

User's Guide

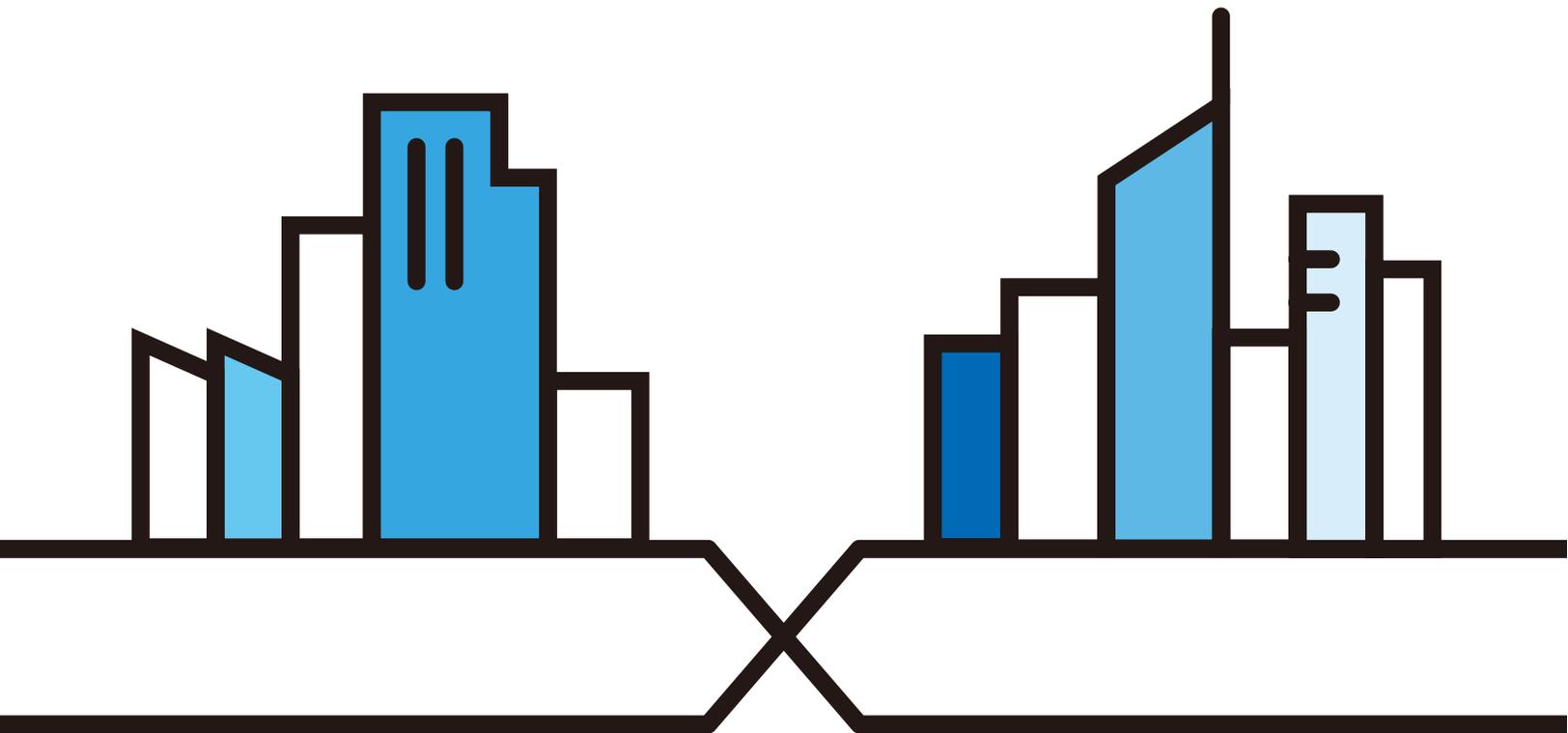
NBG6615

AC1200 MU-MIMO Dual-Band Wireless Gigabit Router

Default Login Details

Login URL	http://192.168.212.1
User Name	admin
Password	1234

Version 1.0 Edition 1, 07/2018



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from what you see due to differences in release versions 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 managed device.
- More Information
Go to support.zyxel.com to find other information on the NBG6615.



Contents Overview

User's Guide	10
Introduction	11
The Web Configurator	16
Connection Wizard	20
Modes	28
Tutorials	39
Technical Reference	53
Wireless LAN	54
WAN	68
LAN	78
DHCP Server	82
Network Address Translation	86
Dynamic DNS	95
Static Route	97
Firewall	100
Content Filter	104
Remote Management	107
Universal Plug-and-Play (UPnP)	110
Bandwidth MGMT	118
System	121
Logs	124
Tools	126
Sys OP Mode	131
Language	133
Troubleshooting	135

Table of Contents

Contents Overview	3
Table of Contents	4
Part I: User's Guide.....	10
Chapter 1	
Introduction	11
1.1 Overview	11
1.2 Securing the NBG6615	12
1.3 LEDs	13
1.4 The WPS Button	13
1.4.1 Using the WPS Button	14
1.5 Reboot/Reset Button	14
1.6 Wall Mounting	14
Chapter 2	
The Web Configurator.....	16
2.1 Overview	16
2.2 Accessing the Web Configurator	16
2.3 Resetting the NBG6615	18
Chapter 3	
Connection Wizard	20
3.1 Wizard Setup	20
Chapter 4	
Modes	28
4.1 Overview	28
4.2 Setting your NBG6615 to Router Mode	29
4.2.1 Status Screen (Router Mode)	29
4.2.2 Router Mode Navigation Panel	33
4.3 Setting your NBG6615 to AP Mode	34
4.3.1 Status Screen (AP Mode)	35
4.3.2 AP Navigation Panel	37
Chapter 5	
Tutorials	39

5.1 Overview 39

5.2 How to Connect to the Internet from an AP 39

5.3 Configure Wireless Security Using WPS on both your NBG6615 and Wireless Client 39

 5.3.1 Push Button Configuration 40

 5.3.2 PIN Configuration 41

5.4 Enable and Configure Wireless Security without WPS on your NBG6615 43

 5.4.1 Configure Your Wireless Client 44

5.5 Using Multiple SSIDs on the NBG6615 46

 5.5.1 Configuring Security Settings of Multiple SSIDs 47

5.6 Installing UPnP in Windows 7 Example 50

5.7 Using Bandwidth Management on the NBG6615 50

Part II: Technical Reference 53

**Chapter 6
Wireless LAN 54**

6.1 Overview 54

6.2 What You Can Do 55

6.3 What You Should Know 55

 6.3.1 Wireless Security Overview 56

 6.3.2 MBSSID 56

 6.3.3 MAC Address Filter 56

 6.3.4 Encryption 57

 6.3.5 WPS 57

6.4 General Wireless LAN Screen 57

 6.4.1 No Security 59

 6.4.2 WPA2-PSK or WPA-PSK/WPA2-PSK 59

6.5 MAC Filter 60

6.6 Wireless LAN Advanced Screen 61

6.7 WPS Screen 62

6.8 WPS Station Screen 64

6.9 Scheduling Screen 64

6.10 MBSSID Screen 65

**Chapter 7
WAN 68**

7.1 Overview 68

7.2 What You Need To Know 68

 7.2.1 Configuring Your Internet Connection 68

7.3 Internet Connection Screen 69

 7.3.1 Static IP 69

7.3.2 DHCP Client	71
7.3.3 PPPoE Connection	72
7.3.4 PPTP Connection	74
7.4 Advanced Screen	76
Chapter 8	
LAN	78
8.1 Overview	78
8.2 What You Need To Know	78
8.2.1 IP Address and Subnet Mask	79
8.2.2 DNS Server Address Assignment	79
8.2.3 IP Pool Setup	80
8.2.4 LAN TCP/IP	80
8.3 LAN IP Screen	80
Chapter 9	
DHCP Server.....	82
9.1 Overview	82
9.2 What You Can Do	82
9.3 What You Need To Know	82
9.4 General Screen	82
9.5 Static DHCP Screen	83
9.6 Client List Screen	84
Chapter 10	
Network Address Translation	86
10.1 Overview	86
10.2 What You Can Do	86
10.2.1 What You Need To Know	87
10.3 General NAT Screen	88
10.4 NAT Application Screen	89
10.5 Port Triggering Screen	91
10.6 Technical Reference	92
10.6.1 NAT Port Forwarding: Services and Port Numbers	93
10.6.2 NAT Port Forwarding Example	93
10.6.3 Trigger Port Forwarding	93
10.6.4 Trigger Port Forwarding Example	94
10.6.5 Two Points To Remember About Trigger Ports	94
Chapter 11	
Dynamic DNS	95
11.1 Overview	95
11.2 Dynamic DNS Screen	95

Chapter 12	
Static Route	97
12.1 Overview	97
12.2 IP Static Route Screen	97
Chapter 13	
Firewall	100
13.1 Overview	100
13.2 What You Can Do	100
13.3 What You Need To Know	101
13.3.1 About the NBG6615 Firewall	101
13.3.2 VPN Pass Through Features	101
13.4 General Firewall Screen	101
13.5 Services Screen	102
13.6 MAC Filter Screen	103
Content Filter	104
13.7 Overview	104
13.8 What You Can Do	104
13.9 Filter Screen	105
Chapter 14	
Remote Management	107
14.1 Overview	107
14.1.1 Remote Management Limitations	108
14.1.2 Remote Management and NAT	108
14.1.3 System Timeout	108
14.2 WWW Screen	108
Chapter 15	
Universal Plug-and-Play (UPnP)	110
15.1 Overview	110
15.2 What You Need to Know	110
15.3 Configuring UPnP	111
15.4 Installing UPnP in Windows 7 Example	111
15.4.1 Using UPnP in Windows XP Example	113
15.4.2 Web Configurator Easy Access	115
Chapter 16	
Bandwidth MGMT	118
16.1 Overview	118
16.2 What You Can Do	118
16.3 What You Need To Know	118

16.4 Bandwidth MGMT Screen	118
16.5 Advanced Screen	119
Chapter 17	
System.....	121
17.1 Overview	121
17.2 What You Can Do	121
17.3 System General Screen	121
17.4 Time Setting Screen	122
Chapter 18	
Logs.....	124
18.1 Overview	124
18.2 What You Need to Know	124
18.3 View Log Screen	124
Chapter 19	
Tools.....	126
19.1 Overview	126
19.2 What You Can Do	126
19.3 Firmware Upload Screen	126
19.4 Configuration Screen	128
19.4.1 Backup Configuration	128
19.4.2 Restore Configuration	128
19.4.3 Back to Factory Defaults	129
19.5 Restart Screen	129
Chapter 20	
Sys OP Mode.....	131
20.1 Overview	131
20.2 General Screen	131
Chapter 21	
Language.....	133
21.1 Language Screen	133
Chapter 22	
Troubleshooting.....	135
22.1 Power, Hardware Connections, and LEDs	135
22.2 NBG6615 Access and Login	136
22.3 Internet Access	137
22.4 Resetting the NBG6615 to Its Factory Defaults	138
22.5 Wireless Problems	139

Appendix A IP Addresses and Subnetting..... 140

Appendix B Pop-up Windows, JavaScripts and Java Permissions 149

Appendix C Setting Up Your Computer's IP Address..... 158

Appendix D Wireless LANs 185

Appendix E Common Services 198

Appendix F Legal Information 201

Appendix G Customer Support 208

Index214

PART I

User's Guide

CHAPTER 1

Introduction

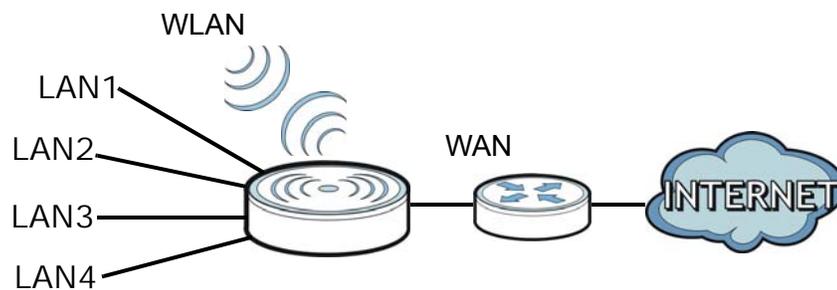
1.1 Overview

The NBG6615 extends the range of your existing wired network without additional wiring, providing easy network access to mobile users.

You can create the following connections using the NBG6615:

- **LAN.** You can connect network devices via the Ethernet ports of the NBG6615 so that they can communicate with each other and access the Internet.
- **WLAN.** Wireless clients can connect to the NBG6615 to access network resources.
- **WAN.** Connect to a broadband modem/router for Internet access.

Figure 1 NBG6615 Network



You can set up the NBG6615 with other IEEE 802.11b/g/n compatible devices in one of the following device modes:

- Router
- Access Point

Use a (supported) web browser to manage the NBG6615. Menus vary according to which mode you're using.

Router Mode



AP Mode



See [Chapter 4 on page 28](#) for more information on these modes.

1.2 Securing the NBG6615

Do the following things regularly to make the NBG6615 more secure and to manage the NBG6615 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 NBG6615 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG6615. 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 	White	On	The NBG6615 is receiving power and functioning properly.
		Off	The NBG6615 is not receiving power.
		Blinking	The NBG6615 is upgrading its firmware, restoring its configurations, or rebooting its system.
Internet 	White	On	An IP connection is available but there is no traffic.
		Blinking	The NBG6615 is sending/receiving data through the WAN.
		Off	An IP connection is not available.
WLAN_2.4G 	White	On	The NBG6615 is ready but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG6615 is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
	Amber	Blinking	The NBG6615 is negotiating a WPS connection with a wireless client via 2.4G.
		Off	The WPS process is inactive.
		Solid for 5 seconds	Successful WPS connection.
WLAN_5G 	White	On	The NBG6615 is ready but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG6615 is sending/receiving data through the wireless LAN.
		Off	The WPS status is not configured or disabled.
	Amber	Blinking	The NBG6615 is negotiating a WPS connection with a wireless client via 5G.
		Off	The WPS process is inactive.
		Solid for 5 seconds	Successful WPS connection.
WPS Button			Press to initiate the WPS process.

1.4 The WPS Button

Your NBG6615 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 Wi-Fi 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** button is located at the front panel of the NBG6615.

1.4.1 Using the WPS Button

- 1 Make sure the power LED is on.
- 2 Press the **WPS** button within 3 seconds to turn on the WPS function

For more information on using **WPS**, see [Section 5.3 on page 39](#).

1.5 Reboot/Reset Button

Your NBG6615 has a recessed reboot/reset button on its back panel. To reboot, press the button with a paperclip or similar object for 3 to 5 seconds. To reset the NBG6615 to factory defaults, press for longer than 10 seconds.

1.6 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.

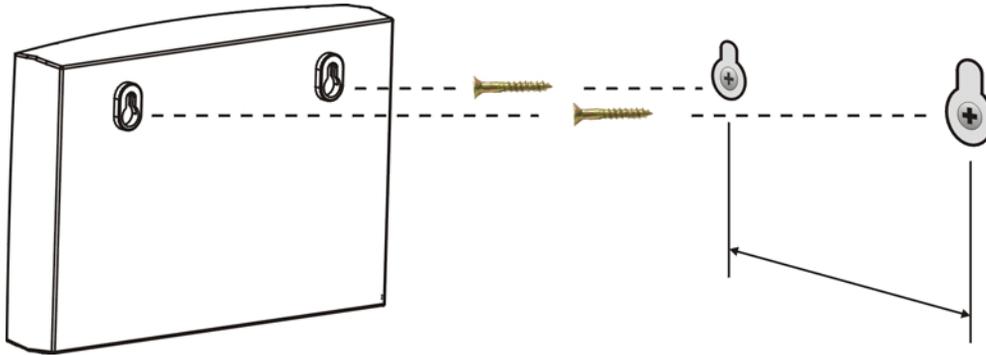
Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

- 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 NBG6615 with the connection cables.
- 5 Align the holes on the back of the NBG6615 with the screws on the wall. Hang the NBG6615 on the screws.

Figure 3 Wall Mounting Example



CHAPTER 2

The Web Configurator

2.1 Overview

This chapter describes how to access the NBG6615 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 NBG6615 via Internet browser. Use Internet Explorer 8.0 and later versions, Mozilla Firefox, Google Chrome or Safari. The recommended screen resolution is 1366 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 22 Troubleshooting](#) to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

- 1 Make sure your NBG6615 hardware is properly connected and prepare your computer or computer network to connect to the NBG6615 (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 When the NBG6615 is in router mode, type "http://192.168.212.1" as the website address in your web browser. 192.168.212.1 is the default LAN IP address in router mode (the default device mode). (The default IP address in AP 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 NBG6615 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 192.168.212.3 and 192.168.212.254 (see the appendices).

