NBG-418N v2

Wireless N300 Home Router

Version 1.0
Edition 1, 07/2014

User's Guide

Default Login Details	
LAN IP Address	http://192.168.1.1
User Name	admin
Password	1234

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the NBG-418N v2 and access the Web Configurator.

Note: It is recommended you use the Web Configurator to configure the NBG-418N v2.

Contents Overview

Table of Contents

PART I
User's Guide

1 Introduction

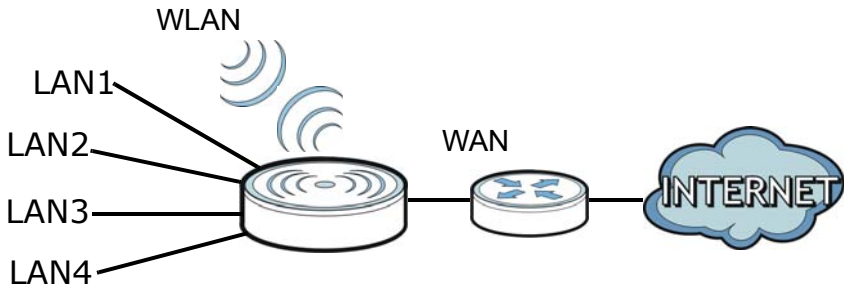
1.1 Overview

The NBG-418N v2 extends the range of your existing wired network without additional wiring, providing easy network access to mobile users.

Your can create the following connections using the NBG-418N v2:

- **LAN**. You can connect network devices via the Ethernet ports of the NBG-418N v2 so that they can communicate with each other and access the Internet.
- **WLAN**. Wireless clients can connect to the NBG-418N v2 to access network resources.
- **WAN**. Connect to a broadband modem/router for Internet access.

Figure 1 NBG-418N v2 Network

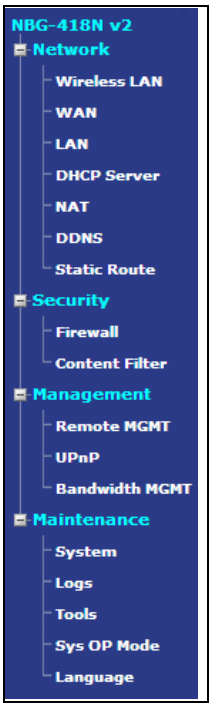


You can set up the NBG-418N v2 with other IEEE 802.11b/g/n compatible devices in one of the following device modes:

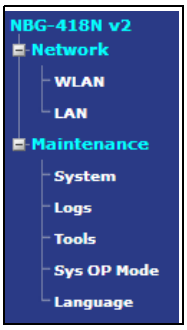
- Router
- Access Point
- Universal Repeater

Use a (supported) web browser to manage the NBG-418N v2. Menus vary according to which mode you're using.

Router Mode



Non-Router Mode



See Chapter 4 on page 29 for more information on these modes.

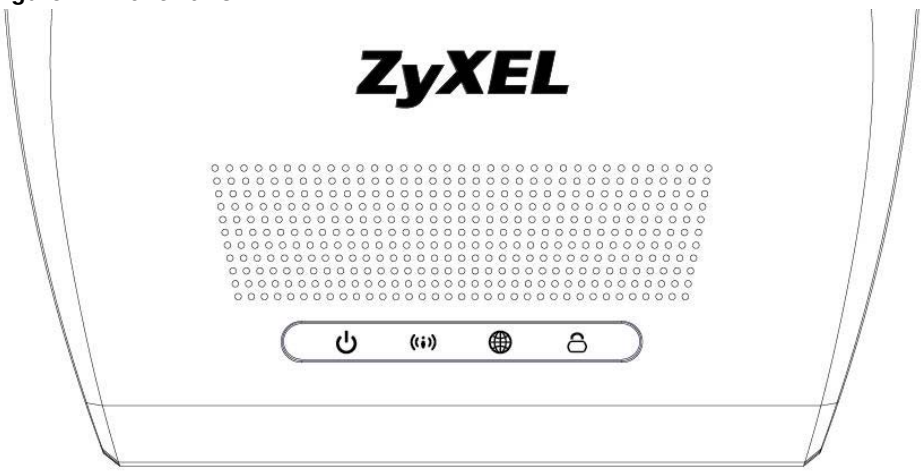
1.2 Securing the NBG-418N v2

Do the following things regularly to make the NBG-418N v2 more secure and to manage the NBG-418N v2 more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the NBG-418N v2 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG-418N v2. You could simply restore your last configuration.

1.3 LEDs

Figure 2 Front Panel



The following table describes the LEDs and the WPS button.

Table 1 Front Panel LEDs and WPS Button

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The NBG-418N v2 is receiving power and functioning properly.
		Off	The NBG-418N v2 is not receiving power.
WAN	Green	On	The NBG-418N v2 has a successful 10/100MB WAN connection.
		Blinking	The NBG-418N v2 is sending/receiving data through the WAN.
		Off	The WAN connection is not ready, or has failed.
WLAN	Green	On	The NBG-418N v2 is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG-418N v2 is sending/receiving data through the wireless LAN. The NBG-418N v2 is negotiating a WPS connection with a wireless client.
		Off	The wireless LAN is not ready or has failed.
WPS	Green	On	WPS status is configured.
		Blinking	The NBG-418N v2 is negotiating a WPS connection with a wireless client.
		Off	The WPS status is not configured or disabled.

1.4 The WPS/RESET Button

Your NBG-418N v2 supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (recommended) on the device itself, or in its configuration utility or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

The **WPS / RESET** single button is located at the back panel of the NBG-418N v2.

1.4.1 Using the WPS/RESET Button

1. Make sure the power LED is on.
2. Press the **WPS / RESET** button within 3 seconds to turn on the WPS function
3. Press the **WPS / RESET** button for longer than 10 seconds to restart/reboot the NBG-418N v2 back to its factory-default configurations.

For more information on using **WPS / RESET**, see Section 5.3 on page 44.

1.5 Wall Mounting

You may need screw anchors if mounting on a concrete or brick wall.

Table 2 Wall Mounting Information

Distance between holes	10.50 cm
M4 Screws	Two
Screw anchors (optional)	Two

1. Select a position free of obstructions on a wall strong enough to hold the weight of the device.
2. Mark two holes on the wall at the appropriate distance apart for the screws.

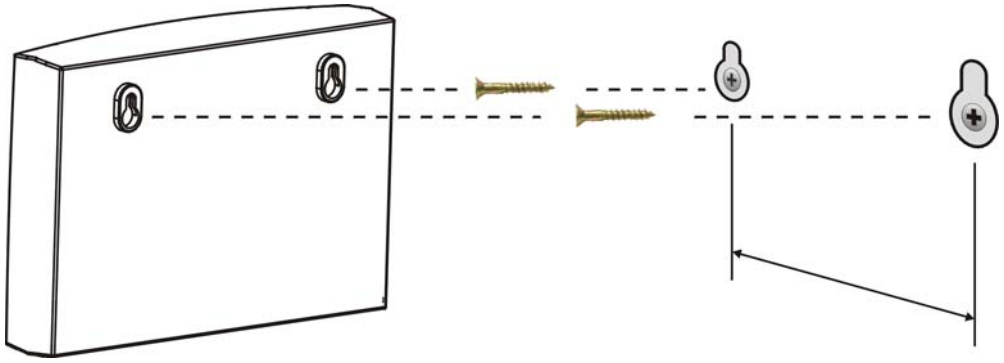
Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

3. If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

   If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.
4. Make sure the screws are fastened well enough to hold the weight of the NBG-418N v2 with the connection cables.

5 Align the holes on the back of the NBG-418N v2 with the screws on the wall. Hang the NBG-418N v2 on the screws.

Figure 3 Wall Mounting Example



2

The Web Configurator

2.1 Overview

This chapter describes how to access the NBG-418N v2 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the NBG-418N v2 via Internet browser. Use Internet Explorer 8.0 and later versions, Mozilla Firefox, Google Chrome or Safari. The recommended screen resolution is 1024 by 768 pixels.

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

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

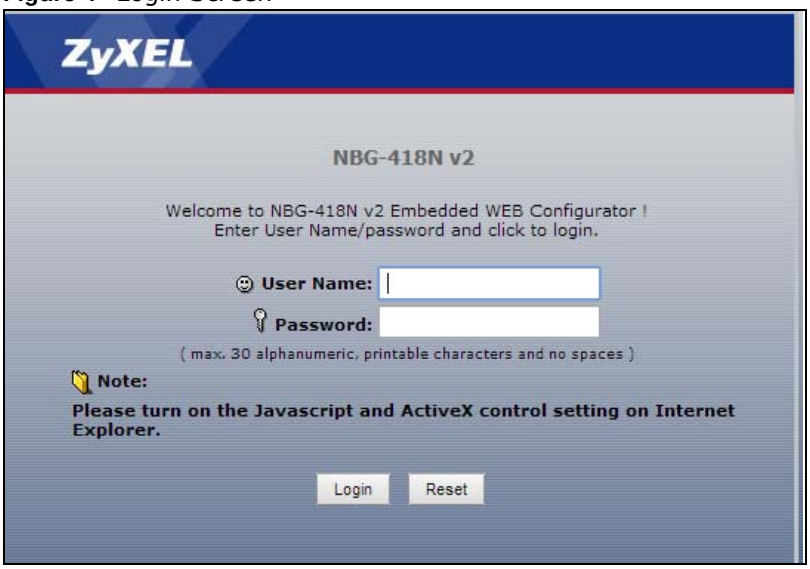
Refer to Chapter 21 Troubleshooting to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

1. Make sure your NBG-418N v2 hardware is properly connected and prepare your computer or computer network to connect to the NBG-418N v2 (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "http://192.168.1.1" as the website address in your web browser. This is the default LAN IP address in router mode (the default device mode). (The default IP address in non-router mode is 192.168.1.2).

   Your computer must be in the same subnet in order to access this website address. In router mode, the NBG-418N v2 can assign your computer an IP address, so you must set your computer to get an IP address automatically (computer factory default) or give it a fixed IP address in the range between 192.168.1.3 and 192.168.1.254 (see the appendices).
4. Type **admin** (default) as the user name and **1234** (default) as the password and click **OK**.

Figure 4 Login Screen

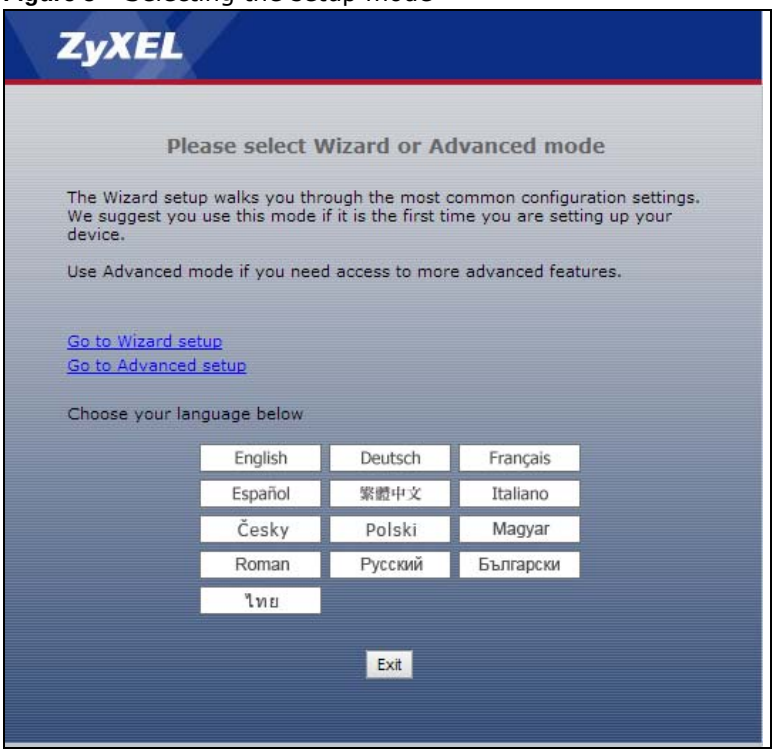


Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the NBG-418N v2 if this happens.

5 Select the setup type you want to use.

- Click **Go to Wizard Setup** to use the Configuration Wizard for basic Internet and Wireless setup.
- Click **Go to Advanced Setup** to view and configure all the NBG-418N v2's settings.
- Select a language to go to the basic Web Configurator in that language. To change to the advanced configurator see Chapter 20 on page 141.

Figure 5 Selecting the setup mode



2.3 Resetting the NBG-418N v2

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **WPS/RESET** button at the back of the NBG-418N v2 to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the username will be reset to **admin** and password will be reset to **1234**. The IP address will be reset to "192.168.1.1".

Make sure the power LED is on and press the **WPS/RESET** button for longer than 10 seconds to restart/reboot and set the NBG-418N v2 back to its factory-default configurations.

3

Connection Wizard

3.1 Wizard Setup

This chapter provides information on the wizard setup screens in the Web Configurator.

The Web Configurator's wizard setup helps you configure your device to access the Internet. Refer to your ISP (Internet Service Provider) checklist in the Quick Start Guide to know what to enter in each field. Leave a field blank if you don't have that information.

1 After you access the NBG-418N v2 Web Configurator, click **Go to Wizard setup**.

Figure 6 Select Go to Wizard setup

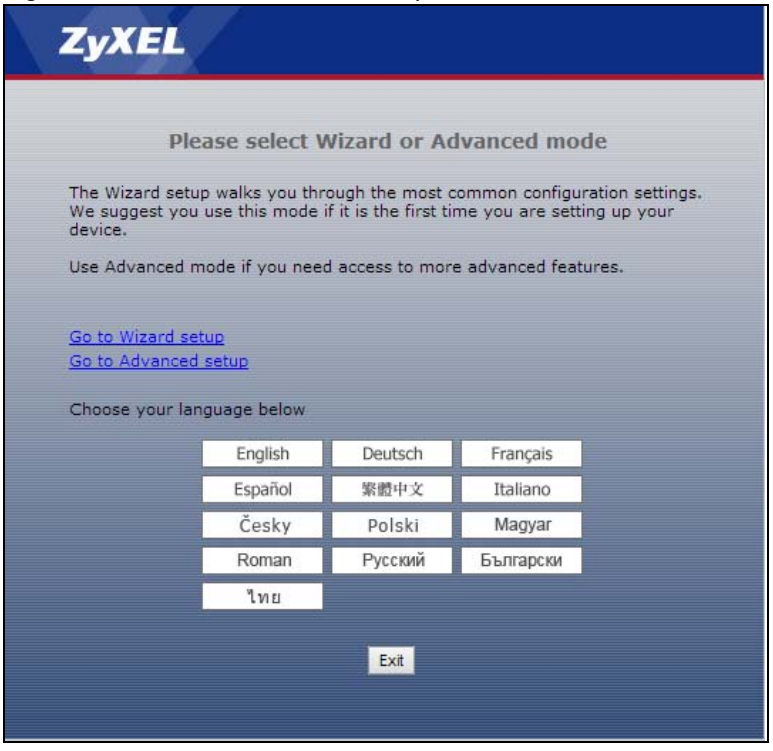
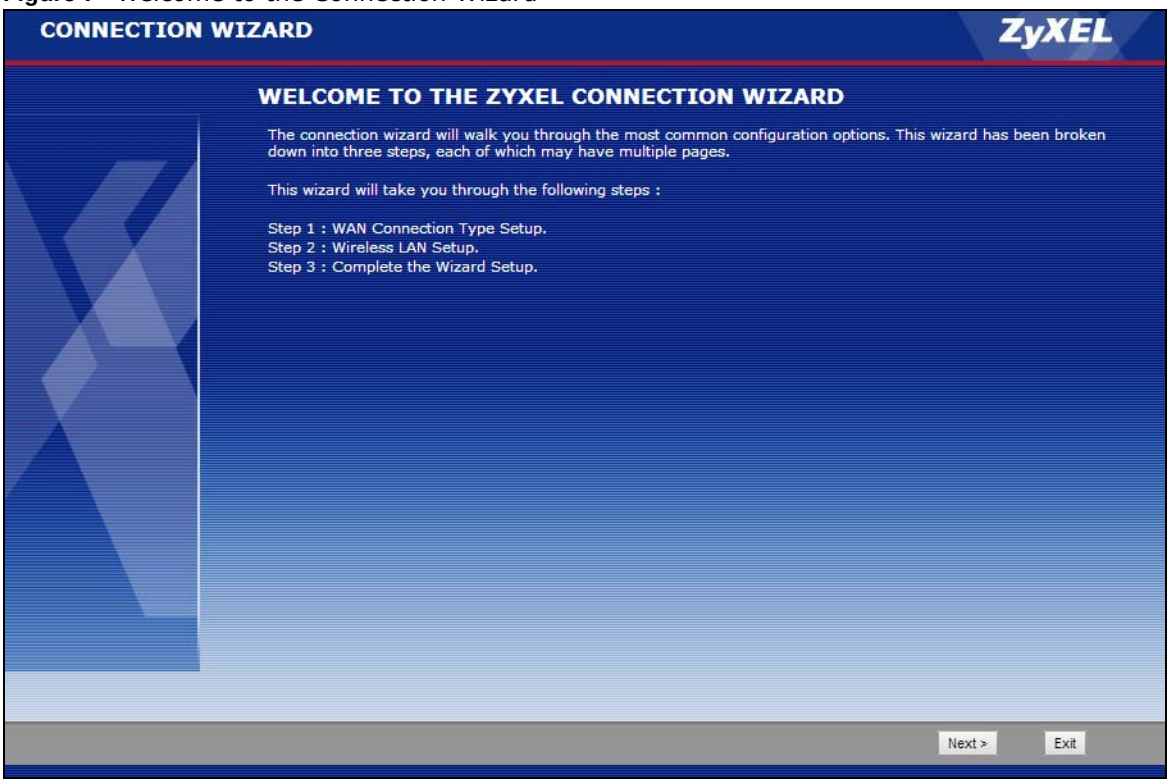


Figure 7 Welcome to the Connection Wizard



2 Read the on-screen information and click **Next**.

3.2 Connection Wizard: STEP 1: WAN Connection Type

The NBG-418N v2 offers three Internet connection types. They are **PPP over Ethernet (PPPoE)** or **Dynamic IP or Static IP**. You must select one from the check box in Step 1 of the Wizard. Check with your ISP to make sure you use the correct type.

Figure 8 Wizard Step 1: WAN Connection Type: PPPoE, Dynamic IP, Static IP

The following table describes the labels in this screen.

Table 3 Wizard Step 1: WAN Connection Type

LABEL	DESCRIPTION
PPPoE	Select **PPPoE** radio button for a dial-up connection.
Dynamic IP	Select **Dynamic IP** radio button if your ISP did not assign you a fixed IP address.
Static IP	Select **Static IP** radio button, provided by your ISP to give the NBG-418N v2 a fixed, unique IP Address.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

3.2.1 PPPoE Connection

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, RADIUS).

One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

By implementing PPPoE directly on the NBG-418N v2 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG-418N v2 does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Figure 9 Wizard Step 2: PPPoE Connection

The following table describes the labels in this screen.

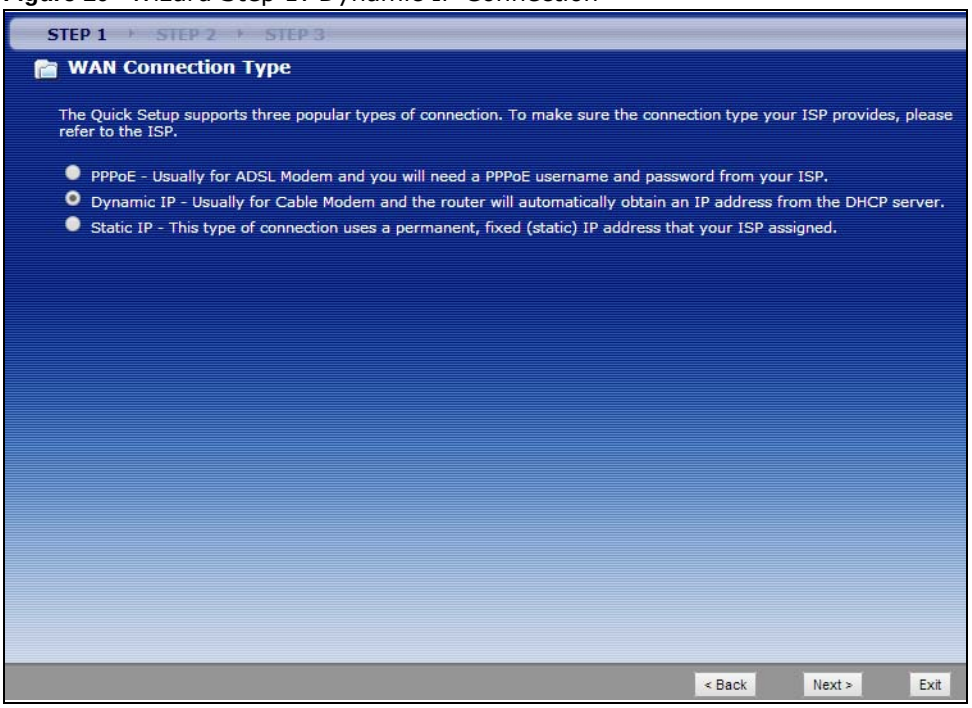
Table 4 Wizard Step 2: PPPoE Connection

LABEL	DESCRIPTION
PPPoE	
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Confirm Password	Type the password again for confirmation.
Account Validate	Click the **Account Validate** button to establish the Internet connection via PPPoE encapsulation.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

3.2.2 Dynamic IP Connection

Use the dynamic IP connection when your network administrator or ISP assigns your IP address dynamically.

Figure 10 Wizard Step 1: Dynamic IP Connection



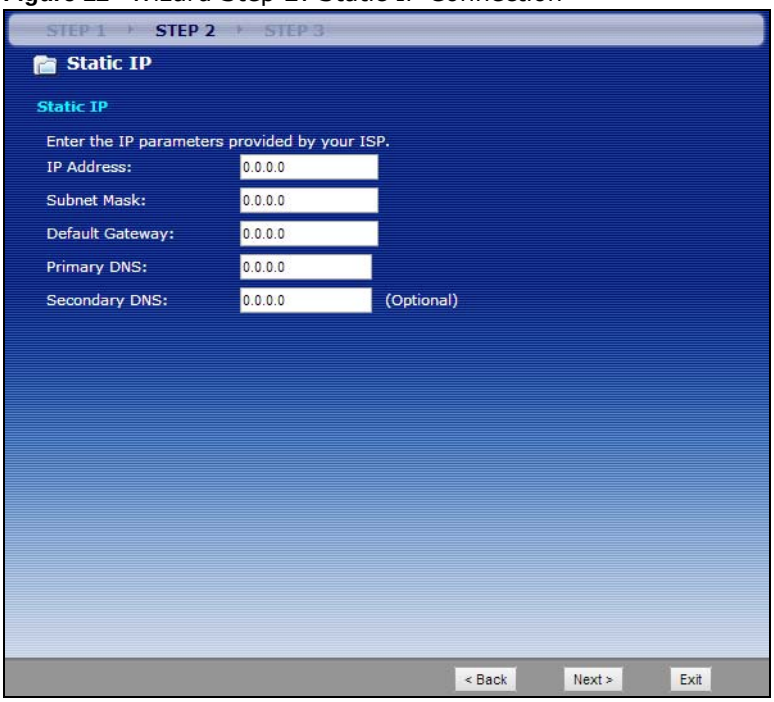
3.2.3 Static IP Connection

The following wizard screen allows you to assign a fixed IP address to the NBG-418N v2

Figure 11 Wizard Step 2: Static IP

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

Figure 12 Wizard Step 2: Static IP Connection



The following table describes the labels in this screen

Table 5 Wizard Step 2: Static IP Connection

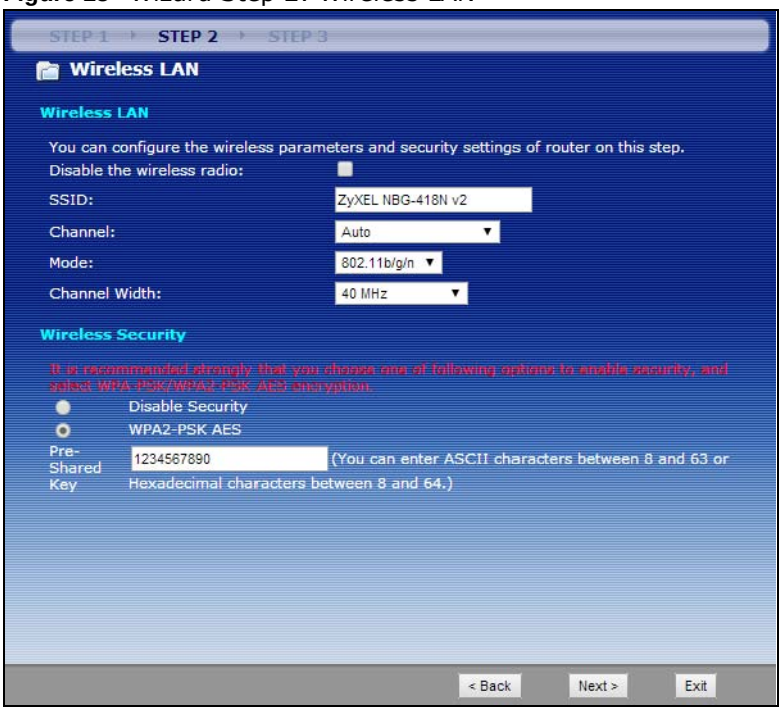
LABEL	DESCRIPTION
IP Address	Select this option if you were given IP address and/or DNS server settings by the ISP. The fixed IP address should be in the same subnet as your broadband modem or router.
Subnet Mask	Enter the subnet mask address in this field.
Default Gateway	Enter the gateway IP address provided by your ISP.
Primary DNS	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The NBG-418N v2 uses a system DNS server (in the order you specify here) to resolve domain names for DDNS and the time server. Enter the primary DNS server's IP address in this field.
Secondary DNS	Enter the secondary DNS server's IP address in this field. This field is optional.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

Click **Next** to configure the WLAN for the NBG-418N v2.

3.3 Connection Wizard: STEP 2: Wireless LAN

Set up your wireless LAN using the following screen.

Figure 13 Wizard Step 2: Wireless LAN



The following table describes the labels in this screen.

Table 6 Wizard Step 2: Wireless LAN

LABEL	DESCRIPTION
Wireless LAN	
Disable the wireless radio	Click this check box to disable the WLAN in the NBG-418N v2.
SSID	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the NBG-418N v2, make sure all wireless stations use the same SSID in order to access the network.
Channel	The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in.
Mode	Select the IEEE 802.11 WLAN mode you wish to use on the NBG-418N v2 from the drop-down list.
Channel Width	Select the channel bandwidth you want to use for your wireless network. Select **Auto 20/40 MHz** to allow theNBG-418N v2 to adjust the channel bandwidth to 40 MHz or 20 MHz depending on network conditions. Select **20 MHz** if you want to lessen radio interference with other wireless devices in your neighborhood.
Wireless Security	
Disable Security	Click this check box to disable security settings for the WLAN.

Table 6 Wizard Step 2: Wireless LAN (continued)

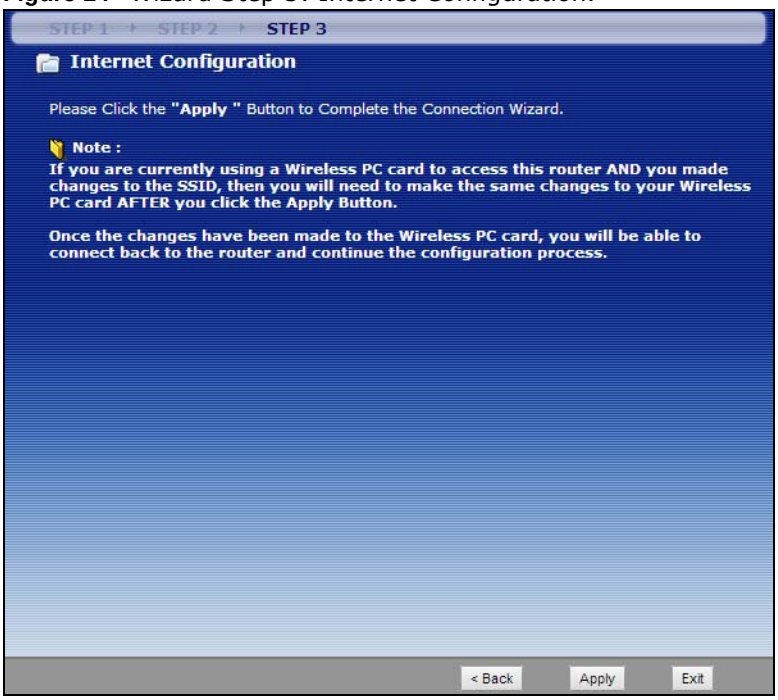
LABEL	DESCRIPTION
WPA2-PSK AES	Choose **WPA2-PSK AES** security to configure a Pre-Shared Key. Choose this option only if your wireless clients support WPA2-PSK. You will need to enter a Pre-Shared Key in the box below.
Pre-Shared Key	Type in a string of ASCII characters between 8 and 63 or hexadecimal characters between 8 and 64 for the Pre-Shared Key field.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

Note: The wireless stations and NBG-418N v2 must use the same SSID, channel ID, WPA-PSK (if WPA-PSK is enabled) or WPA2-PSK (if WPA2-PSK is enabled) for wireless communication.

3.4 Connection Wizard: STEP 3: Internet Configuration

Click **Apply** to finish setting up your NBG-418N v2 to operate on your network and access the Internet.This wizard screen varies according to the connection type that you select.

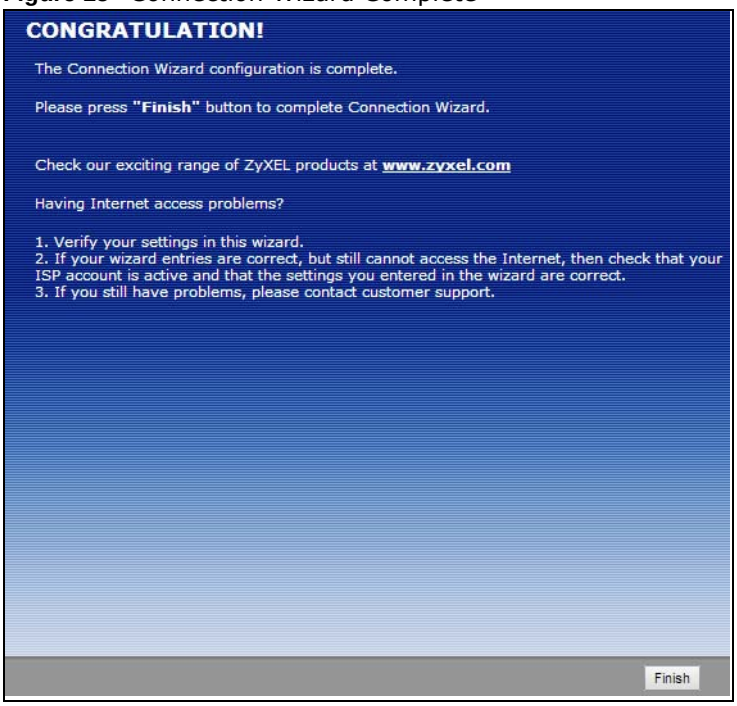
Figure 14 Wizard Step 3: Internet Configuration.



3.5 Connection Wizard Complete

Click **Finish** to complete the wizard setup.

Figure 15 Connection Wizard Complete



Well done! You have successfully set up your NBG-418N v2 to operate on your network and access the Internet.

4

Modes

4.1 Overview

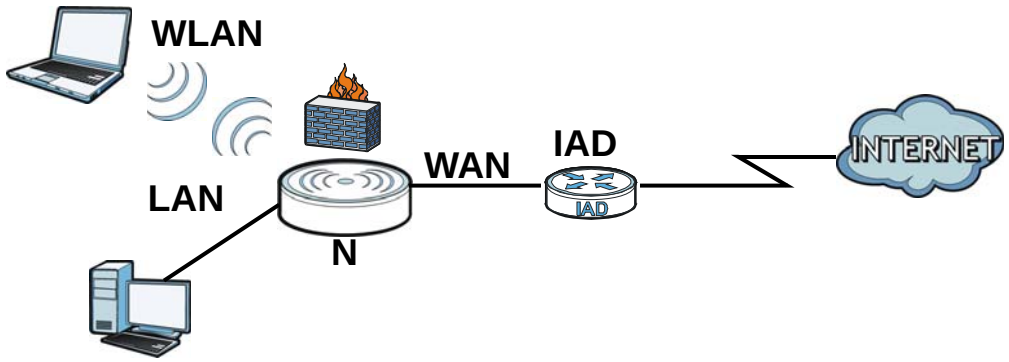
You can set up the NBG-418N v2 with other IEEE 802.11b/g/n compatible devices in different device modes.

Note: Choose your device mode carefully to avoid having to change it later. The NBG-418N v2 automatically restarts when you change modes.

The default LAN IP address of the NBG-418N v2 in Router mode is 192.168.1.1. The default IP address of the NBG-418N v2 in other modes is 192.168.1.2.

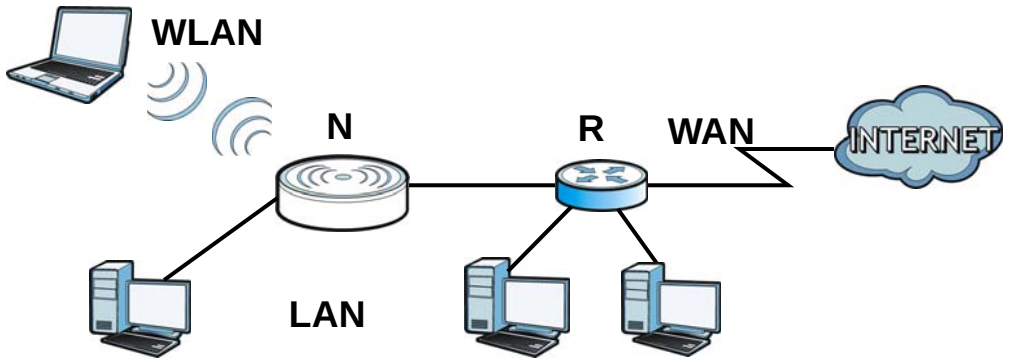
- **Router**: Use this mode if you want to use routing functions such as LAN DHCP, NAT, firewall and so on, on the NBG-418N v2 (N). The NBG-418N v2 has separate LAN and WAN network IP addresses. Connect the WAN port to an Internet Access Device (IAD) such as a broadband modem.

Figure 16 Router



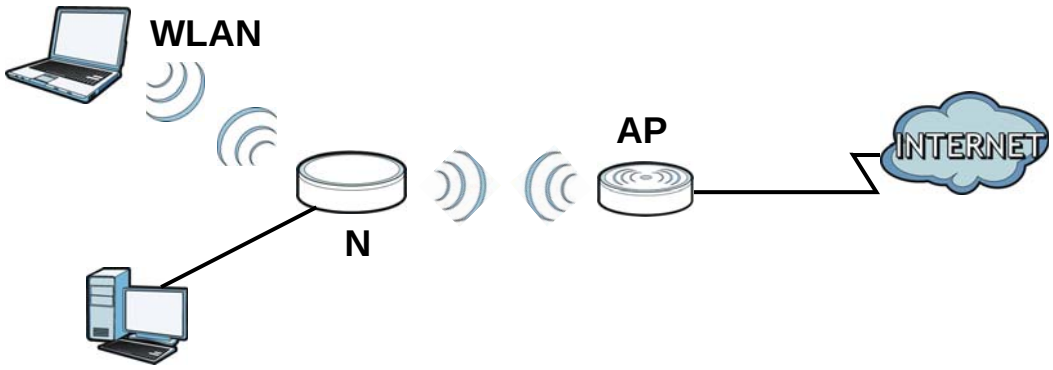
- **Access Point**: Use this mode if you already have a Router (R) in your network and you want to set up a wireless network and bridge the wired and wireless connections on the NBG-416N.

Figure 17 AP Mode



- **Universal Repeater**: In this mode, the NBG-418N v2 (N) can be an access point and a wireless client at the same time. Use this mode if there is an existing wireless router or access point in your network and you want the NBG-418N v2 (N) to wirelessly relay communications from its wireless clients to the access point.

Figure 18 Universal Repeater



4.2 Setting your NBG-418N v2 to Router Mode

The NBG-418N v2 is set to wireless router mode by default. If it was changed and now you want to set it back, do the following procedure.

1 Connect your computer to the LAN port of the NBG-418N v2.

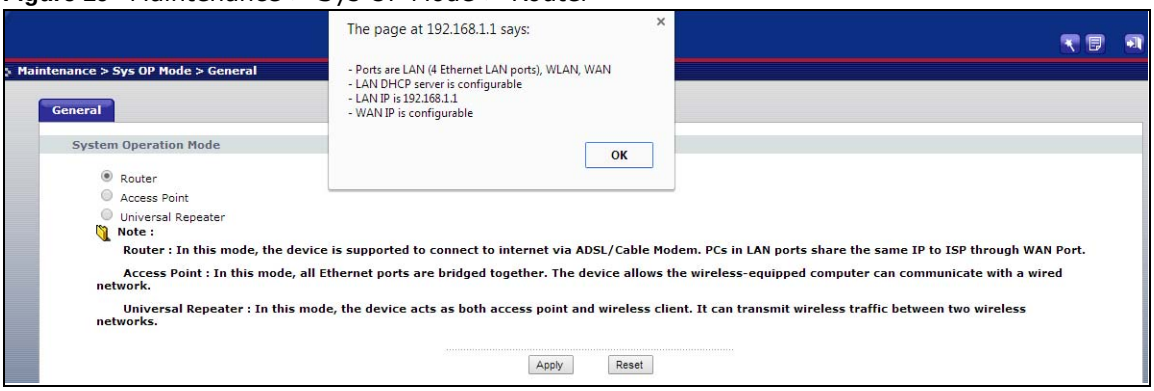
2 The default LAN IP address of the NBG-418N v2 is 192.168.1.1 in router mode (192.168.1.2 by default in non-router mode). In router mode, the NBG-418N v2 can assign your computer an IP address, so you must set your computer to get an IP address automatically (computer factory default) or give it a fixed IP address in the range between 192.168.1.3 and 192.168.1.254.

3 After you've set your computer's IP address, open a web browser such as Internet Explorer and type the IP address of the NBG-418N v2 as the web address in your web browser.

4 Log into the Web Configurator. See the Chapter 2 on page 17 for instructions on how to do this.

5 Go to **Maintenance > Sys OP Mode > General** and select **Router**.

Figure 19 Maintenance > Sys OP Mode > Router



6 A pop-up window appears providing information on this mode. Click **OK** in the pop-up message window. Click **Apply**.

Note: Wait while the NBG-418N v2 restarts, then log in to the Web Configurator again. The NBG-418N v2 IP address is now 192.168.1.1.

4.2.1 Status Screen (Router Mode)

The screen below shows the status screen in **Router** mode.

Figure 20 Status Screen (Router Mode)

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

Table 7 Status Screen Icon Key

ICON	DESCRIPTION
	Click this icon to open the setup wizard.
	Click this icon to view copyright and a link for related product information.
	Click this icon at any time to exit the Web Configurator.

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

Table 8 Web Configurator Status Screen (Router Mode)

LABEL	DESCRIPTION
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance** > **System** > **General** screen. It is for identification purposes.
Firmware Version	This is the current firmware version of the NBG-418N v2.
WAN Information	
- MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
- Connection Type	This shows the current connection type.
- IP Address	This shows the WAN port's IP address.
- IP Subnet Mask	This shows the WAN port's subnet mask.
- Gateway	This shows the WAN port's gateway IP address.
- DNS	This shows the IP address of your DNS server.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP Server	This shows the LAN port's DHCP server status.
WLAN Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - **On**, **Off** or **Off by scheduler**.
- Name (SSID)	This shows a descriptive name used to identify the NBG-418N v2 in the wireless LAN.
- Channel	This shows the channel number which you select manually or the NBG-418N v2 automatically scans and selects.
- Operating Channel	This shows the channel number which the NBG-418N v2 is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG-418N v2 is using.
- 802.11 Mode	This shows the wireless standard.
- WPS	This displays **Configured** when the WPS has been set up. This displays **Unconfigured** if the WPS has not been set up. Click the status to display **Network** > **Wireless LAN** > **WPS** screen.
IPv6	
Network Status	This field displays the IPv6 network connection status.
Connection Type	This field displays the IPv6 connection type that is currently in use.
WAN Address	This field displays the current WAN IPv6 address of the NBG-418N v2.
Default Gateway	This field displays the IPV6's gateway address of the NBG-418N v2.
Primary DNS	This field displays the IPV6's primary DNS server's address of the NBG-418N v2.
Secondary DNS	This field displays the IPV6's secondary DNS server's address of the NBG-418N v2.
DHCP-PD	This field displays the status of the IPv6 DHCP's Prefix Delegation.
DHCP-PD Prefix	This field displays the delegated IPv6 DHCP's Prefixes.

Table 8 Web Configurator Status Screen (Router Mode) (continued)

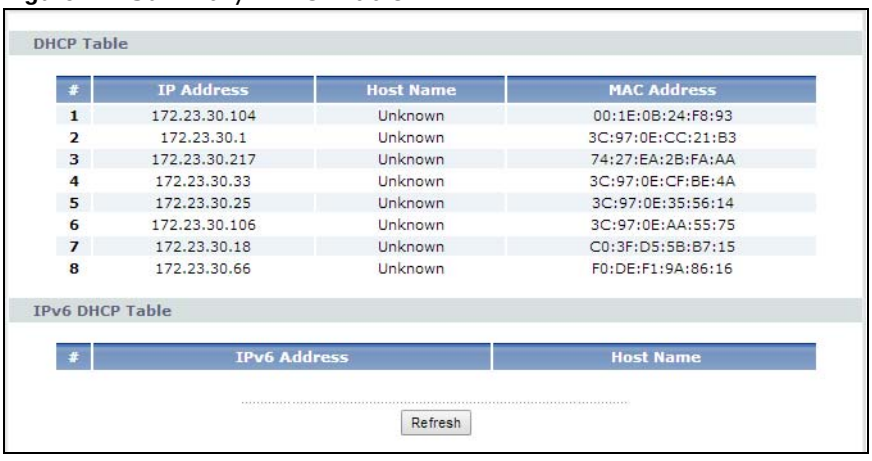
LABEL	DESCRIPTION
Link-Local Address	This field displays the link-local IP address of the NBG-418N v2 LAN port. A link-local address is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device.
LAN Address	This field displays the IPv6 LAN's IP address.
System Status	
Operation Mode	This field shows the device operation mode: **Router**, **Access Point**, or **Universal Repeater**.
System Up Time	This is the total time the NBG-418N v2 has been on.
Current Date/Time	This field displays your NBG-418N v2's present date and time.
System Setting	
- Firewall	This shows whether the firewall is active or not.
- UPnP	This shows whether UPnP is active or not.
Summary	
DHCP Table	Use this screen to view current DHCP client information. Click "**Details**" to see the screen.
Packet Statistics	Use this screen to view port status and packet specific statistics. Click "**Details**" to see the screen.
WLAN Station Status	Use this screen to view the wireless stations that are currently associated to the NBG-418N v2.

4.2.1.1 Summary: DHCP Table

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the NBG-418N v2's LAN as a DHCP server or disable it. When configured as a server, the NBG-418N v2 provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on that network, or else the computer must be manually configured.

Click the **DHCP Table (Details...)** hyperlink in the **Status** screen. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the NBG-418N v2's DHCP server.

Figure 21 Summary: DHCP Table



The following table describes the labels in this screen.

Table 9 Summary: DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
IPv6 DHCP Table	
#	This is the index number of the IPv6 DHCP table.
IPv6 Address	This field displays the IPv6 DHCP address.
Hostname	This field displays the IPv6 DHCP hostname.
Refresh	Click **Refresh** to renew the screen.

