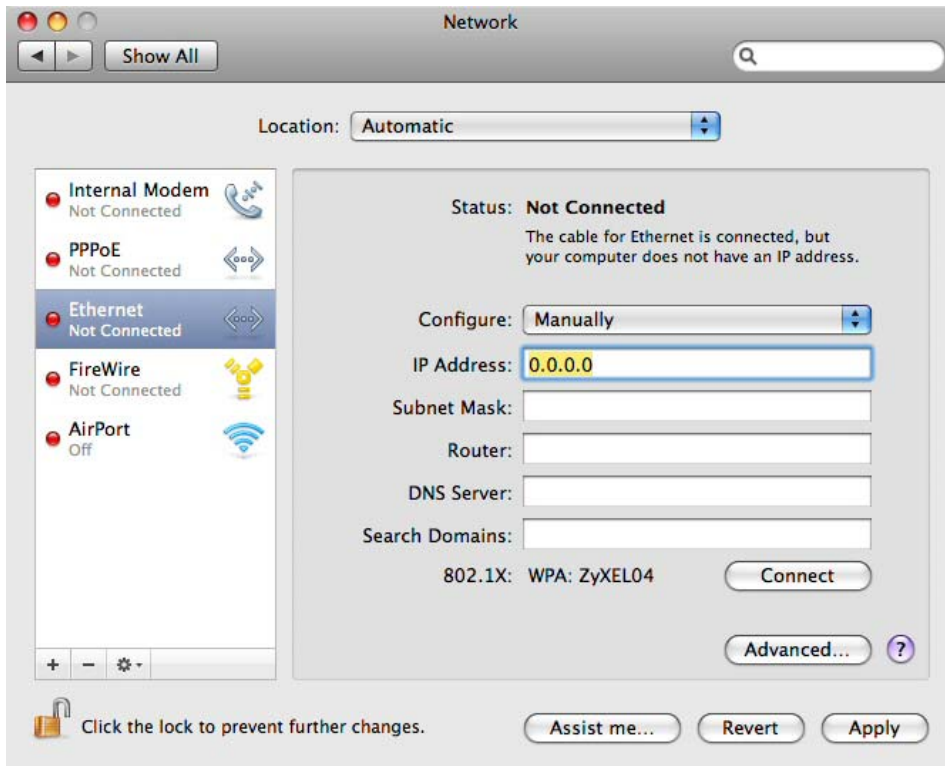


- 3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.



- 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**.

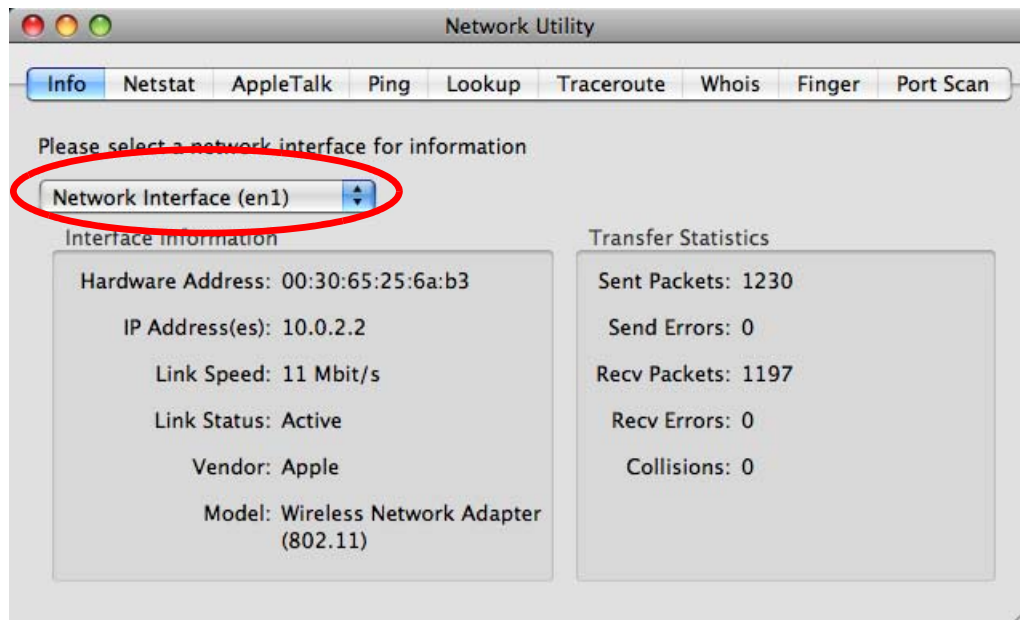
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your NBG-418N.



- 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 128** Mac OS X 10.5: Network Utility

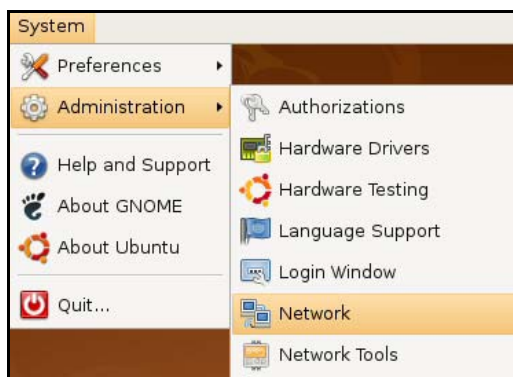
## Linux: Ubuntu 8 (GNOME)

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.