- 4 Type **admin** (default) as the user name and **1234** (default) as the password and click **OK**.

Figure 4 Login Screen

ZYXEL

NBG6615

Welcome to NBG6615 Embedded WEB Configurator!
Enter User Name/password and click to login.

 **User Name:**

 **Password:**

(max. 30 alphanumeric, printable characters and no spaces)

- You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password. Click **Apply** to save your changes. Click **Ignore** if you do not want to change the password this time.

Figure 5 Change Password Screen

ZYXEL

Please enter a new password

Your device is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess. We suggest you combine text with numbers to make it more difficult for an intruder to guess.

The administrator password must be between 8 - 30 characters.

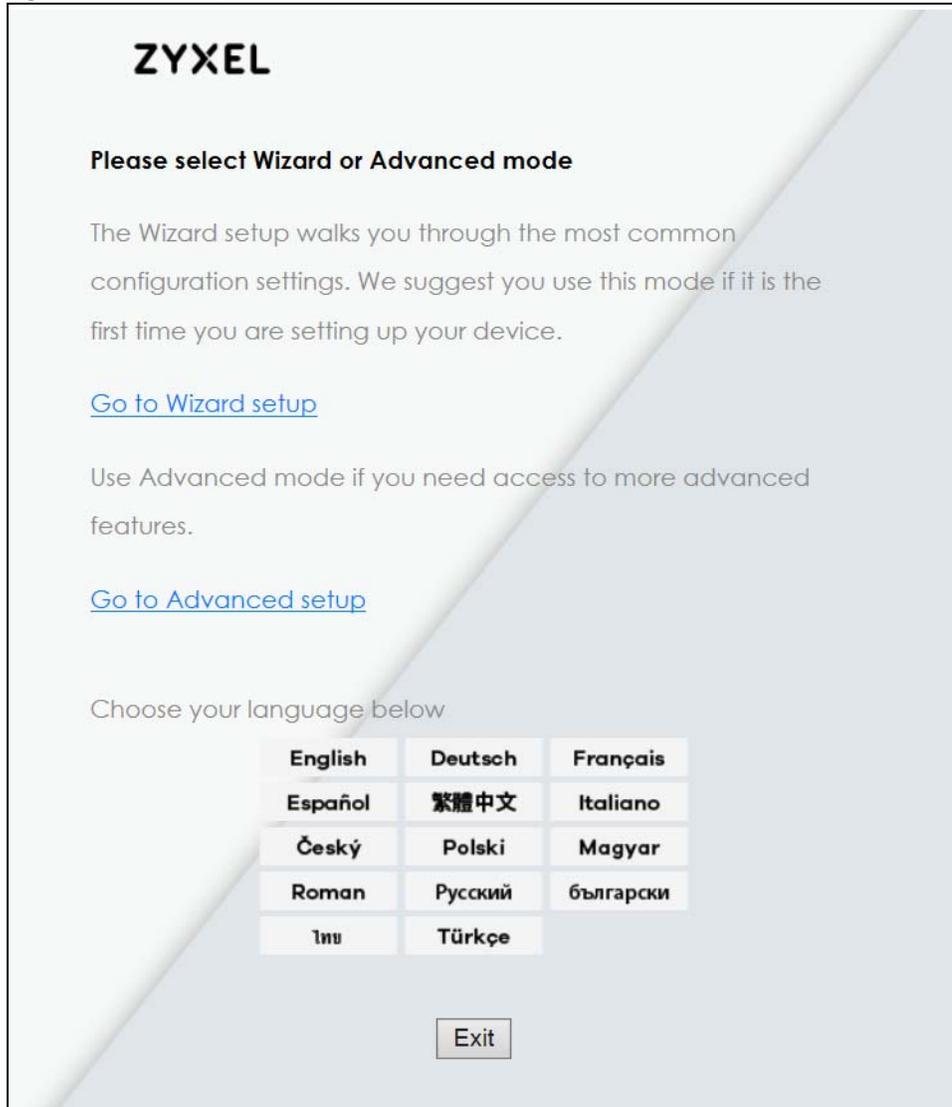
New Password :

Retype to Confirm :

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 NBG6615 if this happens.

- 6 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 NBG6615's settings.
 - Select a language to go to the basic Web Configurator in that language. To change to the advanced configurator see [Chapter 21 on page 133](#).

Figure 6 Selecting the setup mode



2.3 Resetting the NBG6615

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **Reset** button at the back of the NBG6615 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 "192.168.212.1".

Make sure the power LED is on and press the **Reset** button for longer than 10 seconds to restart/reboot and set the NBG6615 back to its factory-default configurations.

CHAPTER 3

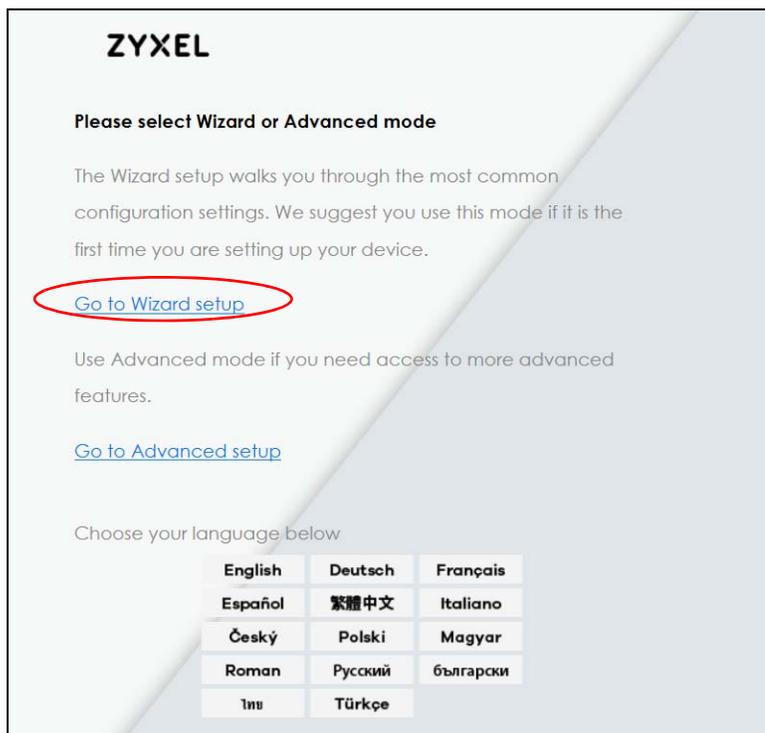
Connection Wizard

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. Leave a field blank if you don't have that information.

- 1 After you access the NBG6615 Web Configurator, click **Go to Wizard setup**.



Use this screen to choose whether you want to use the NBG6615 as a router or an access point. Select **Router** mode if you want the device to route traffic between a local network and another network such

as the Internet. Select **Access Point** if you want the device to bridge traffic between clients on the same network. Click **Next** to save your settings.

- 2 On the **WAN Interface Setup** screen, select an Internet access setting from the drop-down list. The NBG6615 offers four Internet access settings: **Static IP**, **Dynamic Host Configuration Protocol (DHCP Client)**, **PPP over Ethernet (PPPoE)**, and **Point to Point Tunneling Protocol (PPTP)**. Check with your ISP to make sure you use the correct setting. This Wizard screen varies according to the connection type that you select.

The following table describes the labels on this screen.

Figure 7 WAN Interface Setup

LABEL	DESCRIPTION
Static IP	Select Static IP if your ISP assigned you a fixed IP address.
DHCP Client	Select DHCP Client if your ISP did not assign you a fixed IP address.
PPPoE	Select PPPoE for a dial-up connection.
PPTP	Select PPTP to set up a virtual private network (VPN) in unsecured TCP/IP environments.
Cancel	Click Cancel to exit the Wizard without saving.
Back	Click Back to return to the previous screen.
Next	Click Next to proceed to the next screen.

3.1.0.1 Static IP Connection

The following Wizard screen allows you to assign a fixed IP address to the NBG6615.

Figure 8 Connection Type: Static IP

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your device. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

Connection Type:

IP Address:

Subnet Mask:

Default Gateway:

DNS:

The following table describes the labels on this screen.

Figure 9 Connection Type: Static IP

LABEL	DESCRIPTION
Connection Type	Select Static IP to give the NBG6615 a fixed, unique IP address.
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.
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 NBG6615 uses a system DNS server (in the order you specify here) to resolve domain names for DDNS and the time server. Enter the DNS server's IP address in this field.
Cancel	Click Cancel to exit the Wizard without saving.
Back	Click Back to return to the previous screen.
Next	Click Next to proceed to the next screen.

3.1.0.2 DHCP Client

Select **DHCP Client** when your network administrator or ISP assigns your IP address dynamically. This is a connection type often used with cable modems.

Figure 10 Connection Type: DHCP Client

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your device. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

Connection Type

3.1.0.3 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 NBG6615 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG6615 does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Figure 11 Connection Type: PPPoE

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your device. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

Connection Type

User Name:

Password:

The following table describes the labels on this screen.

Table 3 Connection Type: PPPoE

LABEL	DESCRIPTION
Connection Type	Select PPPoE for a dial-up connection.
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.
Cancel	Click Cancel to exit the Wizard without saving.
Back	Click Back to return to the previous screen.
Next	Click Next to proceed to the next screen.

3.1.0.4 PPTP Connection

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

Figure 12 Connection Type: PPTP

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your device. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

Connection Type: PPTP ▼

Dynamic IP (DHCP)
 Static IP

IP Address: 172.1.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Server IP Address: 172.1.1.1

User Name:

Password:

Cancel
<<Back
Next>>

The following table describes the labels on this screen.

Table 4 Connection Type: PPTP

LABEL	DESCRIPTION
Connection Type	Select PPTP from the drop-down list box. Select Dynamic IP (DHCP) if your ISP dynamically assigns DNS server information (and the NBG6615's WAN IP address). Click Static IP if you have the IP address of a DNS server
IP Address	If you selected Static IP , type the static IP address assigned to you by your ISP.

LABEL	DESCRIPTION
Subnet Mask	If you selected Static IP , enter the subnet mask address assigned to you by your ISP (if given).
Default Gateway	If you selected Static IP , enter the gateway IP address of the PPTP server.
Server IP Address	Type the IP address of the PPTP server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Cancel	Click Cancel to exit the Wizard without saving.
Back	Click Back to return to the previous screen.
Next	Click Next to proceed to the next screen.

- 3 You can now set up the wireless LAN. Use this screen to configure the basic settings of the wireless 2.4G band.

Figure 13 Wireless 2.4GSettings

Wireless 2.4G Basic Settings

This page is used to configure the parameters for wireless LAN clients that may connect to your wireless network.

802.11 Mode 2.4 GHz (B+G+N) ▼

Name (SSID) Zyxel545511

Channel Width Auto ▼

Channel Selection Auto ▼

The following table describes the labels on this screen.

Table 5 Wireless Settings

LABEL	DESCRIPTION
Wireless 2.4G Basic Settings	
802.11 Mode	Select the IEEE 802.11 WLAN mode you wish to use on the NBG6615 from the drop-down list.
Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the NBG6615, make sure all wireless stations use the same SSID in order to access the network.
Channel Width	Select whether the NBG6615 uses a wireless channel width of 20MHz, 40MHz, or 80 MHz (available with 5G only). Select Auto to allow the NBG6615 to adjust the channel bandwidth depending on network conditions. Select 20 MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. Select 40 MHz if your 2.4G to bond two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. Select 80MHz (available for 5G only) if you have a network with only a few wireless clients.

Table 5 Wireless Settings

LABEL	DESCRIPTION
Channel Selection	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. Select Auto to have the NBG6615 automatically choose the channel with the least interference.
Cancel	Click Cancel to close the Wizard screen without saving.
Back	Click Back to display the previous screen.
Next	Click Next to proceed to the next screen.

- 4 Next, select whether you want to use encryption to protect the information sent through the wireless network. In the drop-down list, you can choose **None**, **WPA2-PSK**, and **WPA-PSK/WPA2-PSK**. **WPA2-PSK** is currently the strongest form of security and is recommended for all uses. If you have older devices that don't support **WPA2-PSK**, select **WPA-PSK/WPA2-PSK**, which allows newer devices to use **WPA2-PSK** and legacy devices to use **WPA-PSK**. If you select an encryption protocol, create a password in the **Pre-shared Key** field. The password can be 8 to 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters ("0-9," "A-F"). Click **Next** to save the settings.

Wireless 2.4G Security Setup

This page allows you setup wireless security. Using WPA Encryption Keys will help prevent unauthorized access to your wireless network.

Security Mode WPA2-PSK ▼

Pre-Shared Key: 12345678

- 5 Repeat steps 4 and 5 to set up the wireless 5G.

Wireless 5G Basic Settings

This page is used to configure the parameters for wireless LAN clients that may connect to your wireless network.

802.11 Mode 5 GHz (A+N+AC) ▼

Name(SSID) Zyxel545511.speed

Channel Width Auto ▼

Channel Selection Auto ▼

Wireless 5G Security Setup

This page allows you setup wireless security. Using WPA Encryption Keys will help prevent unauthorized access to your wireless network.

Security Mode	<input type="text" value="WPA2-PSK"/>
Pre-Shared Key:	<input type="text" value="12345678"/>

- 6 Click **Finished** to complete the Wizard setup.

Well done! You have successfully set up your NBG6615 to operate on your network and access the Internet.

CHAPTER 4

Modes

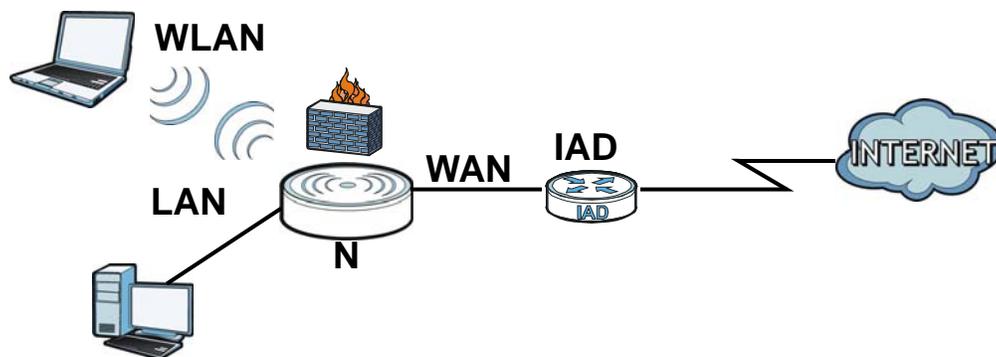
4.1 Overview

You can set up the NBG6615 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 NBG6615 automatically restarts when you change modes.

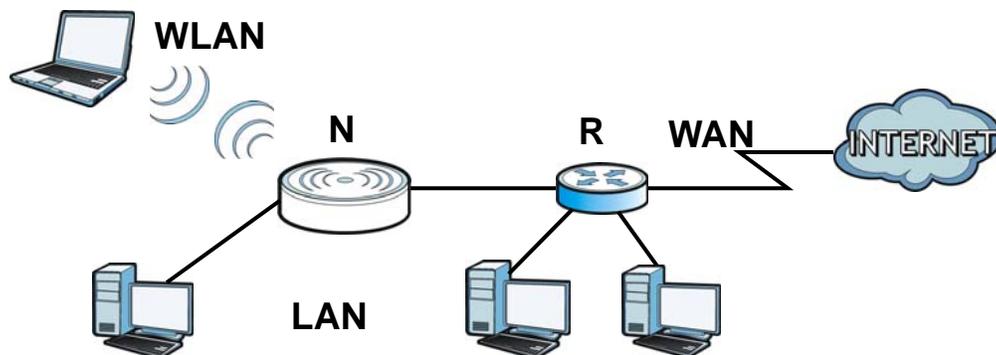
- The default LAN IP address of the NBG6615 in Router mode is 192.168.212.1. The default IP address of the NBG6615 in Access Point mode is 192.168.1.2. **Router:** Use this mode if you want to use routing functions such as LAN DHCP, NAT, firewall and so on, on the NBG6615 (N). The NBG6615 has separate LAN and WAN network IP addresses. Connect the WAN port to an Internet Access Device (IAD) such as a broadband modem.

Figure 14 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 NBG6615.

Figure 15 AP Mode



4.2 Setting your NBG6615 to Router Mode

The NBG6615 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 NBG6615.
- 2 The default LAN IP address of the NBG6615 is 192.168.212.1 in router mode and 192.168.1.2 by default in Access Point mode. In router mode, the NBG6615 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 192.168.212.3 and 192.168.212.254.
- 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 NBG6615 as the web address in your web browser.
- 4 Log into the Web Configurator. See the [Chapter 2 on page 16](#) for instructions on how to do this.
- 5 Go to **Maintenance > Sys OP Mode > General** and select **Router**.



- 6 Click **Apply**.