4.2.1.2 Summary: Packet Statistics

Click the **Packet Statistics (Details...)** hyperlink in the **Status** screen. Read-only information here includes port status, packet specific statistics and the "system up time". The **Poll Interval(s)** field is configurable and is used for refreshing the screen.

Figure 22 Summary: Packet Statistics

The following table describes the labels in this screen.

Table 10 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the NBG-418N v2's port type.
RxPkts	This is the number of received packets on this port.
Rx err	This is the number of received packets with errors on this port.
Rx drop	This is the number of received packets that were dropped on this port.
Txpkts	This is the number of transmitted packets on this port.
Tx err	This is the number of transmitted packets with errors on this port.
Tx drop	This is the number of transmitted packets that were dropped on this port.
System Up Time	This is the total time the NBG-418N v2 has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.

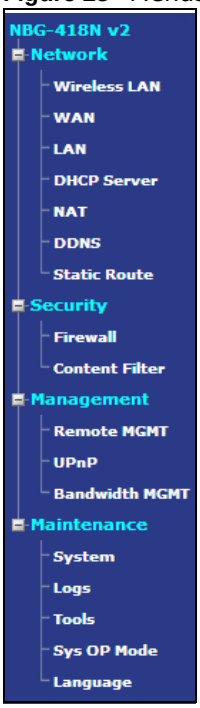
Table 10 Summary: Packet Statistics (continued)

LABEL	DESCRIPTION
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

4.2.2 Router Mode Navigation Panel

Use the menu in the navigation panel menus to configure NBG-418N v2 features in **Router Mode**.

Figure 23 Menus: Router Mode



The following table describes the sub-menus.

Table 11 Menus: Router Mode

LINK	TAB	FUNCTION
Network		
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG-418N v2 to block access to devices or block the devices from accessing the NBG-418N v2.
	Advanced	This screen allows you to configure advanced wireless settings.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
	MBSSID	Use this screen to configure the SSID that is associated with the radio.

Table 11 Menus: Router Mode (continued)

LINK	TAB	FUNCTION
WAN	Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
	Advanced	Use this screen to configure multicast WAN and auto IP setup.
	IPv6	Use this screen to set the IPv6 WAN connection type.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
DHCP Server	General	Use this screen to enable the NBG-418N v2's DHCP server.
	Advanced	Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
	Client List	Use this screen to view current DHCP client information and to always assign an IP address to a MAC address (and host name).
NAT	General	Use this screen to enable NAT.
	Application	Use this screen to configure servers behind the NBG-418N v2.
	Port Triggering	Use this screen to configure port triggering settings on the NBG-418N v2.
DDNS	General	Use this screen to configure Dynamic DNS, a service that allows you to map a fixed domain name to a non-fixed IP address.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	Use this screen to enable or disable ICMP and VPN passthrough features.
Content Filter	Filter	Use this screen to configure content filter settings on the NBG-418N v2.
Management		
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the NBG-418N v2.
UPnP	General	Use this screen to enable UPnP on the NBG-418N v2.
Bandwidth MGMT	General	Use this screen to configure bandwidth management settings on the NBG-418N v2.
Maintenance		
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Time Setting	Use this screen to change your NBG-418N v2's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
Tools	Firmware	Use this screen to upload firmware to your NBG-418N v2.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG-418N v2.
	Restart	This screen allows you to reboot the NBG-418N v2 without turning the power off.
Sys OP Mode	General	This screen allows you to select the device operation mode.
Language	Language	This screen allows you to select the language you prefer.

4.3 Setting your NBG-418N v2 to AP Mode

1 Connect your computer to the LAN port of the NBG-418N v2.

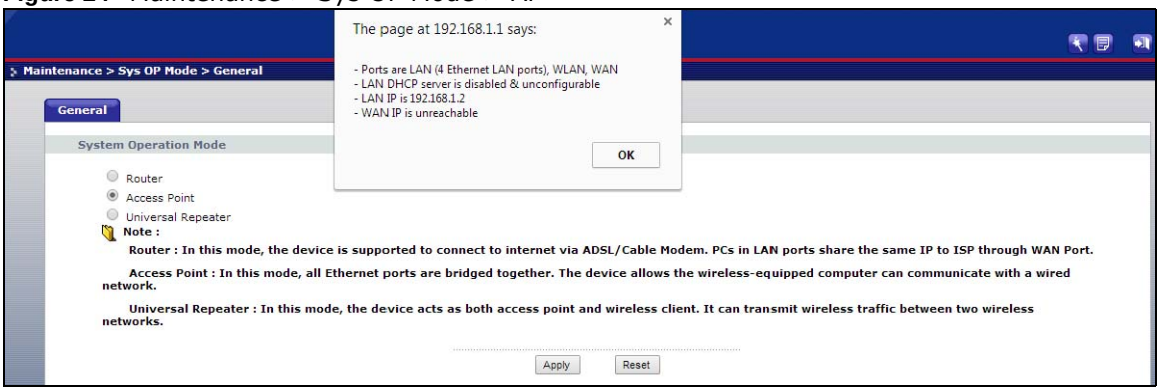
2 The default LAN IP address of the NBG-418N v2 is 192.168.1.1 in router mode (192.168.1.2 by default in non-router mode). In router mode, the NBG-418N v2 can assign your computer an IP address, so you must set your computer to get an IP address automatically (computer factory default) or give it a fixed IP address in the range between 192.168.1.3 and 192.168.1.254.

3 After you've set your computer's IP address, open a web browser such as Internet Explorer and type the IP address of the NBG-418N v2 as the web address in your web browser.

4 Log into the Web Configurator. See the Chapter 2 on page 17 for instructions on how to do this.

5 Go to **Maintenance > Sys OP Mode > General** and select **Access Point**.

Figure 24 Maintenance > Sys OP Mode > AP



6 A pop-up window appears providing information on this mode. Click **OK** in the pop-up message window. Click **Apply**. Your NBG-418N v2 is now in **AP Mode**.

Note: Wait while the NBG-418N v2 restarts, then log in to the Web Configurator again.

4.3.1 Status Screen (AP Mode)

Click on **Status**. The screen below shows the status screen in **AP Mode**.

Figure 25 Status Screen (AP Mode)

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

Table 12 Status Screen (AP Mode)

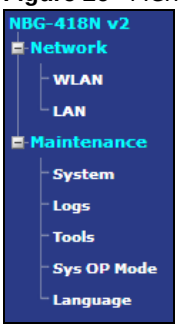
LABEL	DESCRIPTION
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance** > **System** > **General** screen. It is for identification purposes.
Firmware Version	This is the current firmware version of the NBG-418N v2.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP Server	This shows the LAN port's DHCP server status.
WLAN Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - **On**, **Off**, or **Off by scheduler**.
- Name (SSID)	This shows a descriptive name used to identify the NBG-418N v2 in the wireless LAN.
- Channel	This shows the channel number which you select manually or the NBG-418N v2 automatically scans and selects.
- Operating Channel	This shows the channel number which the NBG-418N v2 is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG-418N v2 is using.
- 802.11 Mode	This shows the IEEE 802.11 standard that the NBG-418N v2 supports. Wireless clients must support the same standard in order to be able to connect to the NBG-418N v2
- WPS	This shows the WPS (WiFi Protected Setup) Status. Click the status to display **Network** > **Wireless LAN** > **WPS** screen.
System Status	
Operation Mode	This field shows the device operation mode: **Router**, **Access Point**, or **Universal Repeater**.
System Up Time	This is the total time the NBG-418N v2 has been on.
Current Date/Time	This field displays your NBG-418N v2's present date and time.
System Setting	
Firewall	This shows the firewall settings on the NBG-418N v2.
UPnP	This shows the UPnP
Summary	
DHCP Table	This shows the DHCP clients.
Packet Statistics	Use this screen to view port status and packet specific statistics.

4.3.2 AP Navigation Panel

Use the menu in the navigation panel to configure NBG-418N v2 features in **AP Mode**.

The following screen and table show the features you can configure in **AP Mode**.

Figure 26 Menu: AP Mode



The following table describes the sub-menus.

Table 13 Menu: AP Mode

LINK	TAB	FUNCTION
Network		
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG-418N v2 to block access to devices or block the devices from accessing the NBG-418N v2.
	Advanced	This screen allows you to configure advanced wireless settings.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
	MBSSID	Use this screen to set the SSID for wireless AP.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
Maintenance		
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Time Setting	Use this screen to change your NBG-418N v2's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
Tools	Firmware	Use this screen to upload firmware to your NBG-418N v2.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG-418N v2.
	Restart	This screen allows you to reboot the NBG-418N v2 without turning the power off.
Sys OP Mode	General	This screen allows you to select the device operation mode: **Router**, **Access Point**, or **Universal Repeater**.
Language	Language	This screen allows you to select the language you prefer.

4.4 Setting your NBG-418N v2 to Universal Repeater Mode

1 Connect your computer to the LAN port of the NBG-418N v2.

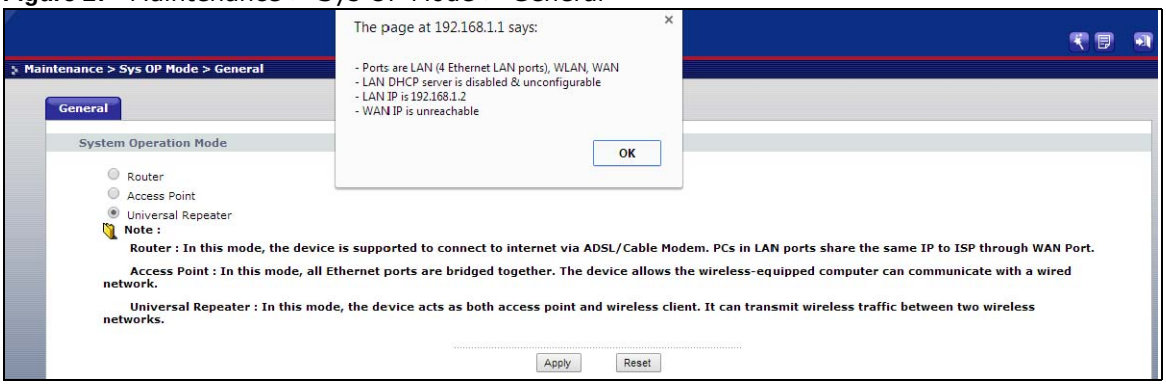
2 The default LAN IP address of the NBG-418N v2 is 192.168.1.1 in router mode (192.168.1.2 by default in non-router mode). In router mode, the NBG-418N v2 can assign your computer an IP address, so you must set your computer to get an IP address automatically (computer factory default) or give it a fixed IP address in the range between 192.168.1.3 and 192.168.1.254.

3 After you've set your computer's IP address, open a web browser such as Internet Explorer and type the IP address of the NBG-418N v2 as the web address in your web browser.

4 Log into the Web Configurator. See the Chapter 2 on page 17 for instructions on how to do this.

5 Go to **Maintenance > Sys OP Mode > General** and select **Universal Repeater**.

Figure 27 Maintenance > Sys OP Mode > General



6 A pop-up window appears providing information on this mode. Click **OK** in the pop-up message window. Click **Apply**. Your NBG-418N v2 is now in **Universal Repeater** mode.

Note: Wait while the NBG-418N v2 restarts, then log in to the Web Configurator again.

4.4.1 Status Screen (Universal Repeater Mode)

Click on **Status**. The screen below shows the status screen in Universal Repeater **Mode**.

Figure 28 Status Screen (Universal Repeater Mode)

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

Table 14 Status Screen (Universal Repeater Mode)

LABEL	DESCRIPTION
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance** > **System** > **General** screen. It is for identification purposes.
Firmware Version	This is the current firmware version of the NBG-418N v2.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP Server	This shows the LAN port's DHCP server.
WLAN AP Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - **On**, **Off**, or **Off by scheduler**.
- Name (SSID)	This shows a descriptive SSID name used to identify the NBG-418N v2 in the wireless LAN.
- Channel	This shows the channel number which you select manually or the NBG-418N v2 automatically scans and selects.
- Operating Channel	This shows the channel number which the NBG-418N v2 is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG-418N v2 is using.
- 802.11 Mode	This shows the IEEE 802.11 standard that the NBG-418N v2 supports. Wireless clients must support the same standard in order to be able to connect to the NBG-418N v2

Table 14 Status Screen (Universal Repeater Mode) (continued)

LABEL	DESCRIPTION
- WPS	This shows the WPS (WiFi Protected Setup) Status. Click the link to display **Network** > **Wireless LAN** > **WPS** screen.
WLAN STA Information	
- SSID	This is the name of the selected AP that the NBG-418N v2 is associating with.
- Security Mode	This shows the wireless security the NBG-418N v2 is using to connect to the AP.
- Connection Status	This shows whether the NBG-418N v2 is currently associated with the selected AP.
System Status	
Operation Mode	This field shows the device operation mode: **Router**, **Access Point**, or **Universal Repeater**.
System Up Time	This is the total time the NBG-418N v2 has been on.
Current Date/Time	This field displays your NBG-418N v2's present date and time.
System Setting	
Firewall	This field shows the firewall status
UPnP	This field shows the UPnP status.
Summary	
DHCP table	Use this screen to view current DHCP client information.
Packet Statistics	Use this screen to view port status and packet specific statistics.
Message	Use this screen to view the status of the NBG-418N v2.

4.4.2 Universal Repeater Navigation Panel

Use the menu in the navigation panel to configure NBG-418N v2 features in **Universal Repeater Mode**.

The following screen and table show the features you can configure in **Universal Repeater Mode**.

Figure 29 Menu: Universal Repeater Mode

The following table describes the sub-menus.

Table 15 Menu: Universal Repeater Mode

LINK	TAB	FUNCTION
Status		This screen shows the NBG-418N v2's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		
WLAN	AP Select	Use this screen to choose an access point that you want the NBG-418N v2 to connect to. You should know the security settings of the target AP.
	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG-418N v2 to block access to devices or block the devices from accessing the NBG-418N v2.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
Maintenance		
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Time Setting	Use this screen to change your NBG-418N v2's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
Tools	Firmware	Use this screen to upload firmware to your NBG-418N v2.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG-418N v2.
	Restart	This screen allows you to reboot the NBG-418N v2 without turning the power off.
Sys OP Mode	General	This screen allows you to select the device operation mode: **Router**, **Access Point**, or **Universal Repeater**.
Language	Language	This screen allows you to select the language you prefer.

5

Tutorials

5.1 Overview

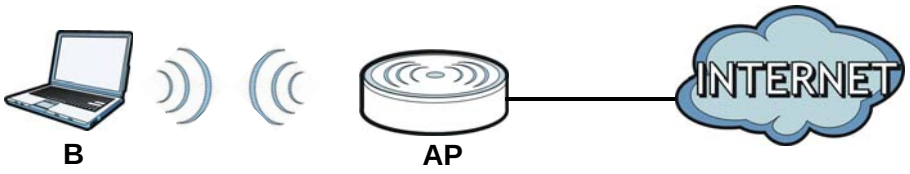
This chapter provides tutorials for your NBG-418N v2 as follows:

- How to Connect to the Internet from an AP
- Configure Wireless Security Using WPS on both your NBG-418N v2 and Wireless Client
- Enable and Configure Wireless Security without WPS on your NBG-418N v2
- Using Multiple SSIDs on the NBG-418N v2
- Using Bandwidth Management on the NBG-418N v2

5.2 How to Connect to the Internet from an AP

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

Figure 30 Wireless AP Connection to the Internet



5.3 Configure Wireless Security Using WPS on both your NBG-418N v2 and Wireless Client

This section gives you an example of how to set up wireless network using WPS. This example uses the NBG-418N v2 as the AP and NWD210N as the wireless client which connects to a notebook.

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

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

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 5.3.1 on page 45.This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the NBG-418N v2's interface. See Section 5.3.2 on page 46. This is the more secure method, since one device can authenticate the other.

5.3.1 Push Button Configuration (PBC)

1. Make sure that your NBG-418N v2 is turned on and that it is within range of your computer.
2. Make sure that you have installed the wireless client (this example uses the NWD210N) driver and utility in your notebook.
3. In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button)
4. Log into NBG-418N v2's Web Configurator and press **Push Button** in the **Network** > **Wireless LAN** > **WPS Station** screen.

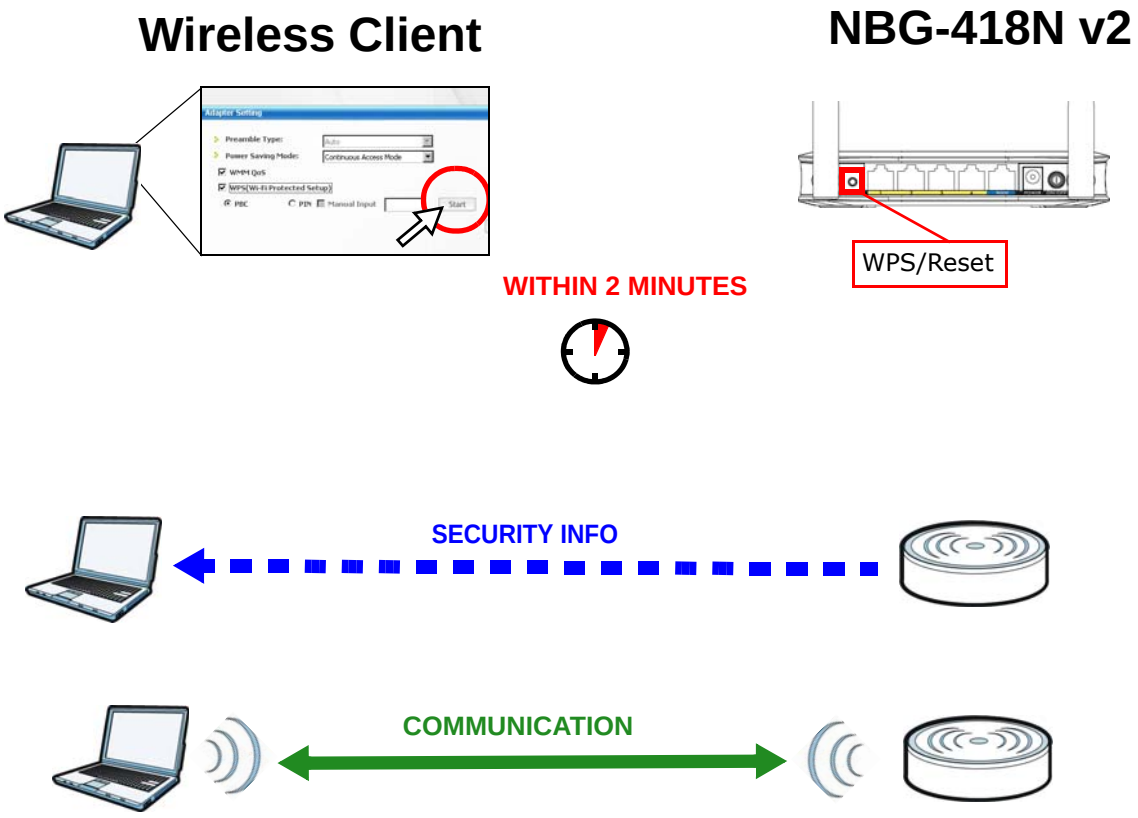
   Note: Your NBG-418N v2 has a WPS/RESET button located on its back panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

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

   The NBG-418N v2 sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NBG-418N v2 securely.

   The following figure shows you an example to set up wireless network and security by pressing a button on both NBG-418N v2 and wireless client (the NWD210N in this example).

Figure 31 Example WPS Process: PBC Method



5.3.2 PIN Configuration

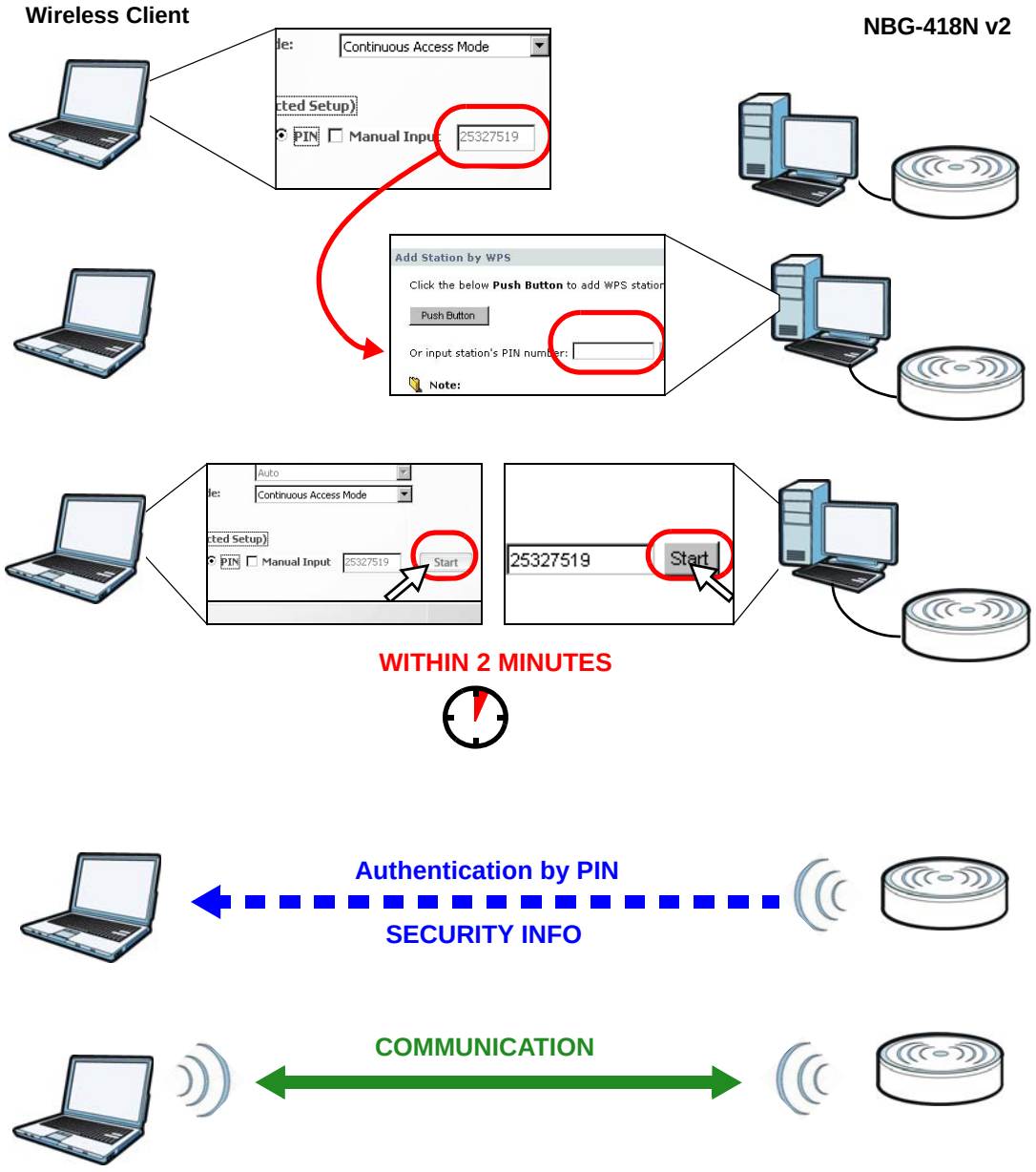
When you use the PIN configuration method, you need to use both NBG-418N v2's configuration interface and the client's utilities.

1. Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.
2. Enter the PIN number to the **PIN** field in the **Network** > **Wireless LAN** > **WPS Station** screen on the NBG-418N v2.
3. Click the **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the NBG-418N v2's **WPS Station** screen within two minutes.

   The NBG-418N v2 authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NBG-418N v2 securely.

   The following figure shows you the example to set up wireless network and security on NBG-418N v2 and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 32 Example WPS Process: PIN Method



5.4 Enable and Configure Wireless Security without WPS on your NBG-418N v2

This example shows you how to configure wireless security settings with the following parameters on your NBG-418N v2.

SSID	SSID_Example3
Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your NBG-418N v2.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see Section 2.2 on page 17).

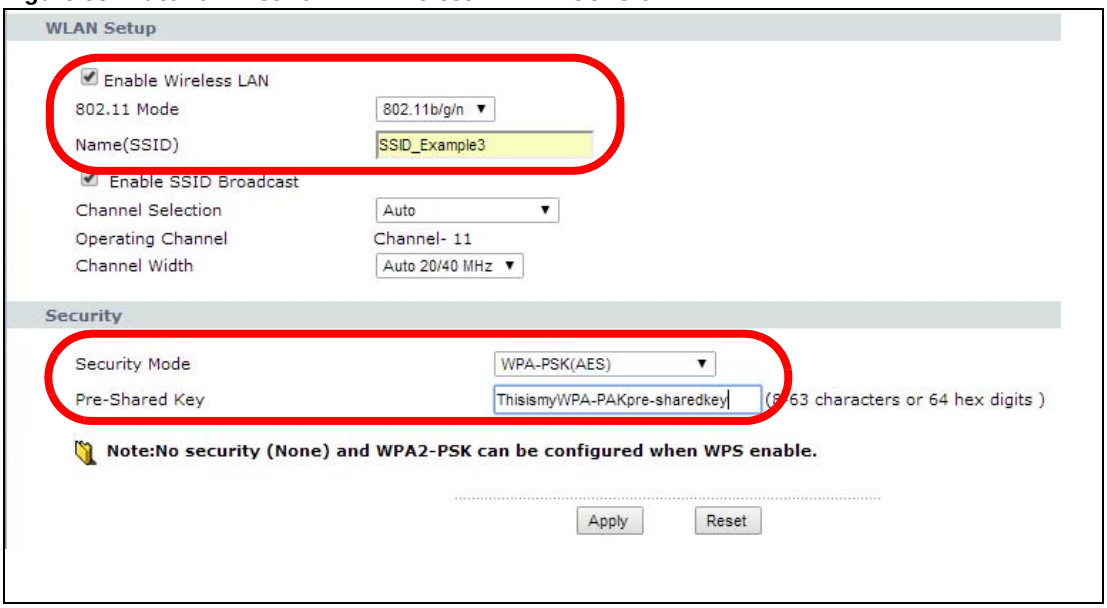
1 Open the **Wireless LAN > General** screen in the NBG-418N v2's Web Configurator.

2 Make sure the **Enable Wireless LAN** check box is selected.

3 Enter **SSID_Example3** as the SSID and select a channel.

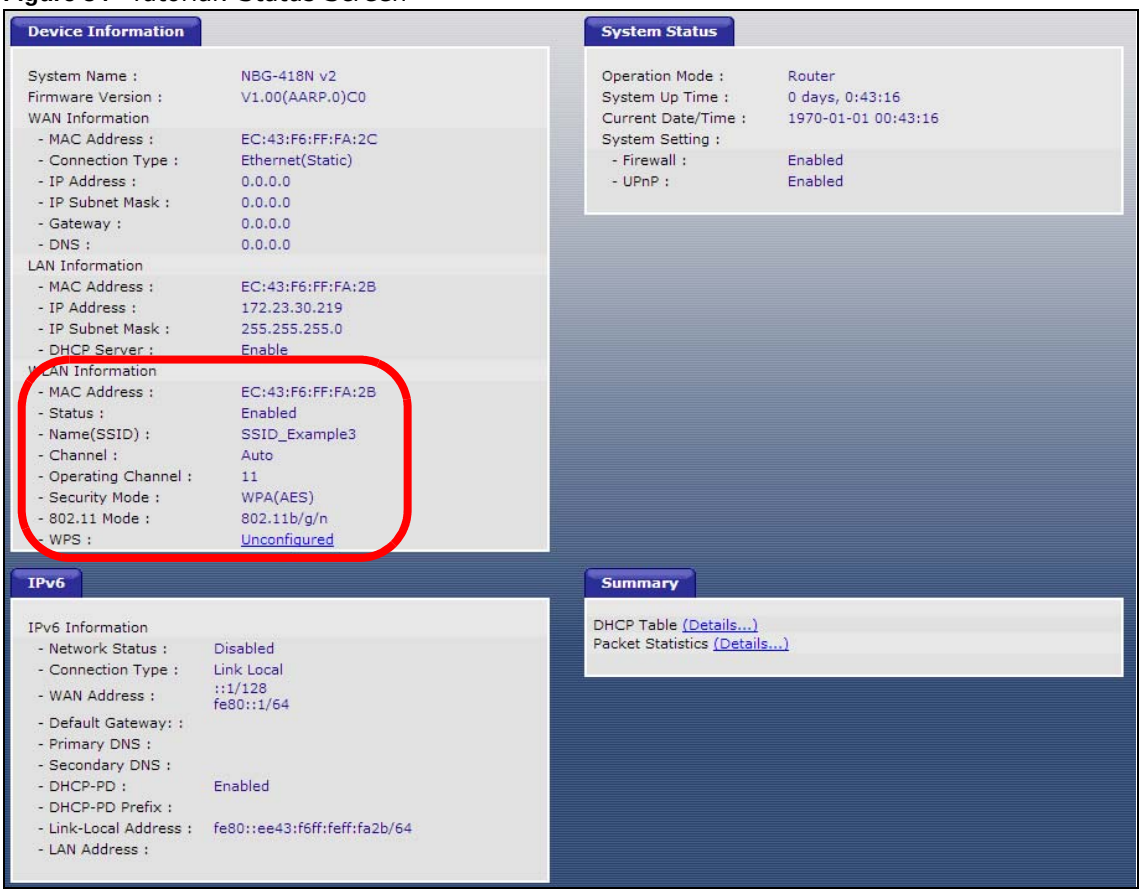
4 Set security mode to **WPA-PSK(AES)** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Figure 33 Tutorial: Network > Wireless LAN > General



5 Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Figure 34 Tutorial: Status Screen



5.4.1 Configure Your Wireless Client

Note: We use the ZyXEL M-302 wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

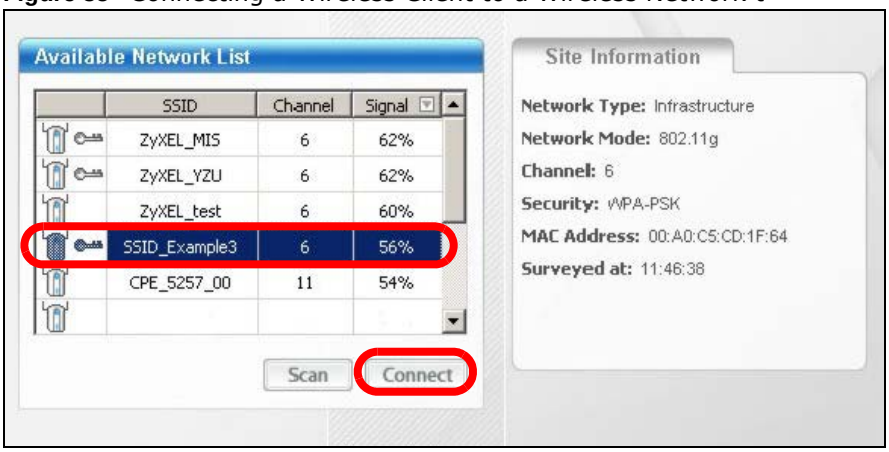
1 The NBG-418N v2 supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

2 Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless adapter's User's Guide for information on how to do that.

3 After you've installed the utility, open it. If you cannot see your utility's icon on your screen, go to **Start > Programs** and click on your utility in the list of programs that appears. The utility displays a list of APs within range, as shown in the example screen below.

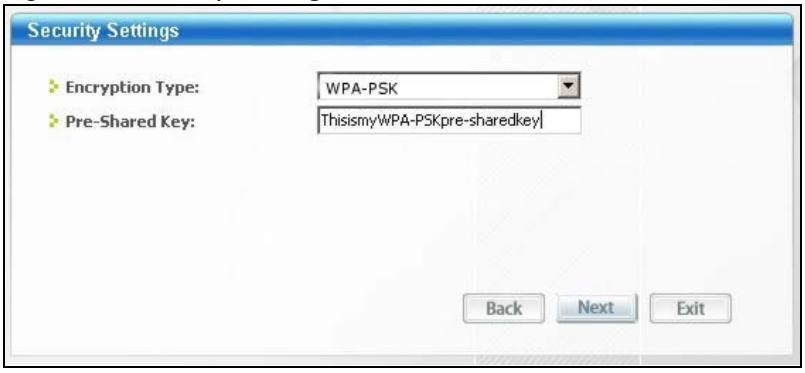
4 Select **SSID_Example3** and click **Connect**.

Figure 35 Connecting a Wireless Client to a Wireless Network t



5 Select WPA2-PSK and type the security key in the following screen. Click **Next**.

Figure 36 Security Settings

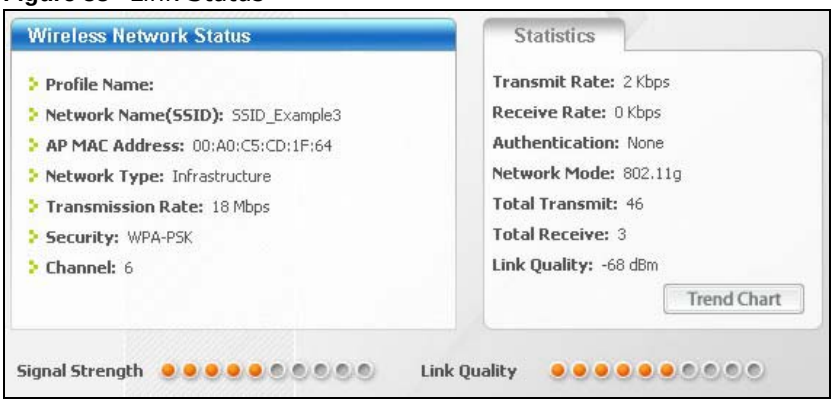


6 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 37 Confirm Save

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

Figure 38 Link Status



If your connection is successful, open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

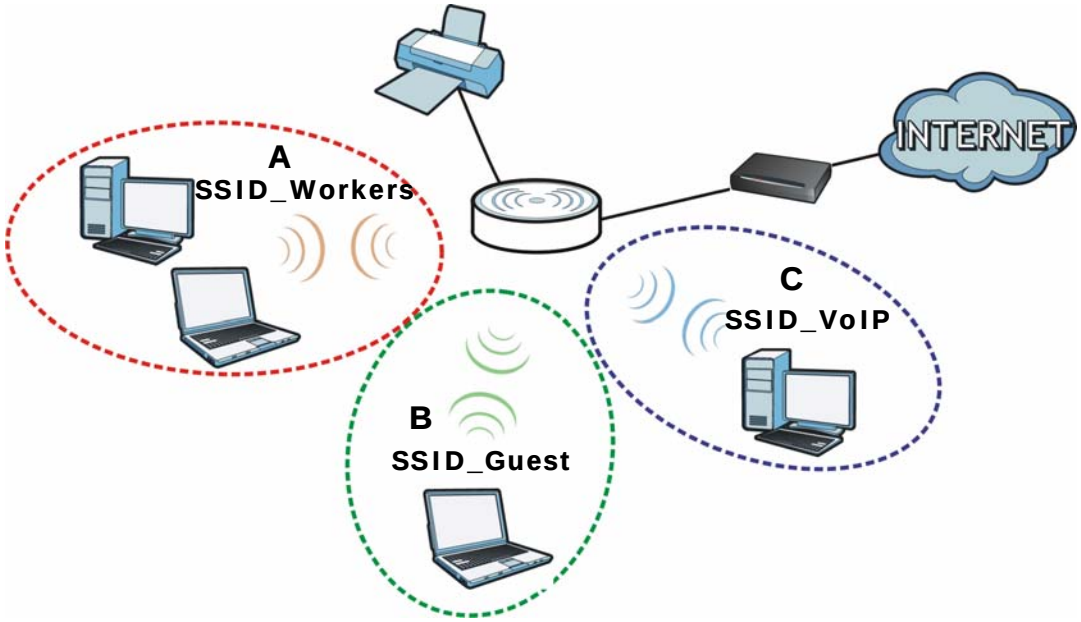
5.5 Using Multiple SSIDs on the NBG-418N v2

You can configure more than one SSID on a NBG-418N v2. See Section 11.4 on page 97.

This allows you to configure multiple independent wireless networks on the NBG-418N v2 as if there were multiple APs (virtual APs). Each virtual AP has its own SSID, wireless security type and MAC filtering settings. That is, each SSID on the NBG-418N v2 represents a different access point/ wireless network to wireless clients in the network.

Clients can associate only with the SSIDs for which they have the correct security settings. Clients using different SSIDs can access the Internet and the wired network behind the NBG-418N v2 (such as a printer).

For example, you may set up three wireless networks (**A**, **B** and **C**) in your office. **A** is for workers, **B** is for guests and **C** is specific to a VoIP device in the meeting room.



5.5.1 Configuring Security Settings of Multiple SSIDs

The NBG-418N v2 is in router mode by default.

This example shows you how to configure the SSIDs with the following parameters on your NBG-418N v2 (in router mode).

SSID	SECURITY TYPE	KEY	MAC FILTERING
SSID_Workers	WPA2-PSK WPA Compatible	DoNotStealMyWirelessNetwork	Disable
SSID_VoIP	WPA-PSK	VoIPOnly12345678	Allow 00:A0:C5:01:23:45
SSID_Guest	WPA-PSK	keyexample123	Disable

1 Connect your computer to the LAN port of the NBG-418N v2 using an Ethernet cable.

2 The default IP address of the NBG-418N v2 in router mode is "192.168.1.1". In this case, your computer must have an IP address in the range between "192.168.1.2" and "192.168.1.254".

3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix B on page 200 for information on changing your computer's IP address.

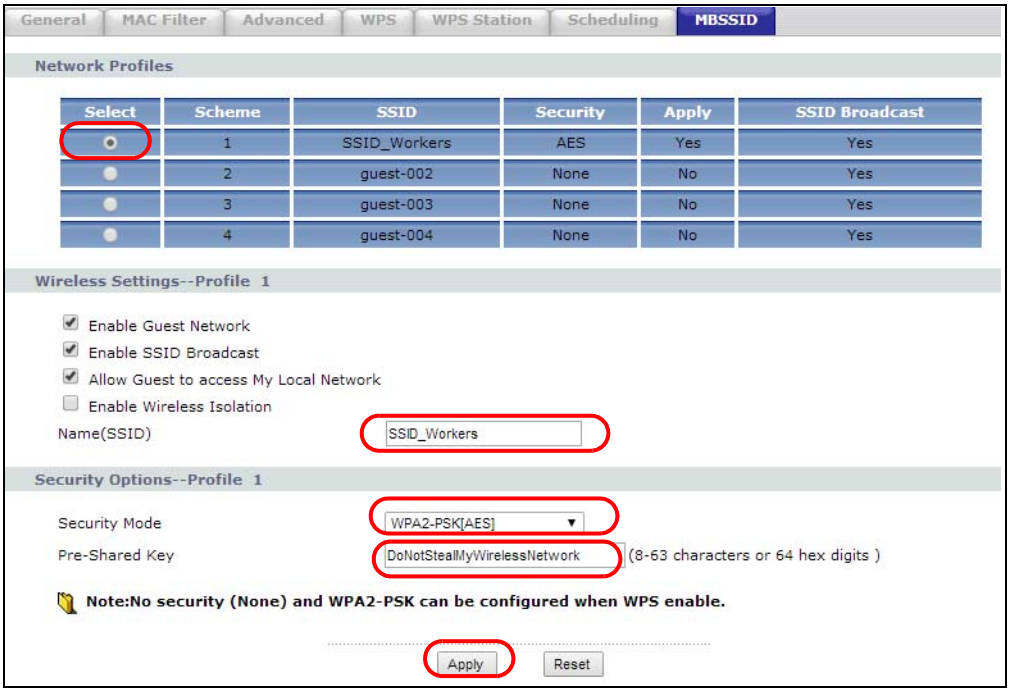
4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.1" as the web address in your web browser.

5 Enter "1234" (default) as the password and click **Login**.

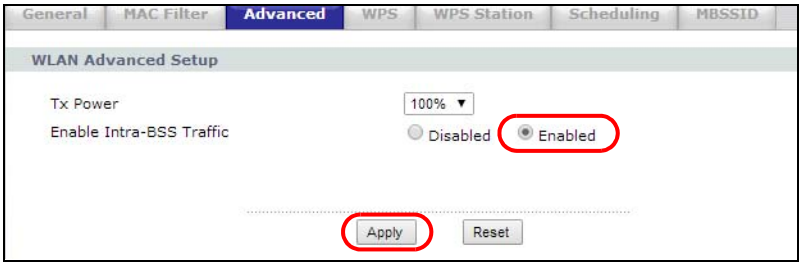
6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.

7 A window appears asking you to select Wizard or Advance mode. Click **Go to Advanced Setup** in the navigation panel.

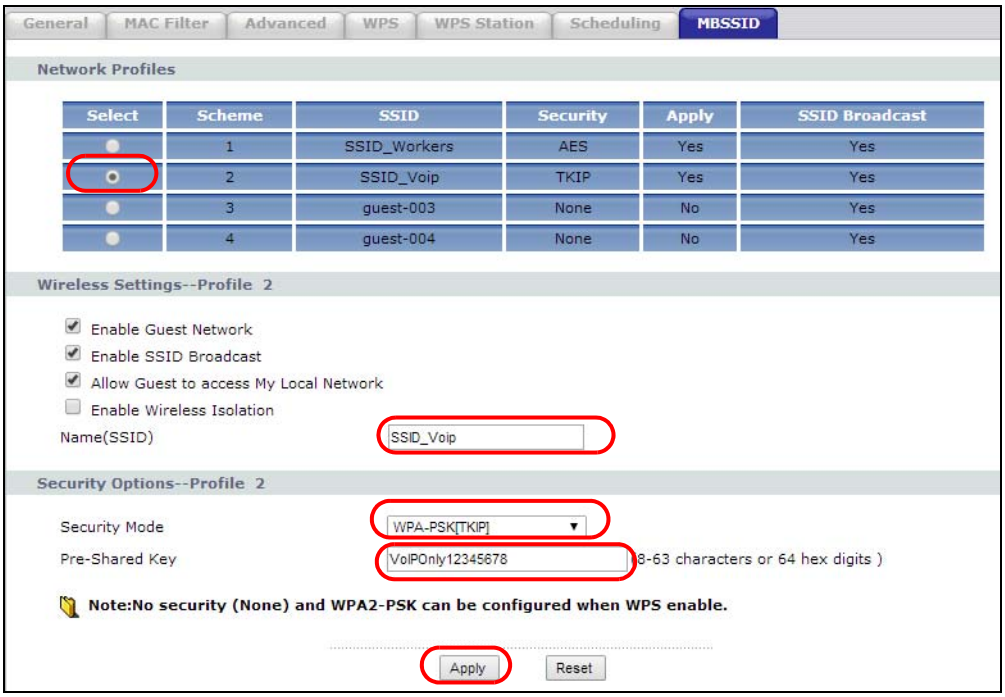
8 Go to **Network > Wireless LAN > MBSSID**. Type **SSID_Workers** in the Name (SSID) field, select **WPA2-PSK(AES)** in the Security drop-down list, enter the pre-share key and click **Apply**.