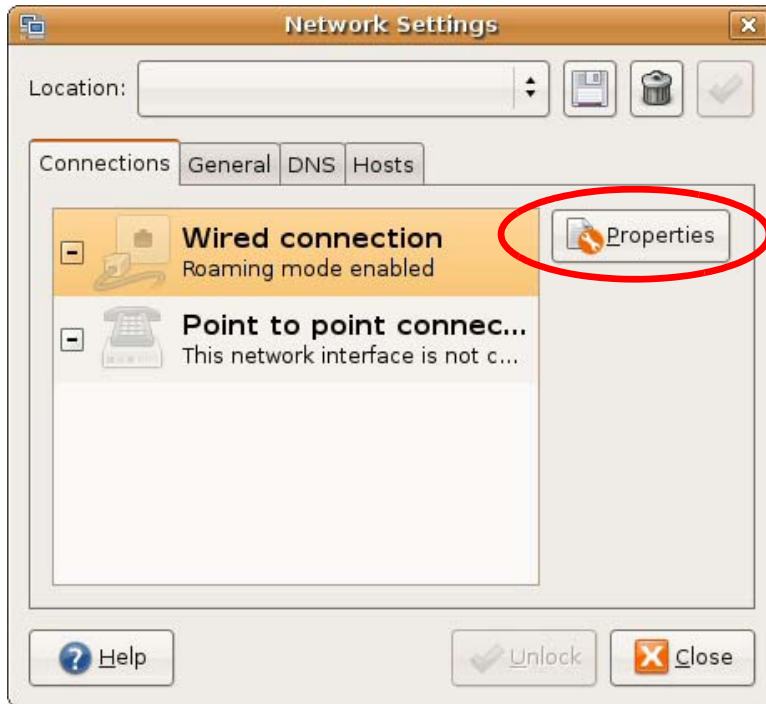


- 3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.



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





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



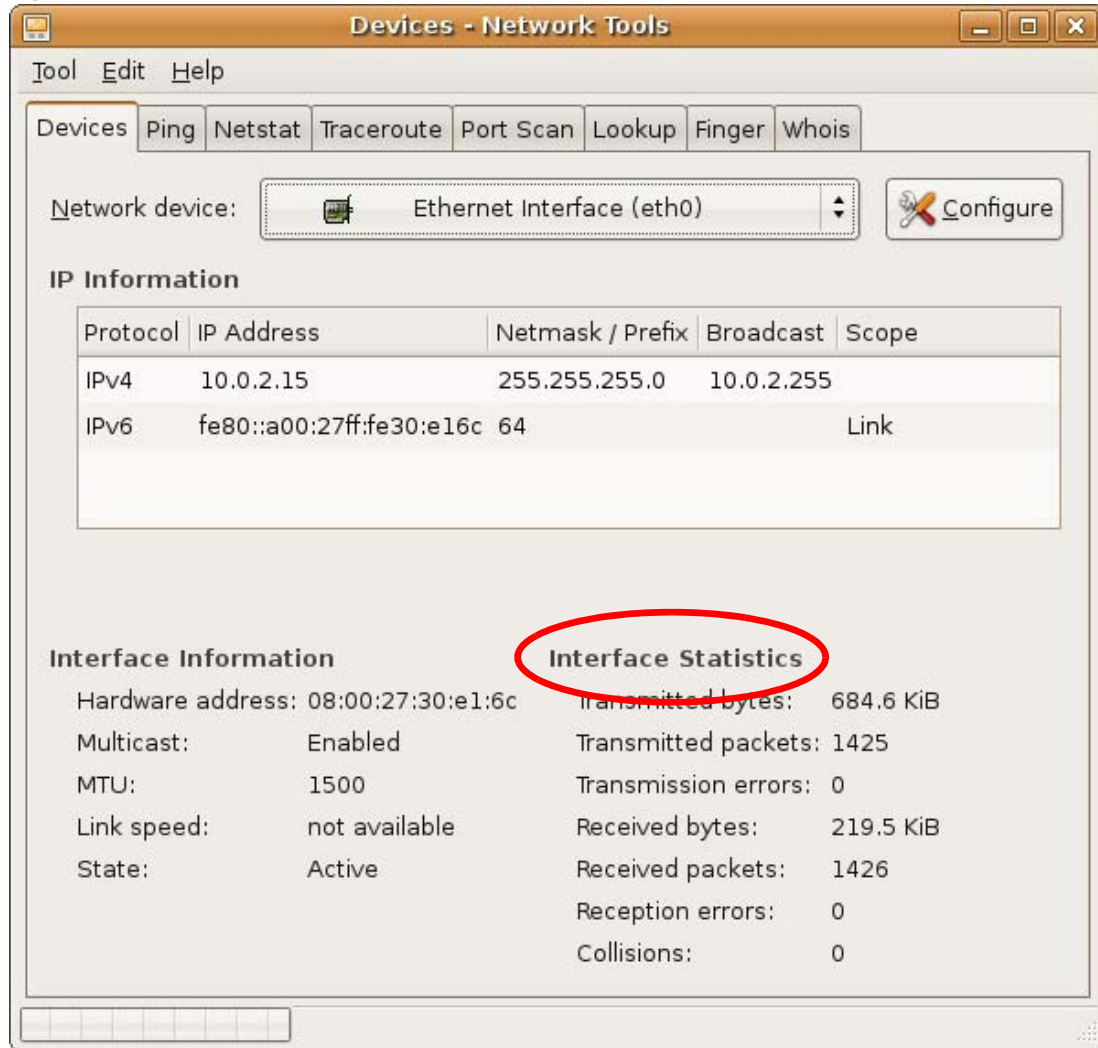
- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
  - In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.
- 6 Click **OK** to 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 129** Ubuntu 8: Network Tools

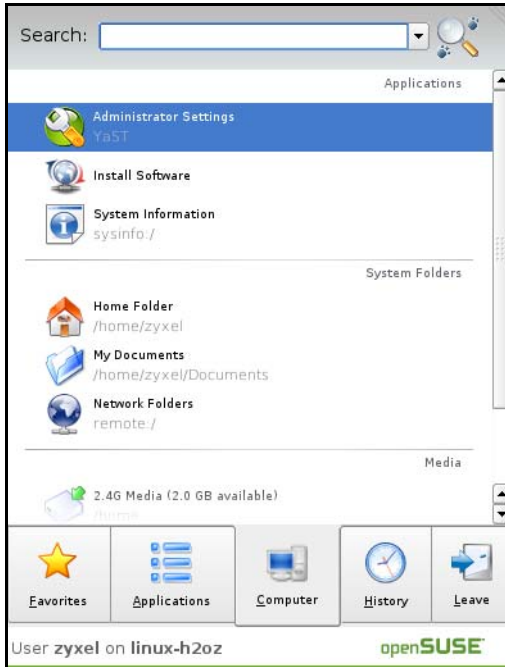
## Linux: openSUSE 10.3 (KDE)