Note: Wait while the NBG6615 restarts, then log in to the Web Configurator again. The NBG6615 IP address is now 192.168.212.1.

4.2.1 Status Screen (Router Mode)

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

Figure 16 Status Screen (Router Mode)

The screenshot shows the Status Screen in Router Mode. At the top right, there is a 'Refresh Interval' dropdown set to 'None' and a 'Refresh Now' button. The screen is divided into four main sections:

- Device Information:** Lists system details including System Name (NBG6615), Firmware Version (V1.00(ABMV.0)B1), WAN Information (MAC Address, Connection Type, IP Address, Subnet Mask, Gateway, DNS), LAN Information (MAC Address, IP Address, Subnet Mask, DHCP Server), and WLAN Information (MAC Address, Status, Name, Channel, Operating Channel).
- System Status:** Shows Operation Mode (Router, circled in red), System Up Time (0day:15h:44m:56s), Current Date/Time (2018-4-12 8:33:33), and System Setting (Firewall: Enabled, UPnP: Disabled).
- Interface Status:** A table showing the status and rate of LAN interfaces.
- Summary:** Includes links for Client Table and Packet Statistics.

Interface	Status	Rate
LAN1	Down	NA
LAN2	Up	1000M
LAN3	Down	NA
LAN4	Down	NA

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

Table 6 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 7 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 NBG6615.
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.

Table 7 Web Configurator Status Screen (Router Mode) (continued)

LABEL	DESCRIPTION
- 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 (5.G/2.4G)	
- 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 NBG6615 in the wireless LAN.
- Channel	This shows the channel number which you select manually or the NBG6615 automatically scans and selects.
- Operating Channel	This shows the channel number which the NBG6615 is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG6615 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.
System Status	
Operation Mode	This field shows the device operation mode: Router , Access Point , Universal Repeater or Client Bridge .
System Up Time	This is the total time the NBG6615 has been on.
Current Date/Time	This field displays your NBG6615'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.
Interface	
-Lan 1	This shows the first LAN port's connection status and operating speed.
-Lan 2	This shows the second LAN port's connection status and operating speed.
-Lan 3	This shows the third LAN port's connection status and operating speed.
-Lan 4	This shows the fourth LAN port's connection status and operating speed.
Summary	
Client Table	Use this screen to view current 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.

4.2.1.1 Summary: Client Table

Click the **Client Table (Details...)** hyperlink on the **Status** screen. The client table shows current client information (including **Host Name**, **IP Address**, and **MAC Address**) of all network clients connected to the NBG6615.

Figure 17 Summary: Client Table

DHCP Client Table				
#	Host Name	IP Address	MAC Address	Interface
1	TWPCZT02727-01	192.168.1.33	1078d2c519cd	lan

Refresh

The following table describes the labels in this screen.

Table 8 Summary: Client Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
Host Name	This field displays the computer host name.
IP Address	This field displays the IPv4 address relative to the # field listed above.
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.
Interface	This field shows the NBG6615's interface to which the client is connected.

4.2.1.2 Summary: Packet Statistics

Click the **Packet Statistics (Details...)** hyperlink on the **Status** screen. Read-only information here includes the number of packets sent and received on each port. The Click the **Refresh** button to update statistics. .

Figure 18 Summary: Packet Statistics

DHCP Client Table		
Wireless 1LAN	Sent Packets	0
	Received Packets	15173477
Wireless 2LAN	Sent Packets	4074
	Received Packets	4214572
EthernetLAN	Sent Packets	19820
	Received Packets	16122
EthernetWAN	Sent Packets	37320
	Received Packets	36325

4.2.2 Router Mode Navigation Panel

Use the menu in the navigation panel menus to configure NBG6615 features in **Router Mode**.

Figure 19 Menus: Router Mode



The following table describes the sub-menus.

Table 9 Menus: Router Mode

LINK	TAB	FUNCTION
Network		
Wireless LAN (2.4G/5G)	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG6615 to block access to devices or block the devices from accessing the NBG6615.
	WLAN Advanced Setup	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 multiple SSIDs on the NBG6615.
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.
LAN	IP	Use this screen to configure LAN IPv4 address and subnet mask.

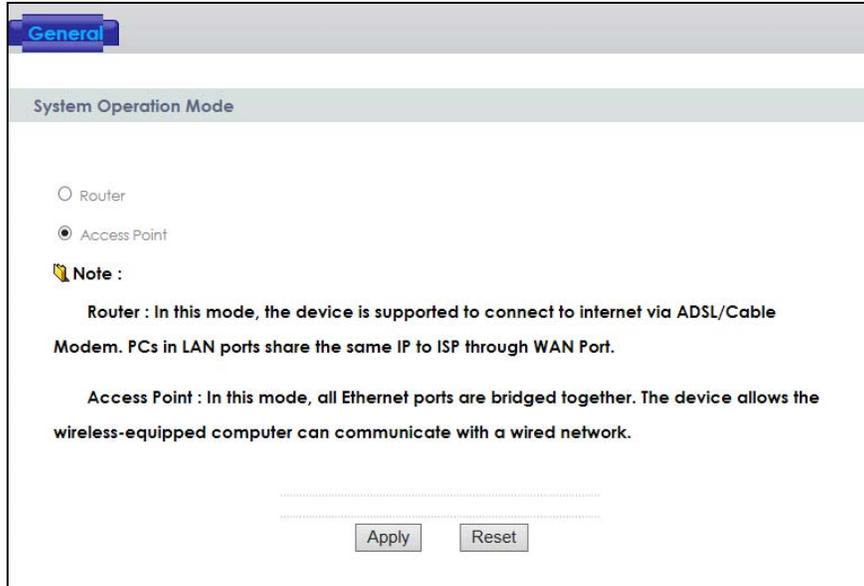
Table 9 Menus: Router Mode (continued)

LINK	TAB	FUNCTION
DHCP Server	General	Use this screen to enable the NBG6615's DHCP server.
	Static DHCP	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 NBG6615.
	Port Triggering	Use this screen to configure port triggering settings on the NBG6615.
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.
Static Route	IP Static Route	Use this screen to configure IP static routes.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	Use this screen to enable or disable ICMP and VPN passthrough features.
	MAC Filter	Use this screen to whitelist or blacklist devices based on their MAC address.
Content Filter	Filter	Use this screen to configure content filter settings on the NBG6615.
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 NBG6615.
UPnP	UPnP	Use this screen to enable UPnP on the NBG6615.
Bandwidth MGMT	General	Use this screen to enable bandwidth management on the NBG6615.
	Advanced	Use this screen to set the upstream bandwidth and edit a bandwidth management rule.
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 NBG6615'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 NBG6615.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG6615.
	Restart	This screen allows you to reboot the NBG6615 without turning the power off.
Sys OP Mode	General	This screen allows you to select the device operating mode.
Language	Language	This screen allows you to select the language you prefer.

4.3 Setting your NBG6615 to AP Mode

- 1 Connect your computer to the LAN port of the NBG6615.
- 2 The default LAN IP address of the NBG6615 is 192.168.212.1 in router mode and 192.168.1.2 in Access Point mode..

- 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 NBG6615 as the web address in your web browser.
- 4 Log into the Web Configurator. See the [Chapter 2 on page 16](#) for instructions on how to do this.
- 5 Go to **Maintenance > Sys OP Mode > General** and select **Access Point**.



The screenshot shows the 'General' configuration page for the NBG6615. At the top, there is a 'General' tab. Below it, the 'System Operation Mode' section is visible. There are two radio button options: 'Router' (unselected) and 'Access Point' (selected). Below the radio buttons, there is a 'Note' section with a yellow icon. The note contains two paragraphs: 'Router : In this mode, the device is supported to connect to internet via ADSL/Cable Modem. PCs in LAN ports share the same IP to ISP through WAN Port.' and 'Access Point : In this mode, all Ethernet ports are bridged together. The device allows the wireless-equipped computer can communicate with a wired network.' At the bottom of the page, there are two buttons: 'Apply' and 'Reset'.

- 6 Click **Apply**. Your NBG6615 is now in **AP Mode**.

Note: Wait while the NBG6615 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 20 Status Screen (AP Mode)

The screenshot displays the Status Screen for an Access Point (AP) mode. It is divided into four main sections:

- Device Information:** Shows System Name (NBG6615), Firmware Version (V1.00(A8MV.0)B1), WAN Information (MAC Address: 00:05:1d:54:55:12, Connection Type: Disconnected, IP Address: 0.0.0.0, Subnet Mask: 0.0.0.0, Gateway: 0.0.0.0, DNS: 0.0.0.0), LAN Information (MAC Address: 00:05:1d:54:55:11, IP Address: 192.168.1.1, Subnet Mask: 255.255.255.0, DHCP Server: Disabled), WLAN Information - 5G (MAC Address: 00:05:1d:54:55:13, Status: Enabled, Name: Zyxe1545511.speed, Channel: 44, Operating Channel: 44, Security Mode: None, 802.11 Mode: 5 GHz (A+N+AC), WPS: Configured), and WLAN Information - 2.4G (MAC Address: 00:05:1d:54:55:14, Status: Enabled, Name: Zyxe1x, Channel: 11, Operating Channel: 11, Security Mode: WPA2, 802.11 Mode: 2.4 GHz (B+G+N), WPS: Configured).
- System Status:** Shows Operation Mode (Access Point, circled in red), System Up Time (0day:1h:47m:58s), Current Date/Time (2018-4-11 18:46:46), and System Setting (Firewall: Enabled, UPnP: Disabled).
- Interface Status:** A table showing the status of LAN interfaces:

Interface	Status	Rate
LAN1	Down	NA
LAN2	Up	1000M
LAN3	Down	NA
LAN4	Down	NA
- Summary:** Provides links for Client Table, Client Table, Packet Statistics, and Packet Statistics, each with a (Details...) link.

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

Table 10 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 NBG6615.
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 (5g/2.4G)	
- MAC Address	This shows the wireless adapter MAC Address of your device.

Table 10 Status Screen (AP Mode) (continued)

LABEL	DESCRIPTION
- 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 NBG6615 in the wireless LAN.
- Channel	This shows the channel number, which you select manually or the NBG6615 automatically scans and selects.
- Operating Channel	This shows the channel number which the NBG6615 is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG6615 is using.
- 802.11 Mode	This shows the IEEE 802.11 standard that the NBG6615 supports. Wireless clients must support the same standard in order to be able to connect to the NBG6615
- 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 operating mode: Router , Access Point , Universal Repeater or Client Bridge .
System Up Time	This is the total time the NBG6615 has been on.
Current Date/Time	This field displays your NBG6615's present date and time.
Summary	
Client Table	Use this screen to view current 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.

4.3.2 AP Navigation Panel

Use the menu in the navigation panel to configure NBG6615 features in **AP Mode**.

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

Figure 21 Menu: AP Mode

NBG6615
- Network
· Wireless LAN 2.4G
· Wireless LAN 5G
· LAN
- Maintenance
· System
· Logs
· Tools
· Sys OP Mode
· Language

The following table describes the sub-menus.

Table 11 Menu: AP Mode

LINK	TAB	FUNCTION
Network		
Wireless LAN (2.4G/5G)	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG6615 to block access to devices or block the devices from accessing the NBG6615.
	WLAN Advanced Setup	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 multiple SSIDs on the NBG6615.
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 NBG6615'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 NBG6615.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG6615.
	Restart	This screen allows you to reboot the NBG6615 without turning the power off.
Sys OP Mode	General	This screen allows you to select the device operating mode: Router and Access Point .
Language	Language	This screen allows you to select the language you prefer.

CHAPTER 5

Tutorials

5.1 Overview

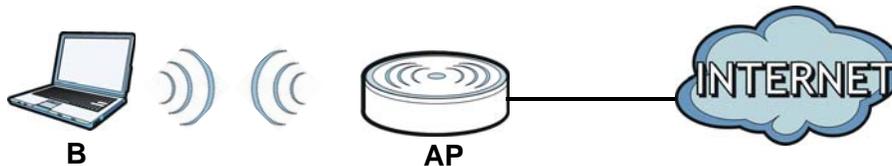
This chapter provides tutorials for your NBG6615 as follows:

- [How to Connect to the Internet from an AP](#)
- [Configure Wireless Security Using WPS on both your NBG6615 and Wireless Client](#)
- [Enable and Configure Wireless Security without WPS on your NBG6615](#)
- [Using Multiple SSIDs on the NBG6615](#)
- [Using Bandwidth Management on the NBG6615](#)

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 22 Wireless AP Connection to the Internet



5.3 Configure Wireless Security Using WPS on both your NBG6615 and Wireless Client

This section gives you an example of how to set up wireless network using WPS. This example uses the NBG6615 as the AP and NWD210N as the wireless client that 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 40](#). 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 NBG6615's interface. See [Section 5.3.2 on page 41](#). This is the more secure method, since one device can authenticate the other.

5.3.1 Push Button Configuration

- 1 Make sure that your NBG6615 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 NBG6615's Web Configurator and press **Push Button** in the **Network > Wireless LAN (2.4G/5G)> WPS Station** screen.

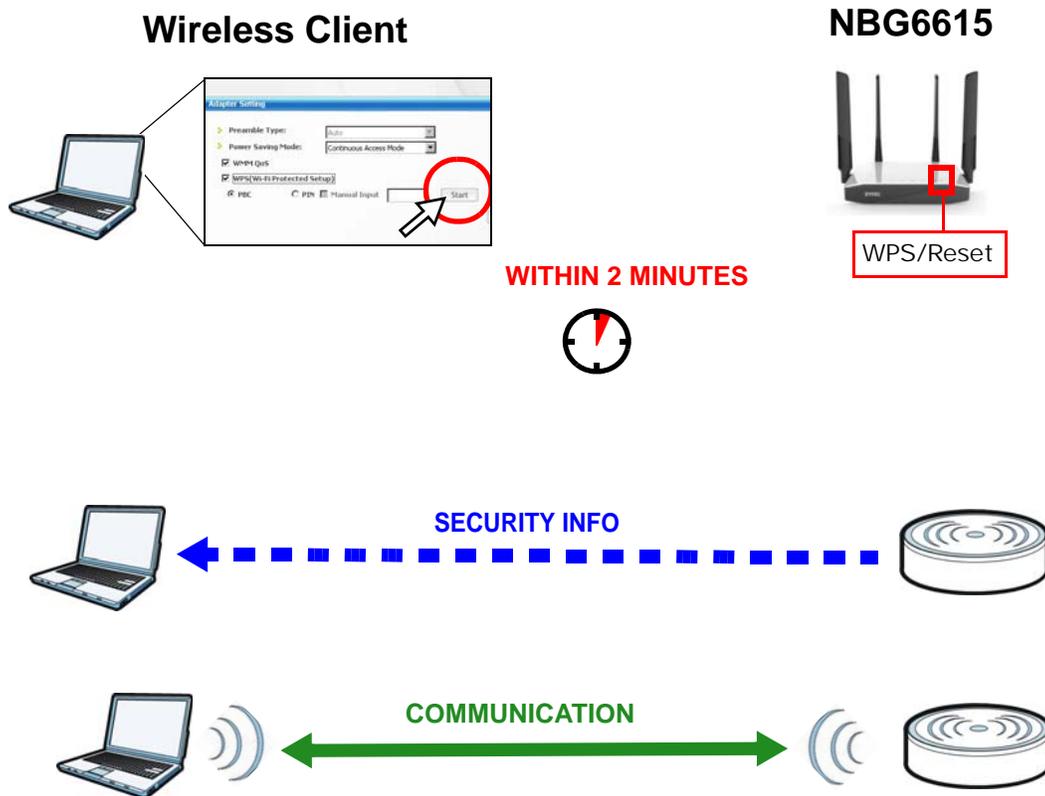
Note: Your NBG6615 has a WPS button located on its front panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

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 NBG6615 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 NBG6615 securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both NBG6615 and wireless client (the NWD210N in this example).