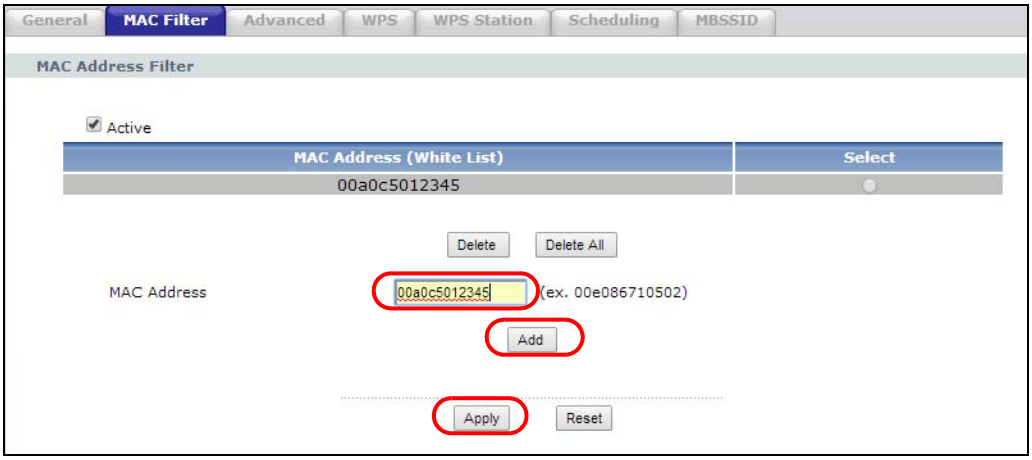
9 Go to **Network > Wireless LAN > Advanced** and click enable **Intra-BSS Traffic** to allow wireless clients in the same wireless network to communicate with each other. Click **Apply**.



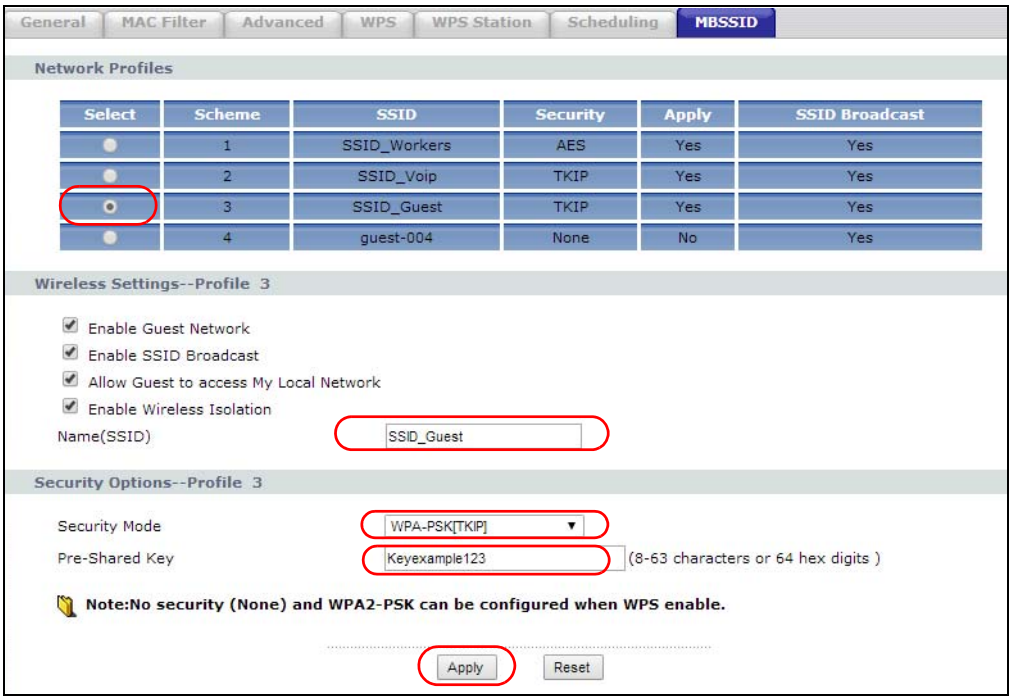
10 To create the SSID_VoIP, go to **Network > Wireless LAN > MBSSID**. click the radio button next to **scheme 2** and Type **SSID_Voip** in the Name (SSID) field, select **WPA-PSK** in the Security drop-down list, enter the pre-share key and click **Apply**.



11 Click the **MAC Filter** tab to configure MAC filtering for the **SSID_VoIP** wireless network. Go to **Network > Wireless LAN > MAC Filter** and click **Active** check box and enter a MAC address of the VoIP device in the **MAC Address** field. Click **Add** to save the MAC address in the white list table. You can delete a MAC address by clicking the **Select** check box and click the **Delete** button. You can also remove all MAC address by clicking **Delete All** button. Lastly, click **Apply** to save the changes in this screen.



12 To create the SSID_Guest, go to **Network > Wireless LAN > MBSSID**. click the radio button next to **scheme 3** and Type **SSID_Guest** in the Name (SSID) field, click **Enable Wireless Isolation** if you do not want the SSID_Guest wireless clients to communicate with each other. select **WPA-PSK** in the Security drop-down list, enter the pre-share key and click **Apply**.



5.6 Installing UPnP in Windows 7 Example

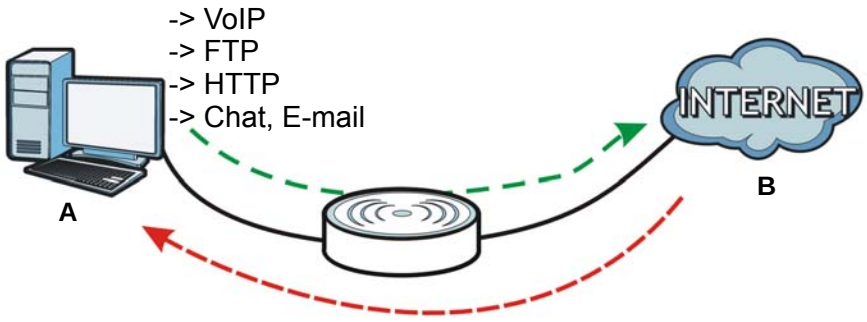
For more information on how to install Universal Plug and Play in Windows on your computer, see Section 14.4 on page 119

5.7 Using Bandwidth Management on the NBG-418N v2

Bandwidth management provides a convenient way to manage the use of various services on the network. It manages general protocols (for example, HTTP and FTP) and applies traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

In the figure below, uplink traffic goes from the LAN device (**A**) to the WAN device (**B**). Bandwidth management is applied before sending the packets out to the WAN. Downlink traffic comes back from the WAN device (**B**) to the LAN device (**A**). Bandwidth management is applied before sending the traffic out to LAN.

Figure 39 Bandwidth Management Example



You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to individual applications (like VoIP, Web, FTP, and E-mail for example).

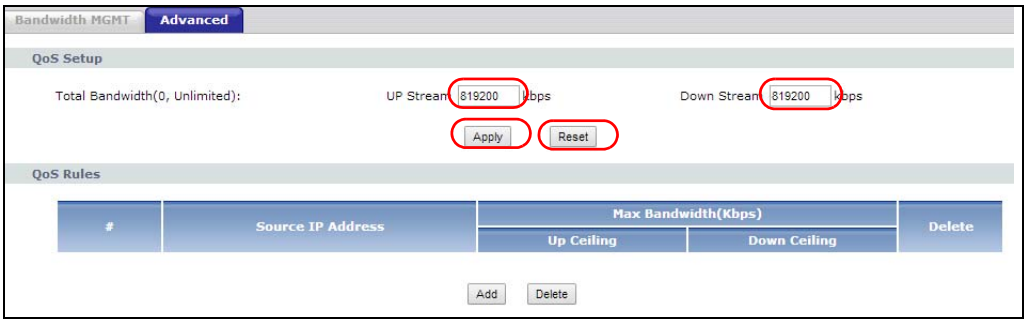
This example shows you how to configure the Bandwidth Management with the following parameters on your NBG-418N v2 (in router mode). This feature is not applicable in Access Point or Universal Repeater mode.

QoS Rule

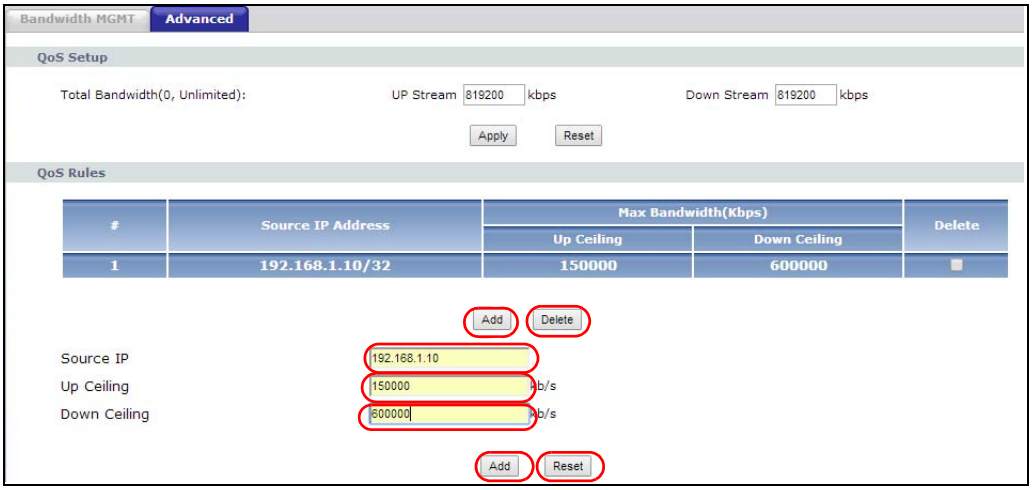
UP Stream	819200 kpbs
Down Stream	819200 kbps
Source IP	192.168.1.10
Up Ceiling	150000 kb/s
Down Ceiling	600000 kb/s

1 Go to **Management > Bandwidth MGMT > Bandwidth MGMT** and click **Enable Bandwidth Management** check box.

2 Go to **Management > Bandwidth MGMT > Advanced** and enter 819200 in the **Total Up Stream** and **Down Stream Bandwidth** fields in the **QoS Setup** section. It is recommended to set this number to match the actual upstream data rate. Click **Apply** or **Reset** to clear the fields.



3 Then, Click **Add** in the **QoS Rules** section and several fields appears. Enter 192.168.1.10 in the **Source IP field**, 192.168.1.10/32 will appear in the field, the 32-bits network is IPv4 addresses block that is assigned by your ISP. Next, enter 150000 for **Up Ceiling** and 600000 for **Down Ceiling** and click **Add**. Note that the Up/Down Ceiling numbers should not exceed the Total Bandwidth. You have successfully set a specific minimum and maximum bandwidth for this particular IP address.



4 If you wish to delete a QoS Rules entry, click the **Delete** check box of the rule and click **Delete** button. To clear the Source IP, Up/Down Ceiling box fields, click the **Reset** button.

PART II
Technical Reference

6

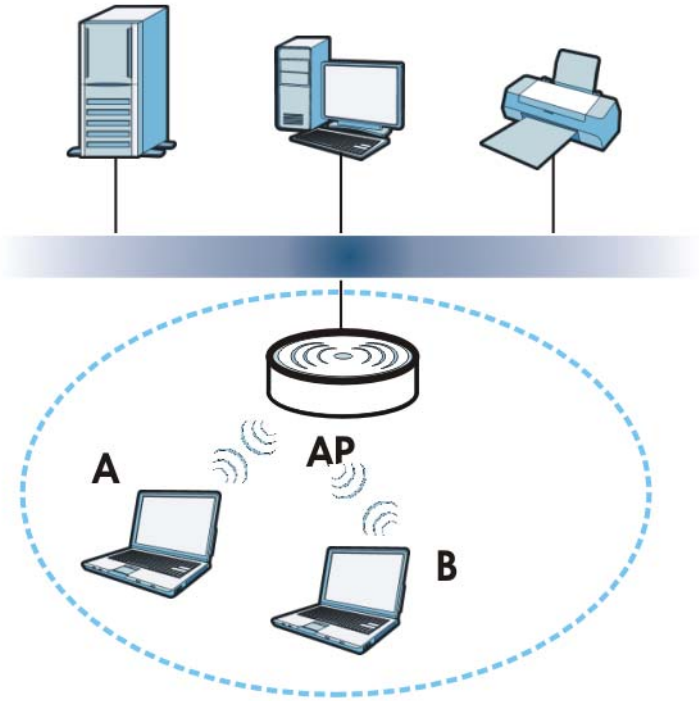
Wireless LAN

6.1 Overview

This chapter discusses how to configure the wireless network settings in your NBG-418N v2. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 40 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (**AP**) to interact with other devices (such as the printer) or with the Internet. Your NBG-418N v2 is the AP in the above example.

6.2 What You Can Do

Wireless screens vary according to the device mode you are using.

Wireless Screen	Router	Access Point	Universal Repeater
General	✔	✔	✔
MAC Filter	✔	✔	✔
Advanced	✔	✔	✔
QoS	✔	✔	✔
WPS	✔	✔	✔
WPS Station	✔	✔	✔
Scheduling	✔	✔	✔
AP Select			✔

See Chapter 4 on page 29 for more information on device modes.

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode (Section 6.4 on page 63).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the NBG-418N v2 (Section 6.5 on page 68).
- Use the **Advanced** screen to allow intra-BSS networking and set the RTS/CTS Threshold (Section 6.6 on page 69).
- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually (Section 6.7 on page 70).
- Use the **WPS Station** screen to add a wireless station using WPS (Section 6.8 on page 71).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off (Section 6.9 on page 71).
- Use the **AP Select** screen to choose an access point that you want the NBG-418N v2 (in universal repeater mode) to connect to. You should know the security settings of the target AP (Section 6.11 on page 74).
- Use the **MBSSID** screen to view the SSID and security of the selected AP wireless network (Section 6.10 on page 72).

6.3 What You Should Know

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.

- If two wireless networks overlap, they should use different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

6.3.1 Wireless Security Overview

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

6.3.2 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The NBG-418N v2's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

6.3.2.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

6.3.3 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

6.3.4 Encryption

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

Table 16 Types of Encryption for Each Type of Authentication

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

For example, if users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA2-PSK. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use WPA2-PSK, or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

When you select **WPA2-PSK** in your NBG-418N v2, you can also select an option (**WPA Compatible**) to support WPA-PSK as well. In this case, if some wireless clients support WPA-PSK and some support WPA2-PSK, you should set up **WPA2-PSK** and select the **WPA Compatible** option in the NBG-418N v2.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

6.3.5 WPS

WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the Section 5.3 on page 44.

6.4 General Wireless LAN Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the NBG-418N v2 from a computer connected to the wireless LAN and you change the NBG-418N v2's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the NBG-418N v2's new settings.

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

Figure 41 Network > Wireless LAN > General (Router or Access Point Mode)

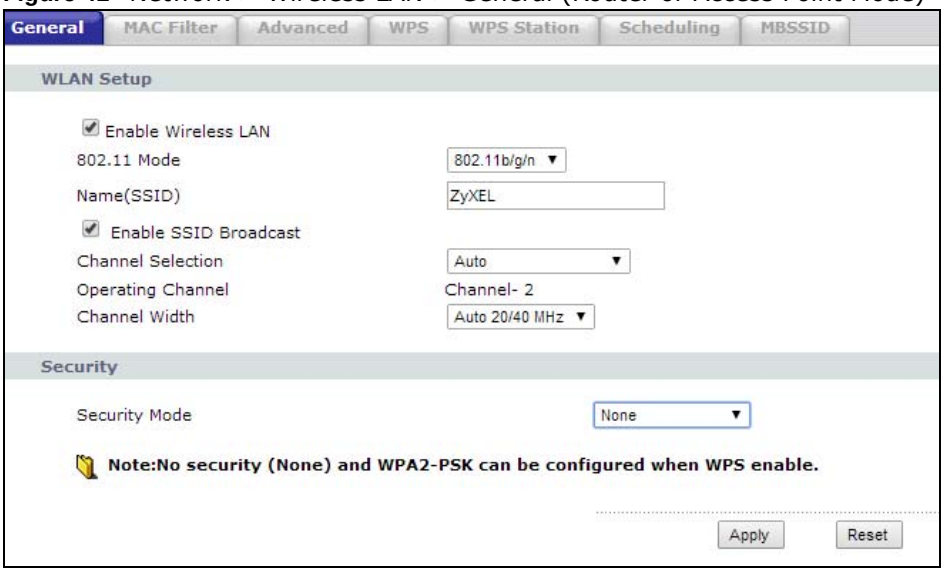
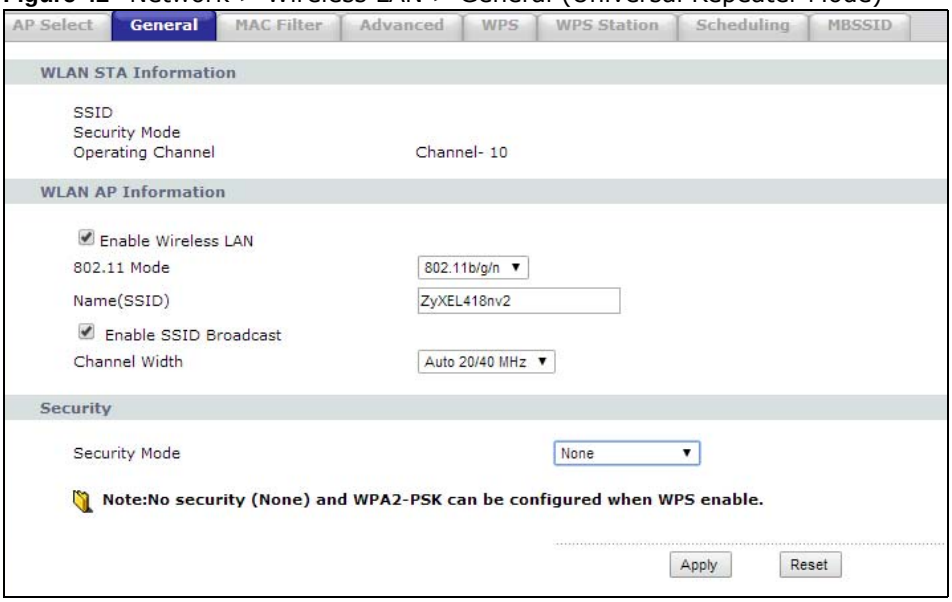


Figure 42 Network > Wireless LAN > General (Universal Repeater Mode)



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

Table 17 Network > Wireless LAN > General

LABEL	DESCRIPTION
WLAN STA Information	This section is available only when the NBG-418N v2 is in universal repeater mode. This shows the wireless and security settings of the selected AP wireless network.
SSID	This displays the Service Set IDentity of the wireless device to which you are connecting.
Security Mode	This displays the type of security configured on the wireless device to which you are connecting.
Operating Channel	This displays the channel used by the wireless device to which you are connecting.
WLAN AP Information / Wireless Setup	Use this section to configure the wireless settings between the NBG-418N v2and its wireless clients.
Enable Wireless LAN	Click the check box to activate wireless LAN.
802.11 Mode	Click the drop-down list to choose the **802.11 mode** you want to operate.
Name(SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Enable SSID Broadcast	Select the **Enable SSID Broadcast** check box to enable the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels. This option is only available if **Auto Channel Selection** is disabled.
Operating Channel	This displays the channel the NBG-418N v2 is currently using.
Channel Width	Select whether the NBG-418N v2 uses a wireless channel width of **20MHz**, **40MHz** or **Auto 20/40MHz**. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. Because not all devices support 40MHz channels, select **Auto 20/40MHz** to allow the NBG-418N v2 to adjust the channel bandwidth automatically.
Security	Use this section to configure the wireless security between the NBG-418N v2 and its wireless clients.
Security Mode	Select **Static WEP**, **WPA-PSK** or **WPA2-PSK** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See 6.4.2 and 6.4.3 sections. Or you can select **No Security** to allow any client to associate this network without authentication.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

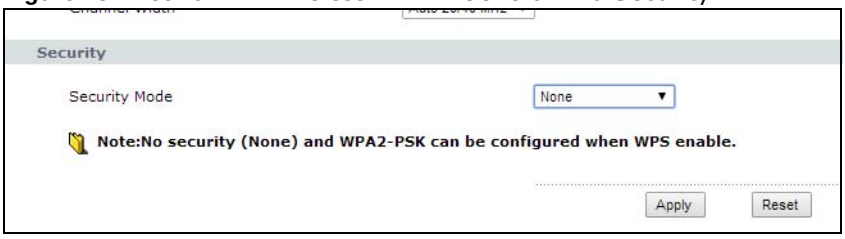
See the rest of this chapter for information on the other labels in this screen.

6.4.1 No Security

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

Note: If you do not enable any wireless security on your NBG-418N v2, your network is accessible to any wireless networking device that is within range.

Figure 43 Network > Wireless LAN > General: No Security



The following table describes the labels in this screen.

Table 18 Network > Wireless LAN > General: No Security

LABEL	DESCRIPTION
Security Mode	Choose **None** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

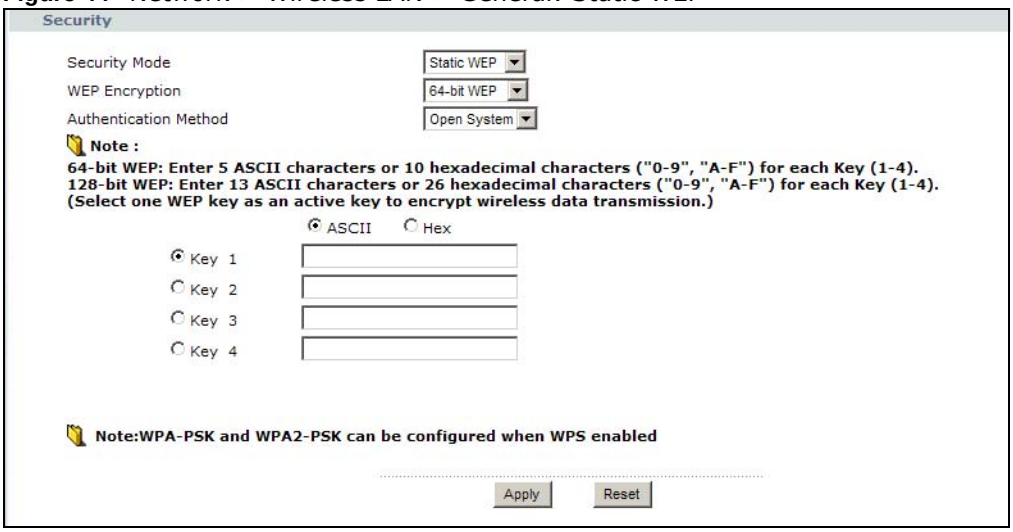
6.4.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your NBG-418N v2 allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption; click **Network** > **Wireless LAN** to display the **General** screen. Select **Static WEP** from the **Security Mode** list.

Figure 44 Network > Wireless LAN > General: Static WEP



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

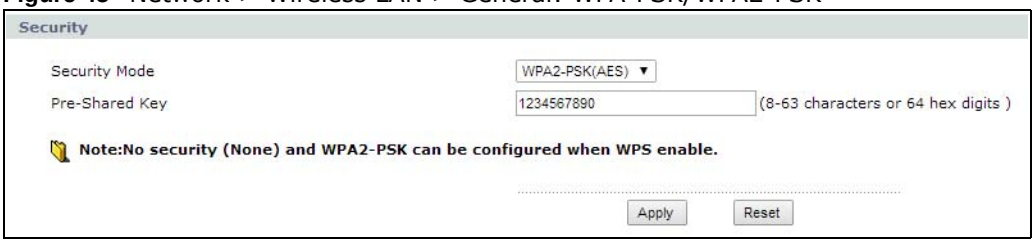
Table 19 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Security Mode	Choose **Static WEP** from the drop-down list box.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Authentication Method	Select **Auto, Open System** or **Shared Key** from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Keep this setting at **Auto** or **Open System** unless you want to force a key verification before communication between the wireless client and the ZyXEL Device occurs. Select **Shared Key** to force the clients to provide the WEP key prior to communication.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the NBG-418N v2 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.4.3 WPA-PSK/WPA2-PSK

Click **Network** > **Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 45 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK



The following table describes the labels in this screen.

Table 20 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Security Mode	Choose **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
WPA Compatible	This option is available only when you select **WPA2-PSK** in the **Security Mode** field. Select this option to have both WPA2 and WPA wireless clients be able to communicate with the NBG-418N v2 even when the NBG-418N v2 is using WPA2-PSK.

Table 20 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK (continued)

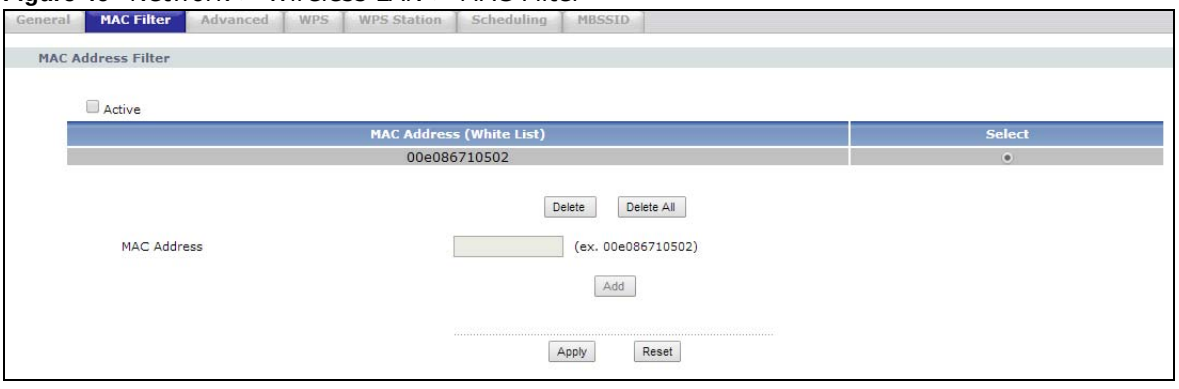
LABEL	DESCRIPTION
Cipher Type	Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption. Select **AES** if your wireless clients can all use AES. Otherwise, select **TKIP** or select **TKIP+AES** to allow the wireless clients to use either TKIP or AES
Pre-Shared Key	**WPA-PSK**/**WPA2-PSK** uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive **ASCII** characters (including spaces and symbols). Type a pre-shared key less than 64 case-sensitive **HEX** characters ("0-9", "A-F").
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK/WPA2-PSK** key management) or RADIUS server (if using **WPA/WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA-PSK/WPA2-PSK** mode.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.5 MAC Filter

The MAC filter screen allows you to configure the NBG-418N v2 to give exclusive access to up to 16 devices (Allow) or exclude up to 16 devices from accessing the NBG-418N v2 (Deny). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your NBG-418N v2's MAC filter settings, click **Network** > **Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 46 Network > Wireless LAN > MAC Filter



The following table describes the labels in this menu.

Table 21 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Active	Click **Active** check box to enable MAC address filtering.
MAC Address (White List)	This field shows the MAC addresses of the wireless station that are allowed or denied access to the NBG-418N v2 in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Select	Click the **Select** radio button to select a MAC filter entry.
Delete	Click the **Delete** button to delete the selected MAC filter entry.
Delete All	Click the **Delete All** button to remove all MAC filter entries.
MAC Address	Enter the **MAC addresses** of the wireless station that are allowed or denied access to the NBG-418N v2 in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Add	Click **Add** to add a new MAC address to the MAC Filtering rule.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.6 Wireless LAN Advanced Screen

Use this screen to allow intra-BSS networking and set the RTS/CTS Threshold.

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

Figure 47 Network > Wireless LAN > Advanced (Universal Repeater Mode)

The following table describes the labels in this screen.

Table 22 Network > Wireless LAN > Advanced (Universal Repeater Mode)

LABEL	DESCRIPTION
Wireless Advanced Setup	
Tx Power	This field controls the transmission power of the NBG-418N v2. When using the NBG-418N v2 with a notebook computer, select a transmission power level from the drop-down list. Choose a lower transmission power level when you are close to the AP in order to conserve battery power.

Table 22 Network > Wireless LAN > Advanced (Universal Repeater Mode)

LABEL	DESCRIPTION
Enable Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless 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.
Apply	Click **Apply** to save your changes to the NBG-418N v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.7 WPS Screen

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

Figure 48 Network > Wireless LAN > WPS

The following table describes the labels in this screen.

Table 23 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Click the **Enable WPS** check box to enable the WPS feature. Click again to disable it.
PIN Number	This displays a PIN number last time system generated. Click **Generate** to generate a new PIN number.
WPS Status	
Status	This displays **Configured** when the NBG-418N v2 has connected to a wireless network using WPS or when **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the NBG-418N v2 or you click **Release_Configuration** to remove the configured wireless and wireless security settings.
Release Configuration	This button is only available when the WPS status displays **Configured**. Click this button to remove all configured wireless and wireless security settings for WPS connections on the NBG-418N v2.

Table 23 Network > Wireless LAN > WPS (continued)

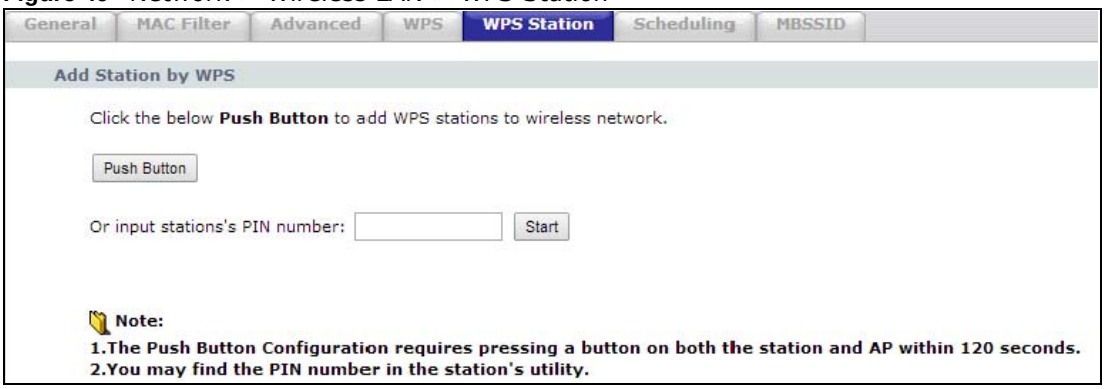
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Refresh	Click **Refresh** to get this screen information afresh.

6.8 WPS Station Screen

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

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

Figure 49 Network > Wireless LAN > WPS Station



The following table describes the labels in this screen.

Table 24 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. See Section 5.3.1 on page 45. Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Or input station's PIN number	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings. See Section 5.3.2 on page 46. Type the same PIN number generated in the wireless station's utility. Then click **Start** to associate to each other and perform the wireless security information synchronization.

6.9 Scheduling Screen

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn on or off on certain days and at certain times. To open this screen, click **Network** > **Wireless LAN** > **Scheduling** tab.

Figure 50 Network > Wireless LAN > Scheduling

The following table describes the labels in this screen.

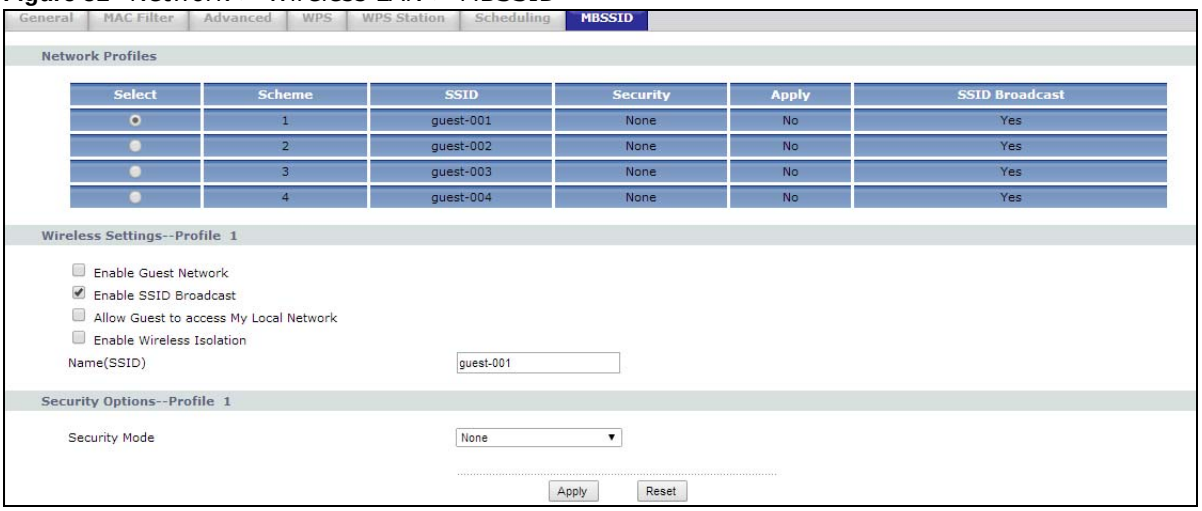
Table 25 Network > Wireless LAN > Scheduling

LABEL	DESCRIPTION
Enable Wireless LAN Scheduling	Select this to enable Wireless LAN scheduling.
Action	Select **On** or **Off** to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the **Day** and **Except for the following times** fields.
Day	Select **Everyday** or the specific days to turn the Wireless LAN on or off. If you select **Everyday** you can not select any specific days. This field works in conjunction with the **Except for the following times** field.
Except for the following times	Select a begin time using the first set of **hour** and minute (**min**) drop down boxes and select an end time using the second set of **hour** and minute (**min**) drop down boxes. If you have chosen **On** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. Note: Entering the same begin time and end time will mean the whole day.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.10 MBSSID Screen

Use this screen to set multiple SSID (MBSSID) for the wireless clients on the NBG-418N v2. Click **Network** > **Wireless LAN** > **MBSSID** to open the following screen.

Figure 51 Network > Wireless LAN > MBSSID



The following table describes the labels in this screen.

Table 26 Network > Wireless LAN > MBSSID

LABEL	DESCRIPTION
Network Profiles	
Select	Click the **Select** radio button to select the Multiple Basic Service Set Identifier (MBSSID) you wish to edit.
Scheme	This field displays the index number of the SSID.
SSID	This field displays the **SSID** name of the Wireless client.
Security	This field displays the **Security** mode of the wireless client. If there's no security, it will display **None**.
Apply	This field displays whether the **Enable Guest Network** check box of the SSID is enabled.
SSID Broadcast	This field displays whether the **Enable SSID Broadcast** check box of the SSID is enabled.
Wireless Settings--Profile 1	
Enable Guest Network	Click the **Enable Guest Network** check box to enable this SSID wireless client.
Enable SSID Broadcast	Click the **Enable SSID Broadcast** check box to activate the SSID broadcast to different wireless clients.
Allow Guest to access My Local Network	Click the **Allow Guest to access my Local Network** check box to allow the client to access the local network resources behind the NBG-418N v2.
Enable Wireless Isolation	Click the **Enable Wireless Isolation** check box to keep the wireless clients in this SSID from communicating with each other through the NBG-418N v2.
Name (SSID)	This field displays the **SSID** name you selected using the select radio button.
Security Options--Profile1	
Security Mode	Select Basic **WEP** or More Secure **WPA2-PSK** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.

Table 26 Network > Wireless LAN > MBSSID

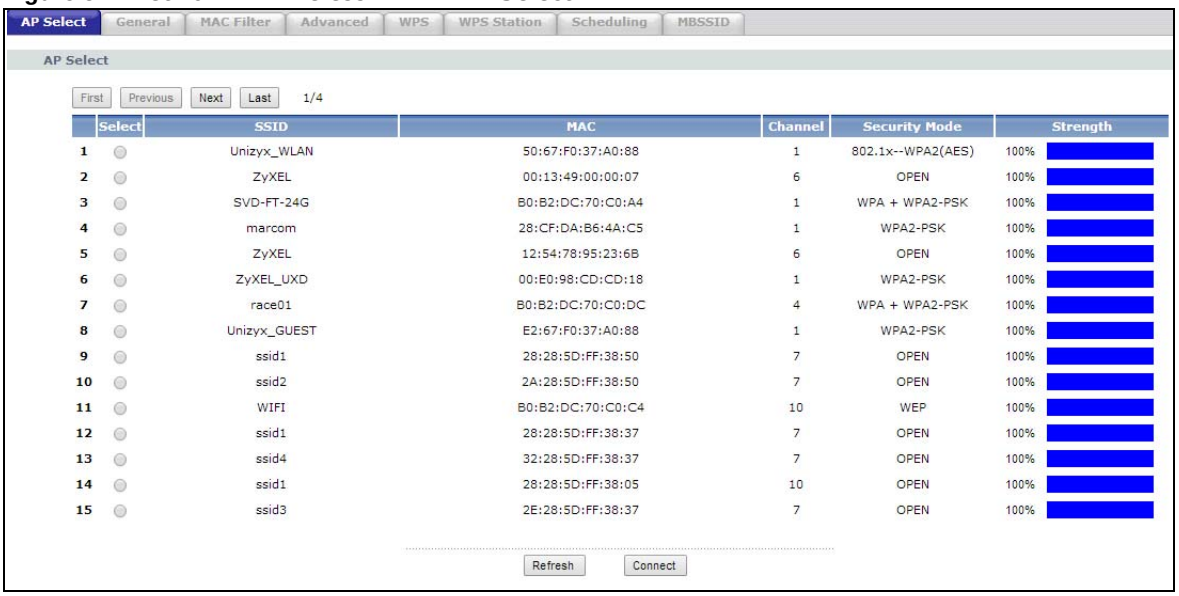
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.11 AP Select Screen

Use this screen to choose an access point that you want the NBG-418N v2 in universal repeater mode) to connect to. You should know the security settings of the target AP.

To open this screen, click **Network** > **Wireless LAN** > **AP Select** tab.

Figure 52 Network > Wireless LAN > AP Select



The following table describes the labels in this screen.

Table 27 Network > Wireless LAN > AP Select

LABEL	DESCRIPTION
AP Select	
First	Click **First** button to go to the first page of the AP select table.
Previous	Click **Previous** button to go to the Previous page in the AP select table.
Next	Click **Next** button to go to the next page in the AP select table.
Last	Click **Last** button to go to the last page of the AP select table.
Select	Use the radio button to select the wireless device to which you want to connect.
SSID	This displays the Service Set IDentity of the wireless device. The SSID is a unique name that identifies a wireless network. All devices in a wireless network must use the same SSID.
MAC	This displays the MAC address of the wireless device.
Channel	This displays the channel number used by this wireless device.

Table 27 Network > Wireless LAN > AP Select (continued)

LABEL	DESCRIPTION
Mode	This displays which IEEE 802.11b/g/n wireless networking standards the wireless device supports.
Security Mode	This displays the type of security configured on the wireless device. **OPEN** means no security is configured and you can connect to it without a password.
Strength	This displays the strength of the wireless signal. The signal strength mainly depends on the antenna output power and the distance between your NBG-418N v2 and this device.
Refresh	Click this button to search for available wireless devices within transmission range and update this table.
Connect	Click this button to associate to the selected wireless device.

7

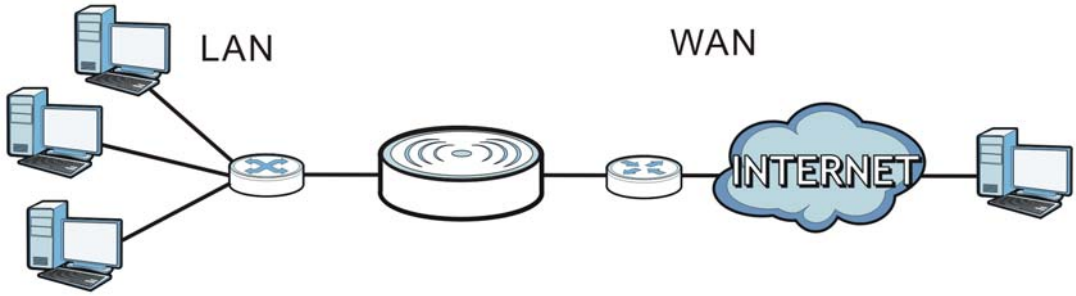
WAN

7.1 Overview

This chapter discusses the NBG-418N v2's **WAN** screens. Use these screens to configure your NBG-418N v2 for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks (such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 53 LAN and WAN



See the chapter about the connection wizard for more information on the fields in the WAN screens.

7.2 What You Need To Know

The information in this section can help you configure the screens for your WAN connection, as well as enable/disable some advanced features of your NBG-418N v2.

7.2.1 Configuring Your Internet Connection

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPTP (Point-to-Point Tunneling Protocol), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the NBG-418N v2, which makes it accessible from an outside network. It is used by the NBG-418N v2 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG-418N v2 tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

DNS Server Address Assignment

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

The NBG-418N v2 can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the NBG-418N v2's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

WAN MAC Address

The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to configuration file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

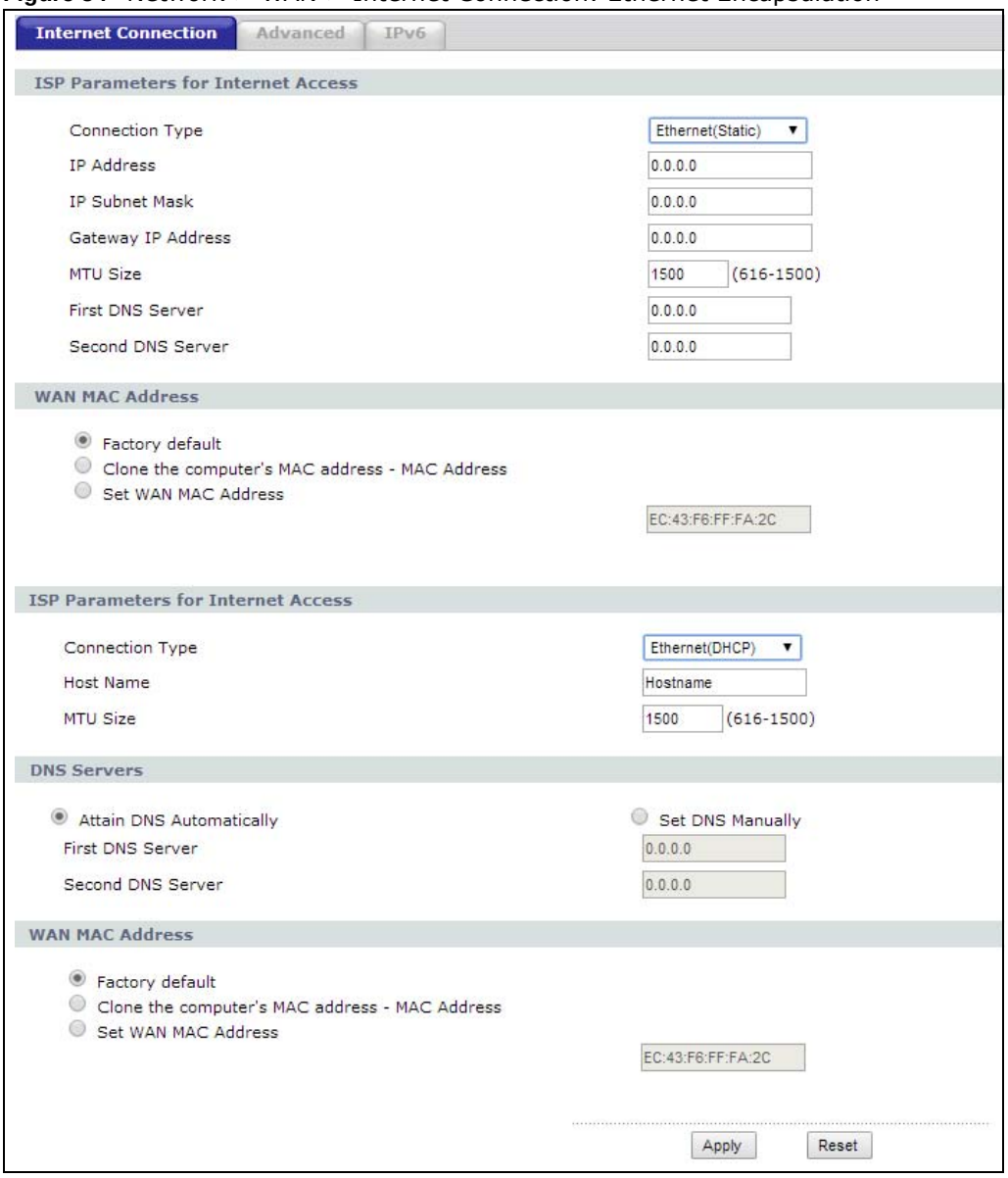
7.3 Internet Connection Screen

Use this screen to change your NBG-418N v2's Internet access settings. Click **Network** > **WAN**. The screen differs according to the encapsulation you choose.