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:

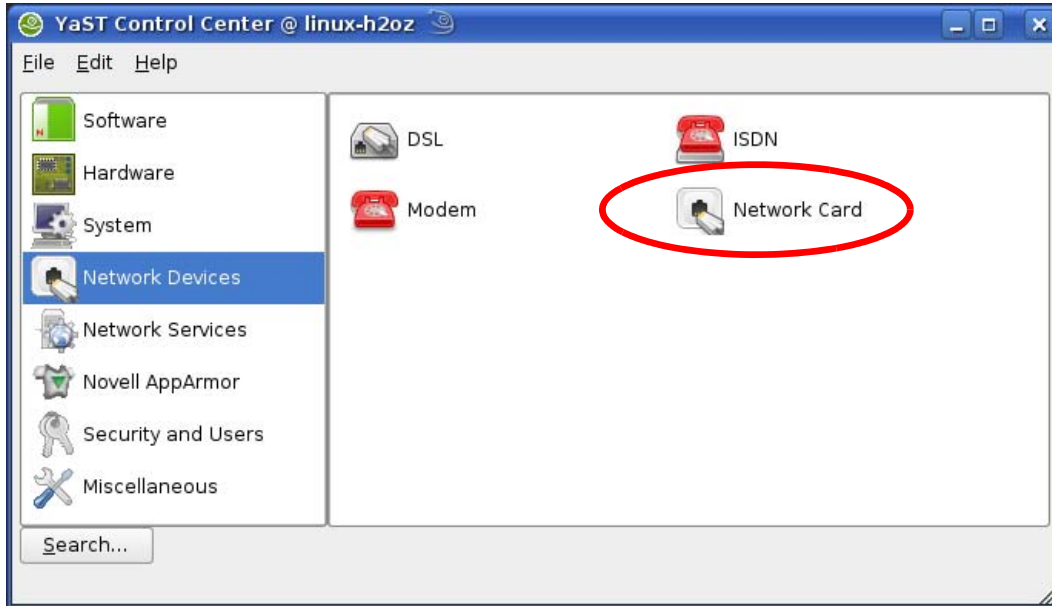
- 1 Click **K Menu > Computer > Administrator Settings (YaST)**.



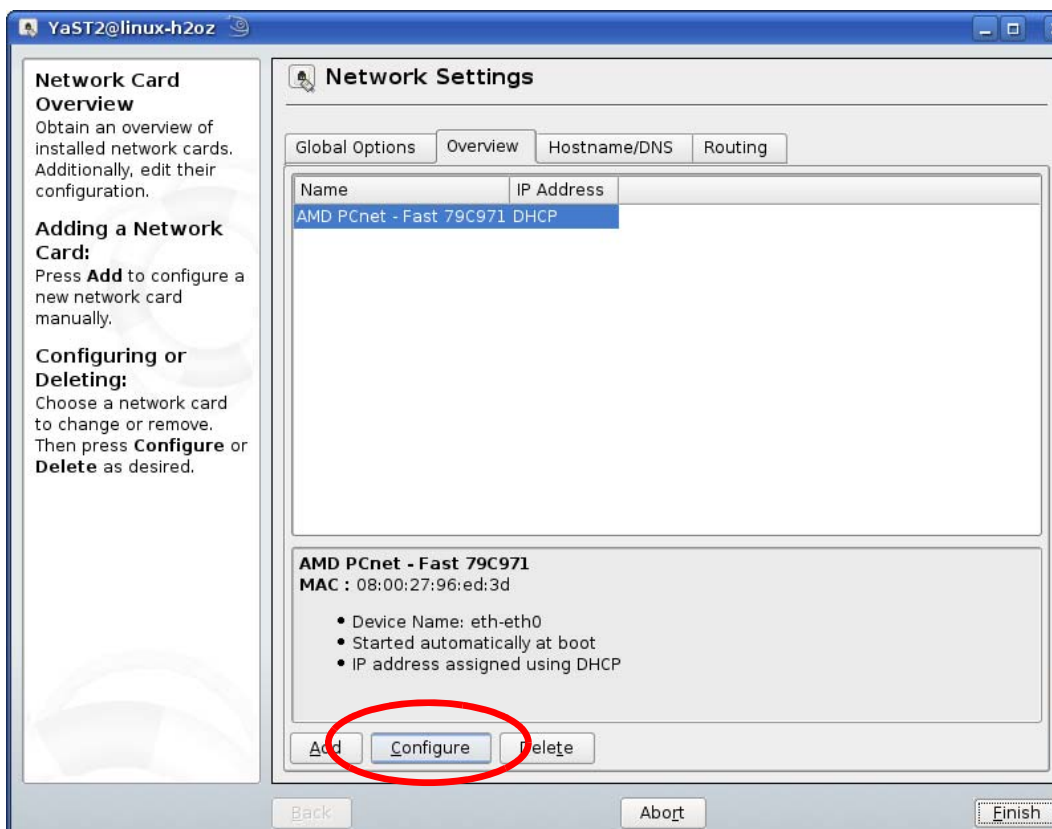
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.