Figure 23 Example WPS Process: Push Button Configuration Method



5.3.2 PIN Configuration

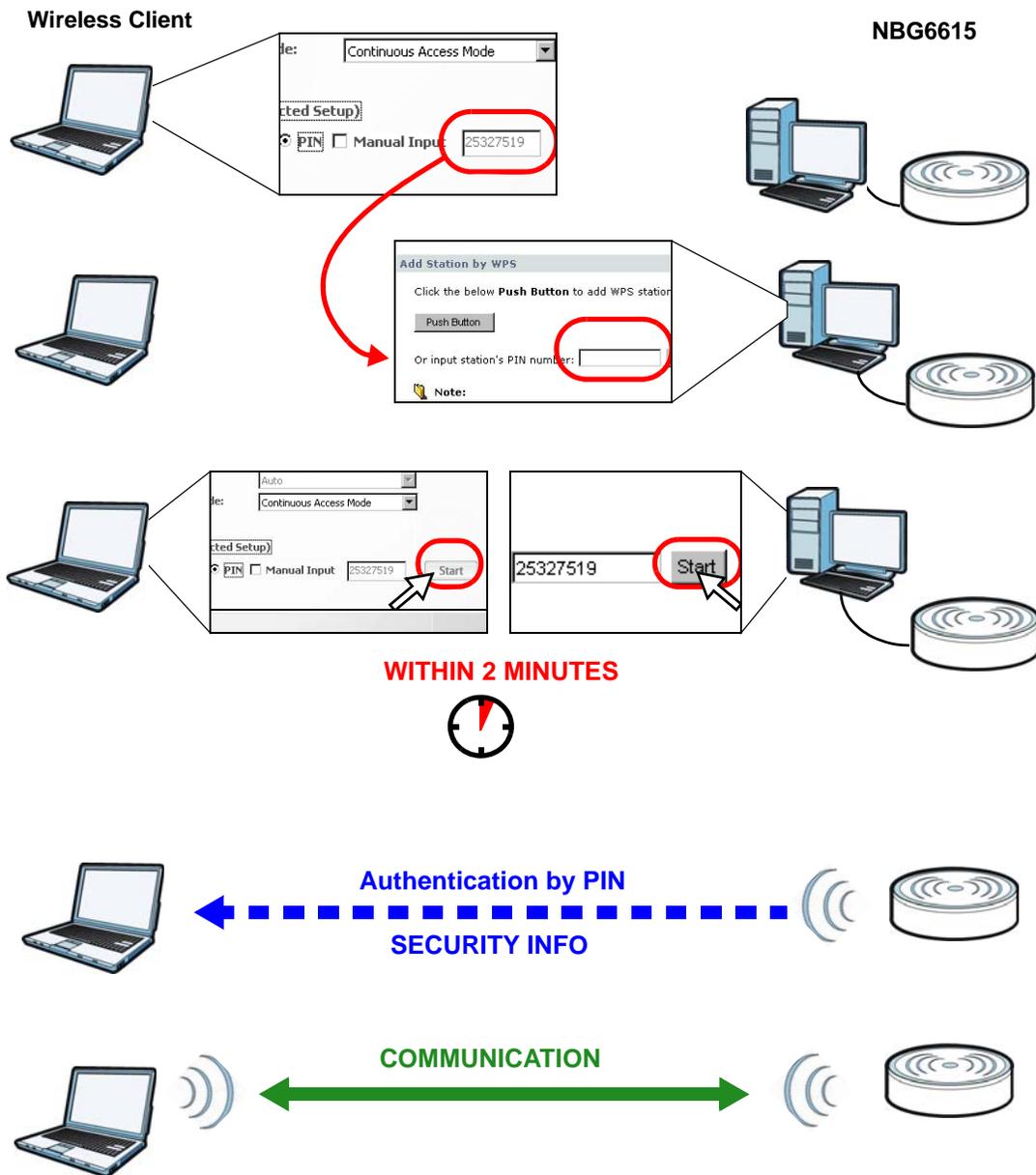
When you use the PIN configuration method, you need to use both NBG6615's configuration interface and the client's utilities.

- 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 (2.4G/5G) > WPS Station** screen on the NBG6615.
- 3 Click the **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the NBG6615's **WPS Station** screen within two minutes.

The NBG6615 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 NBG6615 securely.

The following figure shows you the example to set up wireless network and security on NBG6615 and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 24 Example WPS Process: PIN Method



5.4 Enable and Configure Wireless Security without WPS on your NBG6615

This example shows you how to configure wireless security settings with the following parameters on your NBG6615.

SSID	SSID_Example3
Channel	6
Security	WPA-PSK/WPA2-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your NBG6615.

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 16](#)).

- 1 Open the **Wireless LAN > General** screen in the NBG6615'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/WPA2-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Figure 25 Tutorial: Network > Wireless LAN 2.4G/5G> General

The screenshot shows the 'WLAN Setup' configuration page. The 'WLAN Setup' section includes a checked 'Enable Wireless LAN' box, '802.11 Mode' set to '2.4 GHz (B+G+N)', 'Name (SSID)' set to 'SSID_Example3', a checked 'Enable SSID Broadcast' box, 'Channel Selection' set to '6', 'Operating Channel' set to '6', and 'Channel Width' set to '40MHz'. The 'Security' section shows 'Security Mode' set to 'WPA-PSK/WPA2-PSK' and 'Pre-Shared Key' set to 'ThisismyWPA_PSKpre-sharedkey'. A note at the bottom states: 'Note: No security (None) and WPA2-PSK can be configured ONLY when WPS is enabled.' There are 'Apply' and 'Reset' buttons at the bottom.

- 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 26 Tutorial: Status Screen

The screenshot displays the status screen for the NBG6615 device, organized into several sections:

- Device Information:**
 - System Name : NBG6615
 - Firmware Version : V1.00(ABMV.0)B3_0613
 - WAN Information:**
 - MAC Address : 00:05:1d:54:55:12
 - Connection Type : DHCP
 - IP Address : 10.214.80.38
 - IP Subnet Mask : 255.255.255.0
 - Gateway : 10.214.80.1
 - DNS : 172.21.5.1,172.21.6.1
 - LAN Information:**
 - MAC Address : 00:05:1d:54:55:11
 - IP Address : 192.168.212.1
 - IP Subnet Mask : 255.255.255.0
 - DHCP Server : Enabled
 - WLAN Information - 5G:**
 - MAC Address : 00:05:1d:54:55:13
 - Status : Enabled
 - Name(SSID) : Zyxel545511.spee...
 - Operating Channel : 56
 - Security Mode : WPA2
 - 802.11 Mode : 5 GHz (A+N+AC)
 - WPS : [Configured](#)
 - WLAN Information - 2.4G (highlighted):**
 - MAC Address : 00:05:1d:54:55:14
 - Status : Enabled
 - Name(SSID) : SSID_Example3
 - Operating Channel : 6
 - Security Mode : WPA/WPA2-Mixed
 - 802.11 Mode : 2.4 GHz (B+G+N)
 - WPS : [Configured](#)
- System Status:**
 - Operation Mode : Router
 - System Up Time : 0day:0h:43m:24s
 - Current Date/Time : 2018-6-21 2:30:50
 - System Setting :
 - Firewall : Enabled
 - UPnP : Enabled
- Interface Status:**

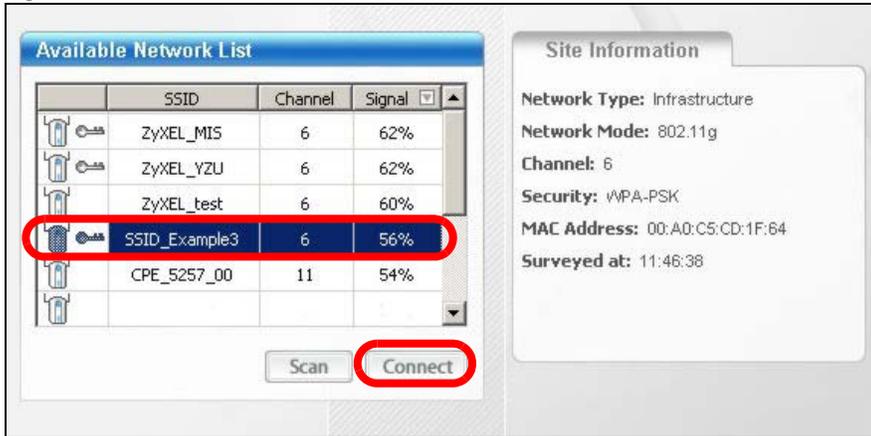
Interface	Status	Rate
LAN1	Down	NA
LAN2	Up	1000M
LAN3	Down	NA
LAN4	Down	NA
- Summary:**
 - Client Table [\(Details...\)](#)
 - Packet Statistics [\(Details...\)](#)

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.

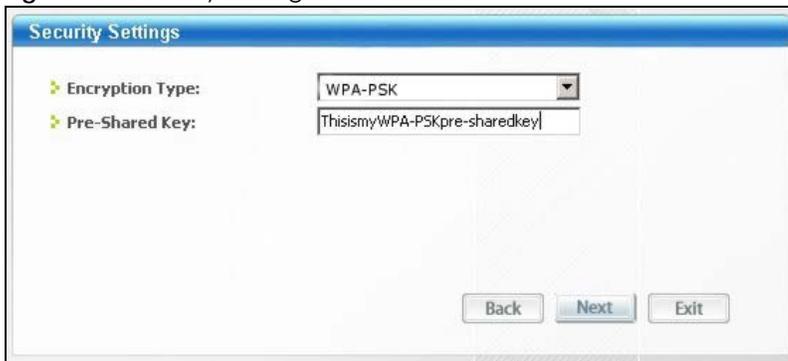
- 1 The NBG6615 supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.
- 2 Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless 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 27 Connecting a Wireless Client to a Wireless Network



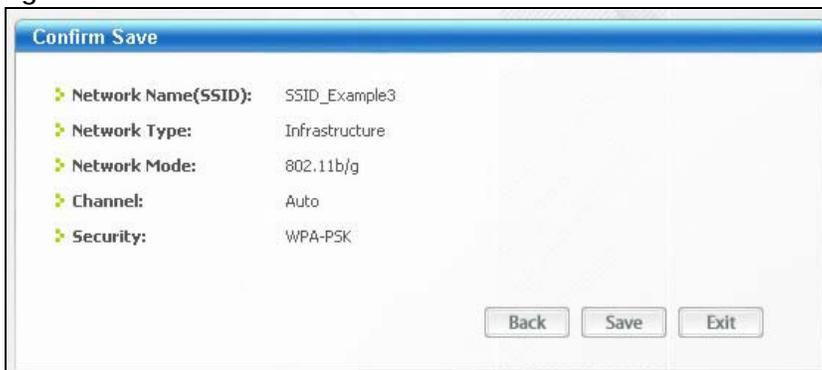
- 5 Select WPA-PSK and type the security key in the following screen. Click **Next**.

Figure 28 Security Settings



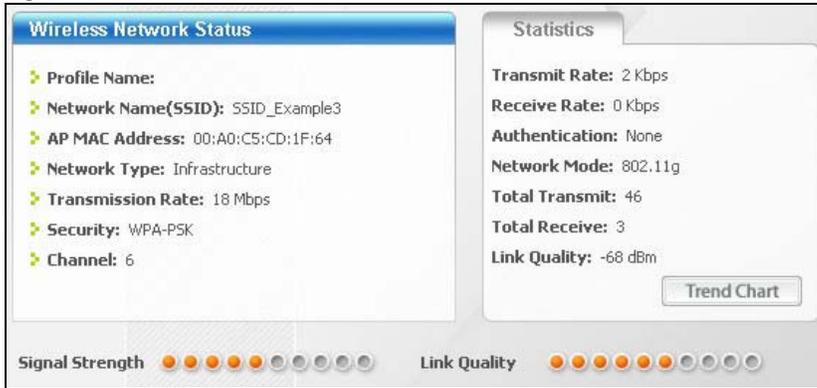
- 6 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 29 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 30 Link Status



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

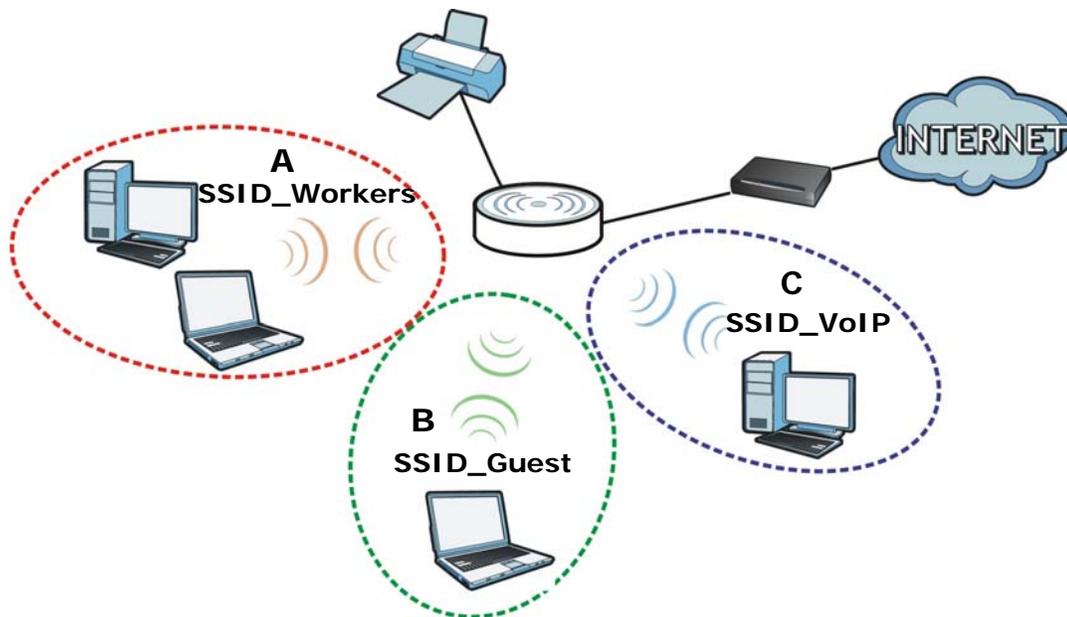
5.5 Using Multiple SSIDs on the NBG6615

You can configure more than one SSID on a NBG6615. See [Section 6.10 on page 65](#).

This allows you to configure multiple independent wireless networks on the NBG6615 as if there were multiple APs (virtual APs). Each virtual AP has its own SSID, and wireless security type. That is, each SSID on the NBG6615 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 NBG6615 (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 NBG6615 is in router mode by default.

This example shows you how to configure the SSIDs with the following parameters on your NBG6615 (in router mode).

SSID	SECURITY TYPE	KEY
SSID_Workers	WPA2-PSK WPA Compatible	DoNotStealMyWirelessNetwork
SSID_VoIP	WPA-PSK/WPA2-PSK	VoIPOnly12345678
SSID_Guest	WPA-PSK/WPA2-PSK	keyexample123

- 1 Connect your computer to the LAN port of the NBG6615 using an Ethernet cable.
- 2 The default IP address of the NBG6615 in router mode is "192.168.212.1". In this case, your computer must have an IP address in the range between "192.168.212.2" and "192.168.212.254".
- 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 C on page 158](#) 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://192.168.212.1" 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 (2.4G/5G) > MBSSID**. Type **SSID_Workers** in the Name (SSID) field, select **WPA2-PSK** in the Security drop-down list, enter the pre-shared key and click **Apply**.

Network Profiles

Select	Scheme	SSID	Security	Status	SSID Broadcast
<input checked="" type="radio"/>	1	Zyxe_SSID1	None	Inactive	Active
<input type="radio"/>	2	Zyxe_SSID2	None	Inactive	Active
<input type="radio"/>	3	Zyxe_SSID3	None	Inactive	Active
<input type="radio"/>	4	Zyxe_SSID4	None	Inactive	Active

Wireless Settings--Profile 1

Enable Guest Network
 Enable SSID Broadcast
 Allow Guest to access My Local Network
 Enable Wireless Isolation

Name (SSID)

Security Options--Profile 1

Security Mode

Pre-Shared Key (8-63 characters or 64 hex digits)

Note: No security (None) and WPA2-PSK can be configured ONLY when WPS is enabled.

- 9 Go to **Network > Wireless LAN (2.4G/5G) > WLAN Advanced Setup** and click enable **Intra-BSS Traffic** to allow wireless clients in the same wireless network to communicate with each other. Click **Apply**.

WLAN Advanced Setup

Tx Power

Enable Intra-BSS Traffic Disabled Enabled

- 10 To create the SSID_VoIP, go to **Network > Wireless LAN (2.4G/5G) > MBSSID**. click the radio button next to **scheme 2** and Type **SSID_Voip** in the Name (SSID) field, select **WPA-PSK/WPA2-PSK** in the Security drop-down list, enter the pre-shared key and click **Apply**.

Network Profiles

Select	Scheme	SSID	Security	Status	SSID Broadcast
<input type="radio"/>	1	Zyxel_SSID1	None	Inactive	Active
<input type="radio"/>	2	Zyxel_SSID2	None	Inactive	Active
<input type="radio"/>	3	Zyxel_SSID3	None	Inactive	Active
<input type="radio"/>	4	Zyxel_SSID4	None	Inactive	Active

Wireless Settings--Profile 2

Enable Guest Network
 Enable SSID Broadcast
 Allow Guest to access My Local Network
 Enable Wireless Isolation

Name (SSID)

Security Options--Profile 2

Security Mode

Pre-Shared Key (8-63 characters or 64 hex digits)

 Note: No security (None) and WPA2-PSK can be configured ONLY when WPS is enabled.