7.3.1 Ethernet Encapsulation

This screen displays when you select **Ethernet** encapsulation.

Figure 54 Network > WAN > Internet Connection: Ethernet Encapsulation



The following table describes the labels in this screen.

Table 28 Network > WAN > Internet Connection: Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access (Ethernet Static)	
Connection Type	Choose the **Ethernet (Static)** option when the WAN port is used as a regular Ethernet.
IP Address	Enter your WAN **IP address** in this field.
IP Subnet Mask	Enter the **IP Subnet Mask** in this field.
Gateway IP Address	Enter a **Gateway IP Address** (if your ISP gave you one) in this field.
MTU Size	Type the **MTU** or maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the NBG-418N v2 divides it into smaller fragments. Allowed values are 576 to 1500. By default this value is 1500

Table 28 Network > WAN > Internet Connection: Ethernet Encapsulation (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server	Enter the **first** and **second DNS server's IP address** in the fields.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG-418N v2's MAC address, copying the MAC address from a computer on your LAN or manually entering a **MAC address**.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - MAC Address	Select this option to **clone the MAC address** of the computer (displaying in the screen) from which you are configuring the NBG-418N v2. Once it is successfully configured, the address will be copied to the rom file. It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the **MAC address** you want to use.
ISP Parameters for Internet Access (Ethernet Dynamic)	
Connection Type	Choose the **Ethernet (Dynamic)** option when the WAN port is used as a regular Ethernet.
Host Name	Type the **host name** or domain name that is associated with this Ethernet connection.
MTU Size	Type the **MTU** or maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the NBG-418N v2 divides it into smaller fragments. Allowed values are 576 to 1500. By default this value is 1500
DNS Services	
Attain DNS Automatically	Click the **Attain DNS Automatically** button if your ISP dynamically assigns DNS server information (and the NBG-418N v2's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.
Set DNS Manually	Select **Set DNS Manually** if you have the IP address of a DNS server. You will need to enter the first and secondary DNS server's IP address in the fields to the bottom.
First DNS Server Second DNS Server	Enter the **first** and **second DNS server's IP address** in the box fields.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG-418N v2's MAC address, copying the MAC address from a computer on your LAN or manually entering a **MAC address**.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - MAC Address	Select this option to **clone the MAC address** of the computer (displaying in the screen) from which you are configuring the NBG-418N v2. Once it is successfully configured, the address will be copied to the rom file. It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the **MAC address** you want to use.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

7.3.2 PPPoE Encapsulation

The NBG-418N v2 supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius).

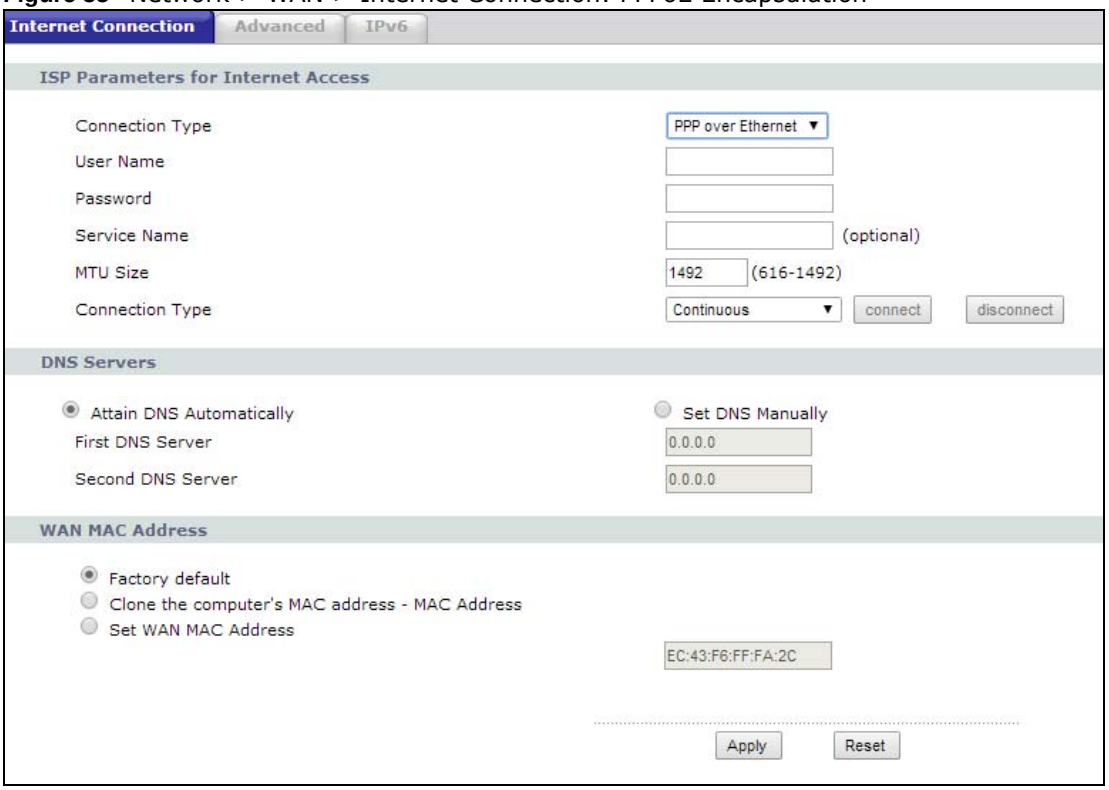
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the NBG-418N v2 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG-418N v2 does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

This screen displays when you select **PPPoE** encapsulation.

Figure 55 Network > WAN > Internet Connection: PPPoE Encapsulation



The following table describes the labels in this screen.

Table 29 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Select **PPP over Ethernet** if you connect to your Internet via dial-up.
User Name	Type the **user name** given to you by your ISP.
Password	Type the **password** associated with the user name above.
Service Name	Type the PPPoE **service name** provided to you. PPPoE uses a service name to identify and reach the PPPoE server.

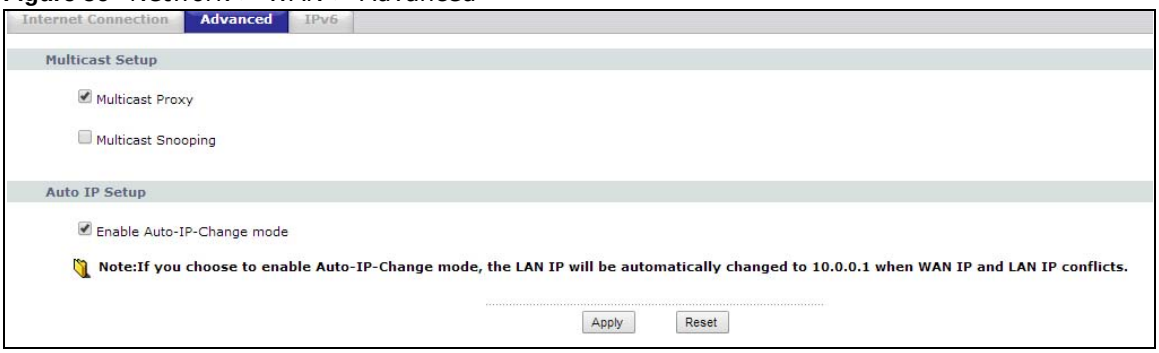
Table 29 Network > WAN > Internet Connection: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
MTU Size	Enter the **MTU** or the largest packet size per frame that your NBG-418N v2 can receive and process.
Connection Type	Select **Continuous** if you do not want the connection to time out. Select **Connection on Demand** if you want to connect for a certain amount of time before the router automatically disconnects from the PPPoE server. If you select this you will need to enter the number of minutes in the Idle timeout field. Select **Manual** if want to make the connection manually.
Connect/ Disconnect	Click **Connect** button to establish the connection with above settings or Click **Disconnect** to stop the connection.
DNS Servers	
Attain DNS Automatically/ Set DNS Manually	Click **Attain DNS Automatically** radio button if your ISP dynamically assigns DNS server information (and the NBG-418N v2's WAN IP address). Or click **Set DNS Manually** if you have if you have the IP address of a DNS server.
First DNS Server Second DNS Server	Enter the **first** and **second DNS server's IP address** in the fields.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the NBG-418N v2's MAC address, copying the MAC address from a computer on your LAN or manually entering a **MAC address**.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - MAC Address	Select this option to **clone the MAC address** of the computer (displaying in the screen) from which you are configuring the NBG-418N v2. Once it is successfully configured, the address will be copied to the rom file. It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the **MAC address** you want to use.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4 Advanced Screen

Use this screen to set up multicast configurations. Click **Network** > **WAN** > **Advanced**.

Figure 56 Network > WAN > Advanced



The following table describes the labels in this screen.

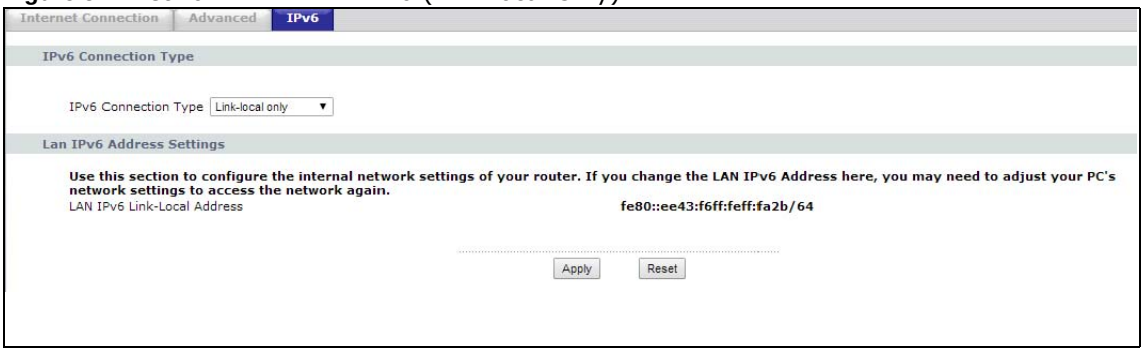
Table 30 Network > WAN > Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast Proxy	Click the **Multicast Proxy** radio button to enable this function on the NBG-418N v2. This allows an IPv6 router to discover the presence of MLD hosts who wish to receive multicast packets and the IP address of multicast groups the hosts want to join on its network.
Multicast Snooping	Click the **Multicast Snooping** radio button to activate it. This allows the NBG-418N v2 to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.
Auto IP Setup	
Enable Auto-IP-Change mode	Click **Enable Auto-IP-Change mode** button to have the NBG-418N v2 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG-418N v2 gets a dynamic WAN IP address in the same subnet as the LAN IP address 192.168.1.1 or 10.0.0.1. The NAT, DHCP server and firewall functions on the NBG-418N v2 are still available in this mode.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

7.5 IPv6 Screen

Use this screen to configure your IPv6 settings. Click **Network** > **WAN** > **IPv6**.

Figure 57 Network > WAN > IPv6 (Link-local Only)

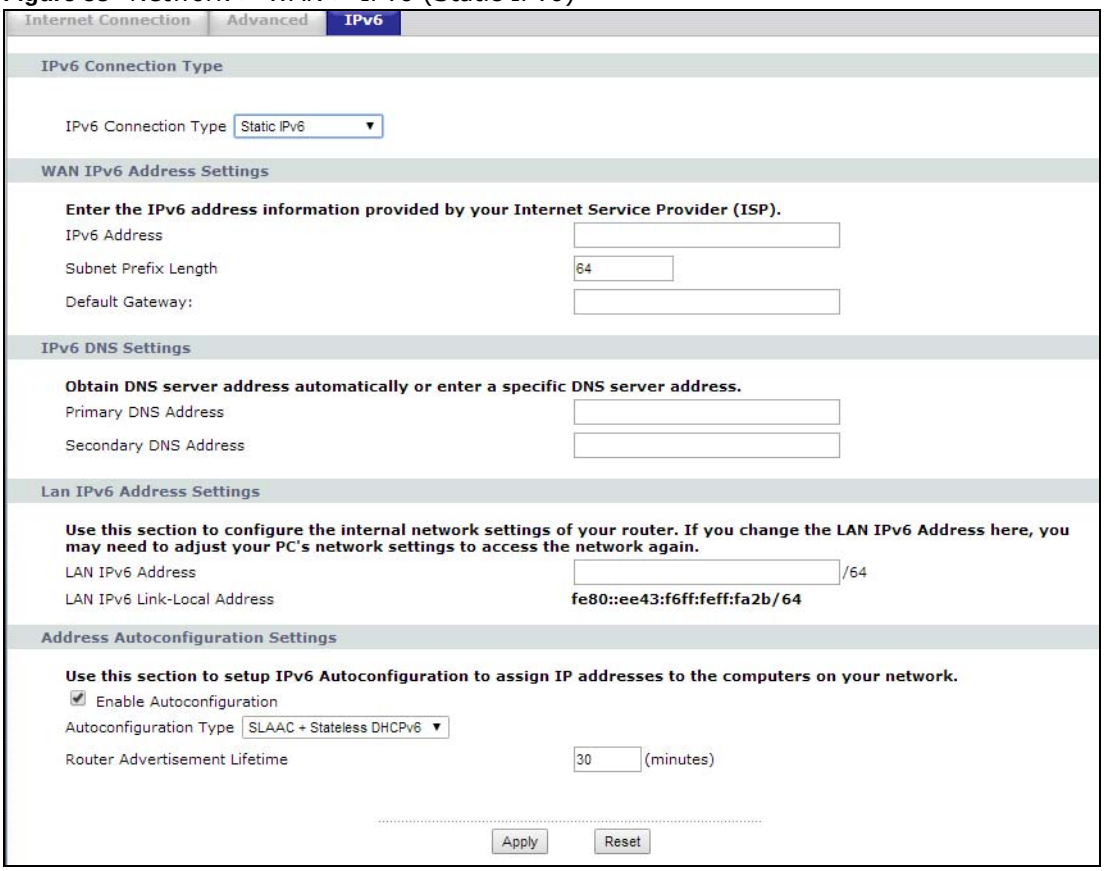


The following table describes the labels in this screen.

Table 31 Network > WAN > IPv6 (Link-local Only)

LABEL	DESCRIPTION
IPv6 Connection Type	Select **Link-local only** to allow NBG-418N v2 to communicate with neighboring devices on the same link. This mode enables IPv6-capable devices to communicate with each other in the LAN side.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

Figure 58 Network > WAN > IPv6 (Static IPv6)



The following table describes the labels in this screen.

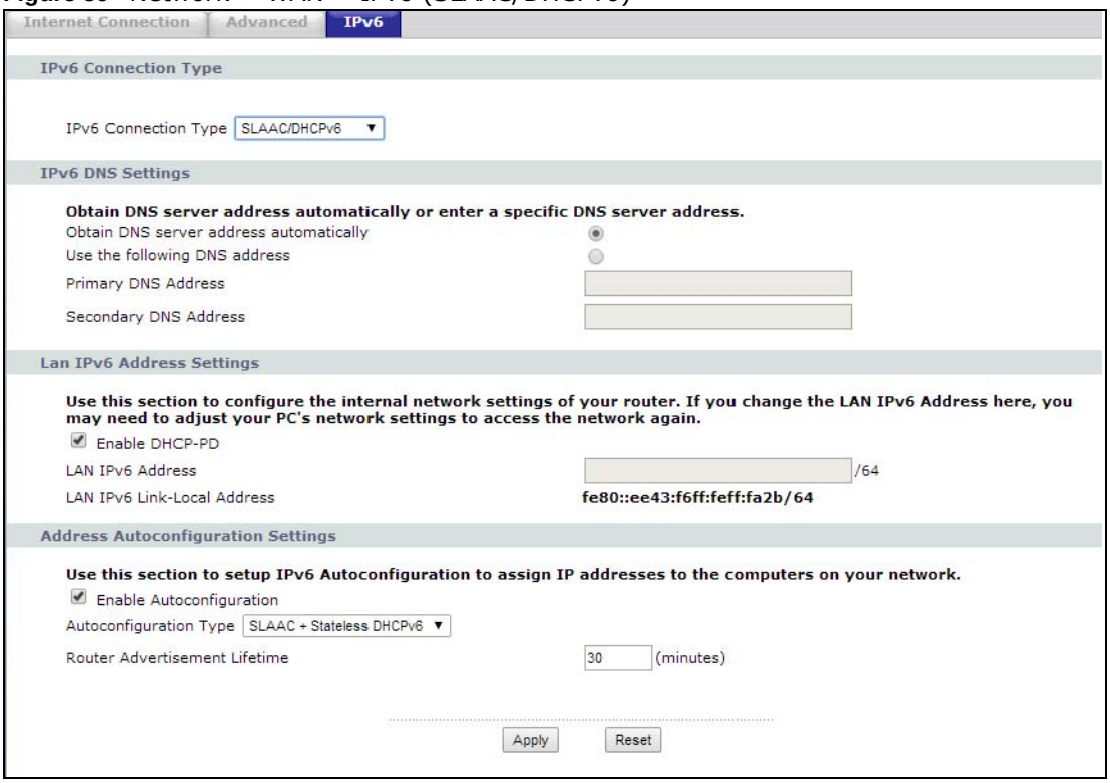
Table 32 Network > WAN > IPv6 (Static IPv6)

LABEL	DESCRIPTION
IPv6 Connection Type	Select **Static IPv6** when your ISP provides you a set IPv6 address that does not change. You must also enter the IPv6 address, Subnet Prefix Length, Default Gateway, Primary and Secondary DNS Server provided by your ISP.
Wan IPv6 Address Settings	
IPv6 Address	Enter the **IPv6 IP address** on the WAN side in this field.
Subnet Prefix Length	The prefix is the part of the address that indicates the bits that have fixed values or are the bits of the network identifier. Prefix is written in address/prefix-length notation. For example (21DA:D3:0:2F3B::/64)The default subnet prefix is 64. A route prefix is 48prefix.Enter the **Subnet Prefix Length** address on the WAN side in this field.
Default Gateway	Enter the **Default Gateway** address on the WAN side in this field.
IPv6 DNS Settings	
Primary DNS Address	Enter the **primary DNS** server address for the IPv6 in this field.
Secondary DNS Address	Enter the **secondary DNS** server address for the IPv6 in this field.
LAN IPv6 Address Settings	
LAN IPv6 Address	Enter the **IPv6 IP address** for the LAN port in this field.
LAN IPv6 Link-Local Address	Enter the **IPv6 Link-local address** in the LAN side. This is used by routers when communicating with neighboring devices on the same link. It allows IPv6-capable devices to communicate with each other in the LAN side.i

Table 32 Network > WAN > IPv6 (continued)(Static IPv6)

LABEL	DESCRIPTION
Address Autoconfiguration Settings	
Enable Autoconfiguration	Click **Enable Autoconfiguration** if you want the devices on your local area network to obtain network address that are not managed by a DHCPv6 server.
Autoconfiguration Type	Select **SLAAC + Stateless DHCPv6** if you want the interface to automatically generate a link-local address via stateless autoconfiguration. Select **Stateful(DHCPv6)** when the devices connected to your LAN needs to have their TCP/IP configuration set to DHCPv6 or obtain an IPv6 address automatically.
Router Advertisement Lifetime	Type in the **Router Advertisement Lifetime** which is the amount of time in minutes that a device may have an IPv6 address before it is required to renew the lease.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

Figure 59 Network > WAN > IPv6 (SLAAC/DHCPv6)



The following table describes the labels in this screen.

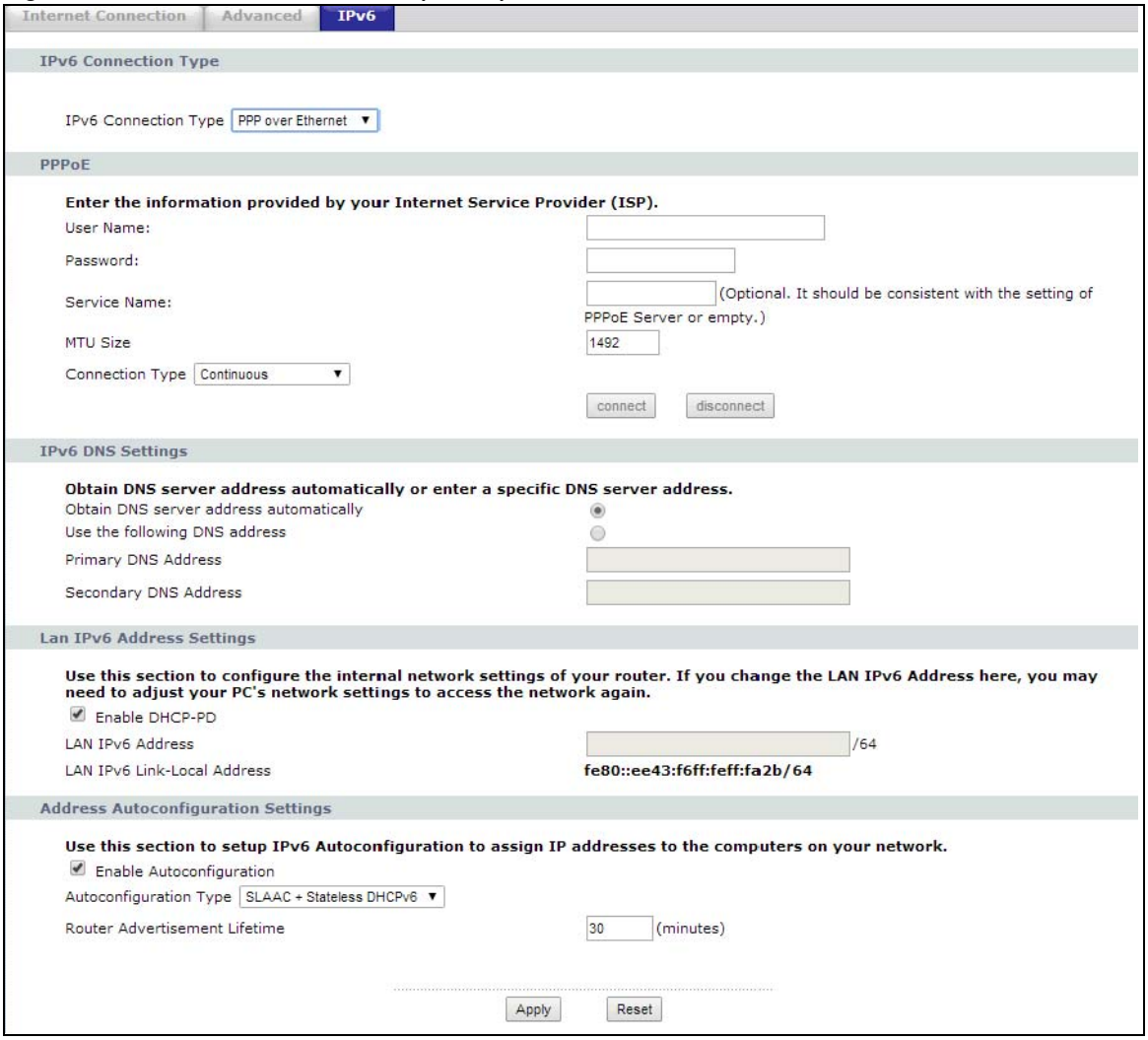
Table 33 Network > WAN > IPv6 (SLAAC/DHCPv6)

LABEL	DESCRIPTION
IPv6 Connection Type	Select **SLAAC/DHCPv6** when your NBG-418N v2 requests an IPv6 address from the ISP's server.
IPv6 DNS Settings	
Obtain DNS server address automatically	Click the **Obtain DNS server address automatically** radio button to get a DNS server address from your ISP's server.

Table 33 Network > WAN > IPv6 (continued)(SLAAC/DHCPv6)

LABEL	DESCRIPTION
Use the following DNS address	Click **Use the following DNS address** radio button to use a fixed DNS address.
Primary and Secondary DNS Address	Enter the **Primary** and **Secondary** DNS address for the IPv6 server in the appropriate box fields.
LAN IPv6 Address Settings	
Enable DHCP-PD	Click **Enable DHCP-PD** (DHCP-Prefix delegation) to allow NBG-418N v2 assign prefixes to DHCP clients. The prefix is the part of the address that indicates the bits that have fixed values or are the bits of the network identifier. Prefix is written in address/prefix-length notation.
LAN IPv6 Address	Enter the **IPv6 IP address** for the LAN port in this field.
LAN IPv6 Link-Local Address	Enter the **IPv6 Link-local address** in the LAN side. This is used by routers when communicating with neighboring devices on the same link. It allows IPv6-capable devices to communicate with each other in the LAN side.i
Address Autoconfiguration Settings	
Enable Autoconfiguration	Click **Enable Autoconfiguration** if you want the devices on your local area network to obtain network address that are not managed by a DHCPv6 server.
Autoconfiguration Type	Select **SLAAC + Stateless DHCPv6** if you want the interface to automatically generate a link-local address via stateless autoconfiguration. Select **Stateful(DHCPv6)** when the devices connected to your LAN needs to have their TCP/IP configuration set to DHCPv6 or obtain an IPv6 address automatically.
Router Advertisement Lifetime	Type in the **Router Advertisement Lifetime** which is the amount of time in minutes that a device may have an IPv6 address before it is required to renew the lease.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

Figure 60 Network > WAN > IPv6 (PPPoE)



The following table describes the labels in this screen.

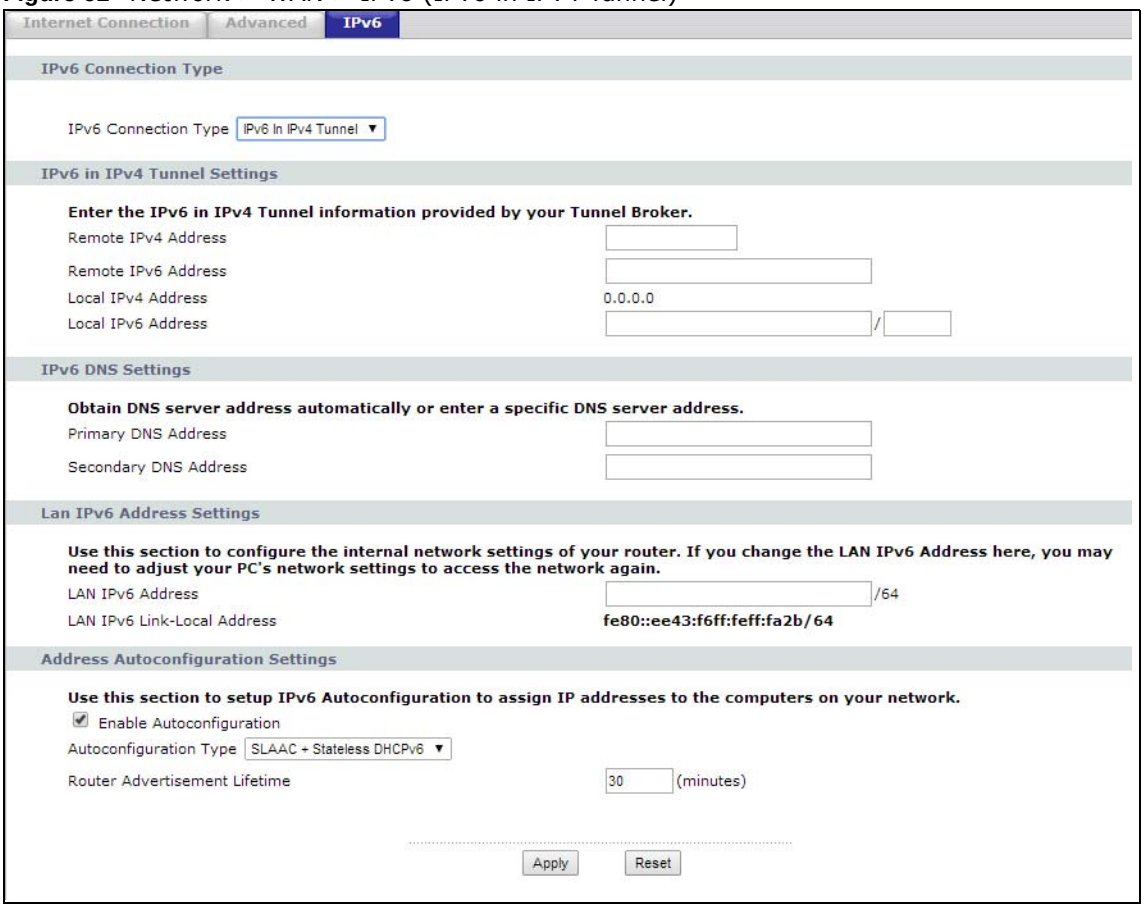
Table 34 Network > WAN > IPv6 (PPPoE)

LABEL	DESCRIPTION
IPv6 Connection Type	Select **PPPoE** if your ISP requires your to use a PPPoE connection to IPv6 Internet. This method of connection typically requires you to enter a Username and Password (provided by your ISP) to gain access to the IPv6 Internet. You need to ensure that any PPPoE client software on your computer is removed or disabled.
PPPoE	
User Name	Enter a **user name** (of up to 31 printable characters) for login using PPPoE connection.
Password	Enter a **password**.
Service Name	Enter a **service name** if your ISP requires one.
MTU Size	Enter the **MTU** or the largest packet size per frame that your NBG-418N v2 can receive and process.

Table 34 Network > WAN > IPv6 (continued)(PPPoE)

LABEL	DESCRIPTION
Connection Type	Select **Continuous** if you do not want the connection to time out. Select **Connection on Demand** if you want to connect for a certain amount of time before the router automatically disconnects from the PPPoE server. If you select this you will need to enter the number of minutes in the Idle timeout field. Select **Manual** if want to make the connection manually.
Connect/ Disconnect	Click **Connect** to establish PPPoE connection to IPv6 Internet or click **Disconnect** to stop the connection.
IPv6 DNS Settings	
Obtain DNS Server address automatically	Click the **Obtain DNS server address automatically** radio button to get a DNS server address from your ISP's server.
Use the following DNS address	Click **Use the following DNS address** radio button to use a fixed DNS address.
Primary/Secondary DNS Address	Enter the **Primary** and **Secondary** DNS address for the IPv6 server in the appropriate box fields.
Lan IPv6 Address Settings	
Enable DHCP-PD	Click **Enable DHCP-PD** (DHCP-Prefix delegation) to allow NBG-418N v2 assign prefixes to DHCP clients.
LAN IPv6 Address	Enter the **IPv6 IP address** for the LAN interface in this field.
LAN IPv6 Link-Local Address	Enter the **IPv6 Link-local address** in the LAN side. This is used by NBG-418N v2 when communicating with neighboring devices on the same link. It allows IPv6-capable devices to communicate with each other in the LAN side.i
Address Autoconfiguration Settings	
Enable Autoconfiguration	Click **Enable Autoconfiguration** if you want the devices on your local area network to obtain network address that are not managed by a DHCPv6 server.
Autoconfiguration Type	Select **SLAAC + Stateless DHCPv6** if you want the interface to automatically generate a link-local address via stateless autoconfiguration. Select **Stateful(DHCPv6)** when the devices connected to your LAN needs to have their TCP/IP configuration set to DHCPv6 or obtain an IPv6 address automatically.
Router Advertisement Lifetime	Type in the **Router Advertisement Lifetime** which is amount of time in minutes that a device may have an IPv6 address before it is required to renew the lease.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

Figure 61 Network > WAN > IPv6 (IPv6 in IPv4 Tunnel)



The following table describes the labels in this screen.

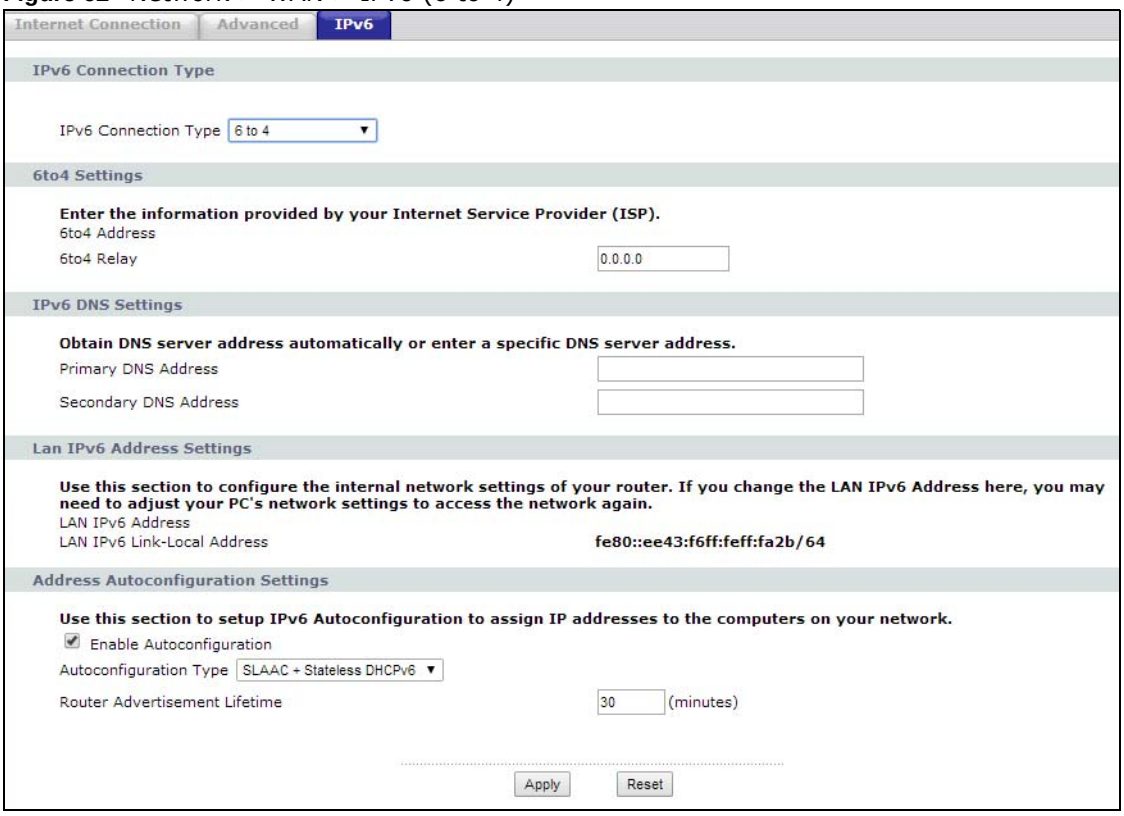
Table 35 Network > WAN > IPv6 (IPv6 in IPv4 Tunnel)

LABEL	DESCRIPTION
IPv6 Connection Type	**IPv6 in IPv4 Tunnel** is the encapsulation of IPv6 packets in IPv4 packets so that IPv6 packets can be sent over an IPv4 infrastructure.
IPv6 in IPv4 Tunnel Settings	
Remote IPv4 Address	Enter the I**Pv4 IP address** of the device on a remote network.
Remote IPv6 Address	Enter the **IPv6 IP address** of the device on a remote network.
Local IPv4 Address	Enter the **IPv4 IP address** of the device on a local network.
Local IPv6 Address	Enter the **IPv6 IP address** of the device on a local network.
IPv6 DNS Settings	
Primary and Secondary DNS Address	Enter the **Primary** and **Secondary** DNS address for the IPv6 server in the appropriate box fields.
Lan IPv6 Address Settings	
LAN IPv6 Address	Enter the **IPv6 IP address** for the LAN port in this field.
LAN IPv6 Link-Local Address	Enter the **IPv6 Link-local address** in the LAN side. This is used by routers when communicating with neighboring devices on the same link. It allows IPv6-capable devices to communicate with each other in the LAN side.i

Table 35 Network > WAN > IPv6 (IPv6 in IPv4 Tunnel)

LABEL	DESCRIPTION
Address Autoconfiguration Settings	
Enable Autoconfiguration	Click **Enable Autoconfiguration** if you want the devices on your local area network to obtain network address that are not managed by a DHCPv6 server.
Autoconfiguration Type	Select **SLAAC + Stateless DHCPv6** if you want the interface to automatically generate a link-local address via stateless autoconfiguration. Select **Stateful(DHCPv6)** when the devices connected to your LAN needs to have their TCP/IP configuration set to DHCPv6 or obtain an IPv6 address automatically.
Router Advertisement Lifetime	Type in the **Router Advertisement Lifetime** which is amount of time in minutes that a device may have an IPv6 address before it is required to renew the lease.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

Figure 62 Network > WAN > IPv6 (6 to 4)



The following table describes the labels in this screen.

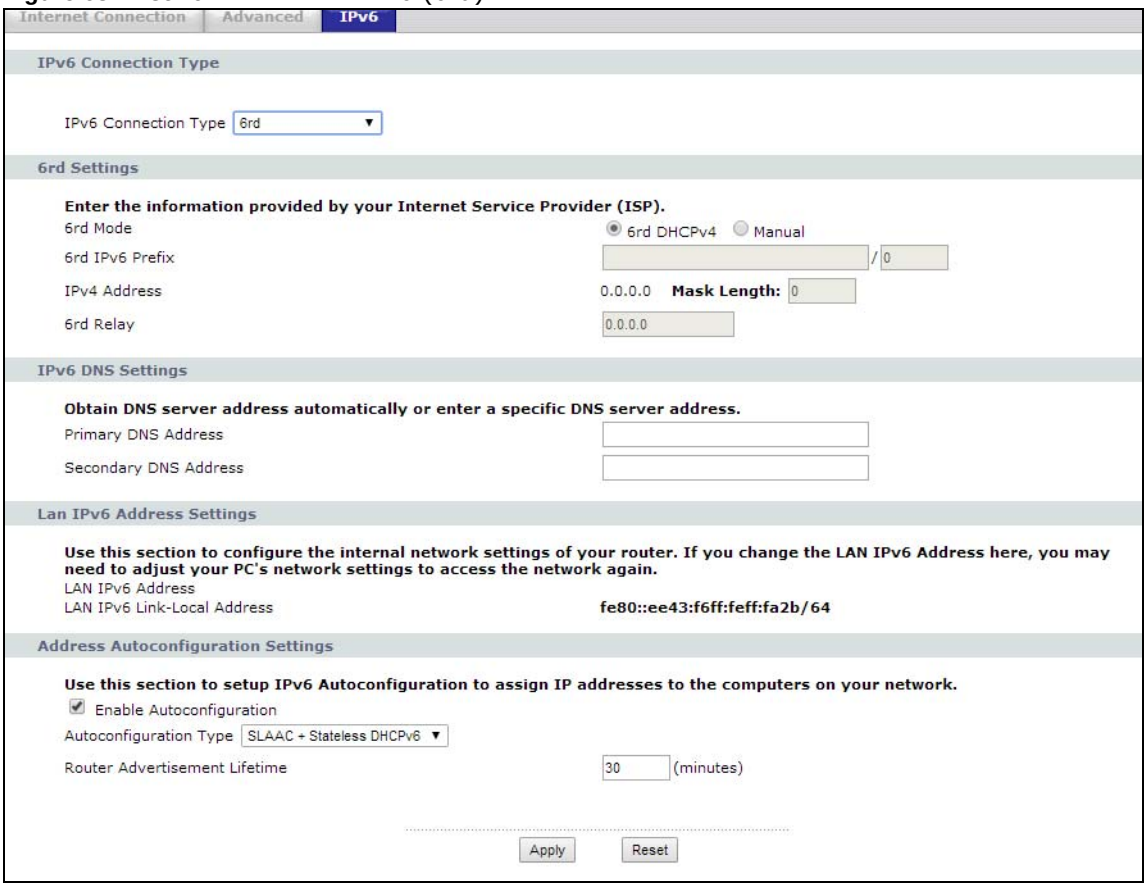
Table 36 Network > WAN > IPv6 (6 to 4)

LABEL	DESCRIPTION
IPv6 Connection Type	**6 to 4** is an IPv6 address assignment and automatic tunneling technology that used to provide unicast IPv6 connectivity between IPv6 sites and hosts across the IPv4 Internet.
6 to 4 Settings	
6 to 4 Address	Enter a **6 to 4 IP address** in this field. This information is provided by your ISP.
6 to 4 Relay	Type the ISP's border **relay server's IPv6 address** in this field.

Table 36 Network > WAN > IPv6 (continued)(6 to 4)

LABEL	DESCRIPTION
IPv6 DNS Settings	
Primary/Secondary DNS Address	Enter the **Primary** and **Secondary** DNS address for the IPv6 server in the appropriate box fields.
Lan IPv6 Address Settings	
LAN IPv6 Address	Enter the I**Pv6 IP address** for the LAN port in this field.
LAN IPv6 Link-Local Address	Enter the **IPv6 Link-local address** in the LAN side. This is used by routers when communicating with neighboring devices on the same link. It allows IPv6-capable devices to communicate with each other in the LAN side.i
Address Autoconfiguration Settings	
Enable Autoconfiguration	Click **Enable Autoconfiguration** if you want the devices on your local area network to obtain network address that are not managed by a DHCPv6 server.
Autoconfiguration Type	Select **SLAAC + Stateless DHCPv6** if you want the interface to automatically generate a link-local address via stateless autoconfiguration. Select **Stateful(DHCPv6)** when the devices connected to your LAN needs to have their TCP/IP configuration set to DHCPv6 or obtain an IPv6 address automatically.
Router Advertisement Lifetime	Type in the **Router Advertisement Lifetim**e which is amount of time in minutes that a device may have an IPv6 address before it is required to renew the lease.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

Figure 63 Network > WAN > IPv6 (6rd)



The following table describes the labels in this screen.

Table 37 Network > WAN > IPv6 (6rd)

LABEL	DESCRIPTION
IPv6 Connection Type	IPv6 Rapid Deployment (**6rd**) is used when the local network uses IPv6 and the ISP has an IPv4 network. When the NBG-418N v2 has an IPv4 WAN address and you set IPv6/IPv4 mode to IPv4 only, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network. The NBG-418N v2 generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's border relay router to connect to the native IPv6 Internet. The local network can also use IPv4 services. The NBG-418N v2 uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.
6rd Settings	
6rd Mode	Click the **6rd DHCPv4** radio button to have your ISP generate a 6rd DHCPv4 address automatically. Choose **Manual** to enter a fixed 6rd DHCPv4 address manually.
6rd IPv6 Prefix	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
IPv4 Address	Enter the **IPv4 address** and the IPv4 subnet mask length (1 to 32) in the box field.
6rd Relay	Enter the ISP's **border relay server's IPv6 address** in this field.
IPv6 DNS Settings	
Primary/Secondary DNS Address	Enter the **Primary** and **Secondary** DNS address for the IPv6 server in the appropriate box fields.
LAN IPv6 Address Settings	
LAN IPv6 Address	Enter the **IPv6 IP address** for the LAN port in this field.
LAN IPv6 Link-Local Address	Enter the I**Pv6 Link-local address** in the LAN side. This is used by routers when communicating with neighboring devices on the same link. It allows IPv6-capable devices to communicate with each other in the LAN side.i
Address Autoconfiguration Settings	
Enable Autoconfiguration	Click **Enable Autoconfiguration** if you want the devices on your local area network to obtain network address that are not managed by a DHCPv6 server.
Autoconfiguration Type	Select **SLAAC + Stateless DHCPv6** if you want the interface to automatically generate a link-local address via stateless autoconfiguration. Select **Stateful(DHCPv6)** when the devices connected to your LAN needs to have their TCP/IP configuration set to DHCPv6 or obtain an IPv6 address automatically.
Router Advertisement Lifetime	Type in the **Router Advertisement Lifetime** which is amount of time in minutes that a device may have an IPv6 address before it is required to renew the lease.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

8

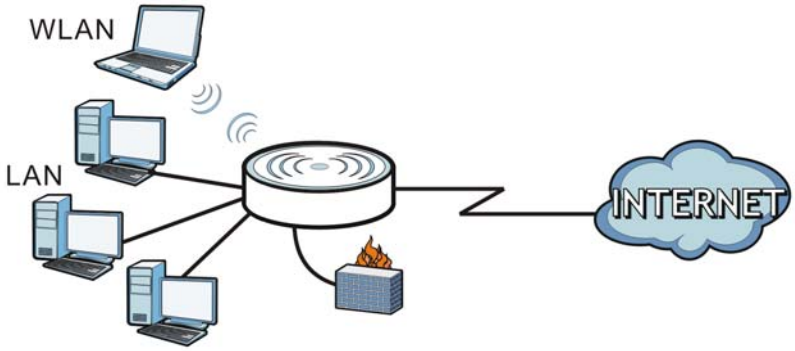
LAN

8.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

Figure 64 LAN Setup

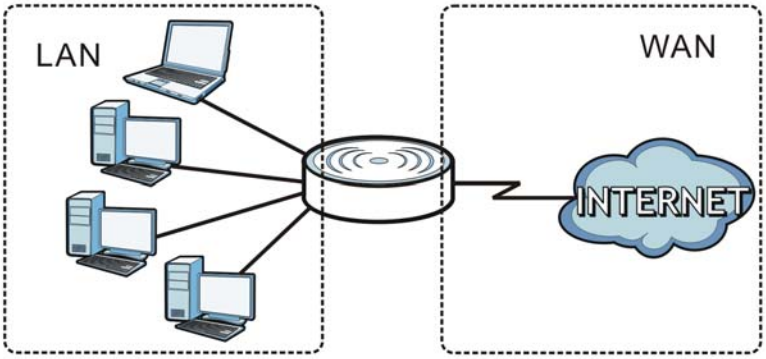


The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

8.2 What You Need To Know

The actual physical connection determines whether the NBG-418N v2 ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 65 LAN and WAN IP Addresses



The LAN parameters of the NBG-418N v2 are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded Web Configurator help regarding what fields need to be configured.