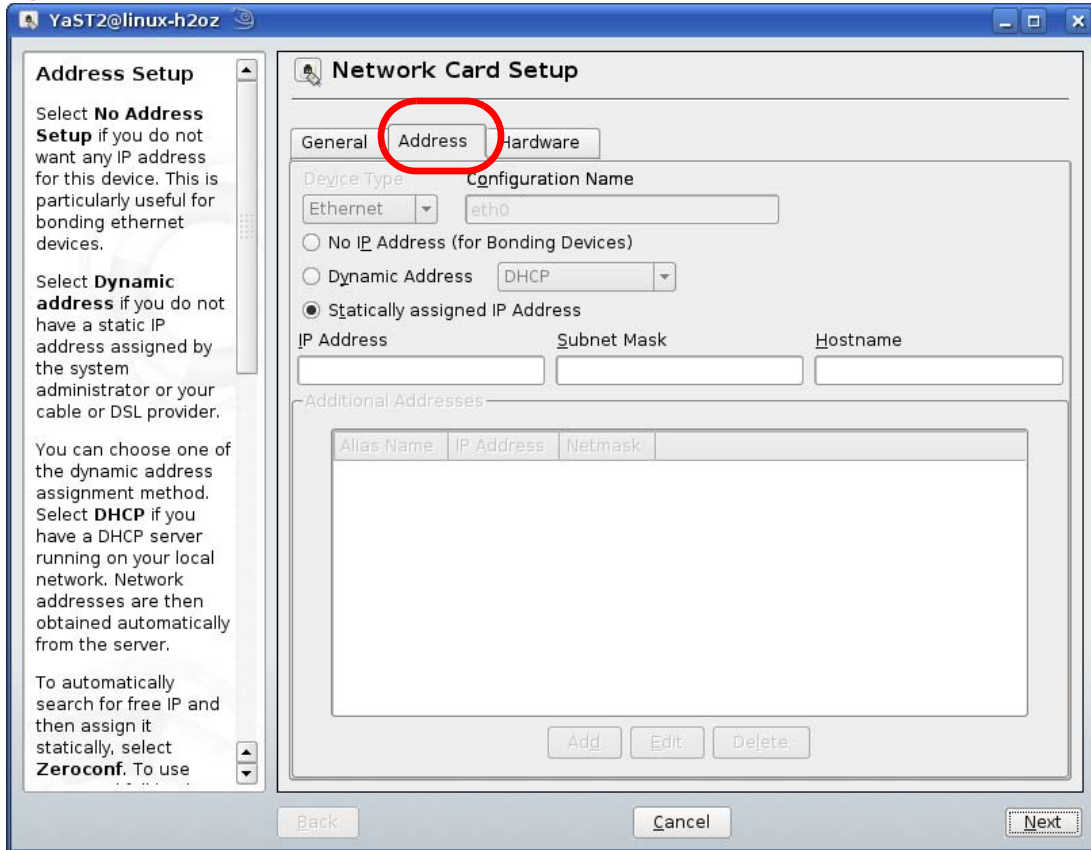
- 3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.



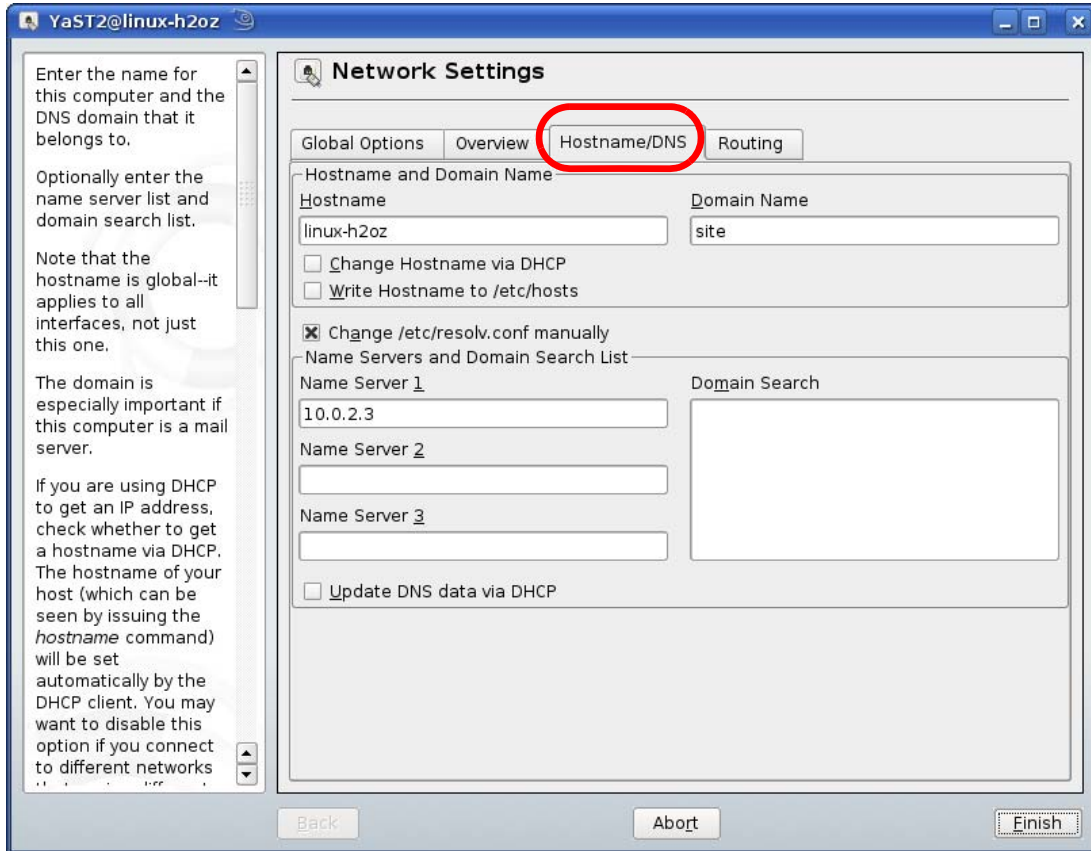
- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



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

**Figure 130** 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.

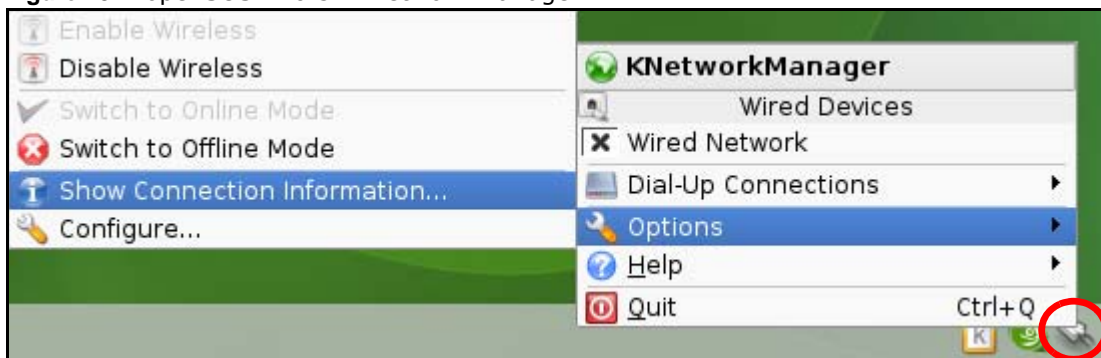


- 9 Click **Finish** to save your settings and close the window.