- 11** To create the SSID_Guest, go to **Network > Wireless LAN (2.4G/5G) > 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/WPA2-PSK** in the Security drop-down list, enter the pre-shared key and click **Apply**.

Network Profiles

Select	Scheme	SSID	Security	Status	SSID Broadcast
<input type="radio"/>	1	Zyxe_SSID1	None	Inactive	Active
<input checked="" type="radio"/>	2	Zyxe_SSID2	None	Inactive	Active
<input type="radio"/>	3	Zyxe_SSID3	None	Inactive	Active
<input type="radio"/>	4	Zyxe_SSID4	None	Inactive	Active

Wireless Settings--Profile 3

Enable Guest Network
 Enable SSID Broadcast
 Allow Guest to access My Local Network
 Enable Wireless Isolation

Name(SSID)

Security Options--Profile 3

Security Mode

Pre-Shared Key (8-63 characters or 64 hex digits)

 Note:No security(None) and WPA2-PSK can be configured ONLY when WPS is enabled.

5.6 Installing UPnP in Windows 7 Example

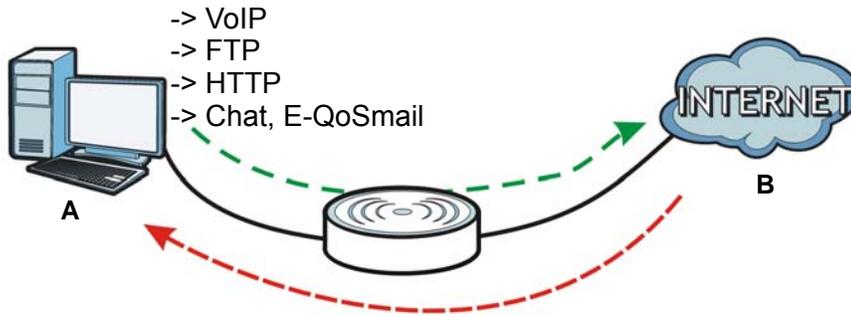
For more information on how to install Universal Plug and Play in Windows on your computer, see [Section 15.4 on page 111](#)

5.7 Using Bandwidth Management on the NBG6615

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 31 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 NBG6615 (in router mode).

QoS Rule

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

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

The screenshot shows a web interface titled 'Service Management'. There is a checkbox labeled 'Enable Bandwidth Management' which is checked. Below the checkbox are two buttons: 'Apply' and 'Reset'.

- 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.

The screenshot shows a web interface titled 'QoS Setup'. It displays 'Total Bandwidth(0, Unlimited):' followed by 'UP Stream 819200 kpbs' and 'Down Stream 819200 kpbs'. The values 819200 are circled in red. At the bottom, there are 'Apply' and 'Reset' buttons, with the 'Apply' button also circled in red.

- Then, click **Add** in the **QoS Rules** section and several box fields will appear. Enter 192.168.1.10 in the **Source IP** field. Next, enter 150000 for **Up Ceiling** field and 600000 for **Down Ceiling** field 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.

#	Source IP Address	Max Bandwidth(Kbps)		Delete
		Up Ceiling	Down Ceiling	
		<input type="button" value="Add"/>	<input type="button" value="Select All"/>	<input type="button" value="Delete"/>
Source IP	<input type="text" value="192.168.1.10"/>			
Up Ceiling	<input type="text" value="150000"/>	kb/s		
Down Ceiling	<input type="text" value="600000"/>	kb/s		
		<input type="button" value="Add"/>	<input type="button" value="Reset"/>	

- 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 **Reset** button.

PART II

Technical Reference

CHAPTER 6

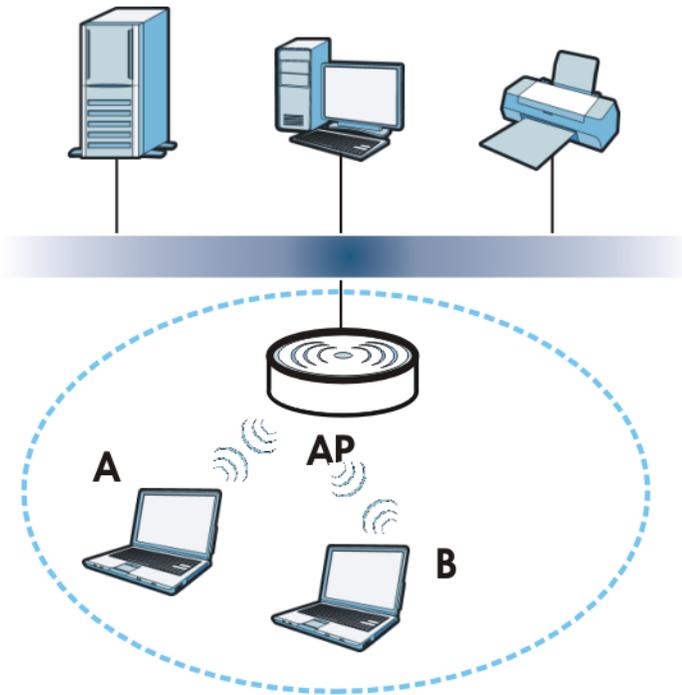
Wireless LAN

6.1 Overview

This chapter discusses how to configure the wireless network settings in your NBG6615. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 32 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 NBG6615 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	Client Bridge
General	✓	✓	✓	
MAC Filter	✓	✓	✓	
Advanced	✓	✓	✓	✓
WPS	✓	✓	✓	
WPS Station	✓	✓	✓	
Scheduling	✓	✓	✓	
MBSSID	✓	✓	✓	
AP Select			✓	✓
WLAN Information				✓

See [Chapter 4 on page 28](#) 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 57](#)).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the NBG6615 ([Section 6.5 on page 60](#)).
- Use the **Advanced** screen to allow intra-BSS networking and set the RTS/CTS Threshold ([Section 6.6 on page 61](#)).
- 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 62](#)).
- Use the **WPS Station** screen to add a wireless station using WPS ([Section 6.8 on page 64](#)).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off ([Section 6.9 on page 64](#)).
- Use the **MBSSID** screen to configure multiple wireless networks on the NBG6615 ([Section 6.10 on page 65](#)).

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 NBG6615'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 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 characters²; 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 12 Types of Encryption for Each Type of Authentication

NO AUTHENTICATION	
Weakest	No Security
↕	
	WPA-PSK/WPA2-PSK
Strongest	WPA2-PSK

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

It is recommended that wireless networks use WPA2-PSK or stronger encryption if supported. If you have older devices that don't support **WPA2-PSK**, select **WPA-PSK/WPA2-PSK**, which allows newer devices to use **WPA2-PSK** and legacy devices to use **WPA-PSK**.

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 39](#).

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 NBG6615 from a computer connected to the wireless LAN and you change the NBG6615'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 NBG6615's new settings.

Click **Network > Wireless LAN (2.4G/5G)** to open the **General** screen.

Figure 33 Network > Wireless LAN (2.4G/5G) > General (Router or Access Point Mode)

WLAN Setup	
<input checked="" type="checkbox"/> Enable Wireless LAN	
802.11 Mode	2.4 GHz (B+G+N) ▾
Name(SSID)	Zyxe1545511
<input checked="" type="checkbox"/> Enable SSID Broadcast	
Channel Selection	5 ▾
Operating Channel	11
Channel Width	40MHz ▾
Security	
Security Mode	None ▾
 Note: No security(None) and WPA2-PSK can be configured ONLY when WPS is enabled.	

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

Table 13 Network > Wireless LAN > General

LABEL	DESCRIPTION
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)	The Service Set Identity (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. Select Auto to have the NBG6615 automatically choose the channel with the least interference.
Operating Channel	This displays the channel the NBG6615 is currently using.

Table 13 Network > Wireless LAN > General (continued)

LABEL	DESCRIPTION
Channel Width	<p>Select whether the NBG6615 uses a wireless channel width of 20MHz, 40MHz, or 80MHz (available with 5GHz).</p> <p>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.</p> <p>Select Auto to have the NBG6615 adjust channel bandwidth automatically based on network conditions.</p> <p>Select 20MHz if you have 2.4G wireless clients in an environment with a lot of wireless clients.</p> <p>Select 40MHz if your 2.4G wireless clients support channel bonding.</p> <p>Select 80MHz if your 5G wireless clients support channel bonding.</p>
Security Mode	This displays the type of security configured on the wireless device to which you are connecting.
Apply	Click Apply to save your changes back to the NBG6615.
Reset	Click Reset to reload the previous configuration for this screen.

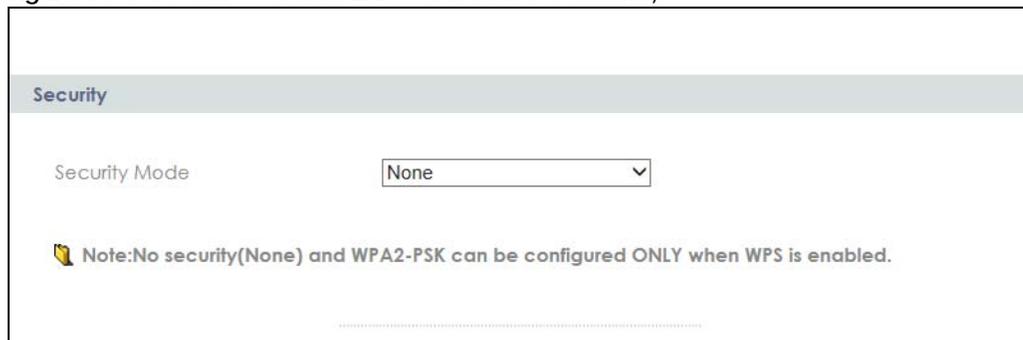
See the rest of this chapter for information on the other labels in this screen.

6.4.1 No Security

Select **None** 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 NBG6615, your network is accessible to any wireless networking device that is within range.

Figure 34 Network > Wireless LAN > General: No Security



6.4.2 WPA2-PSK or WPA-PSK/WPA2-PSK

Click **Network > Wireless LAN (2.4G/5G)** to display the **General** screen. Select **WPA2-PSK** or **WPA-PSK/WPA2-PSK** from the **Security Mode** list.

Figure 35 Network > Wireless LAN > General: WPA2-PSK or WPA-PSK/WPA2-PSK

The following table describes the labels on this screen.

Table 14 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Security Mode	Choose WPA2-PSK or WPA-PSK/WPA2-PSK from the drop-down list box. Select WPA-PSK/WPA2-PSK to have both WPA2 and WPA wireless clients be able to communicate with the NBG6615 even when the NBG6615 is using WPA2-PSK.
Pre-Shared Key	WPA2-PSK and 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").
Apply	Click Apply to save your changes back to the NBG6615.
Reset	Click Reset to reload the previous configuration for this screen.

6.5 MAC Filter

The MAC filter screen allows you to configure the NBG6615 to give exclusive access to up to 16 devices (Allow) or exclude up to 16 devices from accessing the NBG6615 (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 NBG6615's MAC filter settings, click **Network > Wireless LAN (2.4G/5G) > MAC Filter**. The screen appears as shown.

Figure 36 Network > Wireless LAN (2.4G/5G)> MAC Filter

The following table describes the labels in this menu.

Table 15 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Wireless Active Control Mode	In the drop-down list, select Allow Listed to activate the whitelist mode, which allows only listed MAC addresses to join the wireless network. Select Deny Listed to activate the blacklist mode, which prevents listed MAC address from joining the wireless network. Select Disable to turn off MAC address filtering.
MAC Address	Enter the MAC addresses that are to be whitelisted or blacklisted in a valid MAC address format (that is, six hexadecimal character pairs.) Example: 12:34:56:78:9a:8c. Do not use colons when entering the MAC address.
Comment	This field can be used to add identifying information or other notes about MAC addresses in the whitelist or blacklist.
Apply	Click Apply to save your changes back to the NBG6615.
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 (2.4G/5G)> WLAN Advanced Setup**. The screen appears as shown.

Figure 37 Network > Wireless LAN (2.4G/5G)> WLAN Advanced Setup

The following table describes the labels on this screen.

Table 16 Network > Wireless LAN (2.4G/5G)> WLAN Advanced Setup

LABEL	DESCRIPTION
Tx Power	This field controls the transmission power of the NBG6615. If there is a high density of APs in an area, decrease the output power of the NBG6615 to reduce interference with other APs.
Enable Intra-BSS Traffic	<p>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).</p> <p>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.</p>
MU-MIMO and TX Beamforming	<p>Select Enabled to turn on both Multi User-MIMO and Transmit Beamforming. This will improve WiFi performance with MU MIMO-compatible wireless clients.</p> <p>Multi User-MIMO allows the NBG6615 to communicate with multiple wireless clients simultaneously, dividing its bandwidth evenly among all MIMO-compatible wireless clients and keeping the WiFi signal constant for them all.</p> <p>Transmit Beamforming lets the NBG6615 focus its signals directly to wireless clients to effectively extend wireless coverage and minimize dead spots.</p>
Apply	Click Apply to save your changes to the NBG6615.
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 2.5G/5G> WPS** tab.

Figure 38 Network > Wireless LAN (2.4G/5G)> WPS

WPS Setup

Enable WPS

Enable Disable PIN Number

WPS Status:

WPS Status: Configured UnConfigured

Reset to UnConfigured

Current Key Info:

Authentication	Encryption	Key
WPA2 PSK	AES	

Apply **Reset**

The following table describes the labels in this screen.

Table 17 Network > Wireless LAN (2.4G/5G)> WPS

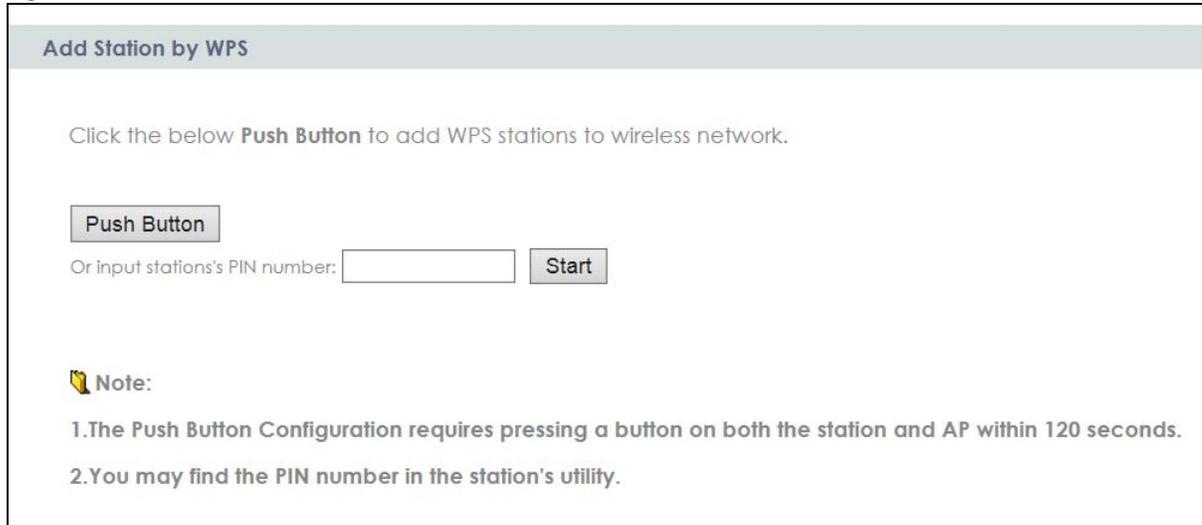
LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Click the Enable WPS check box to enable the WPS feature. Click again to disable it.
PIN Number	This displays a PIN number last time system generated. Click Generate to generate a new PIN number.
WPS Status	
WPS Status	This displays Configured when the NBG6615 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 NBG6615 or you click Reset to Unconfigured to remove the configured wireless and wireless security settings.
Reset to Unconfigured	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 NBG6615.
Apply	Click Apply to save your changes back to the NBG6615.
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 (2.4G/5G) > 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 39 Network > Wireless LAN (2.4G/5G) > WPS Station



Add Station by WPS

Click the below **Push Button** to add WPS stations to wireless network.

Push Button

Or input stations's PIN number: **Start**

Note:

1. The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2. You may find the PIN number in the station's utility.

The following table describes the labels on this screen.

Table 18 Network > Wireless LAN (2.4G/5G) > WPS Station

LABEL	DESCRIPTION
Push Button	Use this button when you use the Push Button Configuration method to configure wireless station's wireless settings. See Section 5.3.1 on page 40 . 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 41 . 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 (2.4G/5G) > Scheduling** tab.

Figure 40 Network > Wireless LAN (2.4G/5G)> Scheduling

Enable	Day	From	To
<input type="checkbox"/>	Everday	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Monday	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Tuesday	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Wednesday	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Thursday	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Friday	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Saturday	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Sunday	00 (hour) 00 (min)	00 (hour) 00 (min)

The following table describes the labels on this screen.