8.2.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

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. 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. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your NBG-418N v2, 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 v2 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 v2 unless you are instructed to do otherwise.

8.2.2 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely

important because without it, you must know the IP address of a computer before you can access it.

The NBG-418N v2 can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **Wizard** and/or **WAN > Internet Connection** screen.

2 If the ISP did not give you DNS server information, leave the **DNS Server** fields set to **0.0.0.0** in the **Wizard** screen and/or set to **From ISP** in the **WAN > Internet Connection** screen for the ISP to dynamically assign the DNS server IP addresses.

8.2.3 IP Pool Setup

The NBG-418N v2 is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the NBG-418N v2 itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

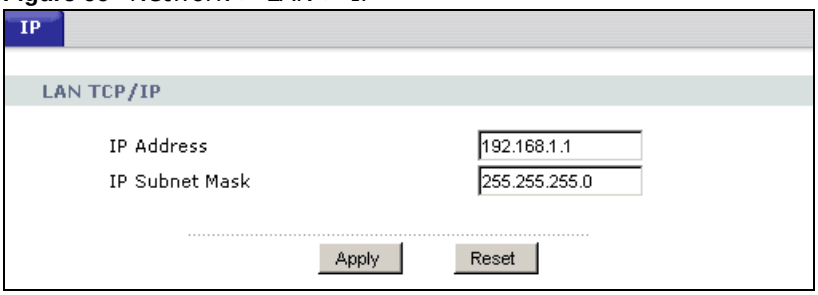
8.2.4 LAN TCP/IP

The NBG-418N v2 has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

8.3 LAN IP Screen

Use this screen to change your basic LAN settings. Click **Network** > **LAN**.

Figure 66 Network > LAN > IP



The following table describes the labels in this screen.

Table 38 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your NBG-418N v2 in dotted decimal notation 192.168.1.1 (factory default).

Table 38 Network > LAN > IP (continued)

LABEL	DESCRIPTION
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG-418N v2 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG-418N v2.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

9

DHCP Server

9.1 Overview

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the NBG-418N v2's LAN as a DHCP server or disable it. When configured as a server, the NBG-418N v2 provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

9.2 What You Can Do

- Use the **General** screen to enable the DHCP server (Section 9.4 on page 96).
- Use the **Advanced** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 9.5 on page 97).
- Use the **Client List** screen to view the current DHCP client information (Section 9.6 on page 98).

9.3 What You Need To Know

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

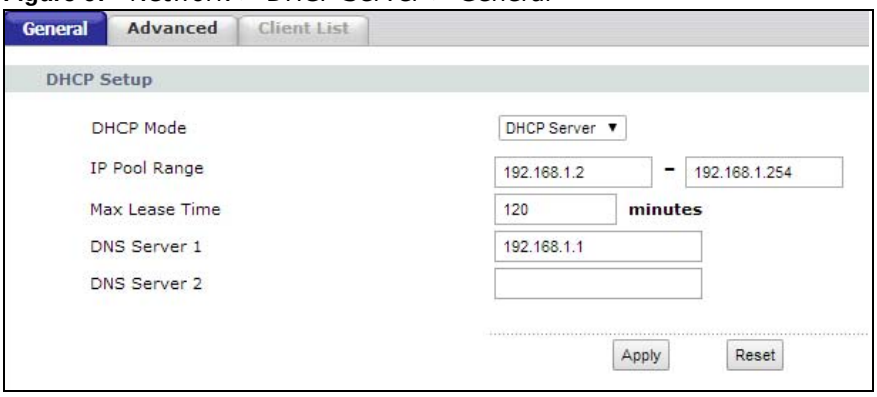
Refer to Section 8.2.1 on page 93 for information on IP Address and Subnet Mask.

Refer to the Section 8.2.2 on page 93 section for information on System DNS Servers.

9.4 General Screen

Use this screen to enable the DHCP server. Click **Network** > **DHCP Server**. The following screen displays.

Figure 67 Network > DHCP Server > General



The following table describes the labels in this screen.

Table 39 Network > DHCP Server > General

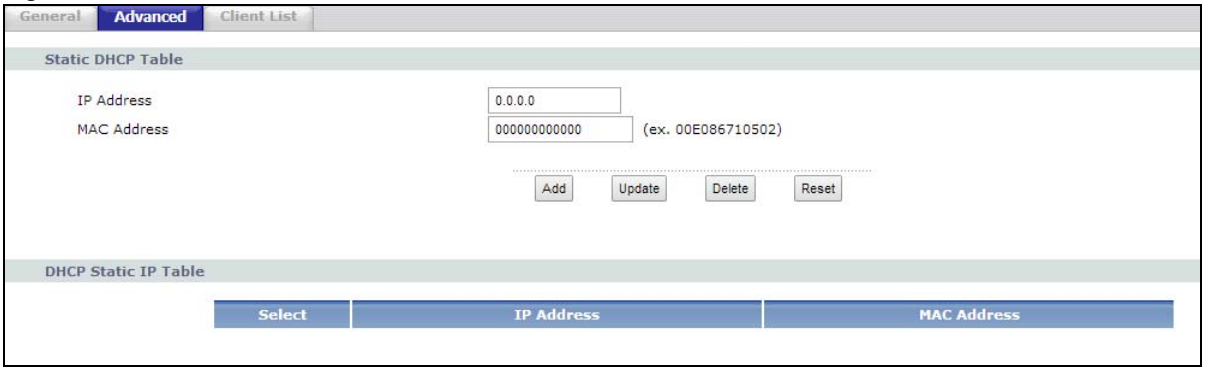
LABEL	DESCRIPTION
DHCP Mode	Select **DHCP server** from the drop-down list to have the NBG-418N v2 act as a DHCP server. Otherwise, select **None**. DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Choose **DHCP Server** option unless your ISP instructs you to do otherwise. Choose **None** to disable the NBG-418N v2 acting as a DHCP server. When configured as a server, the NBG-418N v2 provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Range	This field specifies the range of the contiguous addresses in the **IP address pool** for LAN.
Max Lease Time	This field specifies the **Maximum time** interval the device can be idle before the IP address on the LAN link is disconnected. Default is 120 minutes, maximum is 525600 minutes
DNS Sever1	Type the **First DNS server IP address** of the DHCP server.
DNS Sever2	Type the **Second DNS server IP address** of the DHCP server.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

9.5 Advanced Screen

This screen allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses. You can also use this screen to configure the DNS server information that the NBG-418N v2 sends to the DHCP clients.

To change your NBG-418N v2's static DHCP settings, click **Network** > **DHCP Server** > **Advanced**. The following screen displays.

Figure 68 Network > DHCP Server > Advanced



The following table describes the labels in this screen.

Table 40 Network > DHCP Server > Advanced

LABEL	DESCRIPTION
Static DHCP Table	
IP Address	Type the LAN **IP address** of a computer on your LAN.
MAC Address	Type the **MAC address** (with colons) of a computer on your LAN.
Add	Click **Add** button to add a new static DHCP entry.
Update	Click **Update** button to see the updated DHCP Static IP table.
Delete	Click **Delete** button to delete a static DHCP entry.
Reset	Click **Reset** to clear the IP Address and MAC address box fields.
DHCP Static IP Table	
Select	Click the **Select** radio button to select a static DHCP entry.
IP Address	This field displays the LAN **IP address** of a computer on your LAN.
MAC Address	This field displays the **MAC address** of a computer on your LAN.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

9.6 Client List Screen

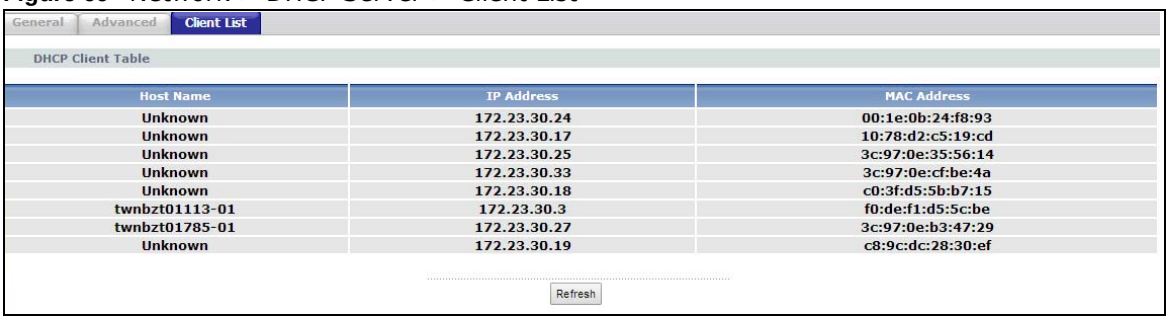
The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of network clients using the NBG-418N v2's DHCP servers.

Configure this screen to always assign an IP address to a MAC address (and host name). Click **Network** > **DHCP Server** > **Client List**.

Note: You can also view a read-only client list by clicking the **DHCP Table (Details...)** hyperlink in the **Status** screen.

The following screen displays.

Figure 69 Network > DHCP Server > Client List



The following table describes the labels in this screen.

Table 41 Network > DHCP Server > Client List

LABEL	DESCRIPTION
Host Name	This field displays the computer **Host name**.
IP Address	This field displays the **IP address** of the computers on the LAN port.
MAC Address	The **MAC** (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Refresh	Click **Refresh** to reload the DHCP table.

10

Network Address Translation

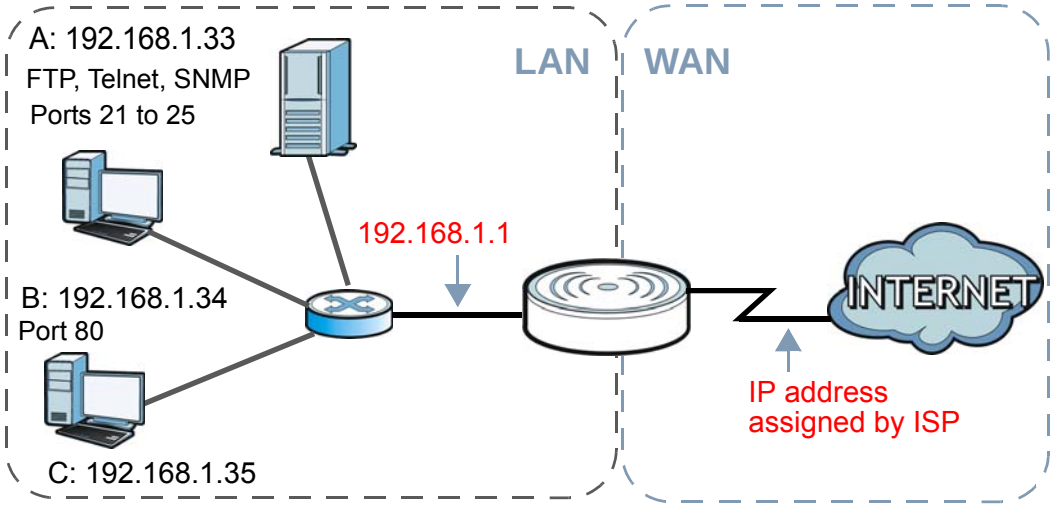
10.1 Overview

This chapter discusses how to configure NAT on the NBG-418N v2.

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

Each packet has two addresses – a source address and a destination address. For outgoing packets, NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address in each packet and then forwards it to the Internet. The NBG-418N v2 keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 70 NAT Example



For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the NBG-418N v2.

10.2 What You Can Do

- Use the **General** screen to enable NAT and set a default server (Section 10.3 on page 102).
- Use the **Application** screen to change your NBG-418N v2's port forwarding settings (Section 10.4 on page 103).

10.2.1 What You Need To Know

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

Inside/Outside

This denotes where a host is located relative to the NBG-418N v2, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

This denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note: Inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet.

An inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 42 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

Note: NAT never changes the IP address (either local or global) of an outside host.

What NAT Does

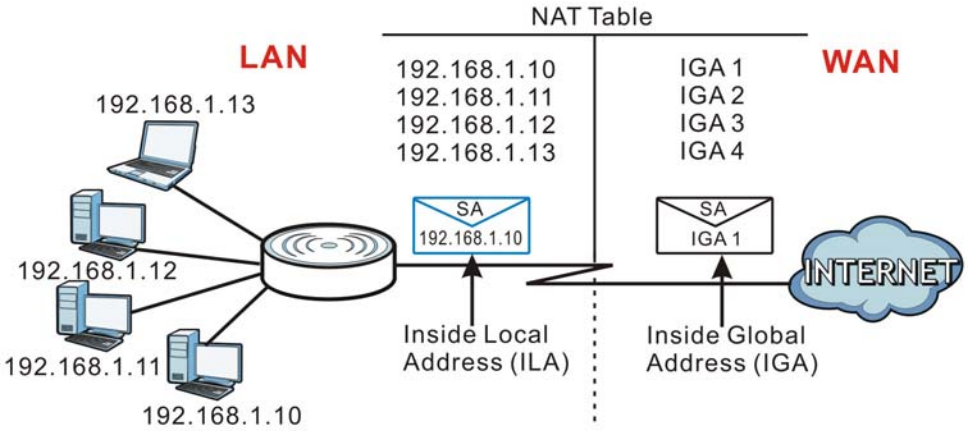
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your NBG-418N v2 filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address in each packet and then forwards it to the Internet. The NBG-418N v2 keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

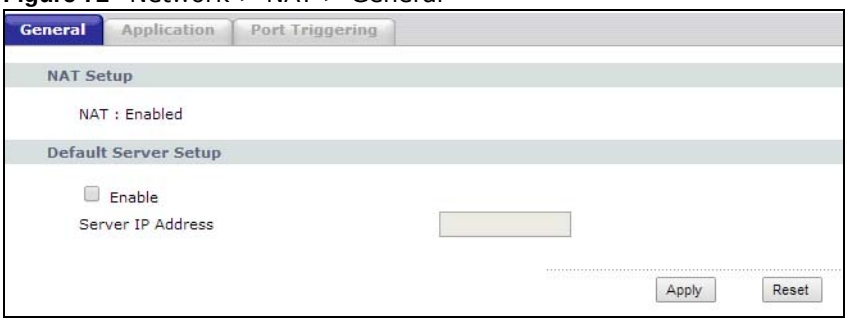
Figure 71 How NAT Works



10.3 General NAT Screen

Use this screen to enable NAT and set a default server. Click **Network > NAT** to open the **General** screen.

Figure 72 Network > NAT > General



The following table describes the labels in this screen.

Table 43 Network > NAT > General

LABEL	DESCRIPTION
NAT Setup	
Network Address Translation	**Network Address Translation** (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). This field displays whether the NAT is enabled or disabled.
Default Server Setup	
Enable	Click the **Enable** check box to activate the default server.
Server IP Address	In addition to the servers for specified services, NAT supports a **default server**. A default server receives packets from ports that are not specified in the **Application** screen. If you do not assign a **Default Server IP address**, the NBG-418N v2 discards all packets received for ports that are not specified in the **Application** screen or remote management.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

10.4 NAT Application Screen

Use the **Application** screen to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

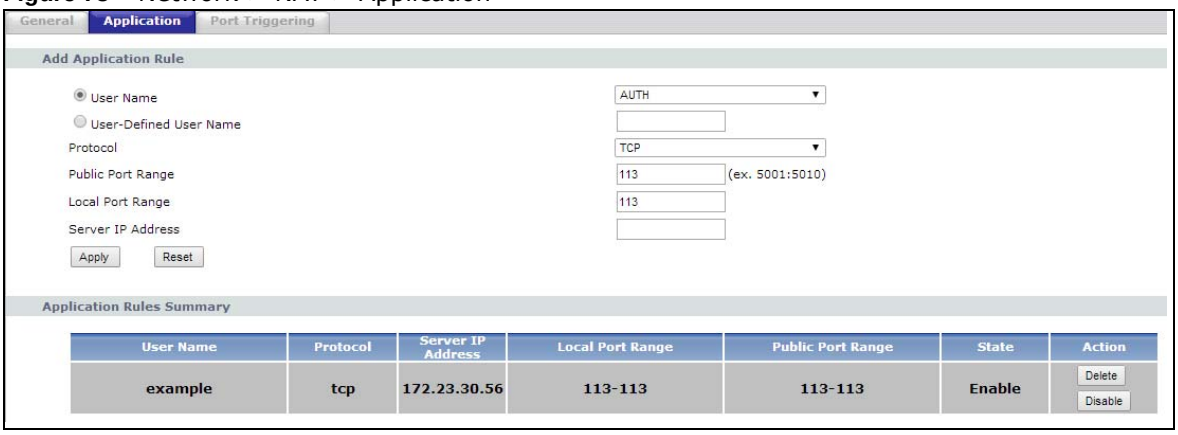
Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your NBG-418N v2's port forwarding settings, click **Network > NAT** > **Application**. The screen appears as shown.

Note: If you do not assign a **Default Server IP address** in the **NAT > General** screen, the NBG-418N v2 discards all packets received for ports that are not specified in this screen or remote management.

Refer to Appendix E on page 209 for port numbers commonly used for particular services.

Figure 73 Network > NAT > Application



The following table describes the labels in this screen.

Table 44 Network > NAT > Application

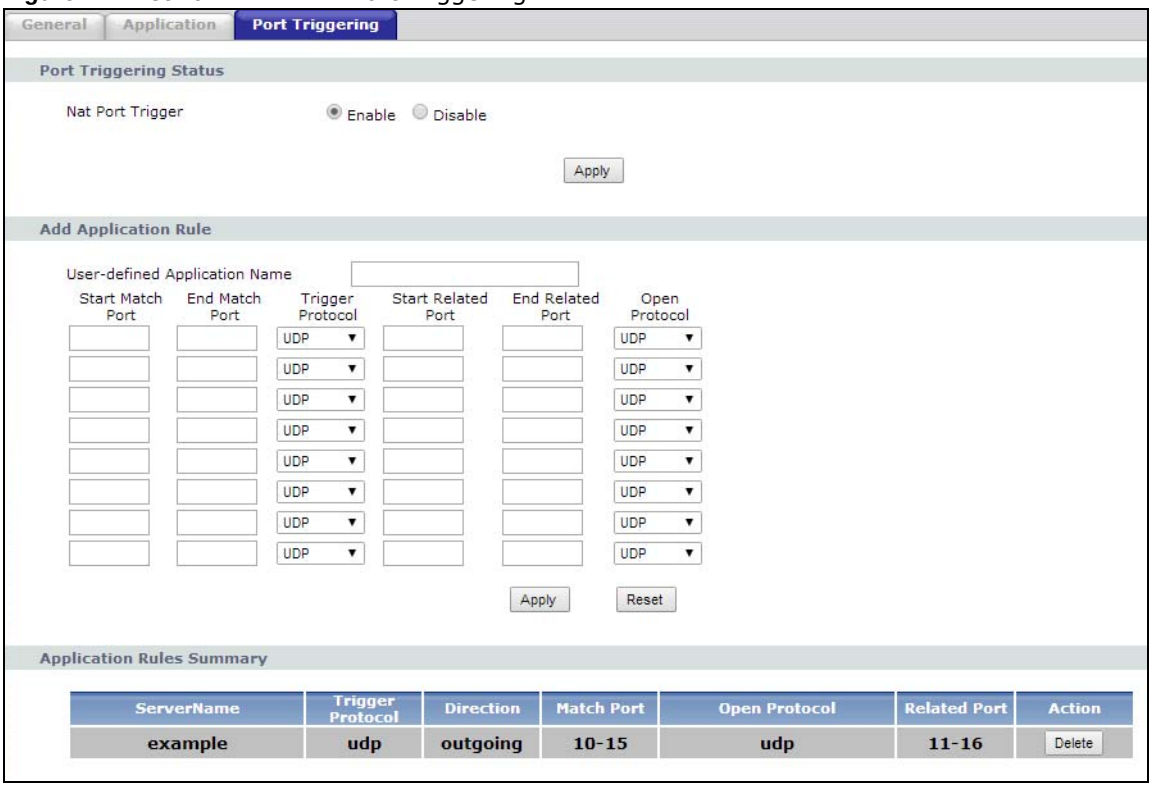
LABEL	DESCRIPTION
Add Application Rule	
User Name	Select an option from the drop-down list to choose a **pre-defined service**. The pre-defined service port number(s) and protocol will display in the fields below.
User-Defined User Name	Type a name (of up to 31 printable characters) to identify this rule in the first field. Otherwise, select a predefined service in the User Name drop-down list. The predefined service name and port number(s) will display in the **User Name,** Public and Local **Port** fields.
Protocol	Select the transport layer protocol used for the service. Choices are **TCP**, **UDP**, or **TCP&UDP**.
Public Port Range Local Port Range	Type a **port number(s)** to be forwarded. To specify a range of ports, enter a hyphen (-) between the first port and the last port, such as 10-20. To specify two or more non-consecutive port numbers, separate them by a comma without spaces, such as 123,567.
Server IP Address	Type the inside IP address of the server that receives packets from the port(s) specified in the **Port** field.
Apply	Click **Apply** to save your changes to the **Application Rules Summary** table.
Reset	Click **Reset** to not save and return your new changes in the **Service Name** and **Port** fields to the previous one.
Application Rules Summary	
User Name	This field displays a name to identify this rule.
Protocol	This field displays the transport layer protocol supported by this server.
Server IP Address	This field displays the inside IP address of the server.
Local Port Range Public Port Range	This field displays the port number(s).
State	This is the transport layer protocol used for the service.
Action	Click the **Disable** icon to display and modify an existing rule setting in the fields under **Add Application Rule**. Click the **Delete** icon to delete a rule.

10.5 Port Triggering Screen

To change your NBG-418N v2's port trigger settings, click **Network > NAT > Port Triggering**. The screen appears as shown.

Note: Only one LAN computer can use a port trigger (range) at a time.

Figure 74 Network > NAT > Port Triggering



The following table describes the labels in this screen.

Table 45 Network > NAT > Port Triggering

LABEL	DESCRIPTION
Port Triggering Status	Click **Enable** radio button to enable NAT Port Trigger or **Disable** to inactivate it.
Apply	Click **Apply** button to apply the NAT Port Trigger status you choose above.
Add Application Rule	
User-defined Application Name	Type a unique **name** (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Start Match Port	**Start match Port** is the starting port in a range of port numbers that a server on the WAN uses when it sends out a particular service. The NBG-418N v2 forwards the traffic with this starting port to the client computer on the LAN that requested the service.
End Match Port	**End match Port** is the ending port in a range of port numbers that a server on the WAN uses when it sends out a particular service. The NBG-418N v2 forwards the traffic with this ending port to the client computer on the LAN that requested the service.
Trigger Protocol	The **trigger protocol** is the protocol (UDP, TCP or UDP/TCP) that causes (or triggers) the NBG-418N v2 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.

Table 45 Network > NAT > Port Triggering (continued)

LABEL	DESCRIPTION
Start Related Port	Type a **Starting port** number that is related to the open protocol.
End Related Port	Type a **Ending port** number that is related to the open protocol.
Open Protocol	The **open protocol** is the protocol (UDP, TCP or UDP/TCP) that causes (or triggers) the NBG-418N v2 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.6 Technical Reference

The following section contains additional technical information about the NBG-418N v2 features described in this chapter.

10.6.1 NAT Port Forwarding: Services and Port Numbers

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use the **Application** screen to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

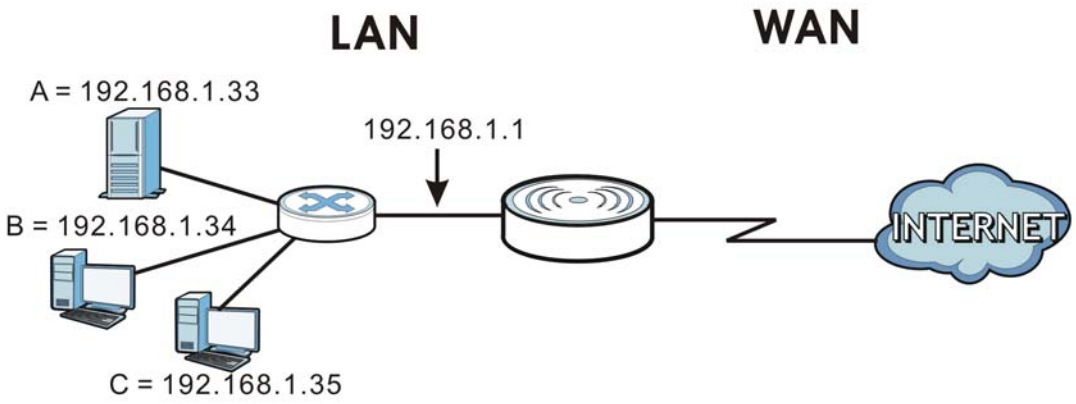
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

10.6.2 NAT Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 75 Multiple Servers Behind NAT Example



10.6.3 Trigger Port Forwarding

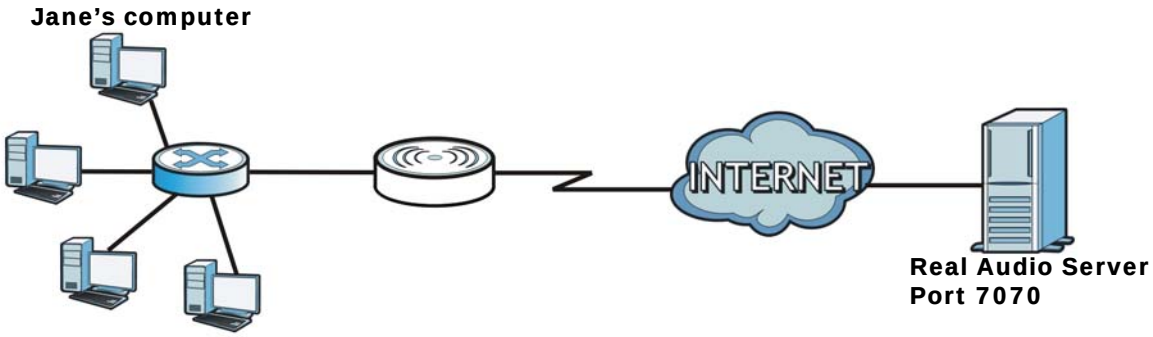
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The NBG-418N v2 records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the NBG-418N v2's WAN port receives a response with a specific port number and protocol ("incoming" port), the NBG-418N v2 forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

10.6.4 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 76 Trigger Port Forwarding Process: Example



1 Jane requests a file from the Real Audio server (port 7070).

2 Port 7070 is a “trigger” port and causes the NBG-418N v2 to record Jane’s computer IP address. The NBG-418N v2 associates Jane's computer IP address with the "incoming" port range of 6970-7170.

3 The Real Audio server responds using a port number ranging between 6970-7170.

4 The NBG-418N v2 forwards the traffic to Jane’s computer IP address.

5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The NBG-418N v2 times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

10.6.5 Two Points To Remember About Trigger Ports

1 Trigger events only happen on data that is coming from inside the NBG-418N v2 and going to the outside.

2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can’t trigger it.

11

Dynamic DNS

11.1 Overview

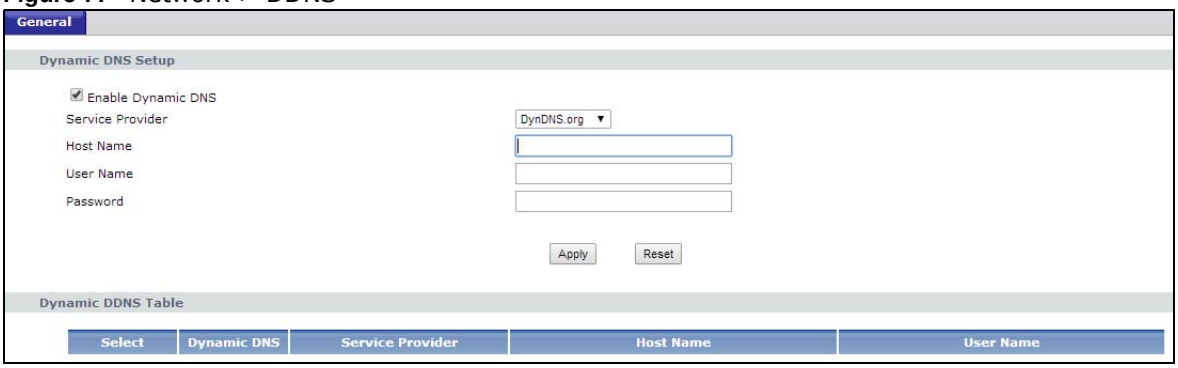
Dynamic Domain Name Service (DDNS) services let you use a fixed domain name with a dynamic IP address. Users can always use the same domain name instead of a different dynamic IP address that changes each time to connect to the NBG-418N v2 or a server in your network.

Note: The NBG-418N v2 must have a public global IP address and you should have your registered DDNS account information on hand.

11.2 Dynamic DNS Screen

To configure your NBG-418N v2's DDNS, click **Network > DDNS**.

Figure 77 Network > DDNS



The following table describes the labels in this screen.

Table 46 Network > DDNS

LABEL	DESCRIPTION
Enable Dynamic DNS	Click the **Enable Dynamic DNS** check box to enable DDNS.
Service Provider	Select the name of your DDNS **Service provider** from the drop-down list.
Host Name	The **Host name** is the domain name that the DDNS service will map to your dynamic global IP address. Type the host name fully qualified, for example, 'yourhost.mydomain.net'. You can specify up to two host names in the field separated by a comma (",").
User Name	Type the **User name** that you used when you registered with the DDNS service.
Password	Type the **Password** associated with the DDNS user name.
Timeout	This is the length of **Time** in hours between updates to the DDNS service. If the update fails, the NBG-418N v2 will disable DDNS.

Table 46 Network > DDNS

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.
Dynamic DDNS Table	
Select	Click the **Select** check box to select the DDNS entry and click **Delete** to remove it or **Apply** to save changes made to it.
Dynamic DNS	This field displays whether the DDNS is **Enabled** or **Disabled**.
Service Provider	This field displays the **Service provider** name of the DDNS.
Host Name	This field displays the **Host name** that is associated with the DDNS.
User Name	This field displays the **User name** that is associated with the DDNS.

12

Firewall

12.1 Overview

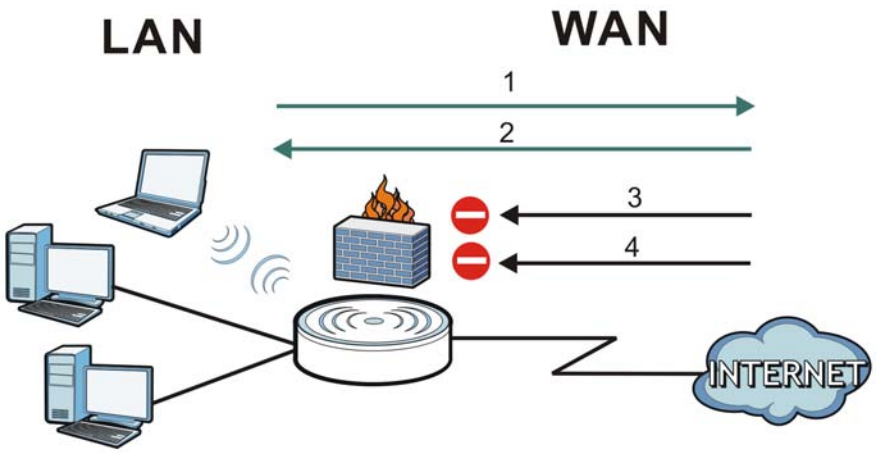
Use these screens to enable and configure the firewall that protects your NBG-418N v2 and your LAN from unwanted or malicious traffic.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (**1**). Return traffic for this session is also allowed (**2**). However other traffic initiated from the WAN is blocked (**3** and **4**).

Figure 78 Default Firewall Action



12.2 What You Can Do

- Use the **General** screen to enable or disable the NBG-418N v2's firewall (Section 12.4 on page 112).
- Use the **Services** screen to enable or disable ICMP and VPN passthrough features (Section 12.5 on page 113).

12.3 What You Need To Know

The NBG-418N v2’s firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

12.3.1 About the NBG-418N v2 Firewall

The NBG-418N v2 firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The NBG-418N v2's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG-418N v2 can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The NBG-418N v2 is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The NBG-418N v2 has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

12.3.2 VPN Pass Through Features

A Virtual Private Network (VPN) is a way to securely connect two networks over the Internet. For example a home network and one in a business office. This requires special equipment on both ends of the connection.

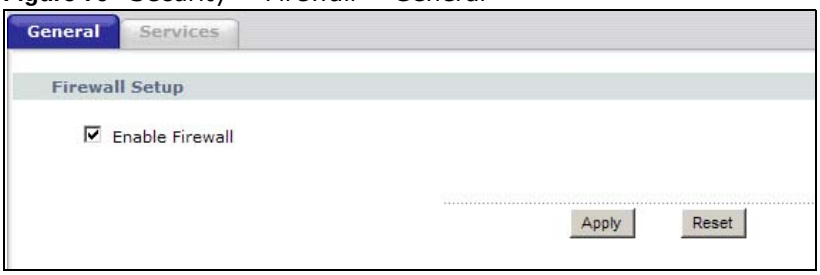
The NBG-418N v2 is not one of the endpoints but it does allow traffic from those endpoints to pass through. The NBG-418N v2 allows the following types of VPN traffic to pass through:

- IP security (IPSec)
- Point-to-Point Tunneling Protocol (PPTP)

12.4 General Firewall Screen

Use this screen to enable or disable the NBG-418N v2’s firewall, and set up firewall logs. Click **Security** > **Firewall** to open the **General** screen.

Figure 79 Security > Firewall > General



The following table describes the labels in this screen.

Table 47 Security > Firewall > General

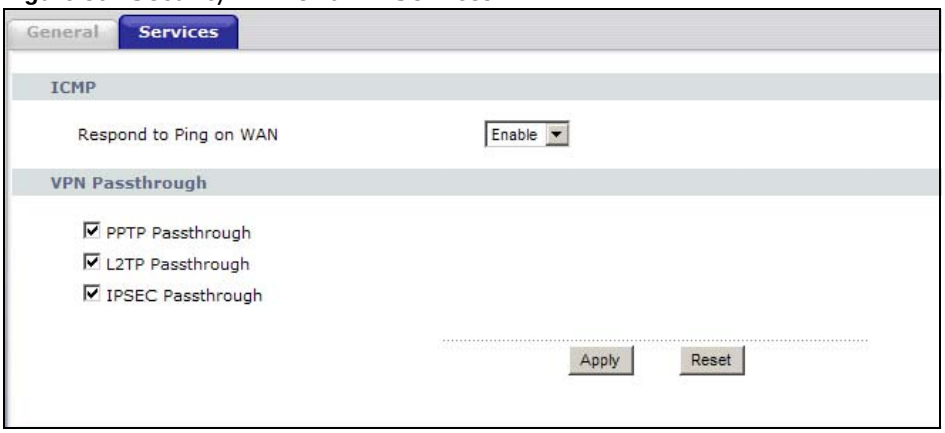
LABEL	DESCRIPTION
Enable Firewall	Select the **Enable Firewall** check box to activate the firewall. The NBG-418N v2 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

12.5 Services Screen

Use the **Services** screen to enable or disable ICMP and VPN passthrough features.

Click **Security** > **Firewall** > **Services**. The screen appears as shown next.

Figure 80 Security > Firewall > Services



The following table describes the labels in this screen.

Table 48 Security > Firewall > Services

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol **(ICMP)** is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on WAN	The NBG-418N v2 will not respond to any incoming Ping requests when **Disable** is selected. Select **Enable** to reply to incoming WAN Ping requests.

Table 48 Security > Firewall > Services (continued)

LABEL	DESCRIPTION
VPN Passthrough	Select the checkbox to enable the advanced pass through features: • **PPTP Passthrough:** Select this option to allow the NBG-418N v2 to pass through VPN traffic using PPTP. • **L2TP Passthrough:** Select this option to enable computers on your LAN to make L2TP VPN connections to servers on the Internet. • **IPSEC Passthrough:** Select this option to allow the NBG-418N v2 to pass through VPN traffic using the IPsec protocol.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

13

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 v2 interface (if any) from which computers.

You may manage your NBG-418N v2 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 v2 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 v2's WAN IP address when configuring from the WAN.
- Use the NBG-418N v2's LAN IP address when configuring from the LAN.

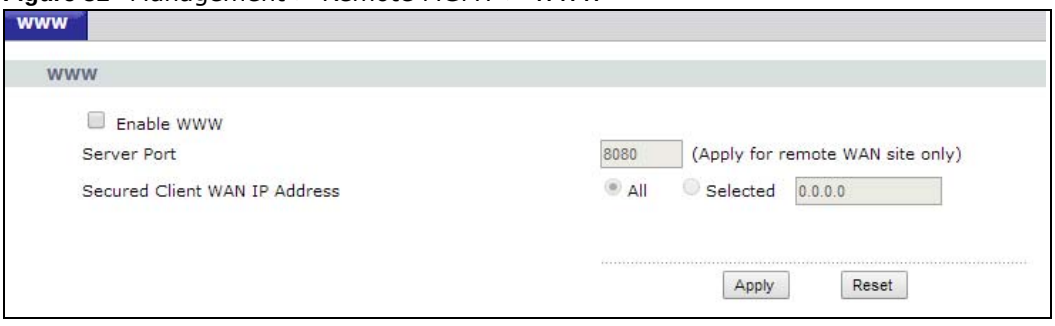
13.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The NBG-418N v2 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 v2's World Wide Web settings, click **Management** > **Remote MGMT** to display the **WWW** screen.

Figure 81 Management > Remote MGMT > WWW



The following table describes the labels in this screen.

Table 49 Management > Remote MGMT > WWW

LABEL	DESCRIPTION
Enable WWW	Click the **Enable WWW** check box to configure your NBG-418N v2 via HTTP using a web browser.
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.
Secured Client WAN IP Address	A secured client is a "trusted" computer that is allowed to communicate with the NBG-418N v2 using this service. Select **All** to allow any computer to access the NBG-418N v2 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the NBG-418N v2 using this service. Note: This only applies on WAN IP.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

14

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 v2 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 50 Management > UPnP > General

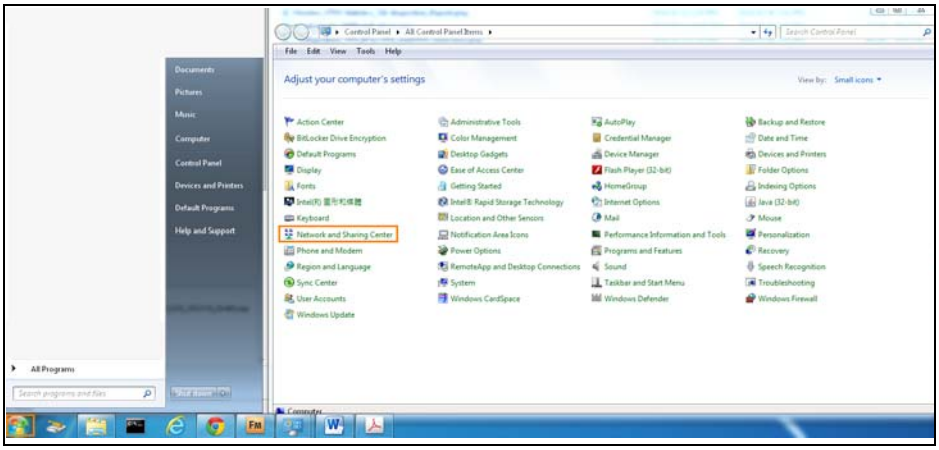
LABEL	DESCRIPTION
Device Name	This field displays the description of the NBG-418N v2 router.
Enable the Universal Plug and Play (UPnP) Feature	Select the **Enable the UPnP Features** check box to activate UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the NBG-418N v2's IP address (although you must still enter the password to access the Web Configurator).
Apply	Click **Apply** to save the setting to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

14.4 Installing UPnP in Windows 7 Example

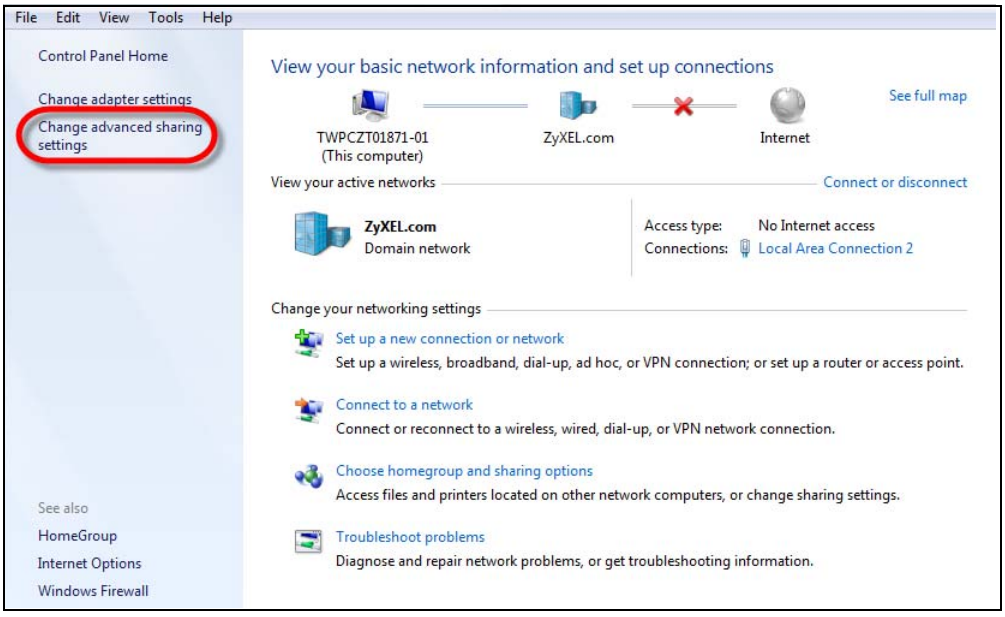
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. You will need to activate UPnP on the VMG4381-B10A.

Make sure the computer is connected to a LAN port of the VMG4381-B10A. Turn on your computer and the VMG4381-B10A.