## Verifying Settings

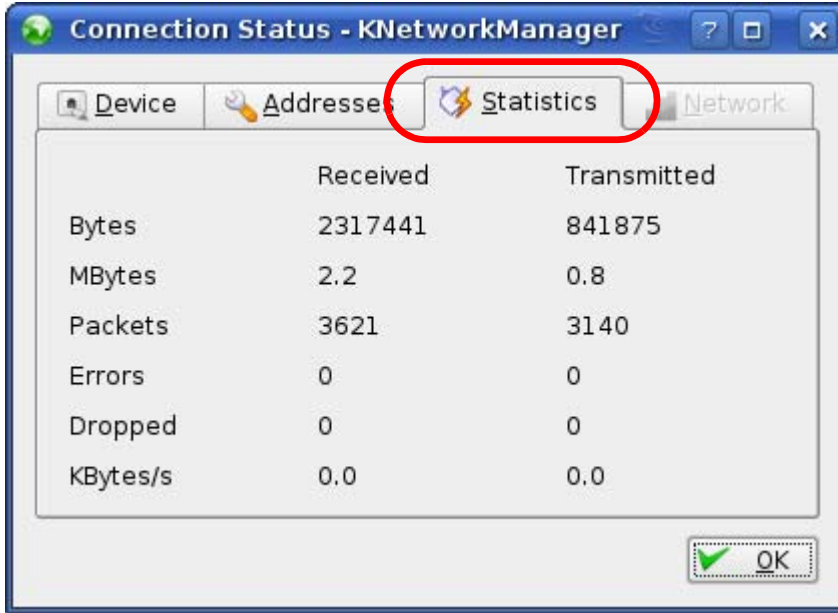
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

**Figure 131** 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 132 openSUSE: Connection Status - KNetwork Manager





# Wireless LANs

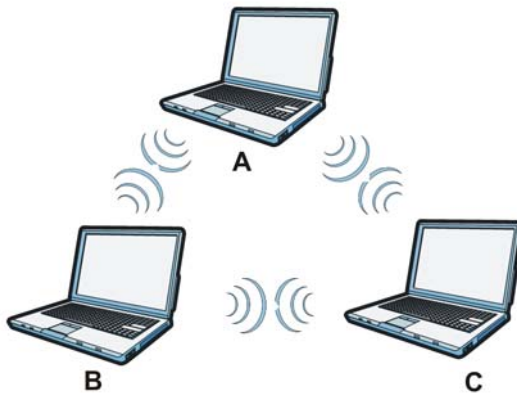
## Wireless LAN Topologies

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

### Ad-hoc Wireless LAN Configuration

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

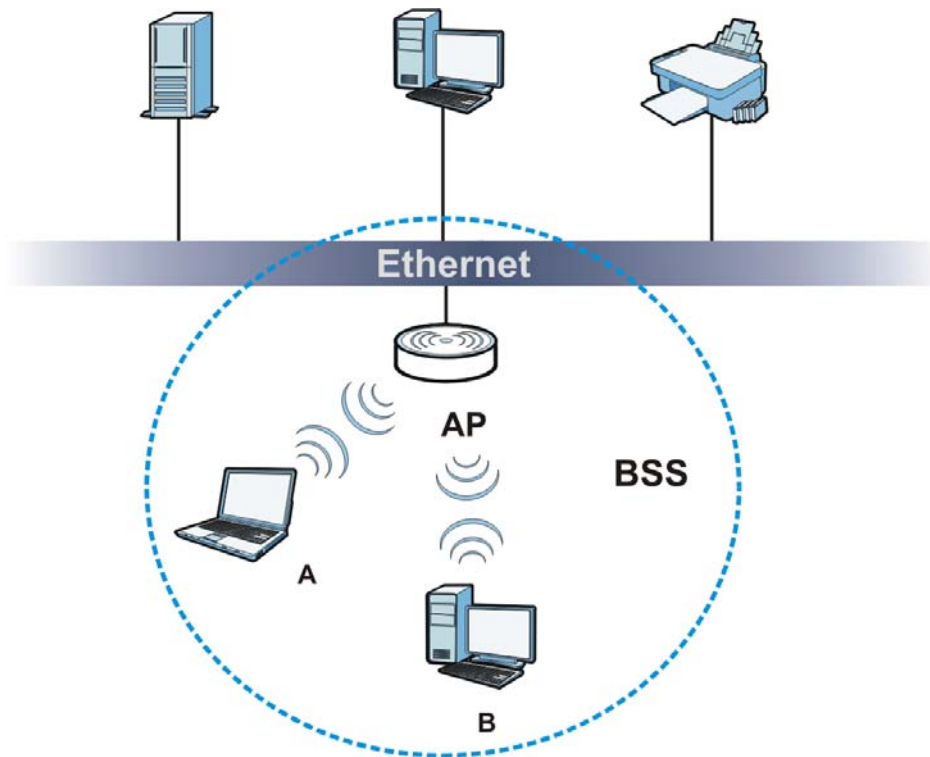
**Figure 133** Peer-to-Peer Communication in an Ad-hoc Network