Table 19 Network > Wireless LAN (2.4G/5G)> Scheduling

LABEL	DESCRIPTION
Enable Wireless LAN Scheduling	Select this to enable Wireless LAN scheduling.
Enable	Select to turn on the Wireless LAN. This field works in conjunction with the Day and From/To 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 From/To fields.
From/To	Note: 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. Entering the same begin time and end time will mean the whole day.
Apply	Click Apply to save your changes back to the NBG6615.
Reset	Click Reset to reload the previous configuration for this screen.

6.10 MBSSID Screen

Use this screen to enable and set multiple SSIDs (MBSSID) on the NBG6615. You can then assign varying security types to different SSIDs. Wireless clients can use different SSIDs to associate with the NBG6615. Click **Network > Wireless LAN > MBSSID** to open the following screen.

Figure 41 Network > Wireless LAN (2.5G/5G)> MBSSID

Select	Scheme	SSID	Security	Status	SSID Broadcast
<input checked="" type="radio"/>	1	Zyxel_SSID1	None	Inactive	Active
<input type="radio"/>	2	Zyxel_SSID2	None	Inactive	Active
<input type="radio"/>	3	Zyxel_SSID3	None	Inactive	Active
<input type="radio"/>	4	Zyxel_SSID4	None	Inactive	Active

Wireless Settings--Profile 1

Enable Guest Network
 Enable SSID Broadcast
 Allow Guest to access My Local Network
 Enable Wireless Isolation

Name(SSID)

Security Options--Profile 1

Security Mode

Note: No security(None) and WPA2-PSK can be configured ONLY when WPS is enabled.

The following table describes the labels on this screen.

Table 20 Network > Wireless LAN (2.4G/5G)> 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 .
Status	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.
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 NBG6615.
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 NBG6615.
Name (SSID)	This field displays the SSID name you selected using the select radio button.
Security Options--Profile 1	

Table 20 Network > Wireless LAN (2.4G/5G)> MBSSID

LABEL	DESCRIPTION
Security Mode	<p>Select WPA2-PSK or WPA-PSK/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.</p> <p>Or you can select None to allow any client to associate this network without any data encryption or authentication.</p> <p>See Section 6.4 on page 57 for more details about this field.</p>
Apply	Click Apply to save your changes back to the NBG6615.
Reset	Click Reset to reload the previous configuration for this screen.

CHAPTER 7

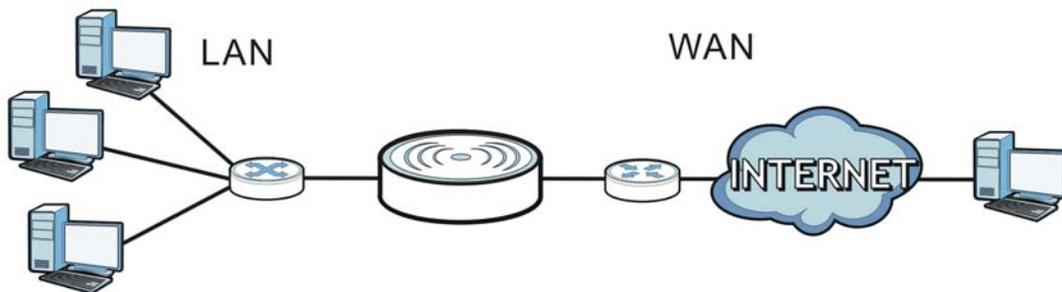
WAN

7.1 Overview

This chapter discusses the NBG6615's **WAN** screens. Use these screens to configure your NBG6615 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 42 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 NBG6615.

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 NBG6615, which makes it accessible from an outside network. It is used by the NBG6615 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG6615 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 NBG6615 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 NBG6615'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 NBG6615's Internet access settings. Click **Network > WAN**. The screen differs according to the connection type you choose.

7.3.1 Static IP

This screen displays when you select **Static IP**.

Figure 43 Network > WAN > Internet Connection: Static IP

The screenshot shows the 'Internet Connection' configuration page in the 'Advanced' tab. The page is titled 'ISP Parameters for Internet Access' and contains several sections:

- Connection Type:** A dropdown menu set to 'Static IP'.
- IP Address:** A text input field containing '172.1.1.1'.
- Subnet Mask:** A text input field containing '255.255.255.0'.
- Default Gateway:** A text input field containing '172.1.1.254'.
- MTU Size:** A text input field containing '1500' with a note '(1400-1500 bytes)'.
- DNS Servers:** Two text input fields. The first contains '172.21.5.1' and the second contains '172.21.6.1'.
- WAN MAC Address:** Three radio button options:
 - Factory default
 - clone the computer's MAC address
 - Set WAN MAC Address
 A text input field next to the third option contains '00:05:1D:54:55:12'.

At the bottom of the page, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels on this screen.

Table 21 Network > WAN > Internet Connection: Static IP

LABEL	DESCRIPTION
ISP Parameters for Internet Access (Static IP)	
Connection Type	Choose the Static IP when the WAN port is used as a regular Ethernet.
IP Address	Enter your WAN IP address in this field.
Subnet Mask	Enter the Subnet Mask in this field.
Default Gateway	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 NBG6615 divides it into smaller fragments. Allowed values are 576 to 1500. By default this value is 1500
First DNS Server	Enter the first and second DNS server's IP address in the fields.
Second DNS Server	
WAN MAC Address	
The MAC address section allows users to configure the WAN port's MAC address by either using the NBG6615's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.	
Factory default	Select this option to use the factory assigned default MAC Address.

Table 21 Network > WAN > Internet Connection: Static IP

LABEL	DESCRIPTION
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 NBG6615. 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 NBG6615.
Reset	Click Reset to begin configuring this screen afresh.

7.3.2 DHCP Client

Select **DHCP Client** when your network administrator or ISP assigns your IP address dynamically.

Figure 44 Connection Type: DHCP Client

ISP Parameters for Internet Access

Connection Type: DHCP Client ▼

MTU Size: 1500 (1280-1500 bytes)

DNS Servers

Attain DNS Automatically Set DNS Manually

First DNS Server: 172.21.5.1

Second DNS Server: 172.21.6.1

WAN MAC Address

Factory default

clone the computer's MAC address

Set WAN MAC Address: 00:05:1D:54:55:12

Apply Reset

The following table describes the labels on this screen.

Table 22 Connection Type: DHCP Client

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Select DHCP Client if your ISP dynamically assigns an IP address on 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 NBG6615 divides it into smaller fragments. Allowed values are 576 to 1500. By default this value is 1500.
DNS Servers	
Attain DNS Automatically	Click the Attain DNS Automatically button if your ISP dynamically assigns DNS server information (and the NBG6615's WAN IP address).
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	If you selected Set DNS Manually , 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 NBG6615's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.	
Factory default	Select this option 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 on the screen) from which you are configuring the NBG6615. 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 NBG6615.
Reset	Click Reset to begin configuring this screen afresh.

7.3.3 PPPoE Connection

The NBG6615 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 NBG6615 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG6615 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 45 Network > WAN > Internet Connection: PPPoE

The following table describes the labels on this screen.

Table 23 Network > WAN > Internet Connection: PPPoE

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 (AC)	Type the PPPoE service name provided by your ISP. PPPoE uses a service name to identify and reach the PPPoE server.
Connection Type	Select Continuous if you do not want the connection to time out. Select Connect 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.

Table 23 Network > WAN > Internet Connection: PPPoE (continued)

LABEL	DESCRIPTION
Idle Time	This field is available only when you select Connect on Demand . Specify the time in minutes that elapses before the router automatically disconnects from the PPPoE server.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your NBG6615 can receive and process.
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 NBG6615'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 box fields.
WAN MAC Address The MAC address section allows users to configure the WAN port's MAC address by either using the NBG6615's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.	
Factory default	Select this option 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 NBG6615. 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 NBG6615.
Reset	Click Reset to begin configuring this screen afresh.

7.3.4 PPTP Connection

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

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

Figure 46 Network > WAN > Internet Connection: PPTP

The following table describes the labels on this screen.

Table 24 Network > WAN > Internet Connection: PPTP

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	To configure a PPTP client, you must configure the User Name and Password fields for a PPP connection and the PPTP parameters for a PPTP connection. Use the radio buttons to select either Dynamic IP (DHCP) or Static IP .
IP Address	If you selected Static IP , enter the IP Address provided by your network administrator or ISP.
Subnet Mask	If you selected Static IP , enter the subnet mask provided by your network administrator or ISP.
Default Gateway	If you selected Static IP , enter the gateway provided by your network administrator or ISP. Use the radio buttons to select either Attain the Server by Domain Name or Attain the Server by Ip Address .
Domain Name	If you selected Attain the Server by Domain Name , enter server domain address provided by your network administrator or ISP in this field.
Server IP Address	Type the IP address of the PPTP server.

Table 24 Network > WAN > Internet Connection: PPTP (continued)

LABEL	DESCRIPTION
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Connection Type	Select Continuous if you do not want the connection to time out. Select Connect 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.
Idle Time	This field is available only when you select Connect on Demand . Specify the time in minutes that elapses before the router automatically disconnects from the PPPoE server.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your NBG6615 can receive and process.
DNS Servers	
Attain DNS Automatically/ Set DNS Manually	Click Attain DNS Automatically radio button if your ISP dynamically assigns DNS server information (and the NBG6615'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 box fields.
WAN MAC Address The MAC address section allows users to configure the WAN port's MAC address by either using the NBG6615's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.	
Factory default	Select this option 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 NBG6615. 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 NBG6615.
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 47 Network > WAN > Advanced

The following table describes the labels on this screen.

Table 25 Network > WAN > Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast Proxy & Snooping	Select Multicast Proxy & Snooping to enable both functions on the NBG6615. Multicast proxy 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 allows the NBG6615 to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.
Apply	Click Apply to save your changes back to the NBG6615.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 8

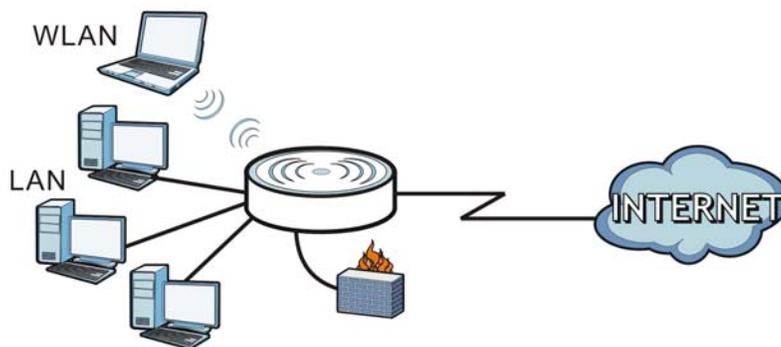
LAN

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.

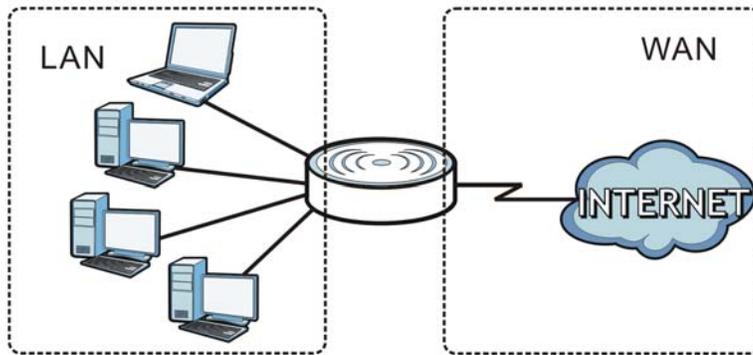
Figure 48 LAN Setup



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 NBG6615 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 49 LAN and WAN IP Addresses

The LAN parameters of the NBG6615 are preset in the factory with the following values:

- IP address of 192.168.212.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 128 client IP addresses starting from 192.168.212.33.

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, 192.168.212.1, for your NBG6615, 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 NBG6615 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 NBG6615 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 NBG6615 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 NBG6615 is pre-configured with a pool of 128 IP addresses starting from 192.168.212.33 to 192.168.212.160. This configuration leaves 31 IP addresses (excluding the NBG6615 itself) in the lower range (192.168.212.2 to 192.168.212.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

8.2.4 LAN TCP/IP

The NBG6615 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 50 Network > LAN > IP

The screenshot shows the 'LAN TCP/IP' configuration screen. It features three input fields for network settings: IP Address (192.168.1.1), Subnet Mask (255.255.255.0), and Default Gateway (192.168.1.1). The Subnet Mask field includes a hint '(ex. 255.255.255.X)'. Below the input fields are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 26 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your NBG6615 in dotted decimal notation 192.168.212.1 (factory default).

Table 26 Network > LAN > IP (continued)

LABEL	DESCRIPTION
Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG6615 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 NBG6615.
Default Gateway	This is the router's LAN IP address. Your NBG6615 will update the default gateway automatically based on the IP address that you entered.
Apply	Click Apply to save your changes back to the NBG6615.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 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 NBG6615's LAN as a DHCP server or disable it. When configured as a server, the NBG6615 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 82](#)).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses ([Section 9.5 on page 83](#)).
- Use the **Client List** screen to view the current DHCP client information ([Section 9.6 on page 84](#)).

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 Server > Client List** screen.

Refer to [Section 8.2.1 on page 79](#) for information on IP Address and Subnet Mask.

Refer to the [Section 8.2.2 on page 79](#) 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 will be displayed.

Figure 51 Network > DHCP Server > General

The following table describes the labels on this screen.

Table 27 Network > DHCP Server > General

LABEL	DESCRIPTION
DHCP Mode	Select DHCP server from the drop-down list to have the NBG6615 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 NBG6615 acting as a DHCP server. When configured as a server, the NBG6615 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. The default is 120 minutes and the maximum is 525600 minutes.
DNS Server1	Type the First DNS server IP address of the DHCP server.
DNS Server2	Type the Second DNS server IP address of the DHCP server.
Apply	Click Apply to save your changes back to the NBG6615.
Reset	Click Reset to begin configuring this screen afresh.

9.5 Static DHCP 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 NBG6615 sends to the DHCP clients.

To change your NBG6615's static DHCP settings, click **Network > DHCP Server > Static DHCP**. The following screen will be displayed.

Figure 52 Network > DHCP Server > Static DHCP

The screenshot shows a web interface for configuring static DHCP entries. It includes two text input fields for 'IP Address' and 'MAC Address'. Below the inputs are five buttons: 'Add', 'Update', 'Select All', 'Delete', and 'Reset'. At the bottom, a table header is visible with columns for 'IP Address', 'MAC Address', and 'Select'.

The following table describes the labels on this screen.

Table 28 Network > DHCP Server > Static DHCP

LABEL	DESCRIPTION
Static DHCP Table	
IP Address	Type the LAN IP address of a computer on your LAN.
MAC Address	Type the MAC address of a computer on your LAN.
Add	Click Add button to add a new static DHCP entry.
Update	Click Update button to modify the selected entry's settings.
Select All	Click Select All to select all static DHCP entries in the DHCP Static IP Table.
Delete	Click Delete button to delete the selected static DHCP entry in the DHCP Static IP Table.
Reset	Click Reset to clear the IP Address and MAC address box fields.
DHCP Static IP Table	
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.
Select	Click the Select radio button to select a static DHCP entry.

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 NBG6615'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 on the **Status** screen.

The following screen will be displayed.

Figure 53 Network > DHCP Server > Client List

DHCP Client Table				
#	Host Name	IP Address	MAC Address	Reserve
1	TWPCZT02727-01	192.168.1.33	1078d2c519cd	<input type="checkbox"/>
2	none	192.168.1.36	00e086710502	<input type="checkbox"/>

The following table describes the labels on this screen.

Table 29 Network > DHCP Server > Client List

LABEL	DESCRIPTION
#	This is the index number of the host computer.
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	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.
Reserve	Select this if you want to reserve the IP address for this specific MAC address.
Apply	Click Apply to save your changes back to the NBG6615.
Refresh	Click Refresh to reload the DHCP table.