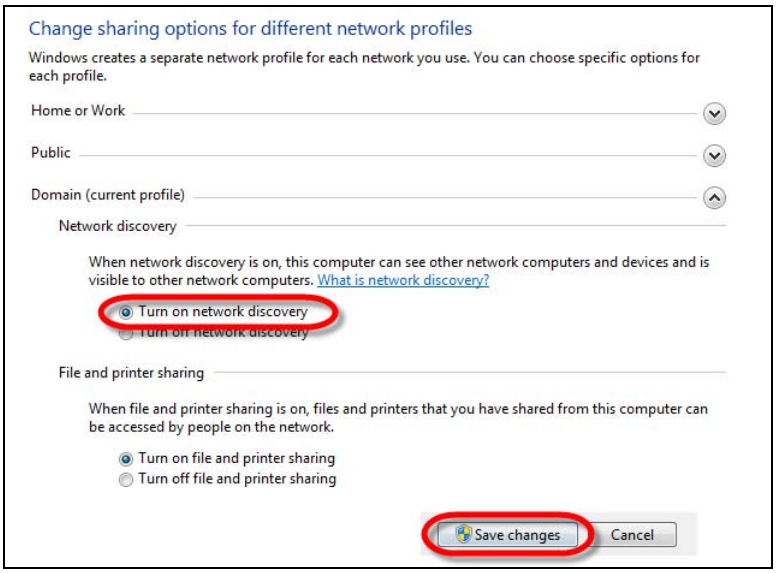
1 Click the **Start** icon, **Control Panel** and then the **Network and Sharing Center.**



2 Click **Change Advanced Sharing Settings**.



3 Under Network Discover section, select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.



14.4.1 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 v2.

Make sure the computer is connected to a LAN port of the NBG-418N v2. Turn on your computer and the NBG-418N v2.

14.4.1.1 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

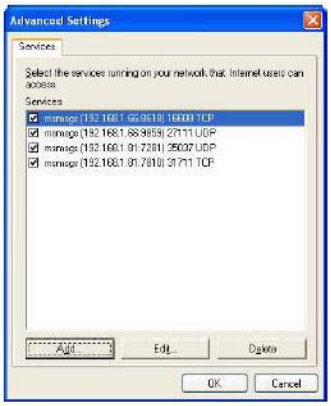
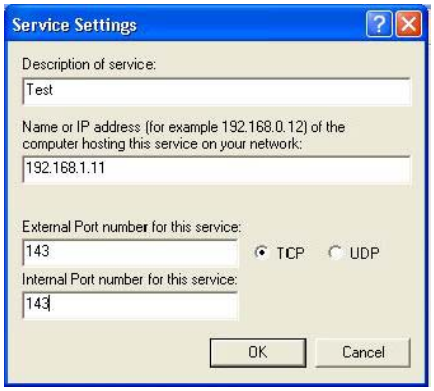


Figure 86 Internet Connection Properties: Advanced Settings: Add



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

14.4.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the NBG-418N v2 without finding out the IP address of the NBG-418N v2 first. This comes helpful if you do not know the IP address of the NBG-418N v2.

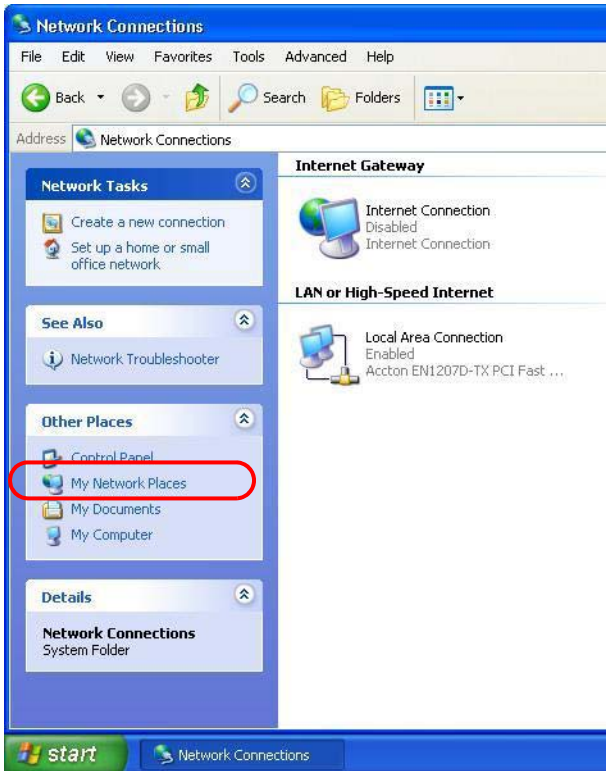
Follow the steps below to access the Web Configurator.

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 v2 and select **Invoke**. The Web Configurator login screen displays.

Figure 90 Network Connections: My Network Places

6 Right-click on the icon for your NBG-418N v2 and select **Properties**. A properties window displays with basic information about the NBG-418N v2.

Figure 91 Network Connections: My Network Places: Properties: Example

15

Bandwidth MGMT

15.1 Overview

Bandwidth management provides a convenient way to manage the use of various services on the network. It manages general protocols (for example, HTTP and FTP) and applies traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

15.2 What You Can Do

- Use the **Bandwidth MGMT** screen to enable this feature in the NBG-418N v2.
- Use the **Advance** screen to configure the QoS (Quality of Service) rule on the NBG-418N v2.

15.3 What You Need To Know

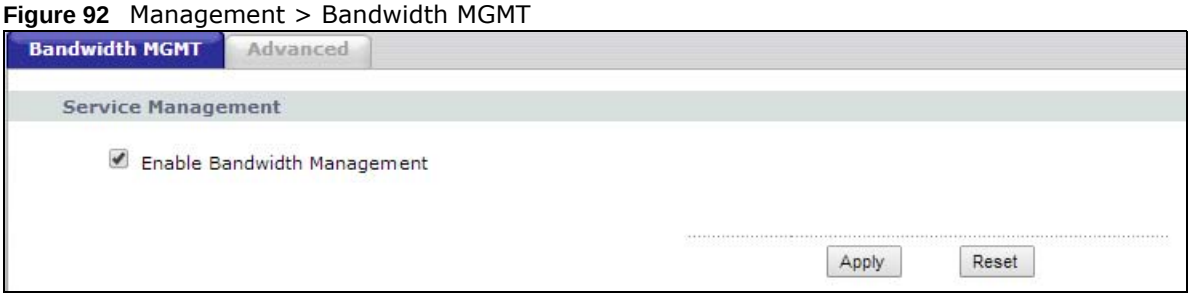
The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN) must be less than or equal to the **Upstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen.

The sum of the bandwidth allotments that apply to the LAN interface (WAN to LAN, WAN to WLAN) must be less than or equal to the **Downstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen.

15.4 Bandwidth MGMT Screen

Use this screen to enable the bandwidth management feature on the NBG-418N v2. Click **Management** > **Bandwidth MGMT**. The following screen displays.

Figure 92 Management > Bandwidth MGMT



The following table describes the labels in this screen.

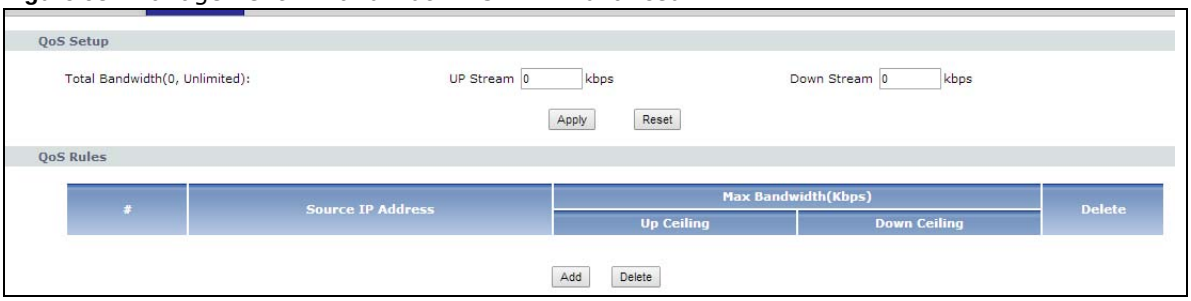
Table 51 Management > Bandwidth MGMT > Bandwidth MGMT

LABEL	DESCRIPTION
Service Management	
Enable Bandwidth Management	Click the **Enable Bandwidth Management** check box to activate the bandwidth management feature in the NBG-418N v2.
Apply	Click **Apply** to save your changes in t his screen.
Reset	Click **Reset** to begin configuring this screen afresh.

15.5 Advanced Screen

Use this screen to setup the QoS rules for the NBG-418N v2. Click **Management** > **Bandwidth MGMT > Advanced**. The following screen displays.

Figure 93 Management > Bandwidth MGMT > Advanced



The following table describes the labels in this screen.

Table 52 Management > Bandwidth MGMT > Advanced

LABEL	DESCRIPTION
QoS Setup	
Total Bandwidth (0, Unlimited)	This field shows the maximum number of data in kbps the NBG-418N v2 is allowed to send out and allowed to come in through a source interface.
Up Stream	Type the **Up Stream** or maximum outgoing transmission data rate (kbps) that is allowed to go through the source interface on the NBG-418N v2.
Down Stream	Type the **Down Stream** or maximum incoming transmission data rate (kbps) that is allowed to go through the source interface on the NBG-418N v2.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.
QoS Rules	
#	This field shows the index number of the QoS rule.
Source IP Address	This field shows the source IP Address of the data traffic.
Max Bandwidth(kpbs)	
Up Ceiling	This field shows the maximum outgoing transmission data rate (kbps) that is allo wed to go through the source interface on the NBG-418N v2.
Down Ceiling	This field shows the maximum outgoing transmission data rate (kbps) that is allowed to go through the source interface on the NBG-418N v2.
Delete	Click the **Delete** check box to select the QoS rule you want to delete.

Table 52 Management > Bandwidth MGMT > Advanced (continued)

LABEL	DESCRIPTION
Add	Click **Add** button to add the QoS rule.
Delete	Click **Delete** to remove the QoS rule.

16

System

16.1 Overview

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

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

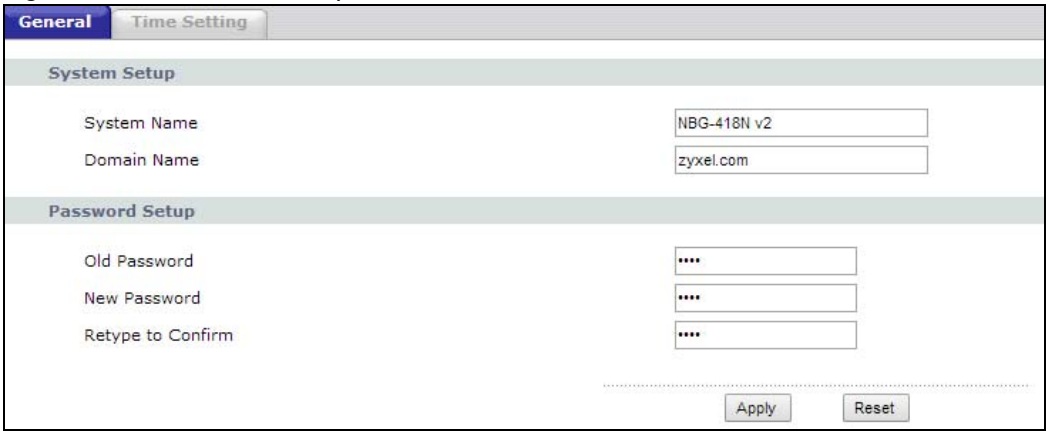
16.2 What You Can Do

- Use the **General** screen to enter a name to identify the NBG-418N v2 in the network and set the password (Section 16.3 on page 129).
- Use the **Time Setting** screen to change your NBG-418N v2's time and date (Section 16.4 on page 130).

16.3 System General Screen

Use this screen to enter a name to identify the NBG-418N v2 in the network and set the password. Click **Maintenance** > **System**. The following screen displays.

Figure 94 Maintenance > System > General



The following table describes the labels in this screen.

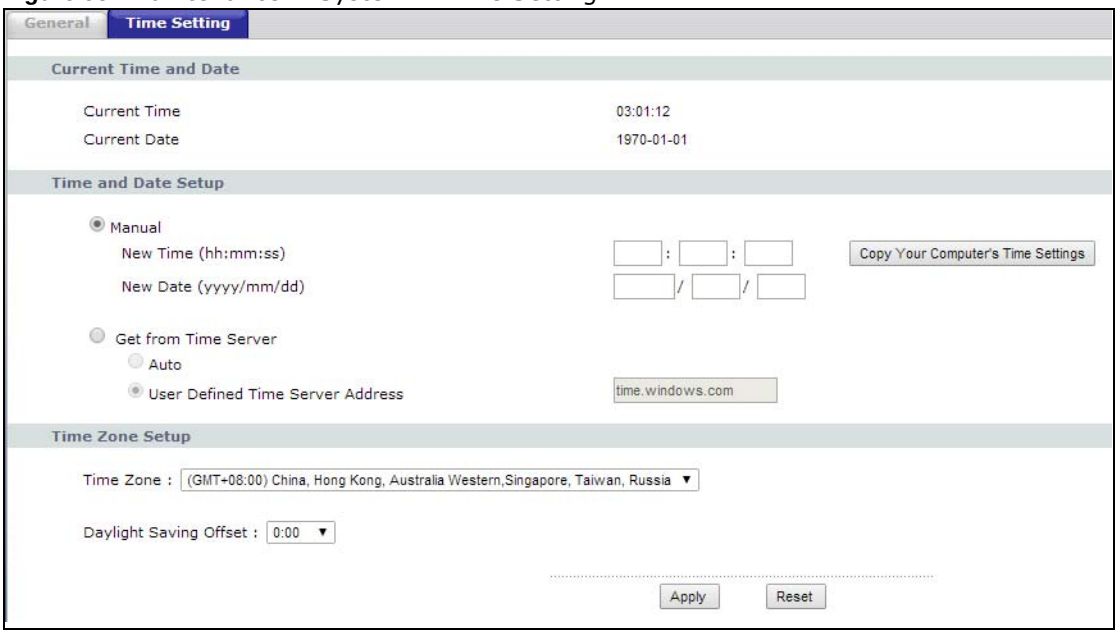
Table 53 Maintenance > System > General

LABEL	DESCRIPTION
System Setup	
System Name	**System Name** is a unique name to identify the NBG-418N v2 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.
Password Setup	Change your NBG-418N v2's **password** (recommended) using the fields as shown.
Old Password	Type the default password or the existing **password** you use to access the system in this field.
New Password	Type your new system **password** (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

16.4 Time Setting Screen

To change your NBG-418N v2's time and date, click **Maintenance** > **System** > **Time Setting**. The screen appears as shown. Use this screen to configure the NBG-418N v2's time based on your local time zone.

Figure 95 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 v2. Each time you reload this page, the NBG-418N v2 synchronizes the time with the time server.
Current Date	This field displays the date of your NBG-418N v2. Each time you reload this page, the NBG-418N v2 synchronizes the date with the time server.
Time and Date Setup	
Manual	Select the **Manual** 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 the **Copy your computer's time settings** button to copy your computer's time settings into the NBG-418N v2'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 **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select the **Get from time server** radio button to have the NBG-418N v2 get the time and date from the time server you specified below.
Auto	Select **Auto** to have the NBG-418N v2 automatically search for an available time server and synchronize the date and time with the time server after you click **Apply**.
User Defined Time Server Address	Select **User Defined Time Server Address** and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the **Time zone** of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings Offset	**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 the number of offset hours you wish to adjust for daylight savings from the drop-down list.
Apply	Click **Apply** to save your changes back to the NBG-418N v2.
Reset	Click **Reset** to begin configuring this screen afresh.

17

Logs

17.1 Overview

This chapter contains information about configuring general log settings and viewing the NBG-418N v2's logs.

The Web Configurator allows you to look at all of the NBG-418N v2's logs in one location.

17.2 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.

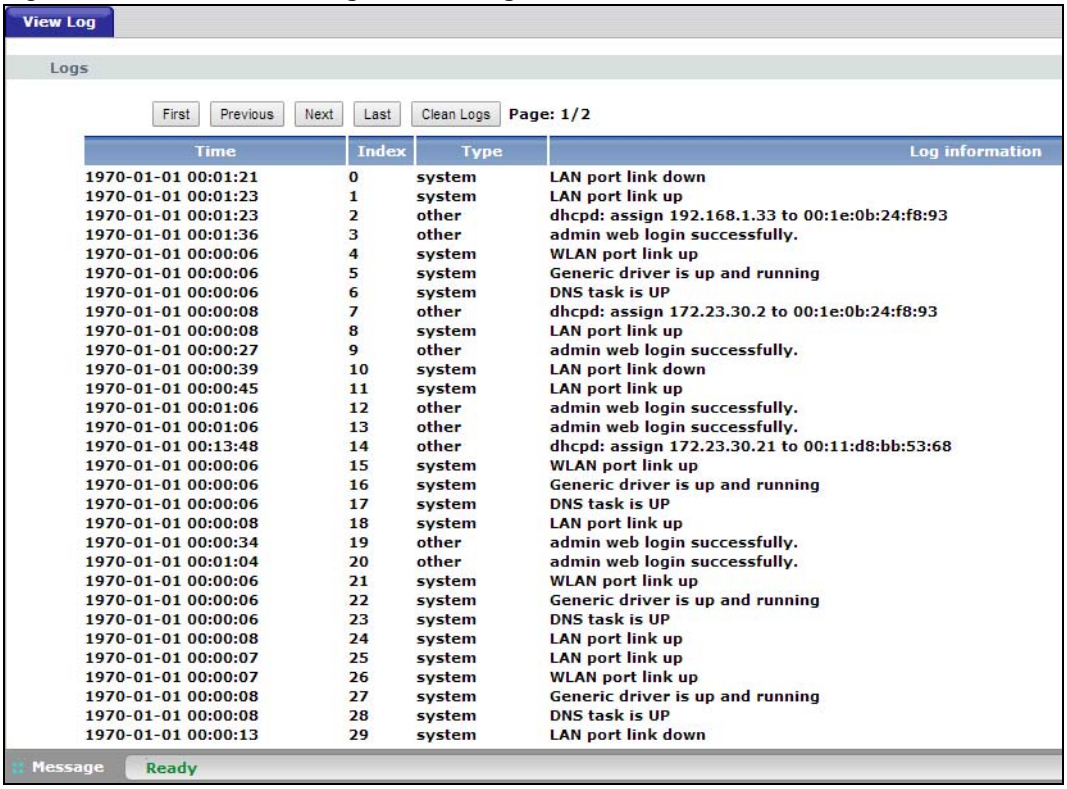
17.3 View Log Screen

Use the **View Log** screen to see the logged messages for the NBG-418N v2. 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 96 Maintenance > Logs > View Log



The following table describes the labels in this screen.

Table 55 Maintenance > Logs > View Log

LABEL	DESCRIPTION
First	Click **First** button to see the first page of the log.
Previous	Click **Previous** button to go back one page from your current log page.
Next	Click **Next** button to go to the following page from your current log page.
Last	Click **Last** button to go to the last page of the log.
Clear Logs	Click **Clear Logs** to delete all the logs.
Message	This field states the reason for the log.

18 Tools

18.1 Overview

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the NBG-418N v2.

18.2 What You Can Do

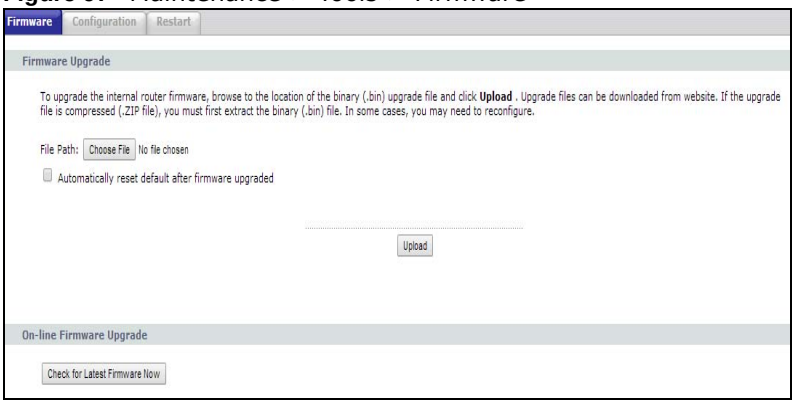
- Use the **Firmware** screen to upload firmware to your NBG-418N v2 (Section 18.3 on page 134).
- Use the **Configuration** screen to view information related to factory defaults, backup configuration, and restoring configuration (Section 18.4 on page 136).
- Use the **Restart** screen to have the NBG-418N v2 reboot (Section 18.5 on page 138).

18.3 Firmware Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "NBG-418N v2.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 v2.

Figure 97 Maintenance > Tools > Firmware



The following table describes the labels in this screen.

Table 56 Maintenance > Tools > Firmware

LABEL	DESCRIPTION
Choose File	Click **Choose File** button to find the.bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Automatically reset default after firmware upgraded	Click the **Automatically reset default after firmware upgraded** check box to have the NBG-418N v2 automatically reset itself after the new firmware is uploaded.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
Check for Latest Firmware Now	Click **Check for Latest Firmware Now** button to have the NBG-418N v2 search for the latest firmware available online at ZyXEL's website.

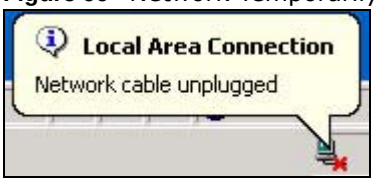
Note: Do not turn off the NBG-418N v2 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait for several minutes before logging into the NBG-418N v2 again.

Figure 98 Upload Warning

The NBG-418N v2 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 99 Network Temporarily Disconnected



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

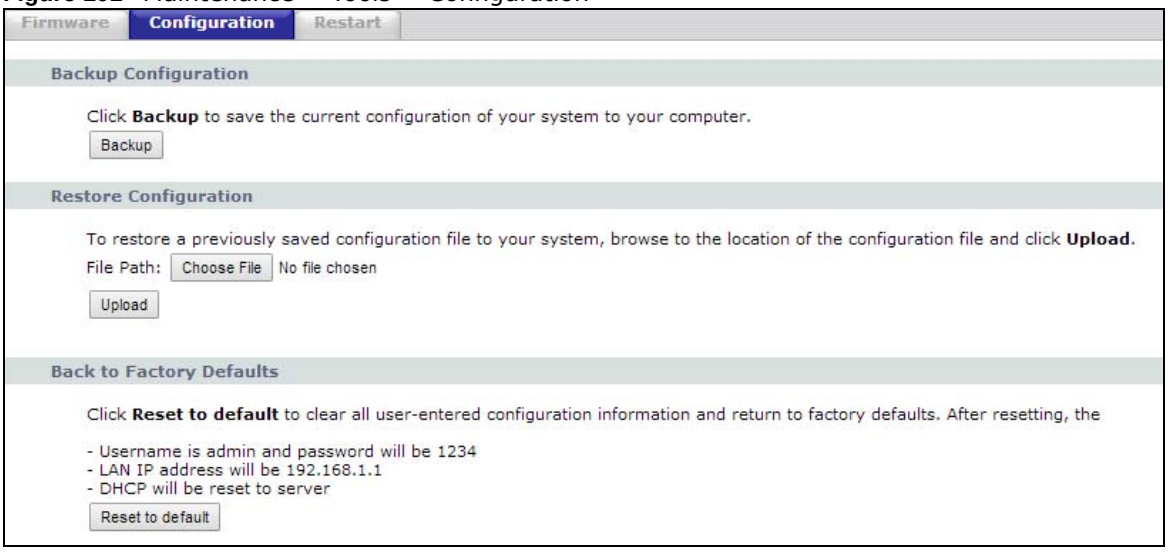
If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

Figure 100 Upload Error Message

18.4 Configuration Screen

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

Figure 101 Maintenance > Tools > Configuration



18.4.1 Backup Configuration

Backup configuration allows you to back up (save) the NBG-418N v2's current configuration to a file on your computer. Once your NBG-418N v2 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 v2's current configuration to your computer.

18.4.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG-418N v2.

Table 57 Maintenance Restore Configuration

LABEL	DESCRIPTION
Choose File	Click **Choose File** button to find the backup file of previous configuration you saved on your computer using the **Backup** button.
Upload	Click **Upload** to begin the upload process.

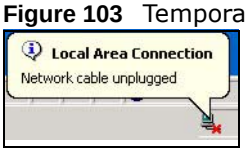
Note: Do not turn off the NBG-418N v2 while configuration file upload is in progress.

After you see a "configuration upload successful" screen, you must then wait one minute before logging into the NBG-418N v2 again.

Figure 102 Configuration Restore Successful

The NBG-418N v2 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 103 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 v2 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 104 Configuration Restore Error

18.4.3 Back to Factory Defaults

Pressing the **Reset to default** button in this section clears all user-entered configuration information and returns the NBG-418N v2 to its factory defaults.

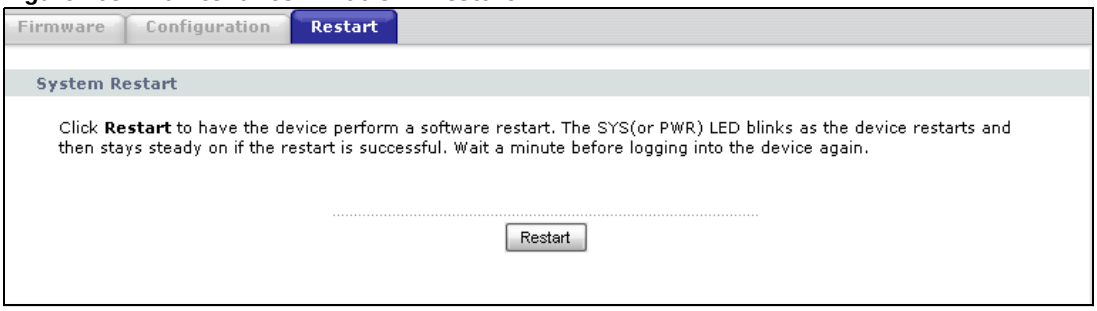
You can also press the **WPS / RESET** button on the rear panel to reset the factory defaults of your NBG-418N v2. Refer to Section 1.4.1 on page 15 for more information on the **WPS / RESET** button.

18.5 Restart Screen

System restart allows you to reboot the NBG-418N v2 without turning the power off.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the NBG-418N v2 reboot. This does not affect the NBG-418N v2's configuration.

Figure 105 Maintenance > Tools > Restart



19

Sys OP Mode

19.1 Overview

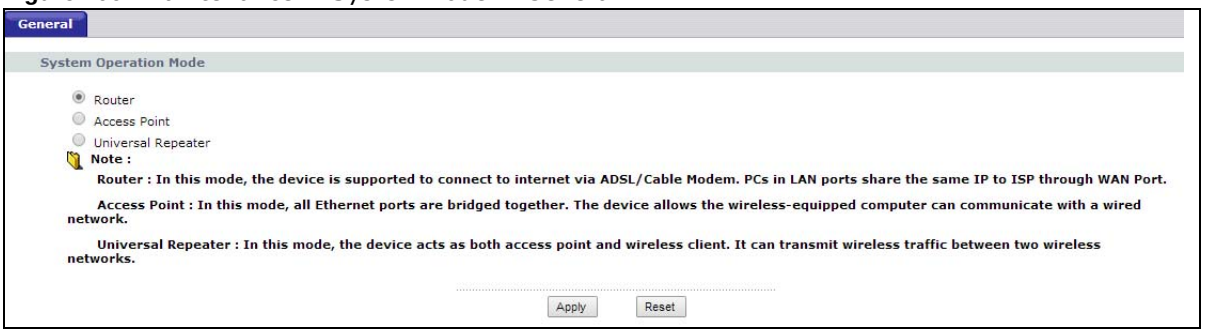
The **Sys OP Mode** (System Operation Mode) function lets you configure select the device operation mode: **Router**, **Access Point**, or **Universal Repeater**.

See Chapter 4 on page 29 for more information on which mode to choose.

19.2 General Screen

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

Figure 106 Maintenance > Sys OP Mode > General



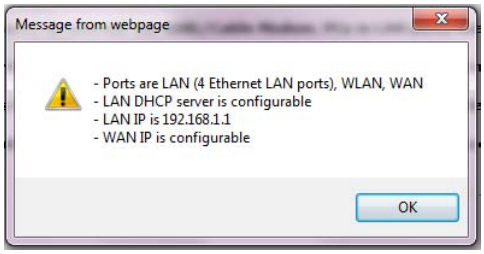
The following table describes the labels in the **General** screen.

Table 58 Maintenance > Sys Op Mode > General

LABEL	DESCRIPTION
System Operation Mode	
Router	Use **Router** mode if you want to use routing functions such as LAN DHCP, NAT, firewall and so on, on the NBG-418N v2 (N). The NBG-418N v2 has separate LAN and WAN network IP addresses.
Access Point	Use **Access Point** mode if you already have a Router (R) in your network and you want to bridge all wired and wireless network connections.
Universal Repeater	Use **Universal Repeater** mode if there is an existing wireless router or access point in your network and you want the NBG-418N v2 to wirelessly relay communications from its wireless clients to it.
Apply	Click **Apply** to save your settings.
Reset	Click **Reset** to return to the previous screen settings.

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

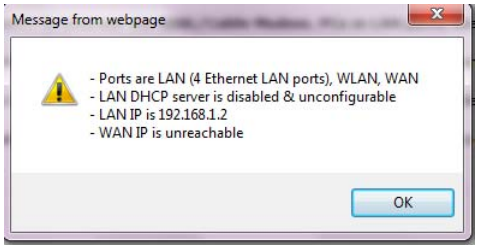
Figure 107 Maintenance > Sys Op Mode > General: Router



- 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 v2 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,** or **Universal Repeater**) the following pop-up message window appears.

Figure 108 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 v2 is set to 192.168.1.2.

20

Language

20.1 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 v2.

Figure 109 Language

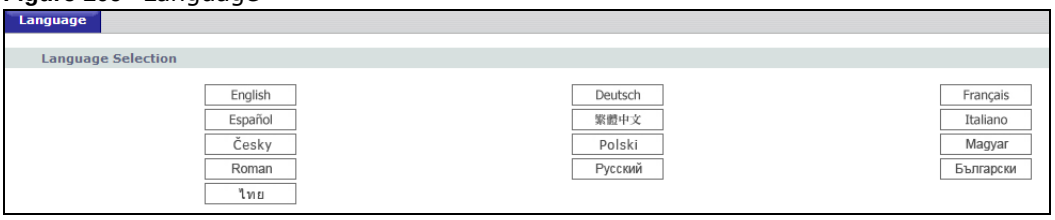
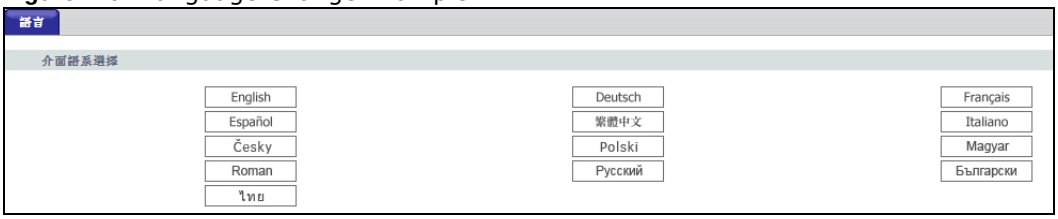


Figure 110 Language Change Example



21

Troubleshooting

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

21.1 Power, Hardware Connections, and LEDs

The NBG-418N v2 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 v2.
2. Make sure the power adaptor or cord is connected to the NBG-418N v2 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 v2.
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 14.
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 v2.
5. If the problem continues, contact the vendor.

21.2 NBG-418N v2 Access and Login

I don't know the IP address of my NBG-418N v2.

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 v2 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 v2 (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 v2'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 v2 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 v2 to change all settings back to their default. This means your current settings are lost. See Section 21.4 on page 145 in the **Troubleshooting** for information on resetting your NBG-418N v2.

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 21.4 on page 145.

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 v2.

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 158.

4 Make sure your computer is in the same subnet as the NBG-418N v2. (If you know that there are routers between your computer and the NBG-418N v2, 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 v2.

5 Reset the device to its factory defaults, and try to access the NBG-418N v2 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 v2.

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 v2.

4 If this does not work, you have to reset the device to its factory defaults. See Section 21.4 on page 145.

21.3 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 v2), 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 14.

2 Reboot the NBG-418N v2.

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 14. If the NBG-418N v2 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 v2 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 v2.

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

21.4 Resetting the NBG-418N v2 to Its Factory Defaults

If you reset the NBG-418N v2, you lose all of the changes you have made. The NBG-418N v2 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 **WPS/RESET** button.

To reset the NBG-418N v2,

1. Make sure the power LED is on.
2. Press the **WPS/RESET** button for longer than 10 second to reboot and restore factory-default configurations on the NBG-418N v2.

   If the NBG-418N v2 restarts automatically, wait for the NBG-418N v2 to finish restarting, and log in to the Web Configurator. The username is **admin** and password is **1234**.

   If the NBG-418N v2 does not restart automatically, disconnect and reconnect the NBG-418N v2's power. Then, follow the directions above again.

21.5 Wireless Problems

I cannot access the NBG-418N v2 or ping any computer from the WLAN.

1. Make sure the wireless LAN is enabled on the NBG-418N v2.
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 v2.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG-418N v2.
5. Check that both the NBG-418N v2 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 v2.
7. Make sure you allow the NBG-418N v2 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.

A

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.

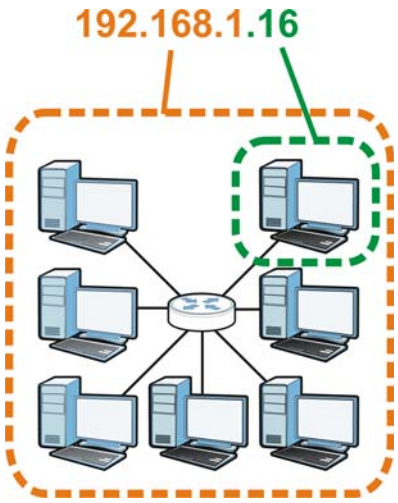
Structure

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 111 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

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

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

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

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

Table 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

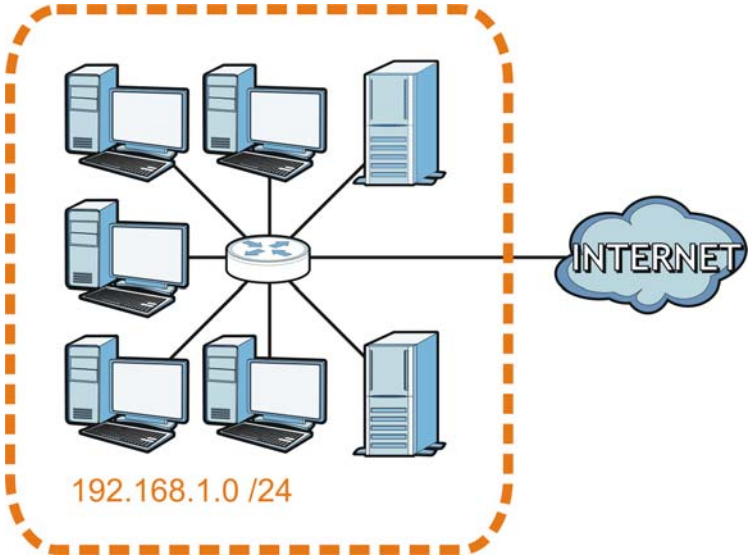
Subnetting

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 112 Subnetting Example: Before Subnetting

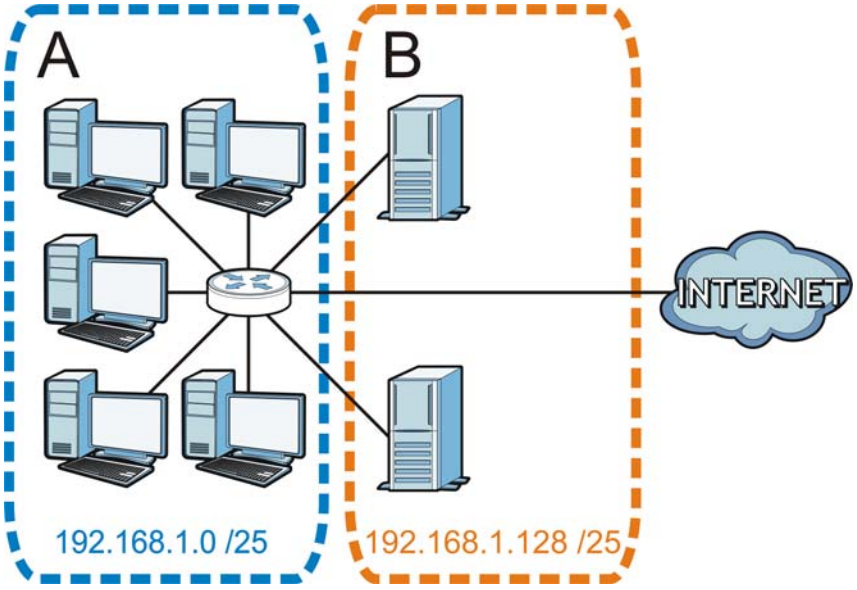


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 113 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.**11**000000) 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.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 v2.

Once you have decided on the network number, pick an IP address for your NBG-418N v2 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 v2 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 v2 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.

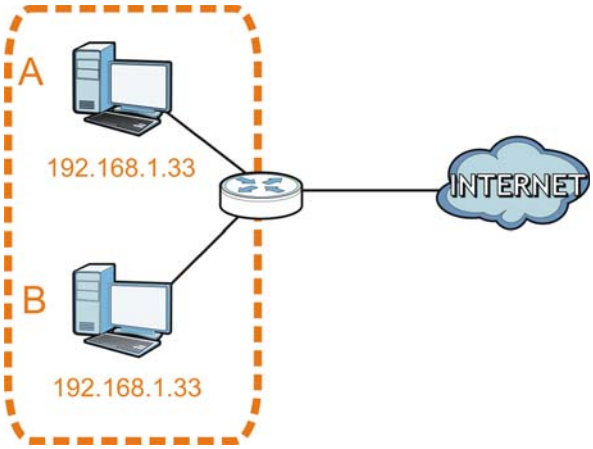
IP Address Conflicts

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.

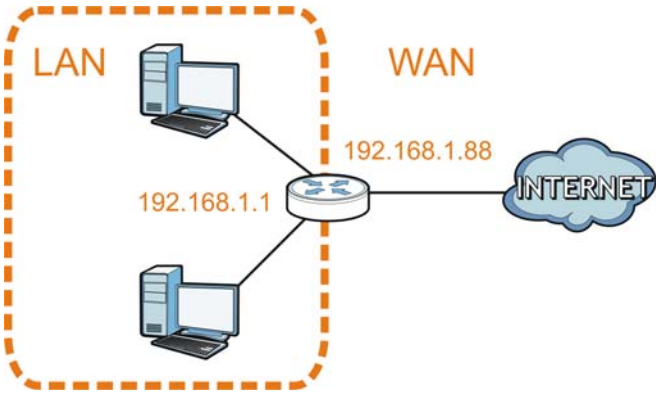
Figure 114 Conflicting Computer IP Addresses Example



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.

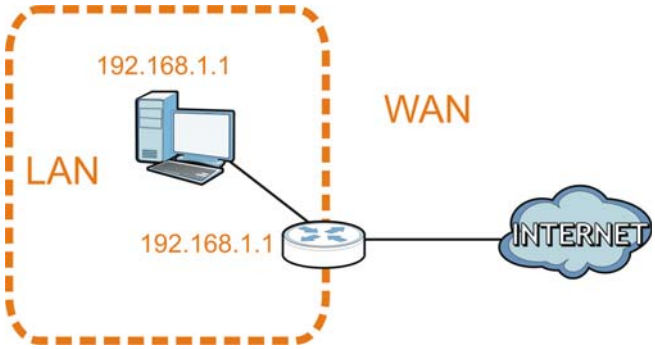
Figure 115 Conflicting Router IP Addresses Example



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 116 Conflicting Computer and Router IP Addresses Example



B

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

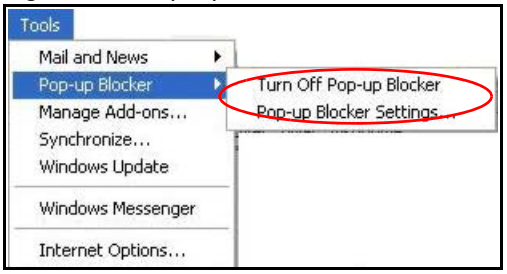
You may have to disable pop-up blocking to log into your device.

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 117 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 118 Internet Options: Privacy

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

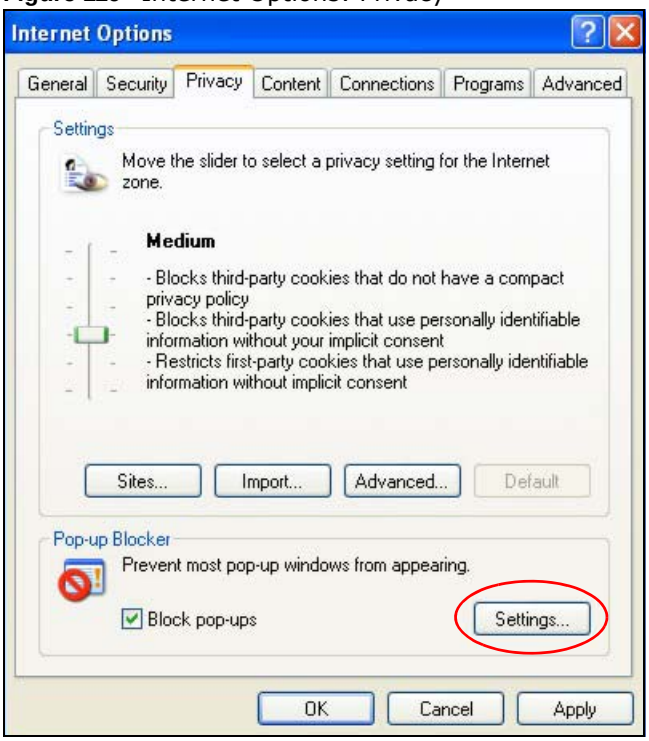
Enable Pop-up Blockers with Exceptions

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 119 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 120 Pop-up Blocker Settings

5 Click **Close** to return to the **Privacy** screen.

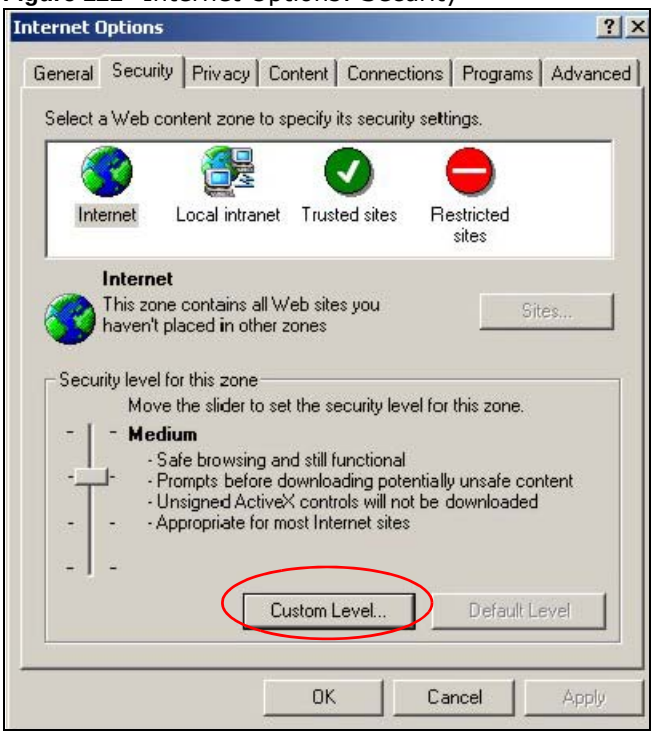
6 Click **Apply** to save this setting.