## BSS

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

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

**Figure 134** Basic Service Set

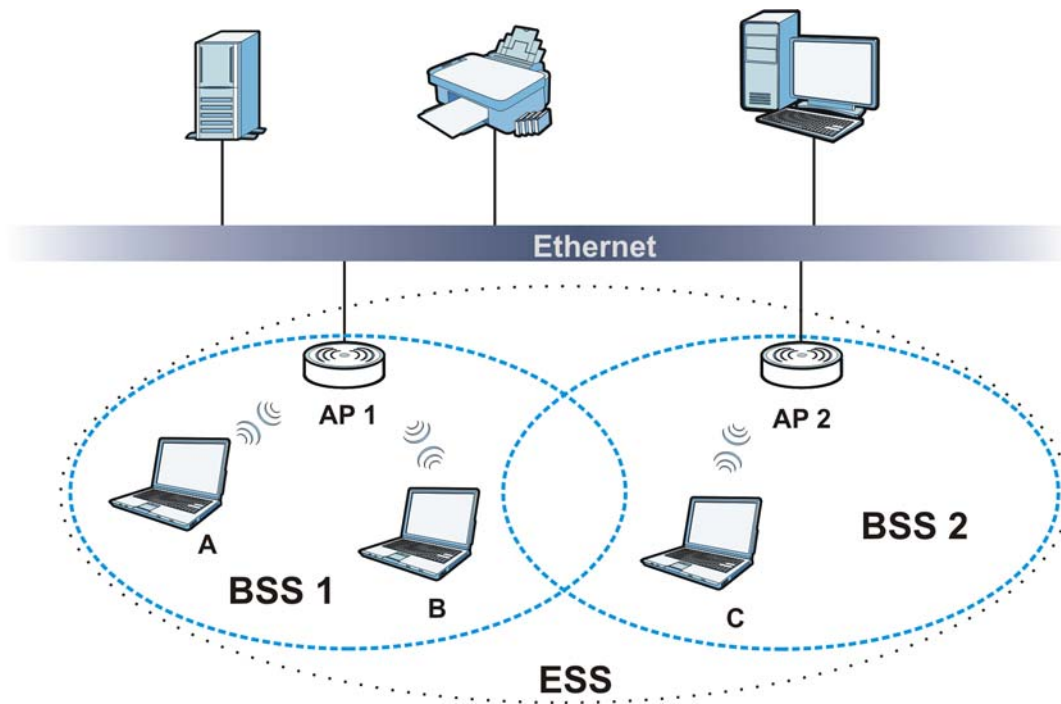
## ESS

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

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

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

Figure 135 Infrastructure WLAN



## Channel

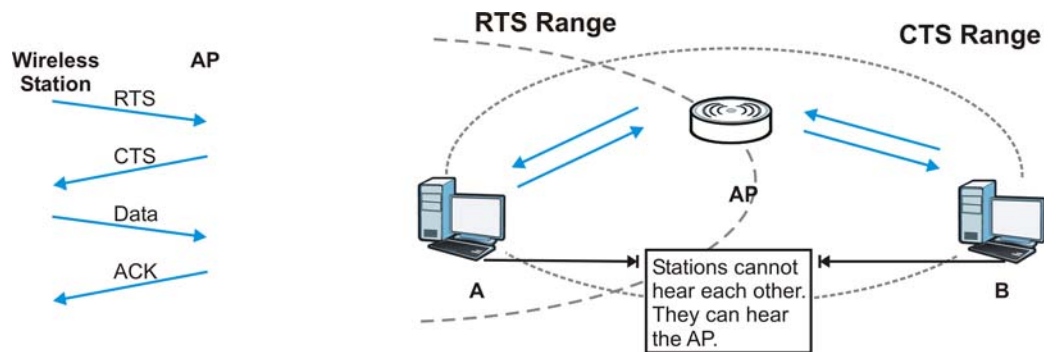
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference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

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

## RTS/CTS

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

Figure 136 RTS/CTS



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

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

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

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

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

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

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

## Fragmentation Threshold

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

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

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

## Preamble Type

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

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

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

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

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the NBG-418N uses long preamble.

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

## IEEE 802.11g Wireless LAN

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

**Table 70** IEEE 802.11g

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

## Wireless Security Overview

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

Wireless security methods available on the NBG-418N are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NBG-418N identity.

The following figure shows the relative effectiveness of these wireless security methods available on your NBG-418N.

**Table 71** Wireless Security Levels

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

Note: You must enable the same wireless security settings on the NBG-418N and on all wireless clients that you want to associate with it.

## IEEE 802.1x

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

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

## RADIUS

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

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

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

## Types of RADIUS Messages

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

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

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

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

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

## Types of EAP Authentication

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

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

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

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

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

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

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

## EAP-TLS (Transport Layer Security)

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

## EAP-TTLS (Tunneled Transport Layer Service)

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

## PEAP (Protected EAP)

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

## LEAP

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

## Dynamic WEP Key Exchange

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



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

**Note:** EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

**Table 72** Comparison of EAP Authentication Types

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

## WPA and WPA2

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

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

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

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

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

## Encryption

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

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm

called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

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

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

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

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

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

## User Authentication

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

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

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

## Wireless Client WPA Supplicants

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

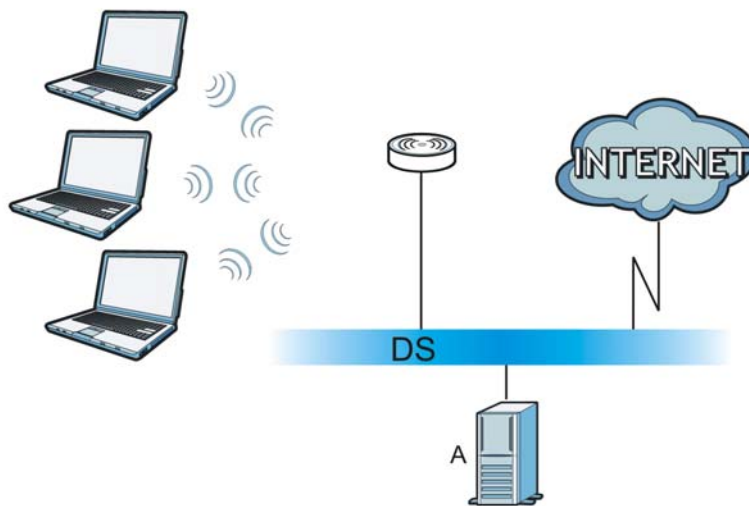
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

## WPA(2) with RADIUS Application Example

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

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
- 4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