CHAPTER 10

Network Address Translation

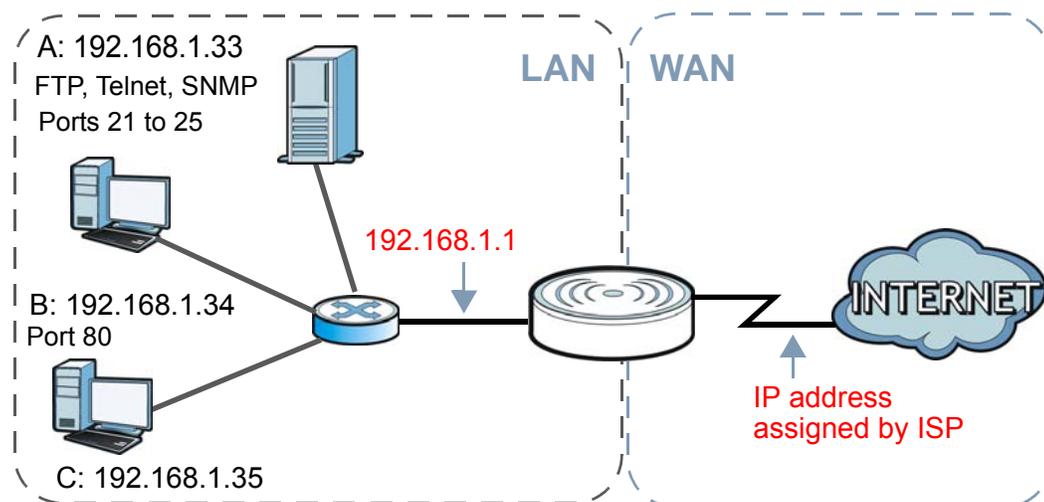
10.1 Overview

This chapter discusses how to configure NAT on the NBG6615.

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 NBG6615 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 54 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 NBG6615.

10.2 What You Can Do

- Use the **General** screen to enable NAT and set a default server ([Section 10.3 on page 88](#)).

- Use the **Application** screen to change your NBG6615's port forwarding settings ([Section 10.4 on page 89](#)).
- Use the **Port Triggering** screen to change your NBG6615's port trigger settings ([Section 10.5 on page 91](#)).

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 NBG6615, 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 30 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.

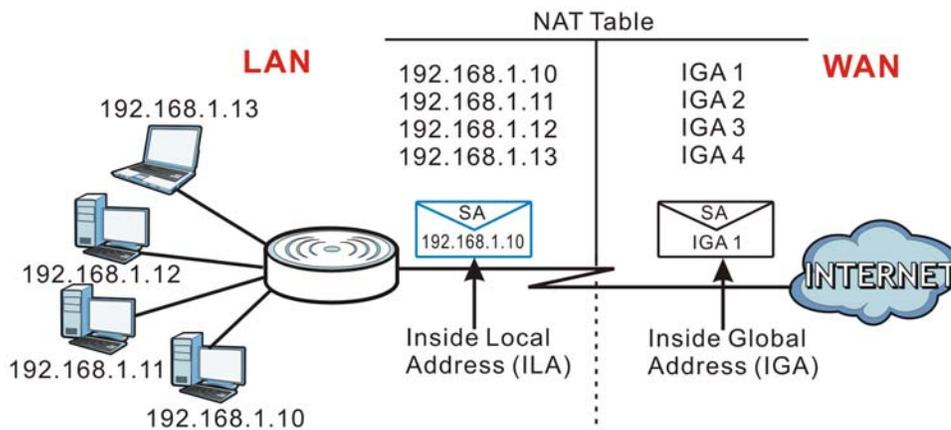
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your NBG6615 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 NBG6615 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 55 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 56 Network > NAT > General

NAT Setup

NAT : Enable Disable

Default Server Setup

Enable

Server IP Address

.....

.....

Apply Reset

The following table describes the labels on this screen.

Table 31 Network > NAT > General

LABEL	DESCRIPTION
NAT Setup	
NAT	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). Use the radio buttons to Enable or Disable the NAT.
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 NBG6615 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 NBG6615.
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 NBG6615'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 NBG6615 discards all packets received for ports that are not specified in this screen or remote management.

Refer to [Appendix E on page 198](#) for port numbers commonly used for particular services.

Figure 57 Network > NAT > Application

Add Application Rule

Application name: AUTH
 User-Defined Application name:
 Protocol: Both
 Public Port Range: 113 - 113
 Local Port Range: 113 - 113
 Server IP Address:

Apply Reset

Application Rules Summary

Application name	Server IP Address	Protocol	Local Port Range	Public Port Range	Select
------------------	-------------------	----------	------------------	-------------------	--------

Select All Delete

The following table describes the labels on this screen.

Table 32 Network > NAT > Application

LABEL	DESCRIPTION
Add Application Rule	
Application 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 Application Name	Type a name (of up to 31 printable characters) to identify this rule. Otherwise, select a predefined service in the Application Name drop-down list.
Protocol	Select the transport layer protocol used for the service. Choices are TCP , and UDP .
Public Port Range	Type a port number(s) to be forwarded.
Local Port Range	To specify a range of ports, enter a colon (:) between the first port and the last port, such as 10:20.
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	
Application Name	This field displays a name to identify this rule.
Server IP Address	This field displays the inside IP address of the server.
Protocol	This field displays the transport layer protocol supported by this server.

The following table describes the labels on this screen.

Table 33 Network > NAT > Port Triggering

LABEL	DESCRIPTION
Port Triggering Status	
Nat Port Trigger	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	Enter the starting port in a range of port numbers that causes (or triggers) the NBG6615 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
End Match Port	Enter the ending port in a range of port numbers that causes (or triggers) the NBG6615 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Trigger Protocol	Specify the protocol (UDP , TCP or UDP/TCP) that causes (or triggers) the NBG6615 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Related Port	Enter the starting port in a range of port numbers that a server on the WAN uses when it sends out a particular service. The NBG6615 forwards the traffic with this starting port to the client computer on the LAN that requested the service.
End Related Port	Enter the ending port in a range of port numbers that a server on the WAN uses when it sends out a particular service. The NBG6615 forwards the traffic with this ending port to the client computer on the LAN that requested the service.
Open Protocol	Specify the protocol (UDP , TCP or UDP/TCP) that a server on the WAN uses when it sends out a particular service.
Apply	Click Apply to save your changes back to the NBG6615.
Reset	Click Reset to begin configuring this screen afresh.
Application Rules Summary	
Server Name	This field displays the name of the application rule.
Trigger Protocol	This field displays the protocol that causes (or triggers) the NBG6615 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Port	This field displays the port(s) that causes (or triggers) the NBG6615 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Open Protocol	This field displays the protocol a server on the WAN uses when it sends out a particular service.
Related Port	This field displays the port(s) a server on the WAN uses when it sends out a particular service. The EMG2926-Q10A forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Action	Click Delete to remove the rule.

10.6 Technical Reference

The following section contains additional technical information about the NBG6615 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.

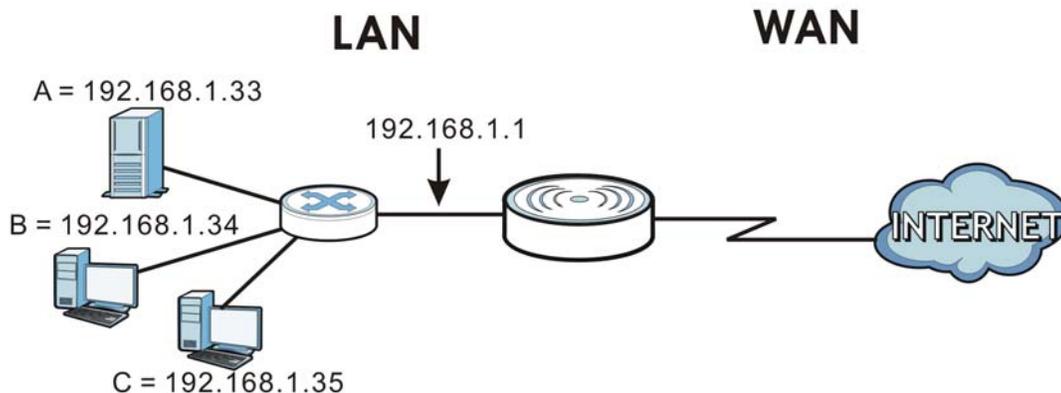
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

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 59 Multiple Servers Behind NAT Example



10.6.3 Trigger Port Forwarding

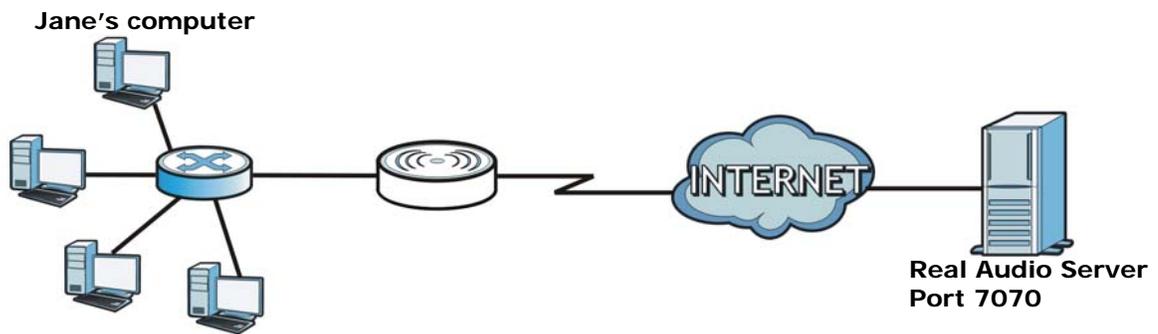
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem 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 NBG6615 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 NBG6615's WAN port receives a response with a specific port number and protocol ("incoming" port), the NBG6615 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 60 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 NBG6615 to record Jane's computer IP address. The NBG6615 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 NBG6615 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 NBG6615 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 NBG6615 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.

CHAPTER 11

Dynamic DNS

11.1 Overview

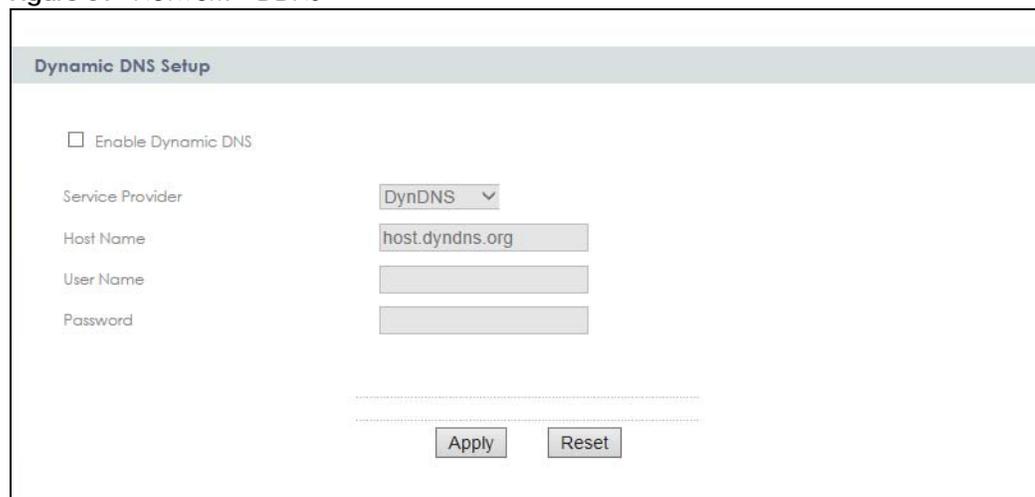
Dynamic Domain Name Service (DDNS) services let you use a fixed domain name with a dynamic IP address. Users can always use the same domain name instead of a different dynamic IP address that changes each time to connect to the NBG6615 or a server in your network.

Note: The NBG6615 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 NBG6615's DDNS, click **Network > DDNS**.

Figure 61 Network > DDNS



The following table describes the labels on this screen.

Table 34 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.

Table 34 Network > DDNS

LABEL	DESCRIPTION
Password	Type the Password associated with the DDNS user name.
Apply	Click Apply to save your changes back to the NBG6615.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 12

Static Route

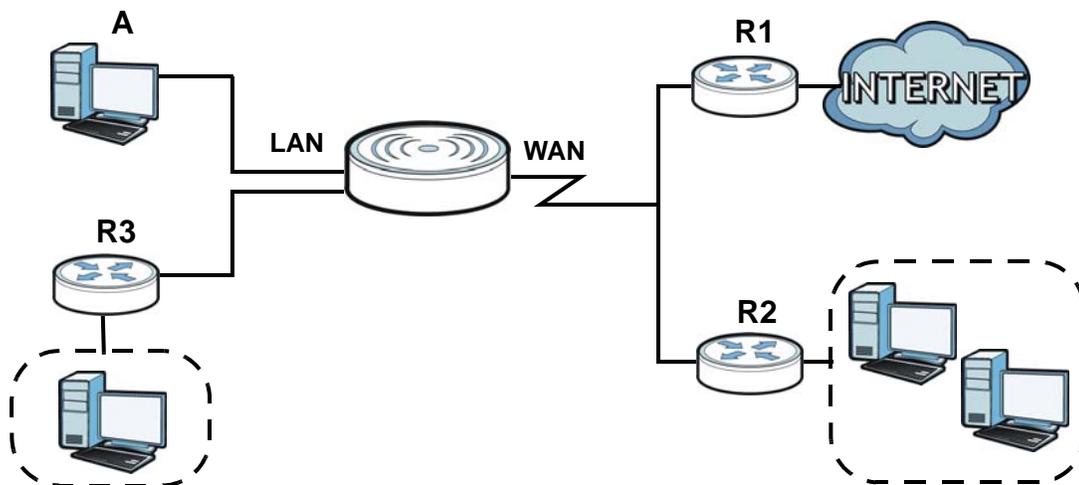
12.1 Overview

This chapter shows you how to configure static routes for your NBG6615.

The NBG6615 usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the NBG6615 send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the NBG6615's LAN interface. The NBG6615 routes most traffic from **A** to the Internet through the NBG6615's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 62 Example of Static Routing Topology



12.2 IP Static Route Screen

Click **Network > Static Route** to open the **Static Route** screen.

Figure 63 Network > Static Route

The screenshot shows the 'Static Route Setup' configuration page. It includes a checkbox for 'Enable', and input fields for 'Destination', 'IP Subnet Mask', 'Gateway', and 'Metric'. Below these fields are four buttons: 'Apply', 'Update', 'Select All', and 'Delete'. The 'Static Route Table' section below shows a header with columns for 'Destination', 'Subnet Mask', 'NextHop', 'Metric', and 'Select', and a note indicating 'Max rule number 32'.

The following table describes the labels on this screen.

Table 35 Network > Static Route

LABEL	DESCRIPTION
Enable	Select this to enable this rule.
Destination	Enter the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your NBG6615's interface(s). The gateway helps forward packets to their destinations.
Metric	The metric represents the "cost of transmission." A router determines the best route for transmission by choosing a path with the lowest "cost." The smaller the number, the lower the "cost". Enter the number of transmission hops (routers) that need to cross from the NBG6615 to the destination.
Apply	Click Apply to save your changes back to the NBG6615.
Update	Click this to modify the selected rule.
Select All	Click this to select all rules in the Static Route Table.
Delete	Click this to remove the selected rule in the Static Route Table.
Static Route Table	
T	
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
NextHop	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.

Table 35 Network > Static Route

LABEL	DESCRIPTION
Metric	This is the number of transmission hops between the NBG6615 and the destination.
Select	Click this to select the rule.

CHAPTER 13

Firewall

13.1 Overview

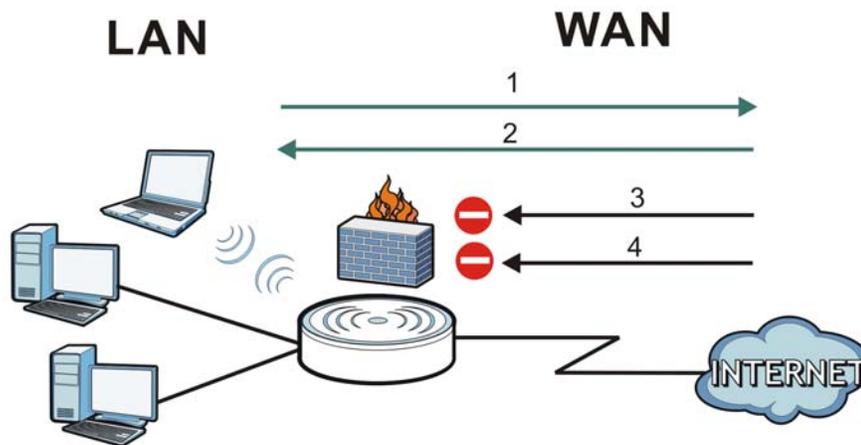
Use these screens to enable and configure the firewall that protects your NBG6615 and your LAN from unwanted or malicious traffic.

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 64 Default Firewall Action



13.2 What You Can Do

- Use the **General** screen to enable or disable the NBG6615's firewall ([Section 13.4 on page 101](#)).
- Use the **Services** screen to enable or disable ICMP and VPN passthrough features ([Section 13.5 on page 102](#)).

13.3 What You Need To Know

The NBG6615's firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

13.3.1 About the NBG6615 Firewall

The NBG6615 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 NBG6615's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG6615 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 NBG6615 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 NBG6615 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.