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 121 Internet Options: Security



2 Click the **Custom Level...** button.

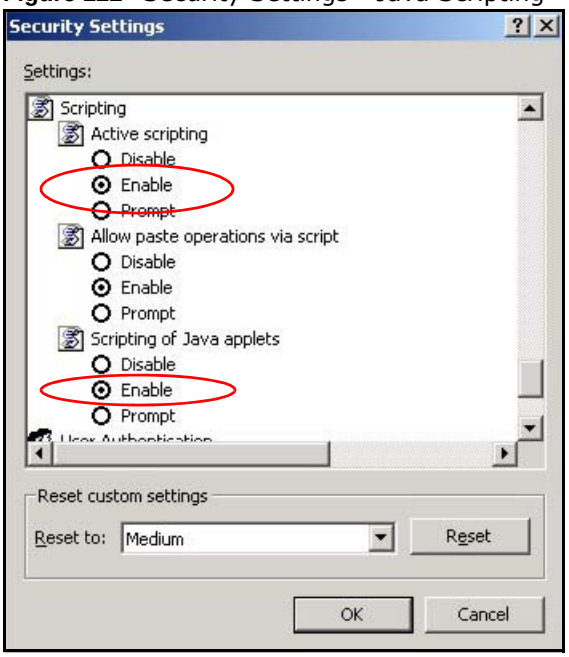
3 Scroll down to **Scripting**.

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 122 Security Settings - Java Scripting



Java Permissions

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

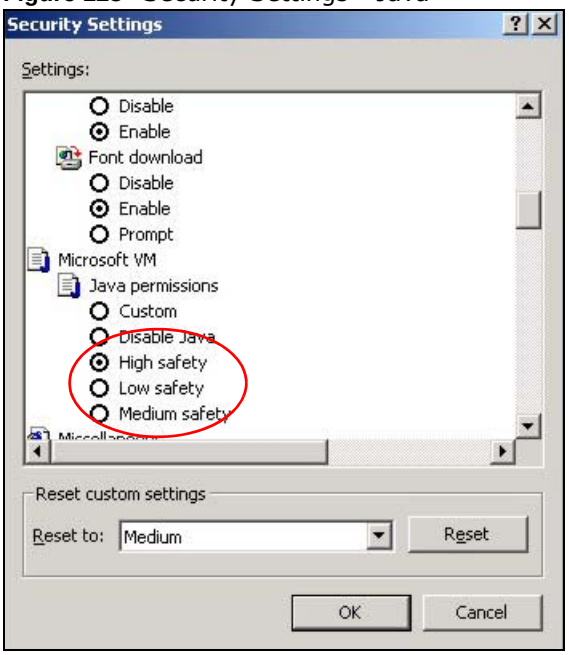
2 Click the **Custom Level...** button.

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 123 Security Settings - Java



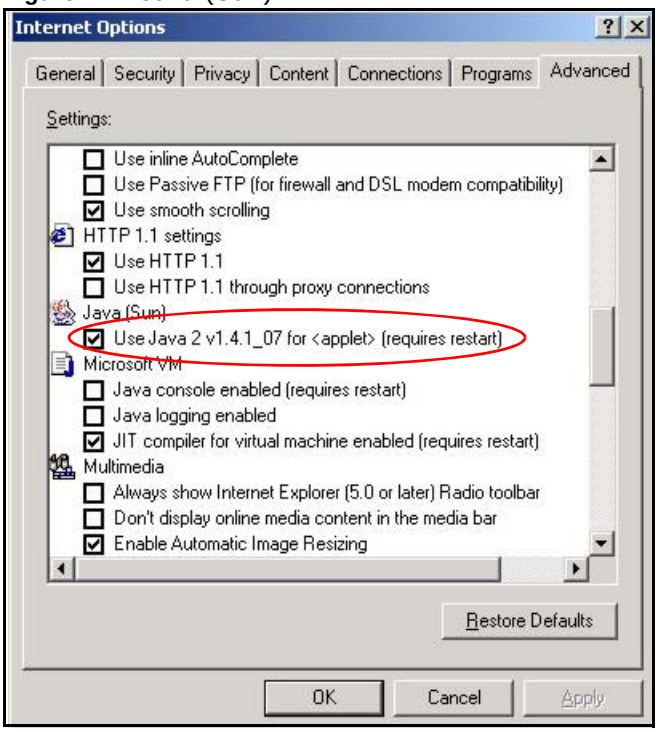
JAVA (Sun)

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 124 Java (Sun)

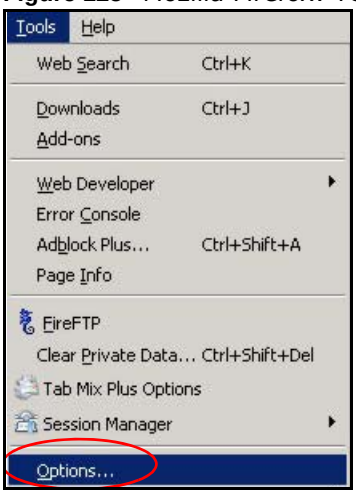


Mozilla Firefox

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.

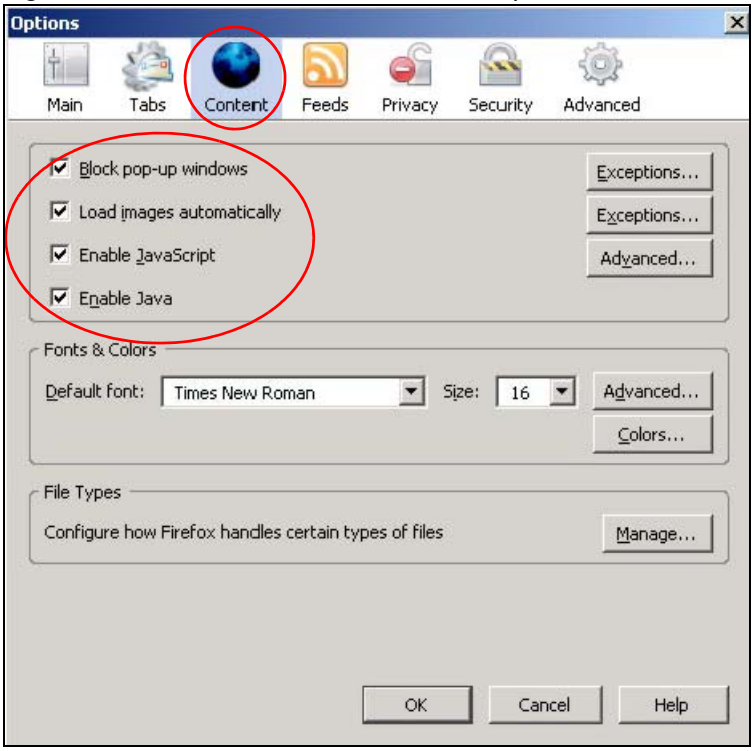
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 125 Mozilla Firefox: TOOLS > Options



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

Figure 126 Mozilla Firefox Content Security



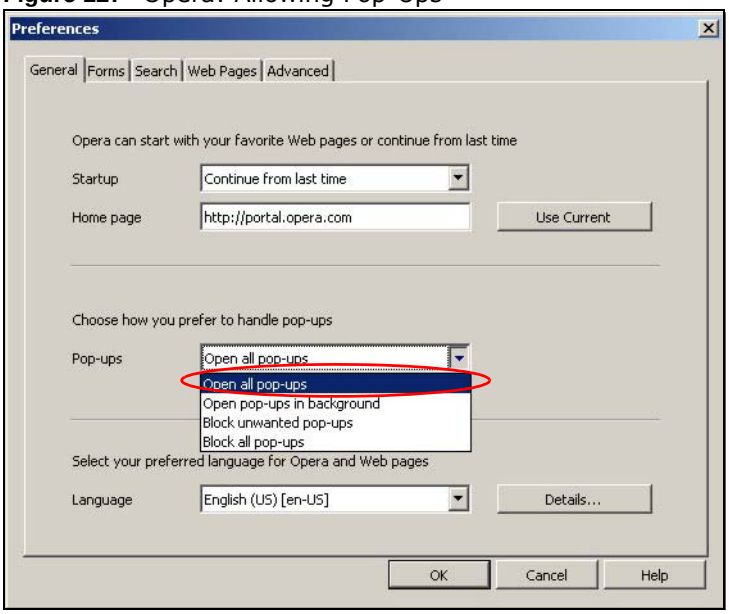
Opera

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**.

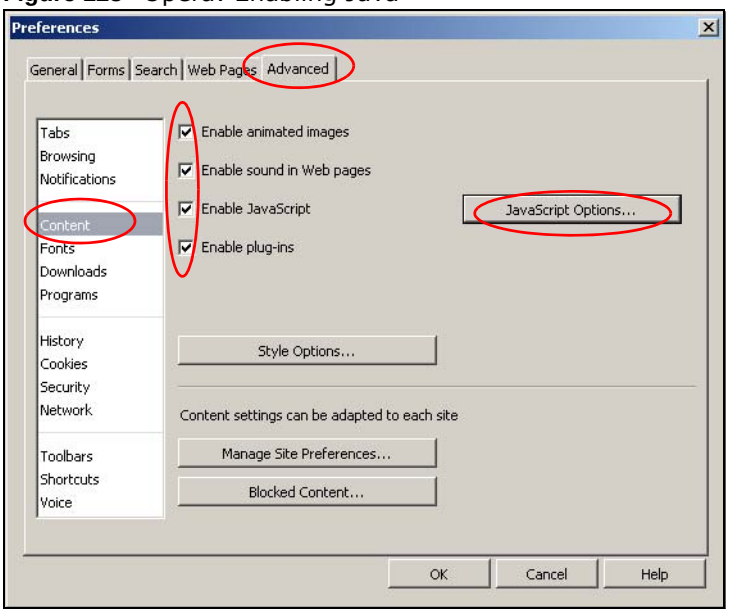
Figure 127 Opera: Allowing Pop-Ups



Enabling Java

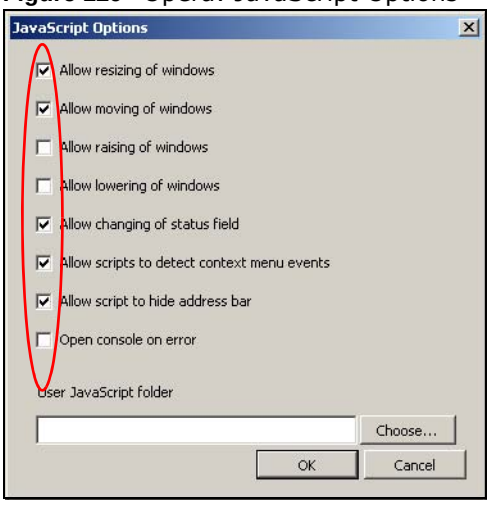
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 128 Opera: Enabling Java



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

Figure 129 Opera: JavaScript Options



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

C

Setting Up Your Computer's IP Address

Note: Your specific NBG-418N v2 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.

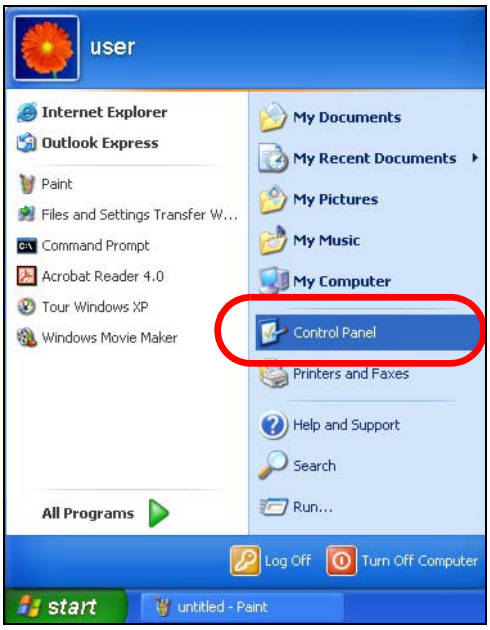
If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

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

Windows XP/NT/2000

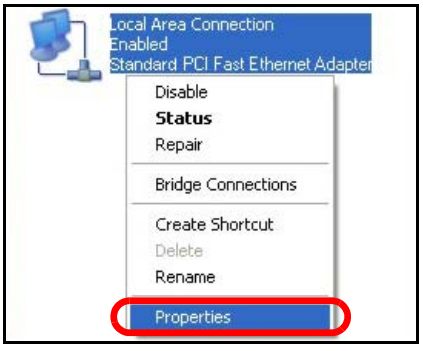
The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

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

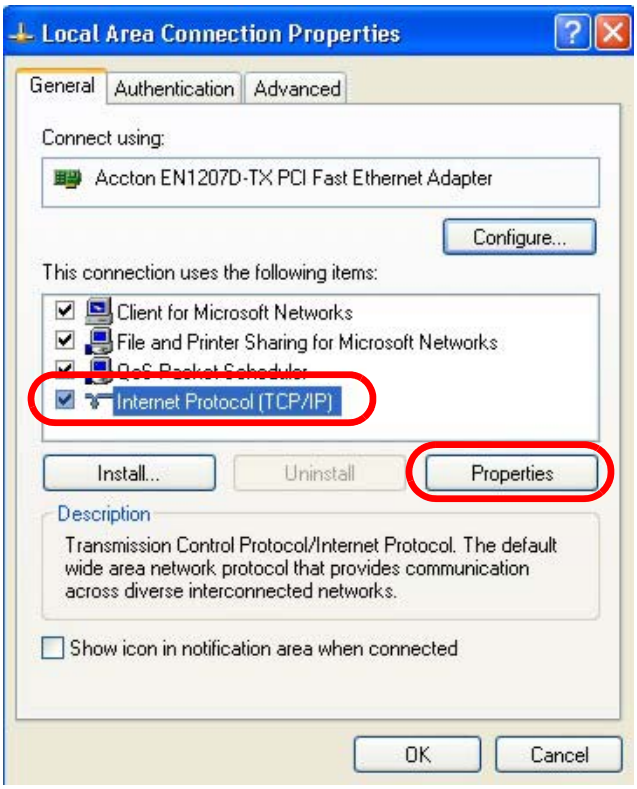


2 In the **Control Panel**, click the **Network Connections** icon.

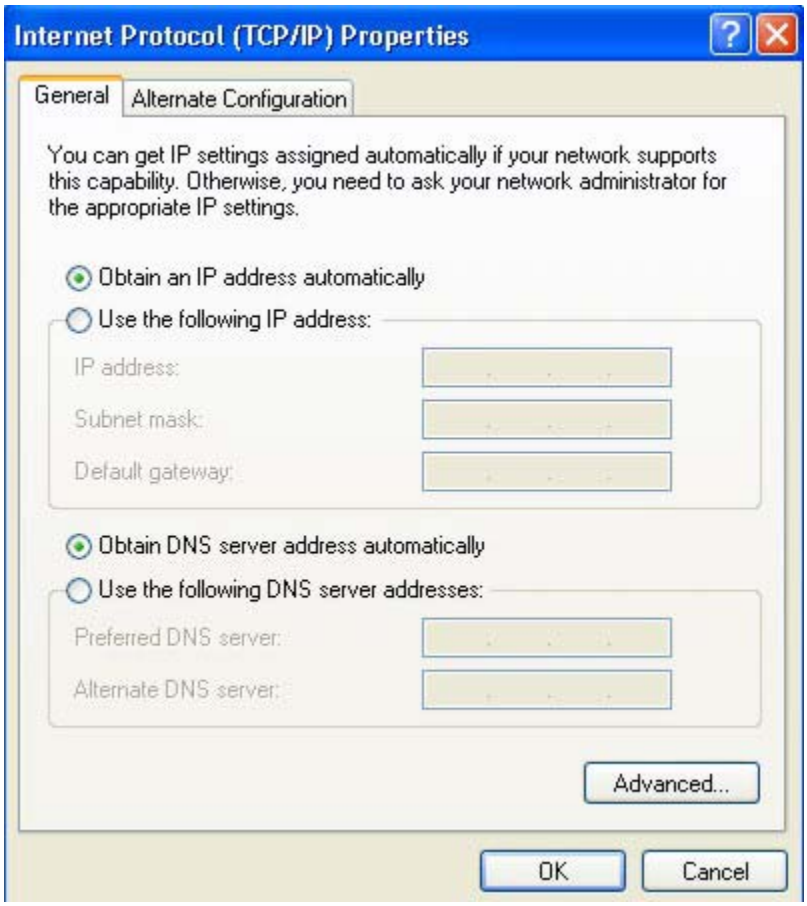
3 Right-click **Local Area Connection** and then select **Properties**.



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**.

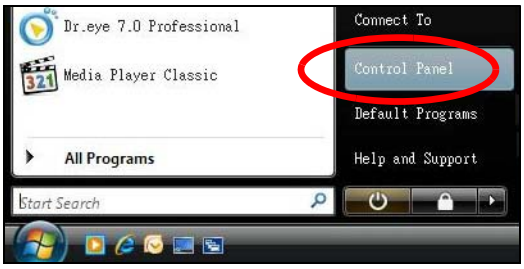
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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.

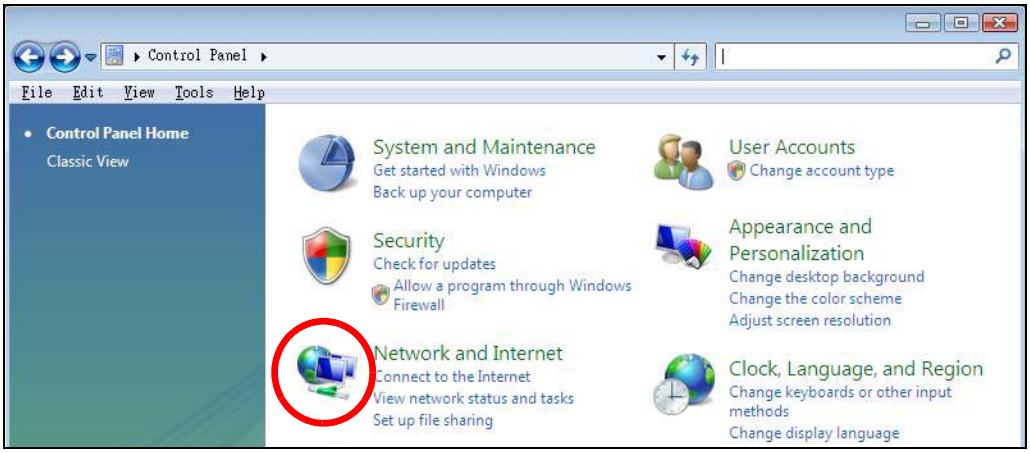
Windows Vista

This section shows screens from Windows Vista Professional.

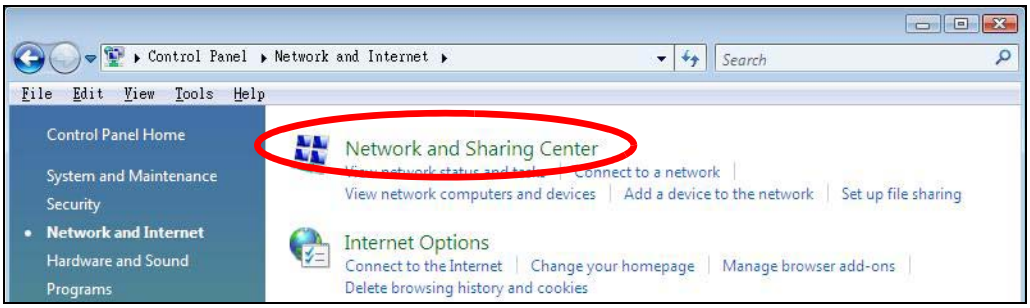
1 Click **Start** > **Control Panel**.



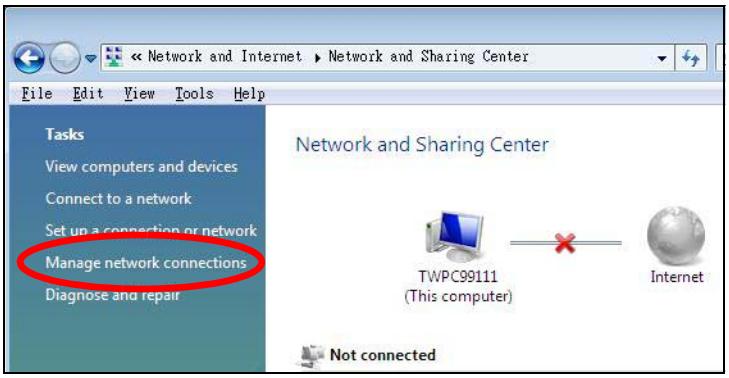
2 In the **Control Panel**, click the **Network and Internet** icon.



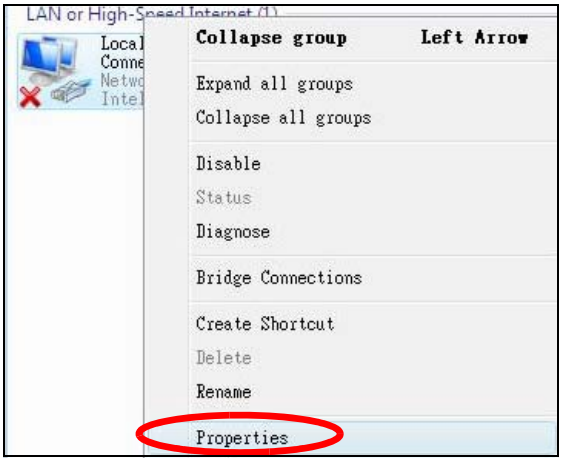
3 Click the **Network and Sharing Center** icon.



4 Click **Manage network connections**.

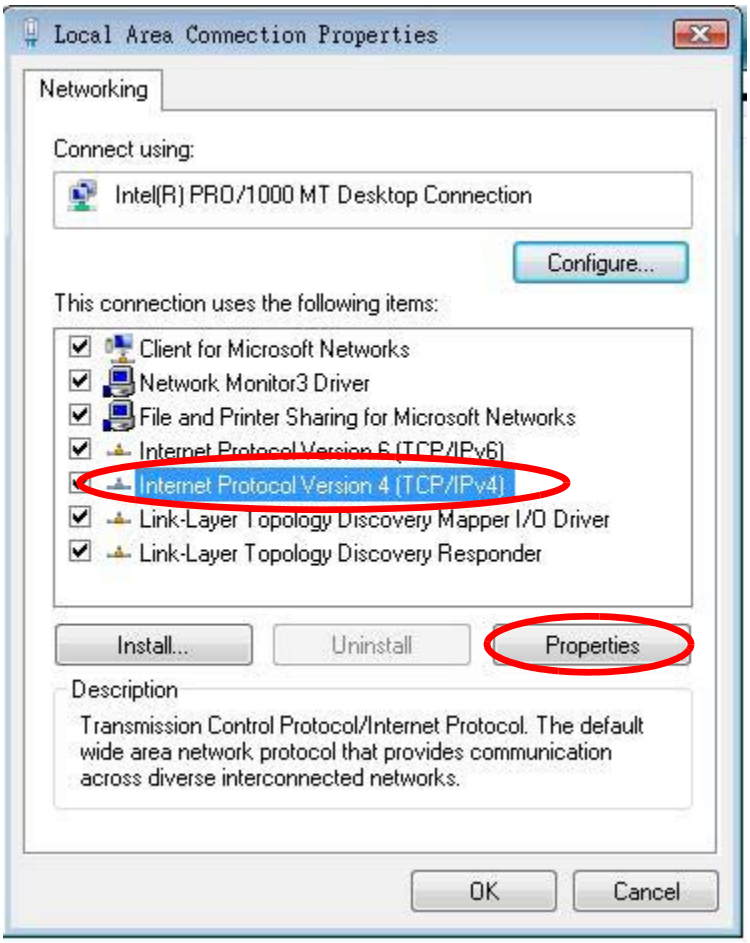


5 Right-click **Local Area Connection** and then select **Properties**.

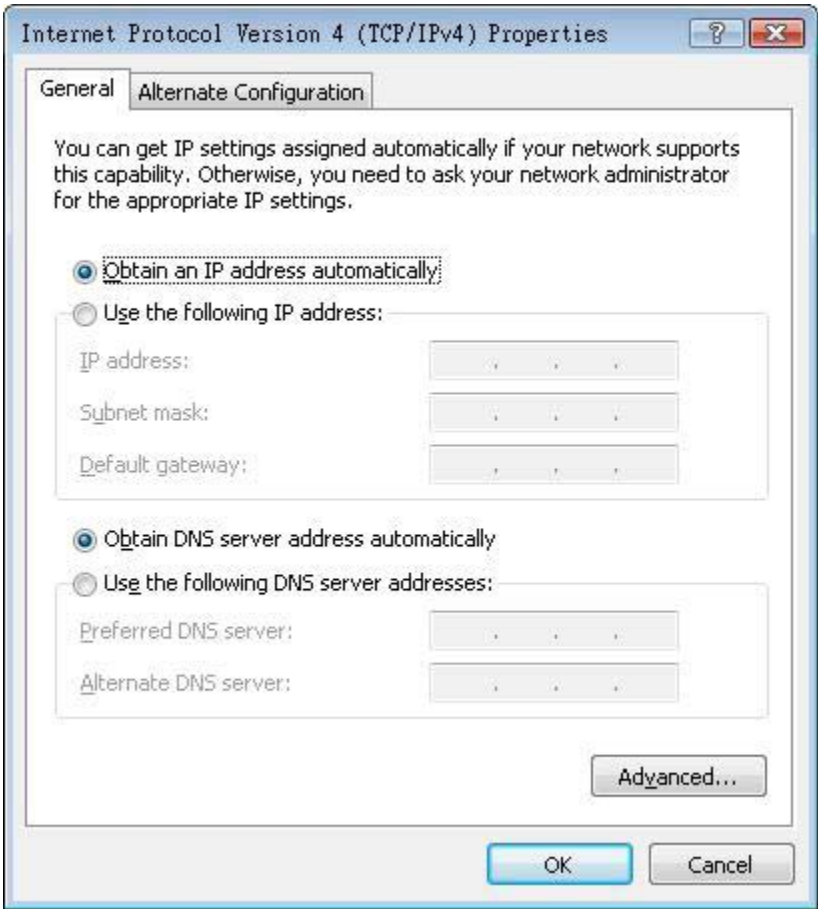


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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**.

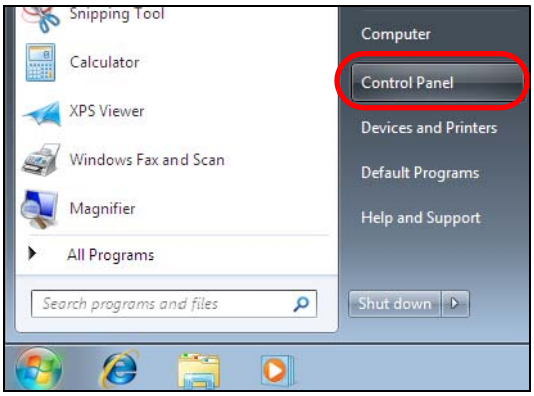
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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.

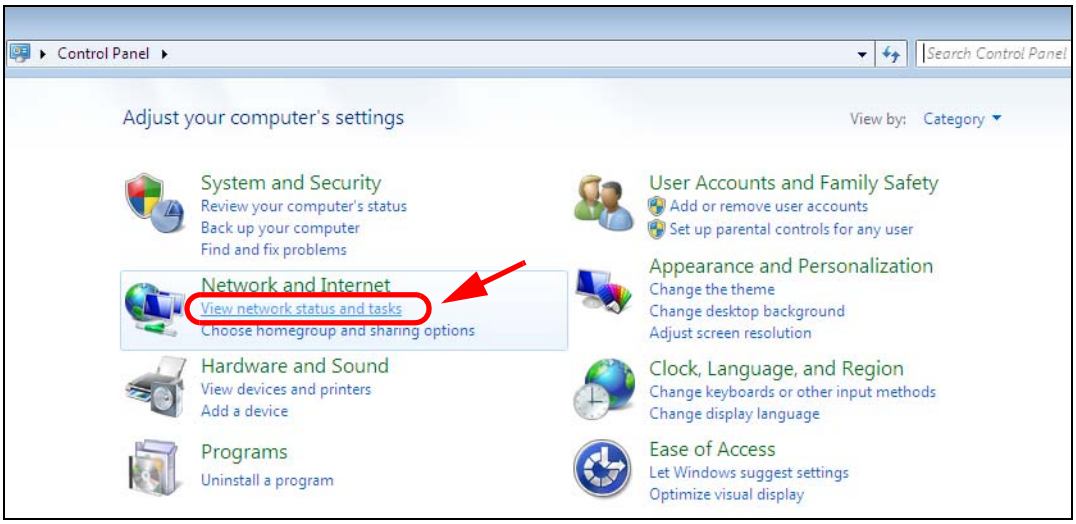
Windows 7

This section shows screens from Windows 7 Enterprise.

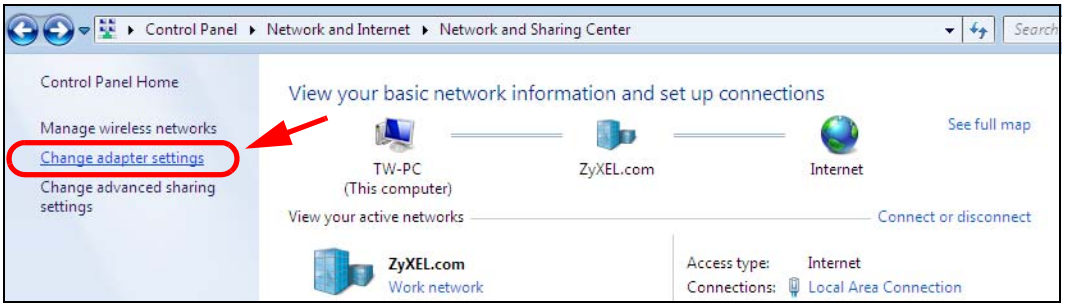
1 Click **Start** > **Control Panel**.



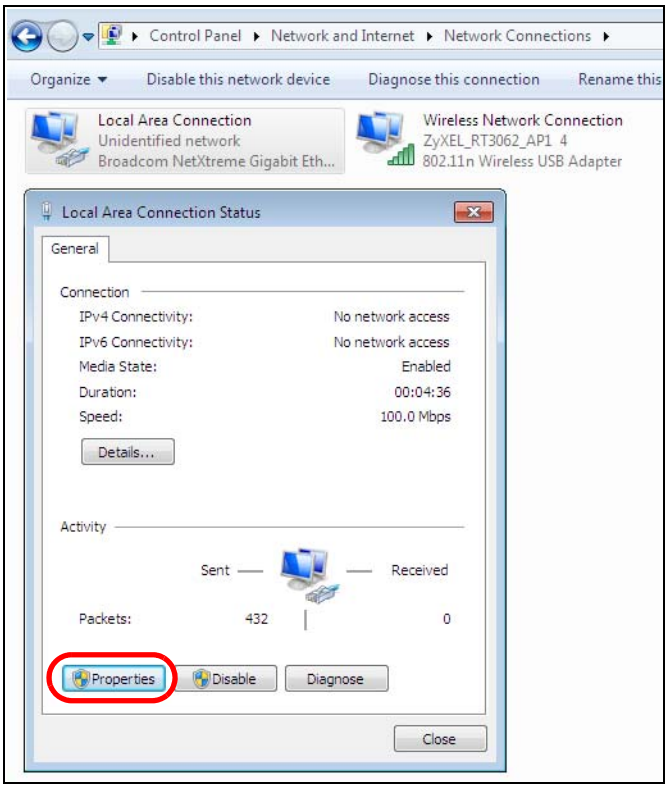
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.



3 Click **Change adapter settings**.

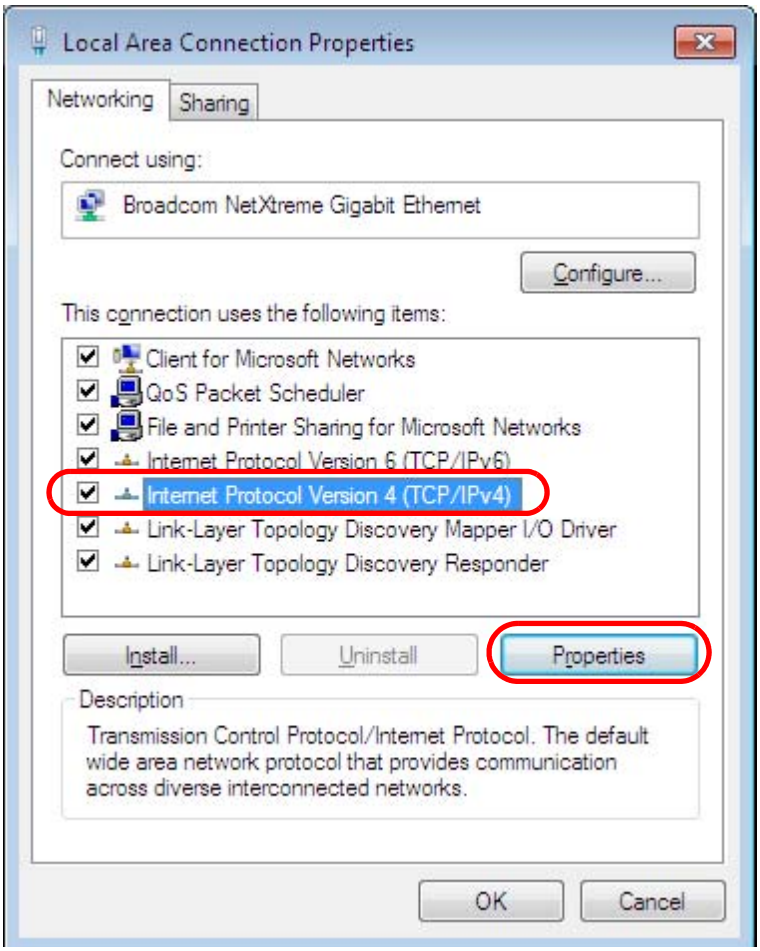


4 Double click **Local Area Connection** and then select **Properties**.

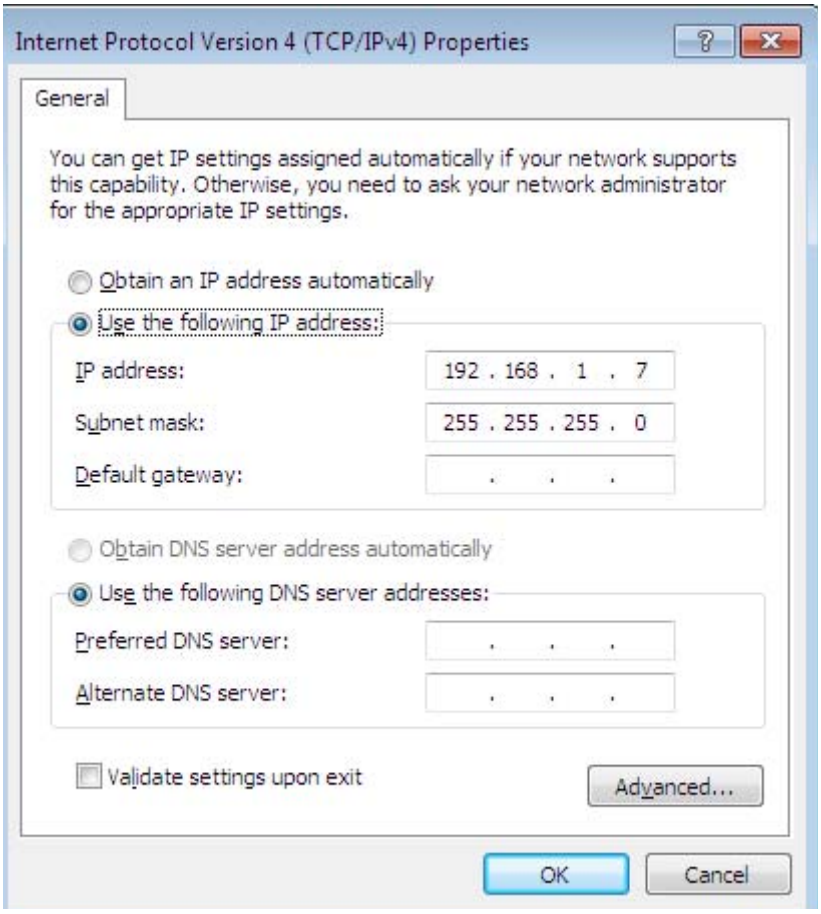


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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.

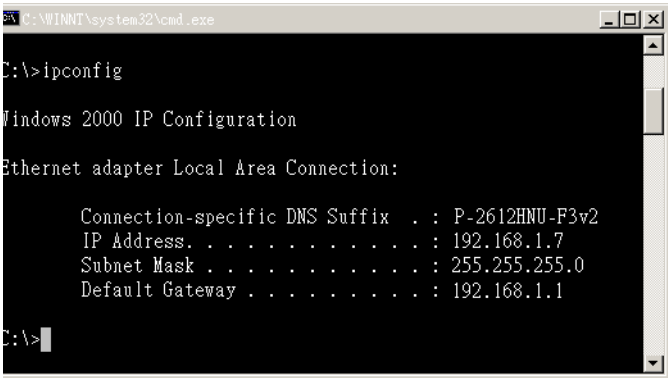
9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

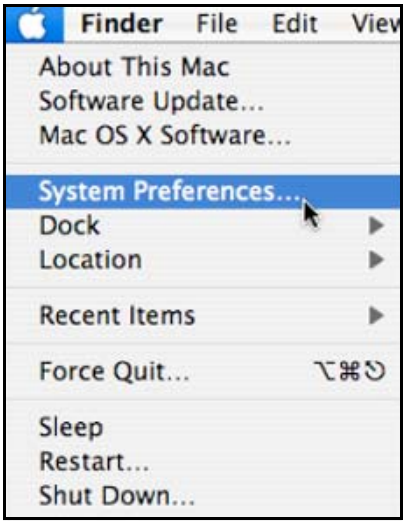
3 The IP settings are displayed as follows.



Mac OS X: 10.3 and 10.4

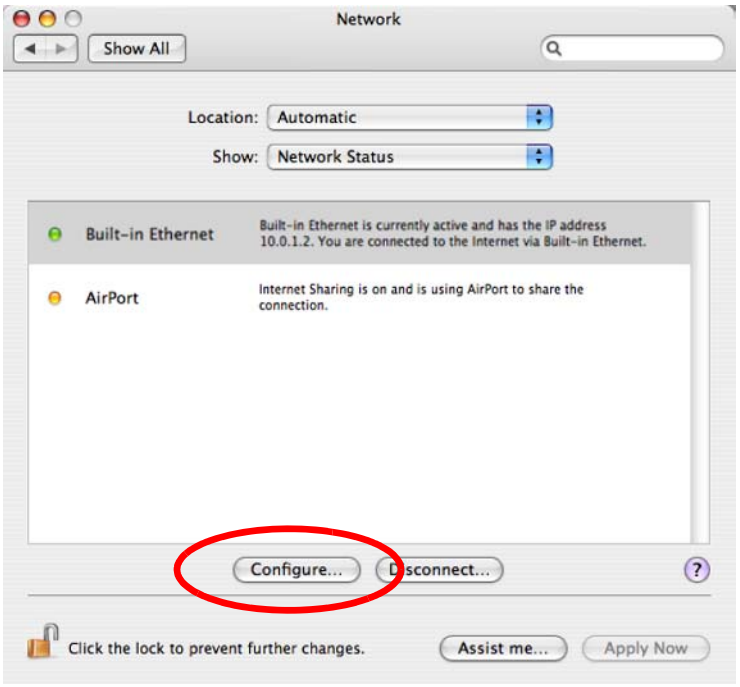
The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

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

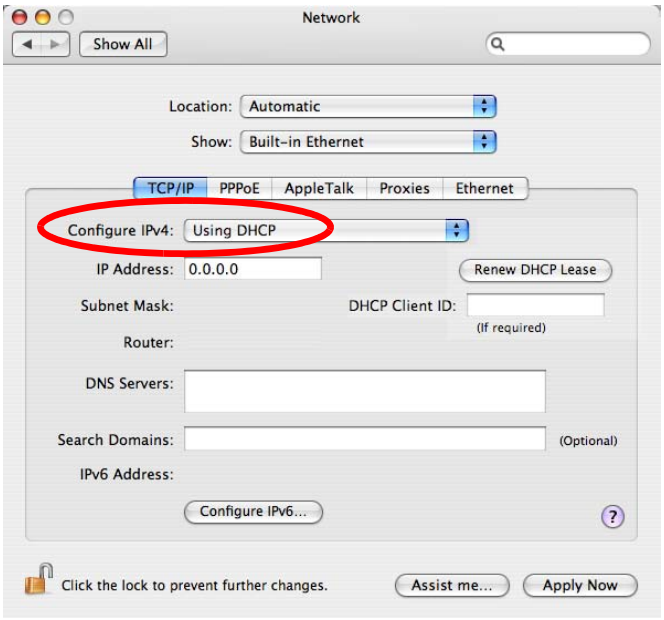


2 In the **System Preferences** window, click the **Network** icon.

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

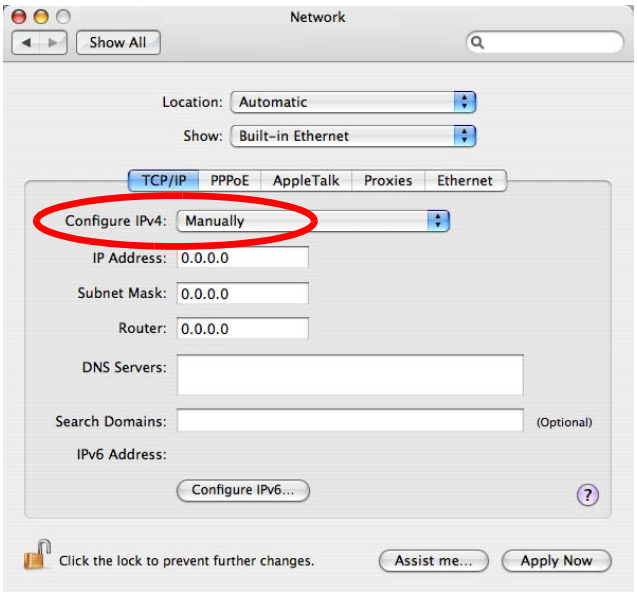


4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.



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.