**Figure 137** WPA(2) with RADIUS Application Example



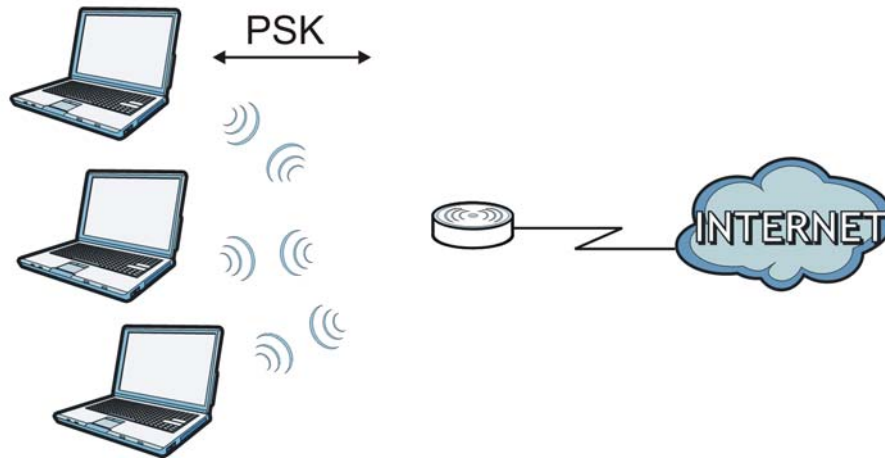
## WPA(2)-PSK Application Example

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

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

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

**Figure 138** WPA(2)-PSK Authentication



## Security Parameters Summary

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

**Table 73** Wireless Security Relational Matrix

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

## Antenna Overview

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

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

## Antenna Characteristics

### Frequency

An antenna in the frequency of 2.4GHz or 5GHz is needed to communicate efficiently in a wireless LAN

### Radiation Pattern

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

### Antenna Gain

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

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

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

## Types of Antennas for WLAN

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

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

## Positioning Antennas

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

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

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

## 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.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.

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

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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).



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

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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 © 2012 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

## Disclaimer

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

## Certifications

### Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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



### FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b, 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.

## 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。

## 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.

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

This Class B digital apparatus complies with Canadian ICES-003.  
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

## Viewing Certifications

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 (all products)

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 zařízení 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/ΕΚ.
[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 taghmir jikkonforma mal-htigijiet 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.

#### France

For 2.4 GHz, the output power is restricted to 10 mW EIRP when the product is used outdoors in the band 2454 - 2483.5 MHz. There are no restrictions when used indoors or in other parts of the 2.4 GHz band. Check <http://www.arcep.fr> for more details.

Pour la bande 2.4 GHz, la puissance est limitée à 10 mW en p.i.r.e. pour les équipements utilisés en extérieur dans la bande 2454 - 2483.5 MHz. Il n'y a pas de restrictions pour des utilisations en intérieur ou dans d'autres parties de la bande 2.4 GHz. Consultez <http://www.arcep.fr/> pour de plus amples détails.

R&TTE 1999/5/EC		
WLAN 2.4 – 2.4835 GHz		
IEEE 802.11 b/g/n		
Location	Frequency Range(GHz)	Power (EIRP)
Indoor (No restrictions)	2.4 – 2.4835	100mW (20dBm)
Outdoor	2.4 – 2.454	100mW (20dBm)
	2.454 – 2.4835	10mW (10dBm)

#### 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

Address Assignment [86](#)  
 Advanced Encryption Standard  
   See AES.  
 AES [203](#)  
 Alert [129](#)  
 alternative subnet mask notation [149](#)  
 antenna  
   directional [207](#)  
   gain [207](#)  
   omni-directional [207](#)  
 AP (access point) [197](#)  
 AP Mode  
   menu [42, 47](#)  
   overview [35](#)  
   status screen [37, 45, 49, 53](#)

## B

Backup configuration [133](#)  
 Basic Service Set, See BSS [195](#)  
 BSS [195](#)

## C

CA [202](#)  
 Certificate Authority  
   See CA.  
 certifications  
   notices [213](#)  
   viewing [214](#)  
 Channel [39, 46, 50, 53](#)  
 channel [69, 197](#)  
   interference [197](#)  
 client bridge [13](#)  
 Configuration  
   backup [133](#)

  reset the factory defaults [134](#)  
   restore [133](#)  
 copyright [213](#)  
 CPU usage [39, 46, 50, 54](#)  
 CTS (Clear to Send) [198](#)

## D

Daylight saving [128](#)  
 DDNS  
   service providers [109](#)  
 device mode [13, 35](#)  
 DHCP [40, 97](#)  
   DHCP server  
     see also Dynamic Host Configuration Protocol  
 DHCP client information [100](#)  
 DHCP client list [100](#)  
 DHCP server [94, 97](#)  
 DHCP table [40, 100](#)  
   DHCP client information  
   DHCP status  
 disclaimer [213](#)  
 DNS [30, 99](#)  
   DNS server  
     see also Domain name system  
 DNS Server [86](#)  
 DNS server [99](#)  
 documentation  
   related [2](#)  
 Domain name [23](#)  
   vs host name. see also system name  
 Domain Name System [99](#)  
 Domain Name System. See DNS.  
 duplex setting [40, 46, 50, 54](#)  
 Dynamic DNS [109](#)  
 Dynamic Host Configuration Protocol [97](#)  
 dynamic WEP key exchange [202](#)  
 DynDNS [109](#)  
 DynDNS see also DDNS [109](#)

**E**

EAP Authentication [201](#)  
encryption [70, 203](#)  
    key [70](#)  
    WPA compatible [70](#)  
ESS [196](#)  
ESSID [145](#)  
Extended Service Set, See ESS [196](#)  
Extended wireless security [24](#)

**F**

Factory LAN defaults [94, 97](#)  
FCC interference statement [213](#)  
Firewall  
    ICMP packets [113](#)  
    ZyXEL device firewall [112](#)  
firewall  
    stateful inspection [111](#)  
Firmware upload [131](#)  
    file extension  
    using HTTP  
firmware version [39, 46, 49, 53](#)  
fragmentation threshold [198](#)

**G**

General wireless LAN screen [70](#)  
Guide  
    Quick Start [2](#)

**H**

hidden node [197](#)

**I**

IANA [154](#)  
IBSS [195](#)

IEEE 802.11g [199](#)  
Independent Basic Service Set  
    See IBSS [195](#)  
initialization vector (IV) [204](#)  
Internet Assigned Numbers Authority  
    See IANA [154](#)  
Internet connection  
    Ethernet  
    PPPoE. see also PPP over Ethernet  
    PPTP  
    WAN connection  
Internet connection wizard [25](#)  
IP Address [95, 104](#)  
IP address [30](#)  
    dynamic  
IP Pool [98](#)

**L**

LAN [93](#)  
    IP pool setup [94](#)  
LAN overview [93](#)  
LAN setup [93](#)  
LAN TCP/IP [94](#)  
Language [139](#)  
Link type [40, 46, 50, 54](#)  
Local Area Network [93](#)  
Log [129](#)

**M**

MAC [75](#)  
MAC address [69, 86](#)  
    cloning [31, 86](#)  
MAC address filter [69](#)  
MAC address filtering [75](#)  
MAC filter [75](#)  
managing the device  
    good habits [14](#)  
Media access control [75](#)  
Memory usage [39, 46, 50, 54](#)  
Message Integrity Check (MIC) [203](#)

mode [13](#)

## N

NAT [101, 104, 154](#)

global [102](#)

how it works [101, 103](#)

inside [102](#)

local [102](#)

outside [102](#)

overview [101](#)

port forwarding [106](#)

see also Network Address Translation

server [103](#)

server sets [106](#)

NAT traversal [119](#)

Navigation Panel [42, 47, 51, 54](#)

navigation panel [42, 47, 51, 54](#)

Network Address Translation [101, 104](#)

## O

operating mode [13](#)

operation mode [35, 137](#)

access point [35](#)

client [36](#)

router [35](#)

universal repeater [36](#)

other documentation [2](#)

overview [13](#)

## P

Pairwise Master Key (PMK) [204, 205](#)

Point-to-Point Protocol over Ethernet [26, 88](#)

Point-to-Point Tunneling Protocol [27, 90](#)

Pool Size [98](#)

Port forwarding [104, 106](#)

default server [104, 106](#)

example [107](#)

local server [104](#)

port numbers

services

port speed [40, 46, 50, 54](#)

PPPoE [26, 88](#)

benefits [26](#)

dial-up connection

see also Point-to-Point Protocol over Ethernet [26](#)

PPTP [27, 90](#)

see also Point-to-Point Tunneling Protocol [27](#)

preamble mode [199](#)

product registration [214](#)

PSK [204](#)

## Q

Quality of Service (QoS) [78](#)

Quick Start Guide [2](#)

## R

RADIUS [200](#)

message types [201](#)

messages [201](#)

shared secret key [201](#)

registration

product [214](#)

related documentation [2](#)

Remote management [115](#)

and NAT [116](#)

and the firewall [115](#)

limitations [116](#)

system timeout [116](#)

Reset button [19, 134](#)

Reset the device [19](#)

Restore configuration [133](#)

Roaming [76](#)

RTS (Request To Send) [198](#)

threshold [197, 198](#)

RTS/CTS Threshold [68, 76, 77](#)

## S

safety warnings [216](#)

- Scheduling [81](#)
- screw anchor [16](#)
- Service Set [72](#)
- Service Set IDentification [72](#), [82](#), [83](#)
- Service Set IDentity. See SSID.
- SSID [39](#), [46](#), [53](#), [69](#), [72](#), [82](#), [83](#)
- stateful inspection firewall [111](#)
- Static DHCP [98](#)
- subnet [147](#)
- Subnet Mask [95](#)
- subnet mask [30](#), [148](#)
- subnetting [150](#)
- Summary
  - DHCP table [40](#)
  - Packet statistics [41](#)
  - Wireless station status [42](#)
- Sys Op Mode [137](#)
- System General Setup [125](#)
- System Name [126](#)
- System name [22](#)
  - vs computer name
- System restart [134](#)

## T

- TCP/IP configuration [97](#)
- Temporal Key Integrity Protocol (TKIP) [203](#)
- Time setting [126](#)

## U

- Universal Plug and Play [119](#)
  - application [119](#)
- universal repeater [13](#)
- UPnP [119](#)
  - security issues [119](#)

## V

- VPN [90](#)

## W

- wall mounting [16](#)
- WAN
  - IP address assignment [29](#)
- WAN (Wide Area Network) [85](#)
- WAN IP address [29](#)
- WAN IP address assignment [30](#)
- WAN MAC address [86](#)
- warranty [214](#)
  - note [214](#)
- Web Configurator
  - how to access [17](#)
  - Overview [17](#)
- WEP Encryption [74](#)
- WEP encryption [73](#)
- WEP key [73](#)
- Wi-Fi Protected Access [203](#)
- Wireless association list [42](#)
- wireless channel [145](#)
- wireless client WPA supplicants [204](#)
- wireless LAN [145](#)
- wireless LAN scheduling [81](#)
- Wireless LAN wizard [23](#)
- Wireless network
  - basic guidelines [68](#)
  - channel [69](#)
  - encryption [70](#)
  - example [67](#)
  - MAC address filter [69](#)
  - overview [67](#)
  - security [69](#)
  - SSID [69](#)
- Wireless security [69](#)
  - overview [69](#)
  - type [69](#)
- wireless security [145](#), [199](#)
- Wireless tutorial [57](#)
  - WPS [57](#)
- Wizard setup [21](#)
  - complete [32](#)
  - Internet connection [25](#)
  - system information [22](#)
  - wireless LAN [23](#)
- WLAN
  - interference [197](#)

- security parameters [206](#)
- WPA [203](#)
  - key caching [204](#)
  - pre-authentication [204](#)
  - user authentication [204](#)
  - vs WPA-PSK [204](#)
  - wireless client supplicant [204](#)
  - with RADIUS application example [205](#)
- WPA compatible [70](#)
- WPA2 [203](#)
  - user authentication [204](#)
  - vs WPA2-PSK [204](#)
  - wireless client supplicant [204](#)
  - with RADIUS application example [205](#)
- WPA2-Pre-Shared Key [203](#)
- WPA2-PSK [203, 204](#)
  - application example [205](#)
- WPA-PSK [203, 204](#)
  - application example [205](#)
- WPS [15](#)
- WPS button [15](#)