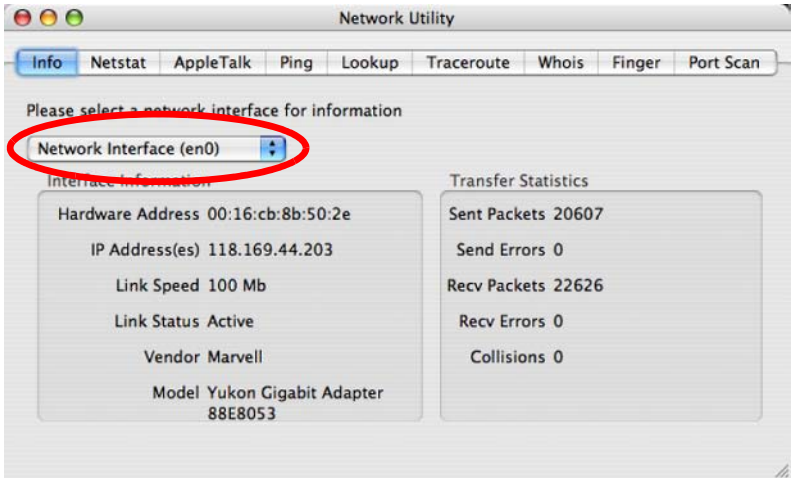


6 Click **Apply Now** and close the window.

Verifying Settings

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

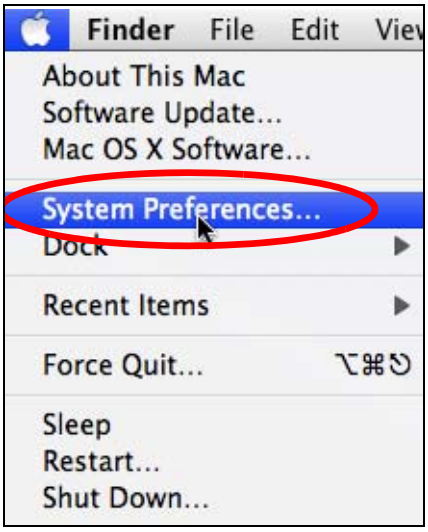
Figure 130 Mac OS X 10.4: Network Utility



Mac OS X: 10.5 and 10.6

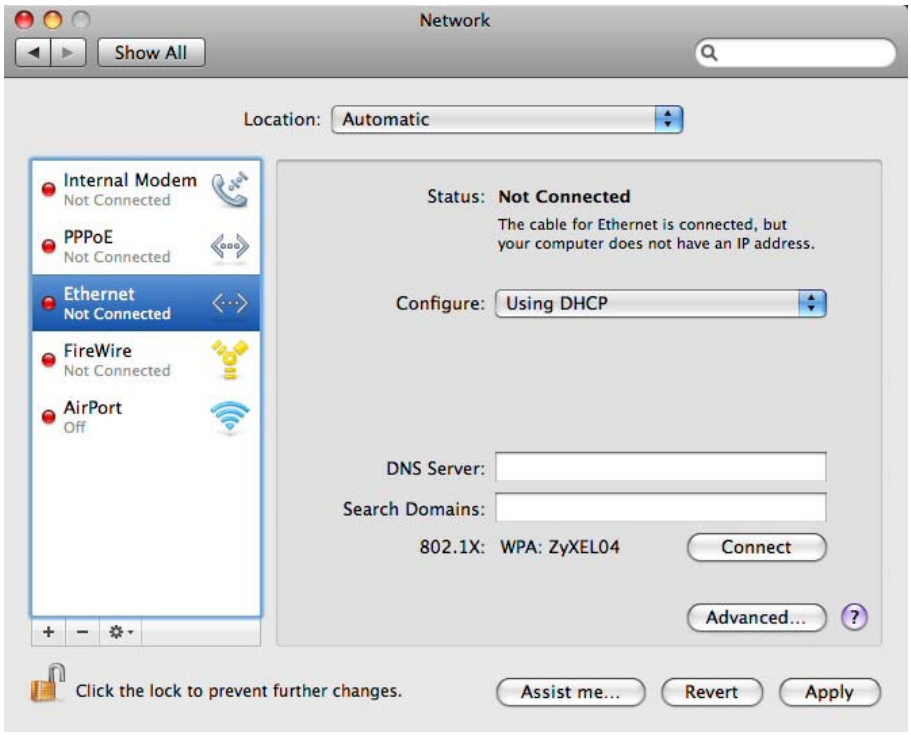
The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

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.

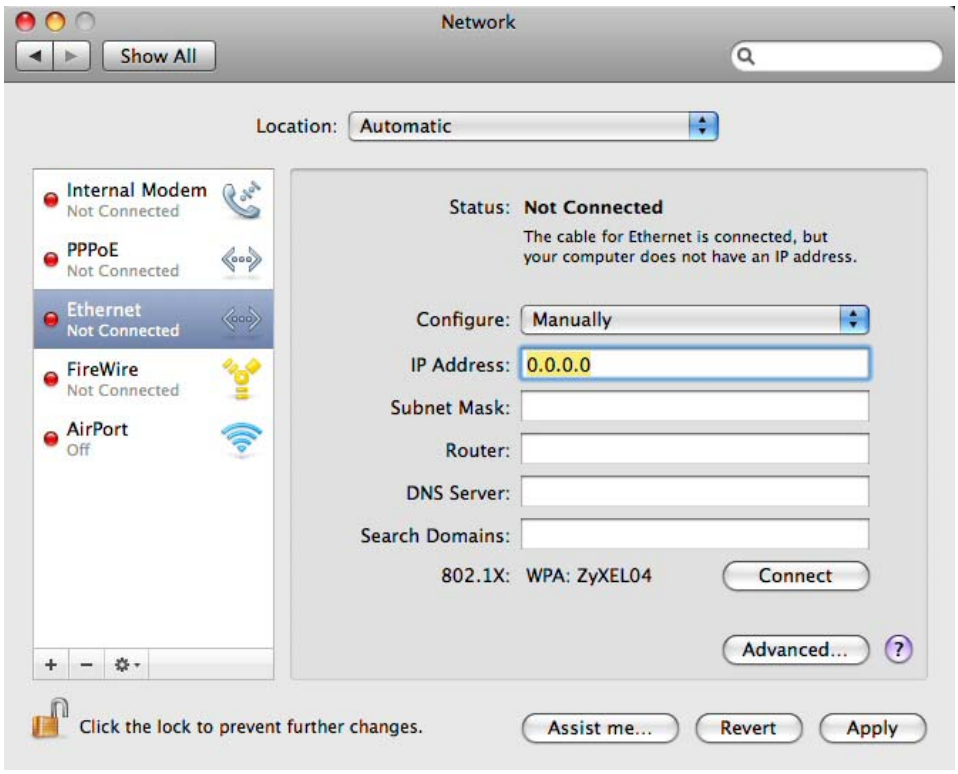


4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

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 v2.

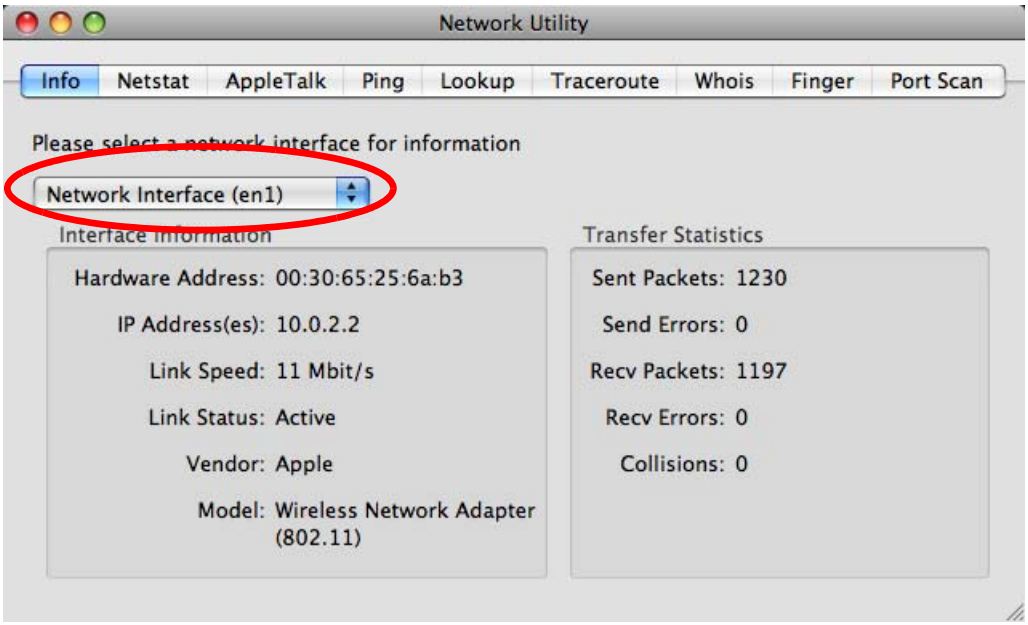


6 Click **Apply** and close the window.

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 131 Mac OS X 10.5: Network Utility



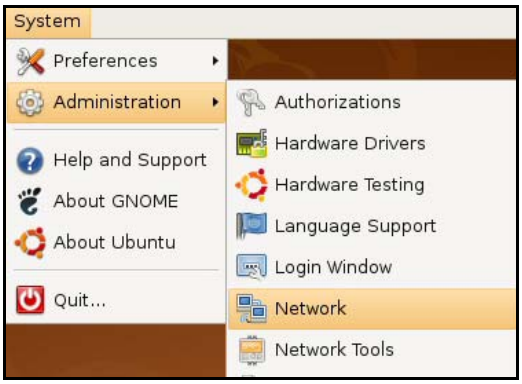
Linux: Ubuntu 8 (GNOME)

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.

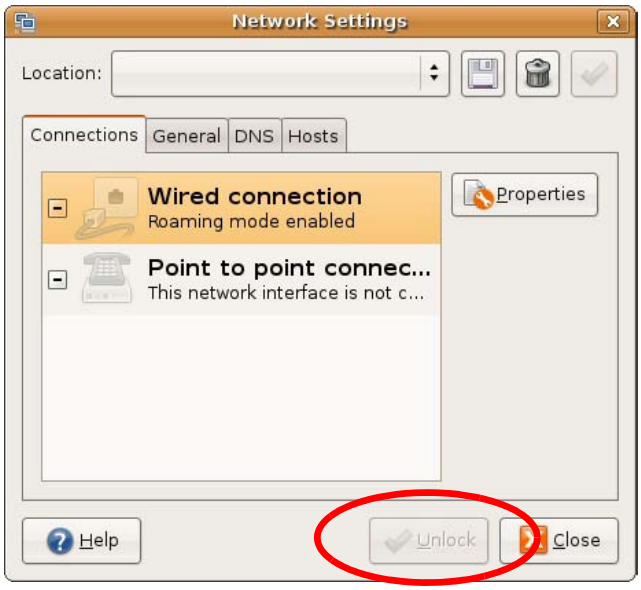
Note: Make sure you are logged in as the root administrator.

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.

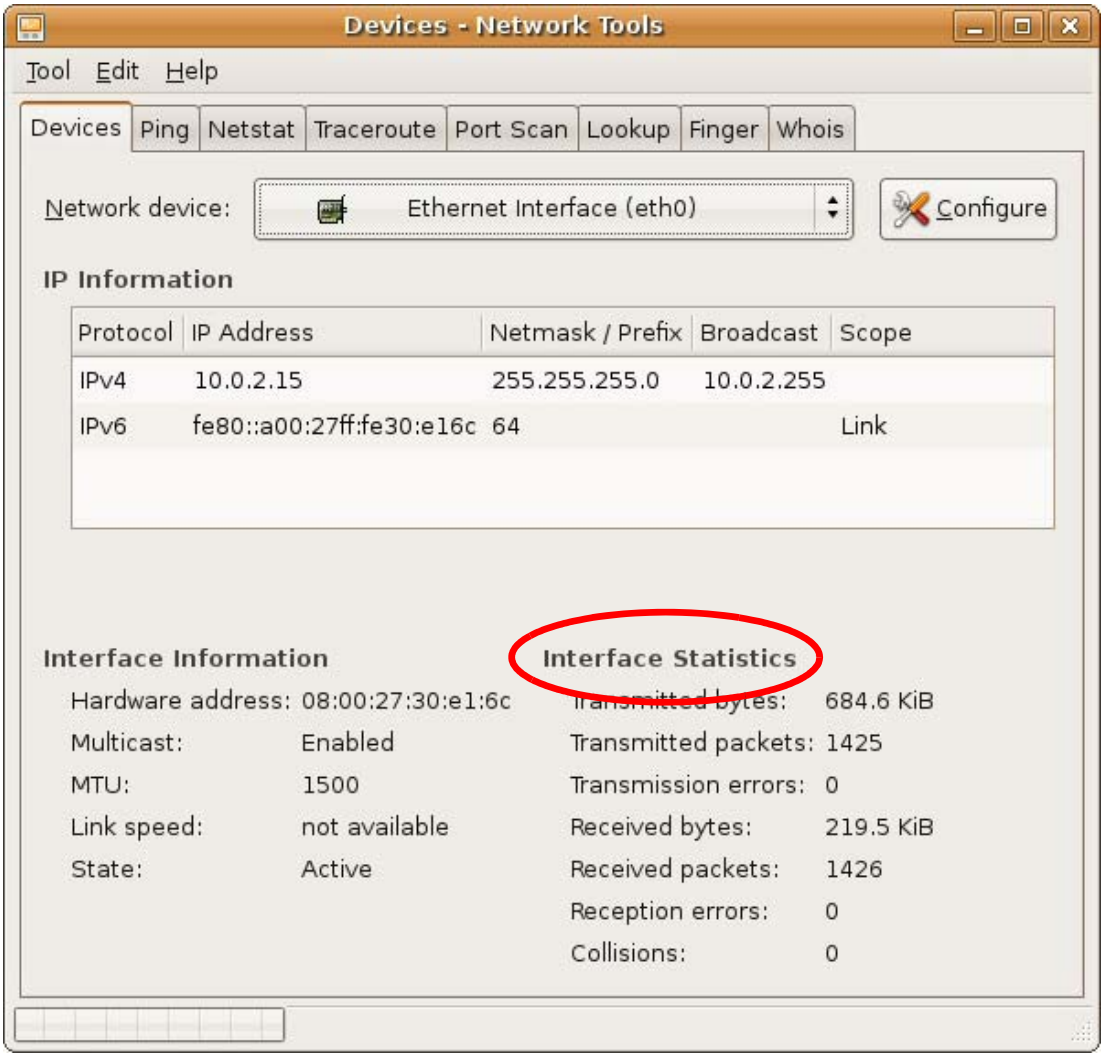
7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

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 132 Ubuntu 8: Network Tools



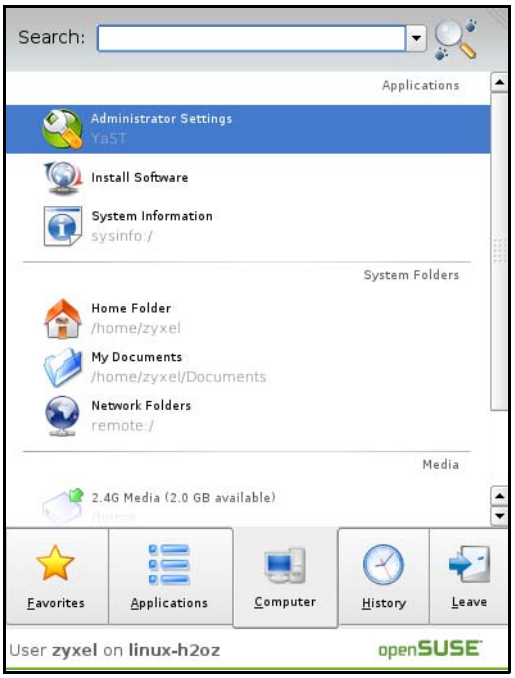
Linux: openSUSE 10.3 (KDE)

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.

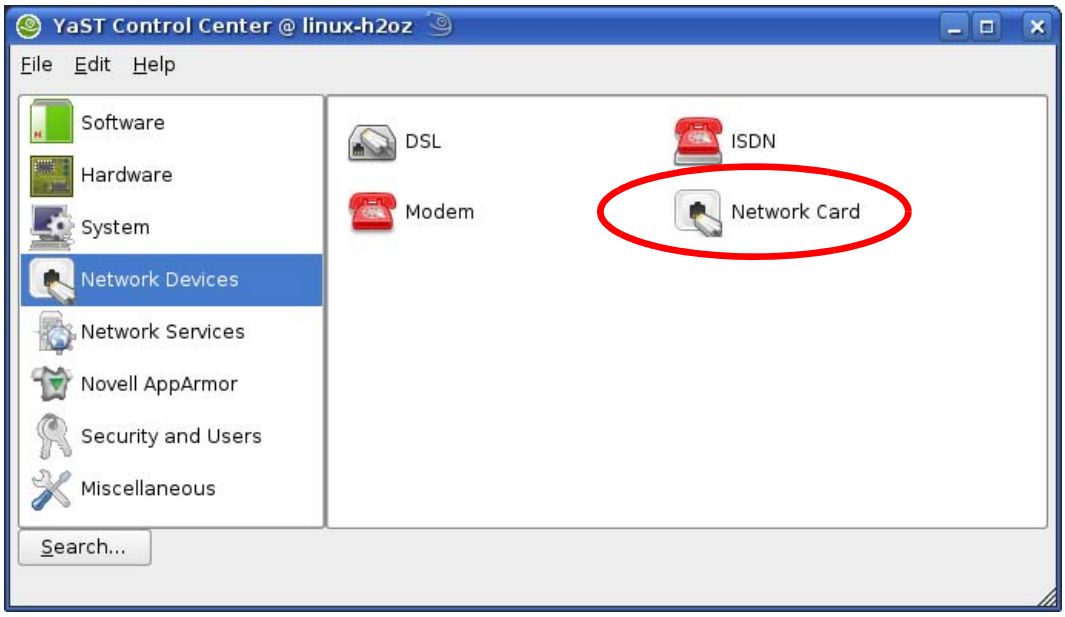
Follow the steps below to configure your computer IP address in the KDE:

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

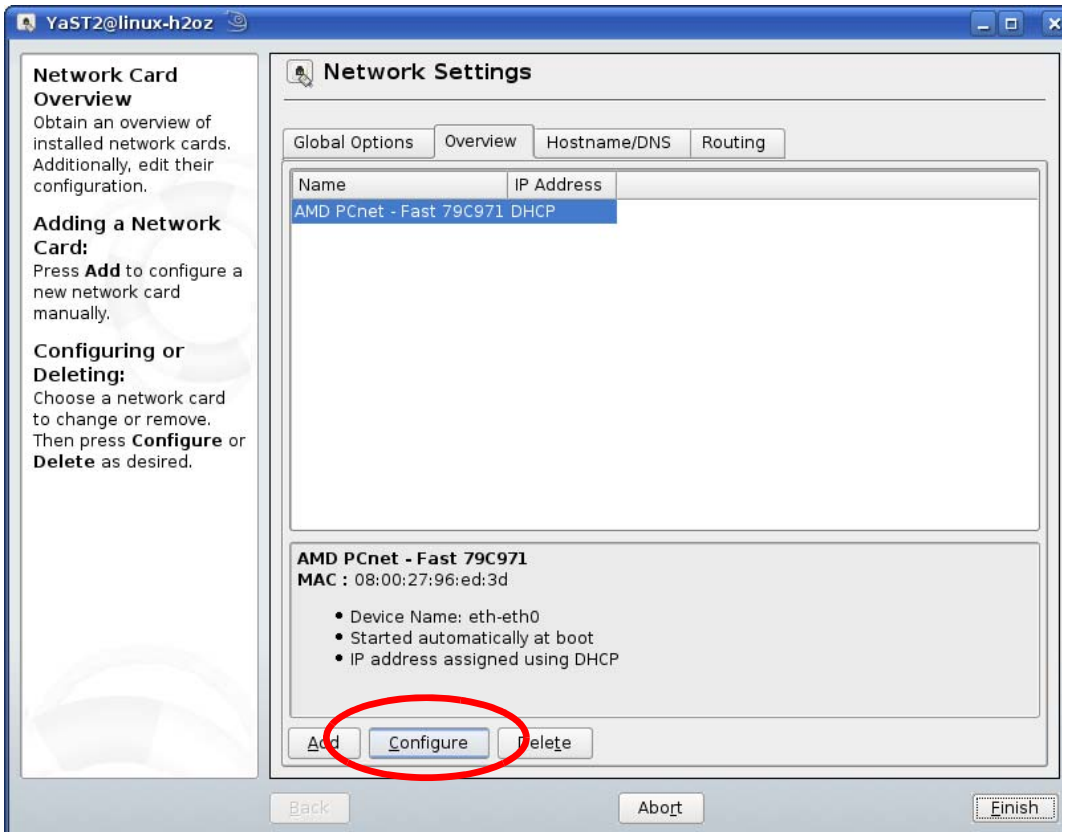


2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

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

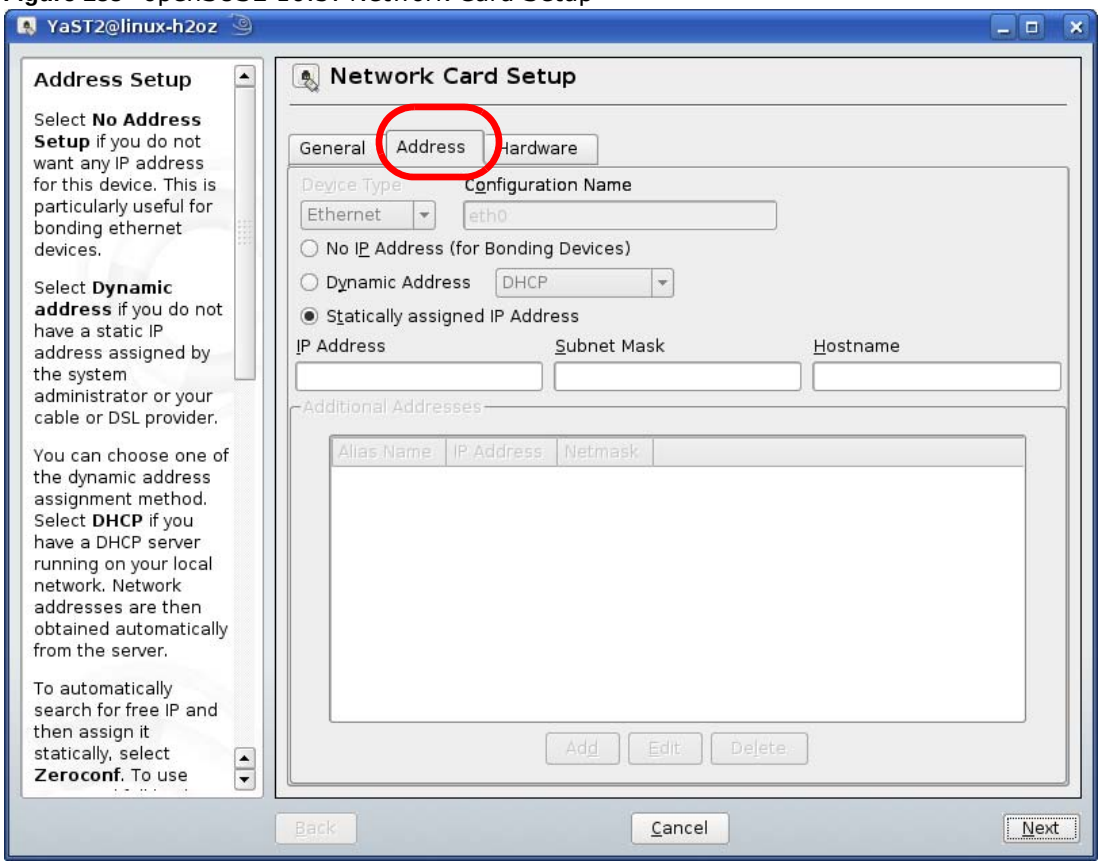


4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



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

Figure 133 openSUSE 10.3: Network Card Setup

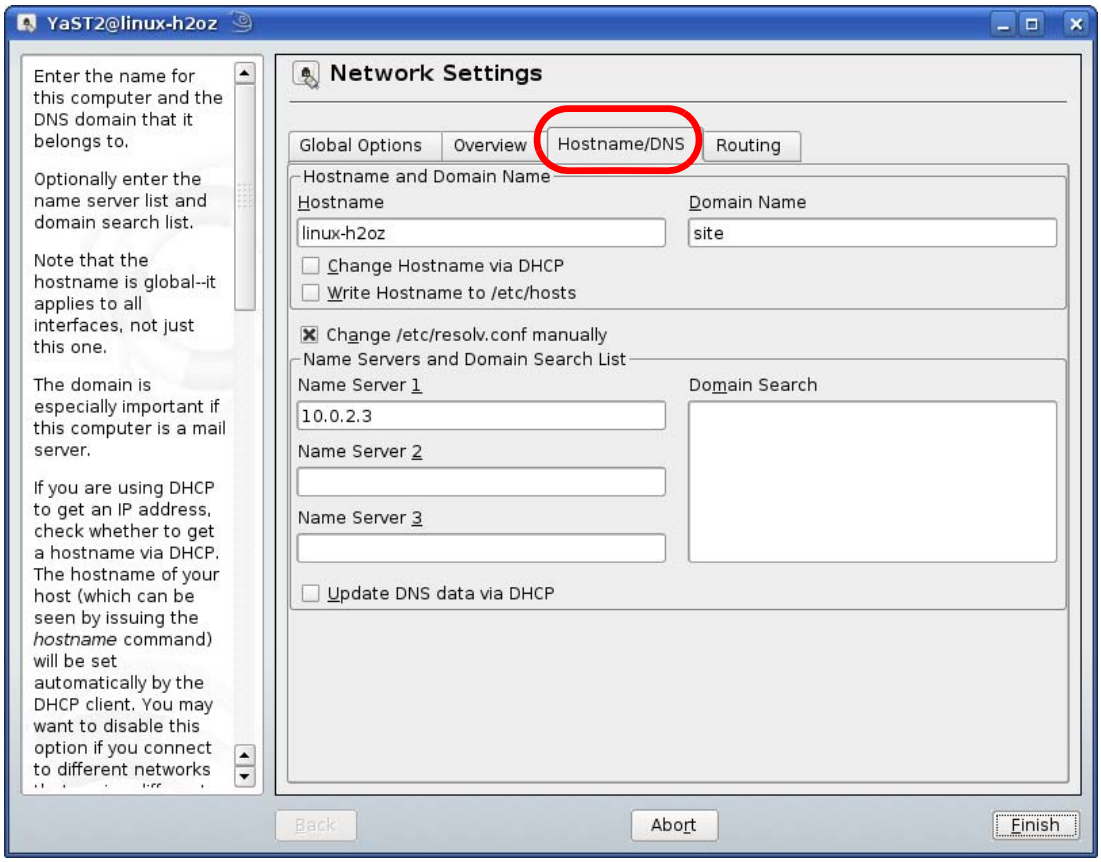


6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

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.

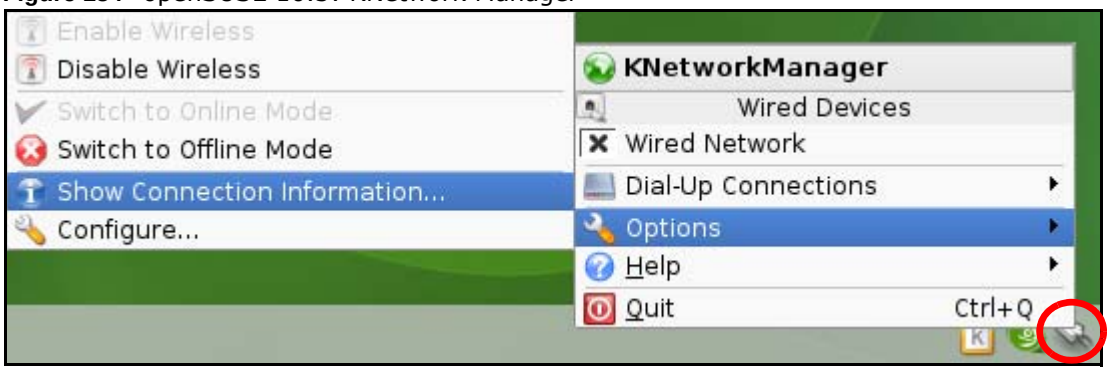


9 Click **Finish** to save your settings and close the window.

Verifying Settings

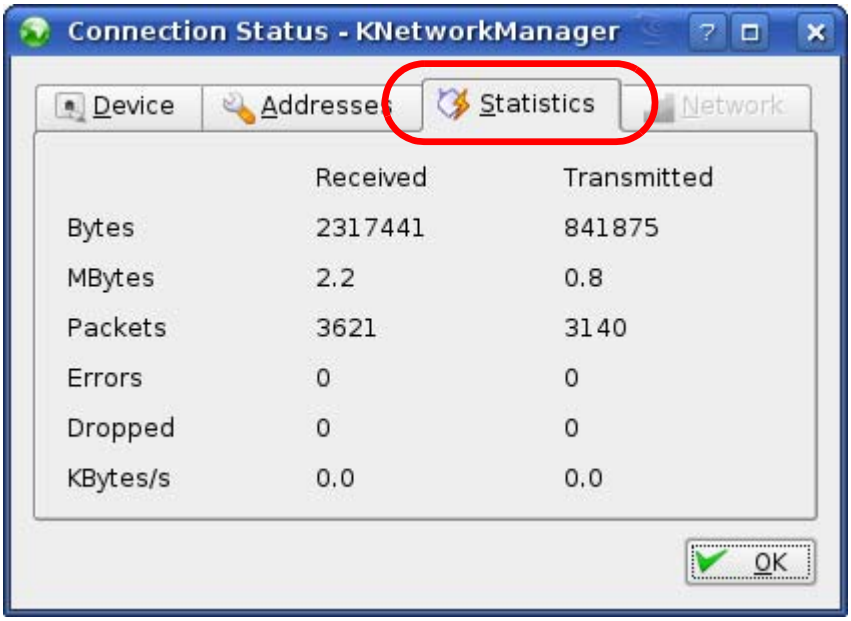
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 134 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 135 openSUSE: Connection Status - KNetwork Manager



D

Wireless LANs

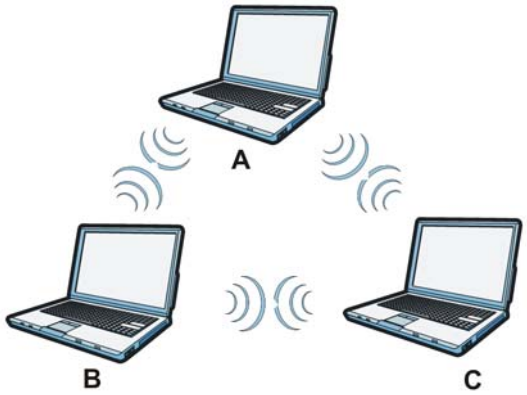
Wireless LAN Topologies

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 136 Peer-to-Peer Communication in an Ad-hoc Network

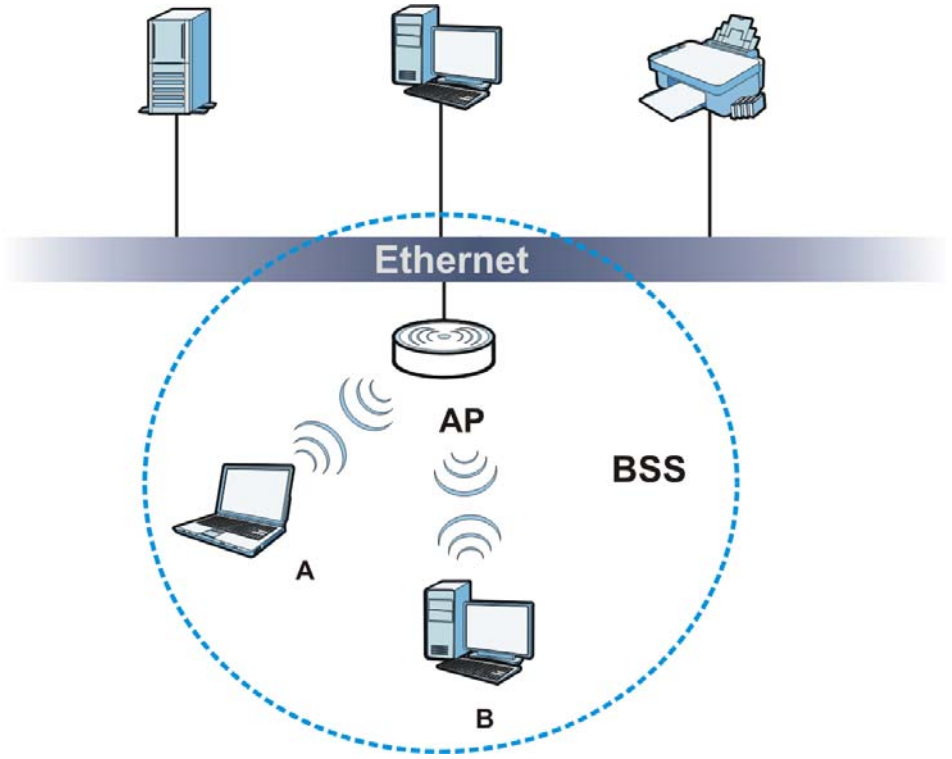


BSS

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 137 Basic Service Set



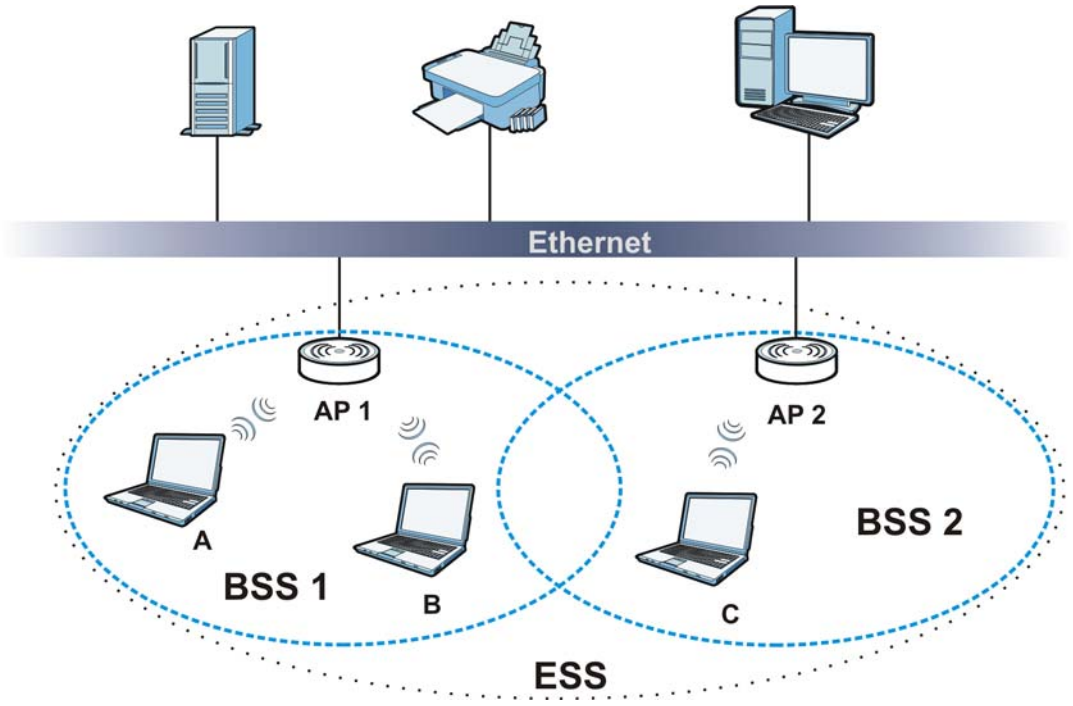
ESS

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 138 Infrastructure WLAN



Channel

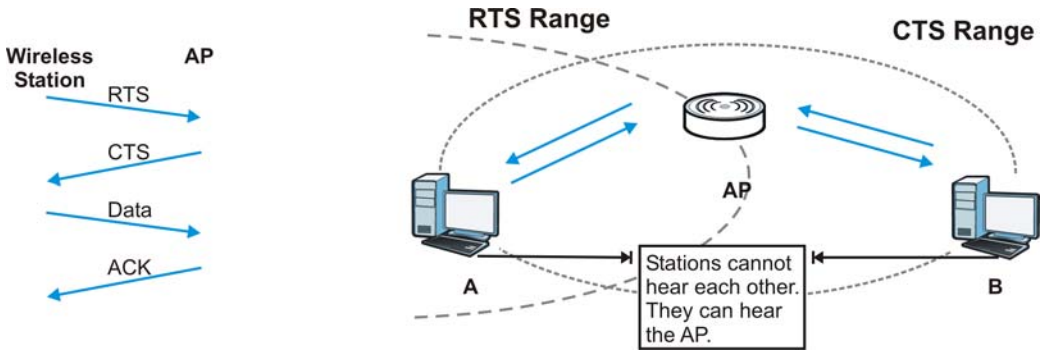
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference 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 139 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 v2 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 v2 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NBG-418N v2 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your NBG-418N v2.

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)
	WPA2
Most Secure	

Note: You must enable the same wireless security settings on the NBG-418N v2 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 re-authentication times out. A new WEP key is generated each time re-authentication 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 prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

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

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

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

Wireless Client WPA Supplicants

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

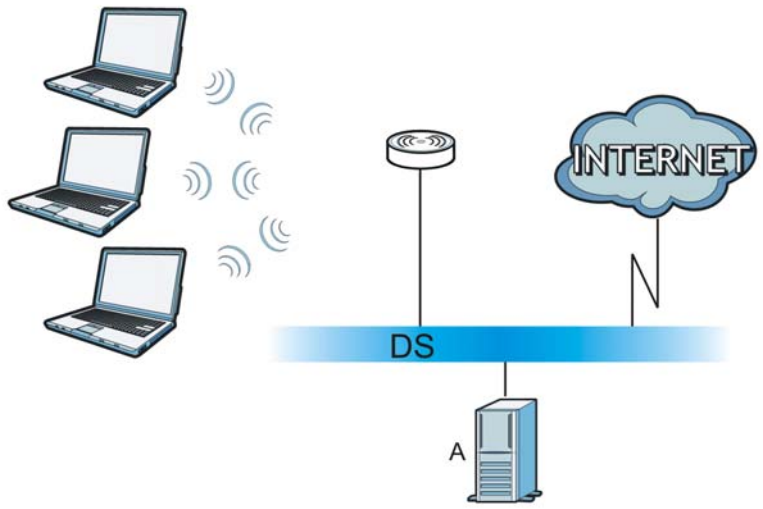
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

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

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

Figure 140 WPA(2) with RADIUS Application Example



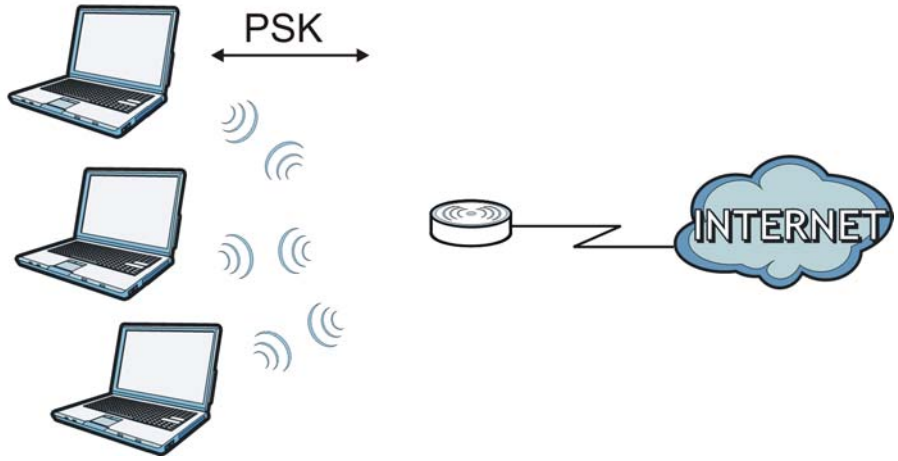
WPA(2)-PSK Application Example

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 141 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
			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.

E

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 video conferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
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 video conferencing solution.

F

Legal Information

Copyright

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

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b, 802.11g or 802.11n (20MHz) operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. IEEE 802.11n (40MHz) operation of this product in the U.S.A. is firmware-limited to channels 3 through 9.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Notices

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

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

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

Cet appareil numérique de la classes B est conforme a la nome NMB-003 du Canada.

Industry Canada Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

1) this device may not cause interference and

2) this device must accept any interference, including interference that may cause undesired operation of the device

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de license. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioéectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

IMPORTANT NOTE:

IC Radiation Exposure Statement

This device meets the exemption from the routine evaluation limits in section 2.5 of RSS 102 and compliance with RSS-102 RF exposure, users can obtain Canada information on RF exposure and compliance.

Le dispositif rencontre l'exemption des limites courantes d'évaluation dans la section 2.5 de RSS 102 et la conformité à l'exposition de RSS-102 rf, utilisateurs peut obtenir l'information candadienne sur l'exposition et la conformité de rf.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

Cet émetteur ne doit pas être Co-placé ou ne fonctionnant en même temps qu'aucune autre antenne ou émetteur. Cet équipement devrait être installé et actionné avec une distance minimum de 20 centimètres entre le radiateur et votre corps.

This radio transmitter with model: NBG-418N v2 has been approved by industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le present emetteur radio with model: NBG418N v2 a ete approuve par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et I'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont stricement interdits pour l'exploitation de l'émetteur.

This device has been designed to operate with an antenna having a maximum gain of 5dBi.

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

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

Antenna List

	Model Name	Antenna Type	Connector	Gain (dBi)
Non-detachable antenna	HWY-24EL5B-106	Dipole	N/A	5
Detachable antenna	HWY-24EL5B-106	Dipole	SMA	5

Viewing Certifications

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

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。
電磁波曝露量 MPE 標準值 1 mW/cm^2，送測產品實測值為 0.860 mW/cm^2

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.

Registration

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

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. To obtain the source code covered under those Licenses, please contact 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 udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[German]	Hiermit erklärt 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 ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕC.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
[Italian]	Ai sensi della Direttiva 2012/19/UE del Parlamento europeo e del Consiglio, del 4 luglio 2012, sui rifiuti di apparecchiature elettrich ed elettroniche (RAEE).
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak.
[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/ЕС.
[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 cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.

CE

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 paesii 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 Außnahme 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)[1] (mW)	Indoor ONLY	Indoor and Outdoor
2400-2483.5	100		V
5150-5350	200	V	
5470-5725	1000		V

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 frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: 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.

G

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional websites are listed below (see also http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml). Please have the following information ready when you contact an office.

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com

Asia

China

- ZyXEL Communications (Shanghai) Corp.
  ZyXEL Communications (Beijing) Corp.
  ZyXEL Communications (Tianjin) Corp.
- http://www.zyxel.cn

India

- ZyXEL Technology India Pvt Ltd
- http://www.zyxel.in

Kazakhstan

- ZyXEL Kazakhstan
- http://www.zyxel.kz

Korea

- ZyXEL Korea Corp.
- http://www.zyxel.kr

Malaysia

- ZyXEL Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- ZyXEL Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- ZyXEL Philippines
- http://www.zyxel.com.ph

Singapore

- ZyXEL Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com

Thailand

- ZyXEL Thailand Co., Ltd
- http://www.zyxel.co.th

Vietnam

- ZyXEL Communications Corporation-Vietnam Office
- http://www.zyxel.com/vn/vi

Europe

Austria

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Belarus

- ZyXEL BY
- http://www.zyxel.by

Belgium

- ZyXEL Communications B.V.
- http://www.zyxel.com/be/nl/

Bulgaria

- ZyXEL България
- http://www.zyxel.com/bg/bg/

Czech

- ZyXEL Communications Czech s.r.o
- http://www.zyxel.cz

Denmark

- ZyXEL Communications A/S
- http://www.zyxel.dk

Estonia

- ZyXEL Estonia
- http://www.zyxel.com/ee/et/

Finland

- ZyXEL Communications
- http://www.zyxel.fi

France

- ZyXEL France
- http://www.zyxel.fr

Germany

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Hungary

- ZyXEL Hungary & SEE
- http://www.zyxel.hu

Latvia

- ZyXEL Latvia
- http://www.zyxel.com/lv/lv/homepage.shtml

Lithuania

- ZyXEL Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

Netherlands

- ZyXEL Benelux
- http://www.zyxel.nl

Norway

- ZyXEL Communications
- http://www.zyxel.no

Poland

- ZyXEL Communications Poland
- http://www.zyxel.pl

Romania

- ZyXEL Romania
- http://www.zyxel.com/ro/ro

Russia

- ZyXEL Russia
- http://www.zyxel.ru

Slovakia

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

Spain

- ZyXEL Spain
- http://www.zyxel.es

Sweden

- ZyXEL Communications
- http://www.zyxel.se

Switzerland

- Studerus AG
- http://www.zyxel.ch/

Turkey

- ZyXEL Turkey A.S.
- http://www.zyxel.com.tr

UK

- ZyXEL Communications UK Ltd.
- http://www.zyxel.co.uk

Ukraine

- ZyXEL Ukraine
- http://www.ua.zyxel.com

Latin America

Argentina

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Ecuador

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Middle East

Egypt

- ZyXEL Communication Corporation
- http://www.zyxel.com/homepage.shtml

Middle East

- ZyXEL Communication Corporation
- http://www.zyxel.com/homepage.shtml

North America

USA

- ZyXEL Communications, Inc. - North America Headquarters
- http://www.us.zyxel.com/

Oceania

Australia

- ZyXEL Communications Corporation
- http://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

W