13.3.2 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 NBG6615 is not one of the endpoints but it does allow traffic from those endpoints to pass through. The NBG6615 allows the following types of VPN traffic to pass through:

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

13.4 General Firewall Screen

Use this screen to enable or disable the NBG6615's firewall, and set up firewall logs. Click **Security > Firewall** to open the **General** screen.

Figure 65 Security > Firewall > General

The screenshot shows a web interface for 'Firewall Setup'. It has a header bar with the title 'Firewall Setup'. Below the header, there are two checkboxes: 'Enable Firewall' which is checked, and 'Enable DoS Defense' which is unchecked. At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels on this screen.

Table 36 Security > Firewall > General

LABEL	DESCRIPTION
Enable Firewall	Select this option to activate the firewall. The NBG6615 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Enable DoS Defense	Select this option to protect against DoS attacks. The NBG6615 will drop sessions that do not become fully established (half-open sessions) and surpass maximum thresholds.
Apply	Click Apply to save the settings.
Reset	Click Reset to start configuring this screen again.

13.5 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 66 Security > Firewall > Services

The screenshot shows a web interface for 'Services'. It has a header bar with the title 'ICMP'. Below the header, there is one checkbox: 'Respond to Ping on WAN' which is unchecked. Below this, there is a section titled 'VPN Passthrough' with three checkboxes: 'IPsec Passthrough' (checked), 'PPTP Passthrough' (checked), and 'L2TP Passthrough' (checked). At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels on this screen.

Table 37 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 NBG6615 will not respond to any incoming Ping requests when the check box is not selected. Select the check box to reply to incoming WAN Ping requests.
VPN Passthrough	Select the checkbox to enable the advanced pass through features: <ul style="list-style-type: none"> • IPSEC Passthrough: Select this option to allow the NBG6615 to pass through VPN traffic using the IPsec protocol. • PPTP Passthrough: Select this option to allow the NBG6615 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. •
Apply	Click Apply to save the settings.
Reset	Click Reset to start configuring this screen afresh.

13.6 MAC Filter Screen

Use this screen to enable or disable MAC address filtering, which enables selected MAC addresses to bypass the firewall.

Click **Security > Firewall > MAC Filter Screen**. The screen appears as shown next.

Figure 67 Security > Firewall > Services

The screenshot shows the 'MAC Filtering Rule' configuration interface. It includes a checkbox for 'Enable MAC Filtering'. Below this are two input fields: 'MAC Address' (with a placeholder example '00E086710502') and 'Comment'. At the bottom of the form are 'Apply' and 'Reset' buttons. Below the form is a section titled 'Current Filter Table' with a table header containing 'MAC Address', 'Application name', and 'Select'.

The following table describes the labels on this screen.

Table 38 Security > Firewall > MAC Filter

LABEL	DESCRIPTION
Enable MAC Filtering	Select Enable to turn on MAC address filtering.
MAC Address	Enter the MAC addresses that are to be whitelisted by the firewall. The entry should be in a valid MAC address format (that is, six hexadecimal character pairs). Example: 12:34:56:78:9a:8c. Do not use colons when entering the MAC address.
Comment	This field can be used to add identifying information or other notes about MAC addresses in the whitelist or blacklist.
Apply	Click Apply to save the settings.
Reset	Click Reset to start configuring this screen afresh.
Current Filter Table	
MAC Address	This field shows the list of allowed MAC addresses.
Application name	This field shows identifying information or other notes about the allowed MAC addresses.
Select	Click to select the entry you wish to edit.

Content Filter

13.7 Overview

Content filter allows you to block specific URLs.

The NBG6615 checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL `www.zyxel.com.tw/news/pressroom.php`, the domain name is `www.zyxel.com.tw`.

The file path is the characters that come after the first slash in the URL. For example, with the URL `www.zyxel.com.tw/news/pressroom.php`, the file path is `news/pressroom.php`.

Since the NBG6615 checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL `www.zyxel.com.tw/news/pressroom.php`, the NBG6615 would find "tw" in the domain name (`www.zyxel.com.tw`). It would also find "news" in the file path (`news/pressroom.php`) but it would not find "tw/news."

13.8 What You Can Do

- Use the **Filter** screen to block the users on your network from accessing certain web sites ([Section 13.9 on page 105](#)).

13.9 Filter Screen

Use the **Filter** screen to enable keyword blocking and add keywords for blocking.

Click **Security > Content Filter**. The screen appears as shown next.

Figure 68 Security > Content Filter > Filter

The following table describes the labels on this screen.

Table 39 Security > Content Filter > Filter

LABEL	DESCRIPTION
Enable URL Keyword Blocking	The NBG6615 can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http://www.website.com/bad.html would be blocked. Select Enable to turn on this feature. Otherwise, select Disable .
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Apply	Click this after you have typed a keyword to create a new entry in the table below. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Reset	Click this to reconfigure the screen afresh.
Current Filter Table	
Filtered Keyword	This displays the keyword already added.
Select	Click this to select an entry and click Delete Selected Keyword to remove it.

Table 39 Security > Content Filter > Filter (continued)

LABEL	DESCRIPTION
Select All	Click this to select all entries.
Delete	Click this to remove the selected entry.

CHAPTER 14

Remote Management

14.1 Overview

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

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

14.1.1 Remote Management Limitations

Remote management over WAN will not work when:

- 1 You have disabled that service in the remote management screen.
- 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 NBG6615 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.

14.1.2 Remote Management and NAT

When NAT is enabled:

- Use the NBG6615's WAN IP address when configuring from the WAN.
- Use the NBG6615's LAN IP address when configuring from the LAN.

14.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The NBG6615 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.

14.2 WWW Screen

To change your NBG6615's World Wide Web settings, click **Management > Remote MGMT** to display the **WWW** screen.

Figure 69 Management > Remote MGMT > WWW

The screenshot shows the 'WWW' configuration page. At the top, there is a header 'WWW'. Below it, there are three main settings:

- Enable HTTP from the WAN side
- Server Port: (Apply for remote WAN site only)
- Secured Client WAN IP Address: All Selected

At the bottom of the form, there are two buttons: **Apply** and **Reset**.

The following table describes the labels on this screen.

Table 40 Management > Remote MGMT > WWW

LABEL	DESCRIPTION
Enable HTTP from the WAN side	Click the check box to configure your NBG6615 via HTTP using a web browser through the WAN interface.
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 NBG6615 using this service. Select All to allow any computer to access the NBG6615 using this service. Choose Selected to just allow the computer with the IP address that you specify to access the NBG6615 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.

CHAPTER 15

Universal Plug-and-Play (UPnP)

15.1 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.

15.2 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 NBG6615 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.

15.3 Configuring UPnP

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

Figure 70 Management > UPnP > General

The following table describes the labels on this screen.

Table 41 Management > UPnP > General

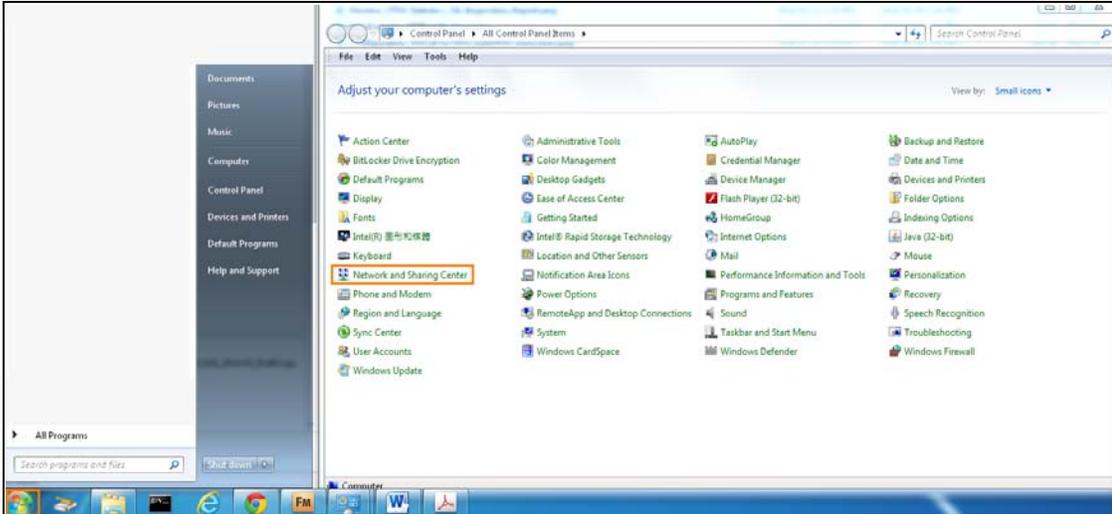
LABEL	DESCRIPTION
Host Name	This field displays the description of the NBG6615 router.
Enable the Universal Plug and Play (UPnP) Feature	Select the Enable the UPnP Features check box to activate UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the NBG6615's IP address (although you must still enter the password to access the Web Configurator).
Apply	Click Apply to save the setting to the NBG6615.
Reset	Click Reset to begin configuring this screen afresh.

15.4 Installing UPnP in Windows 7 Example

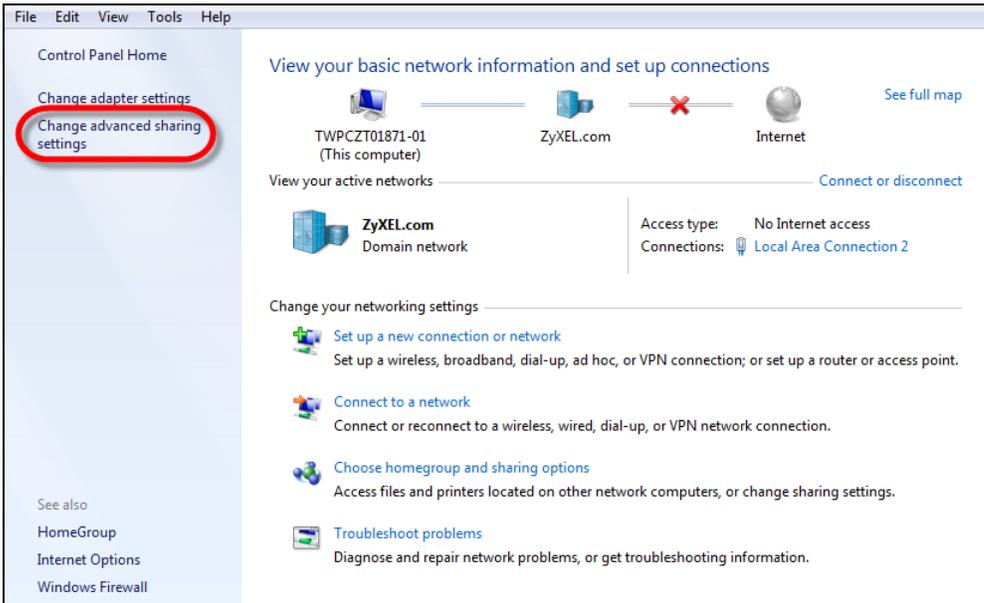
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. You will need to activate UPnP on the NBG6615.

Make sure the computer is connected to a LAN port of the NBG6615. Turn on your computer and the NBG6615.

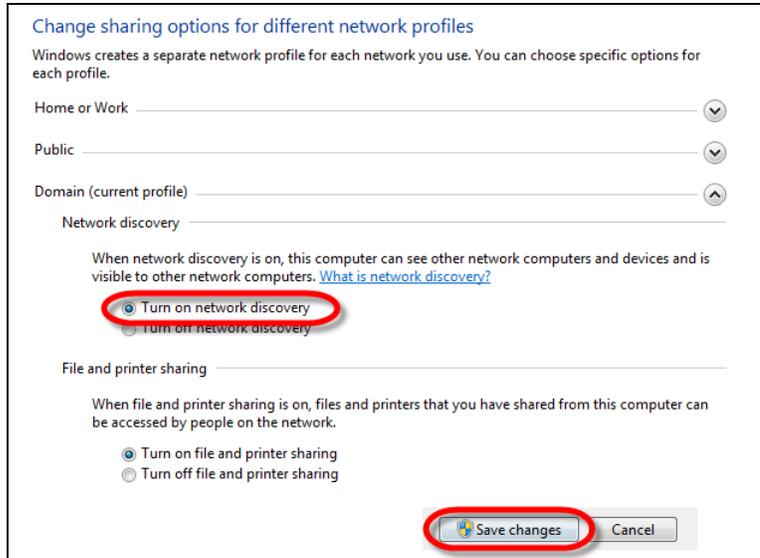
- 1 Click the **Start** icon, **Control Panel** and then the **Network and Sharing Center**.



- 2 Click **Change advanced sharing settings**.



- 3 Under Network Discovery 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.



15.4.1 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 NBG6615.

Make sure the computer is connected to a LAN port of the NBG6615. Turn on your computer and the NBG6615.

15.4.1.1 Auto-discover Your UPnP-enabled Network Device

- 1 Click the **Start** icon and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- 2 Right-click the icon and select **Properties**.

Figure 71 Network Connections



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

Figure 72 Internet Connection Properties



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

Figure 73 Internet Connection Properties: Advanced Settings

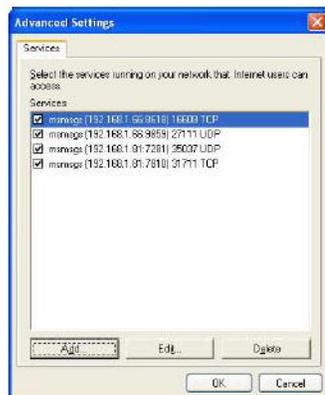


Figure 74 Internet Connection Properties: Advanced Settings: Add



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 75 System Tray Icon

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

Figure 76 Internet Connection Status

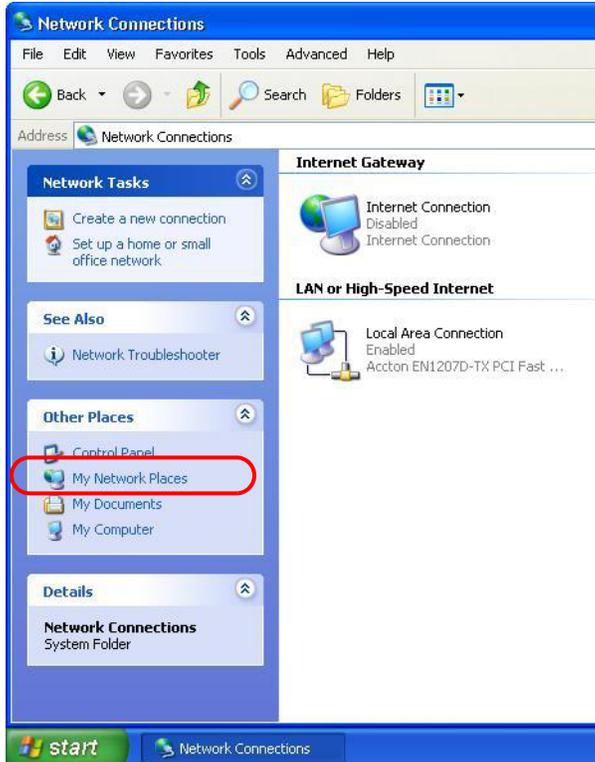
15.4.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the NBG6615 without finding out the IP address of the NBG6615 first. This is helpful if you do not know the IP address of the NBG6615.

Follow the steps below to access the Web Configurator.

- 1 Click the **Start** icon and then **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 Select **My Network Places** under **Other Places**.

Figure 77 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 NBG6615 and select **Invoke**. The Web Configurator login screen will display.

Figure 78 Network Connections: My Network Places



- 6 Right-click on the icon for your NBG6615 and select **Properties**. A properties window displays with basic information about the NBG6615.

Figure 79 Network Connections: My Network Places: Properties: Example



CHAPTER 16

Bandwidth MGMT

16.1 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.

16.2 What You Can Do

- Use the **Bandwidth MGMT** screen to enable this feature in the NBG6615.
- Use the **Advanced** screen to configure the QoS (Quality of Service) rule on the NBG6615.

16.3 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.

16.4 Bandwidth MGMT Screen

Use this screen to enable the bandwidth management feature on the NBG6615. Click **Management > Bandwidth MGMT**. The following screen displays.

Figure 80 Management > Bandwidth MGMT



The following table describes the labels on this screen.

Table 42 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 NBG6615.
Apply	Click Apply to save your changes in t his screen.
Reset	Click Reset to begin configuring this screen afresh.

16.5 Advanced Screen

Use this screen to set up the QoS rules for the NBG6615. Click **Management > Bandwidth MGMT > Advanced**. The following screen will be displayed.

Figure 81 Management > Bandwidth MGMT > Advanced

The screenshot displays the configuration interface for QoS. The top section, titled "QoS Setup", includes input fields for "Total Bandwidth(0, Unlimited):", "UP Stream" (set to 819200 kbps), and "Down Stream" (set to 819200 kbps). Below these fields are "Apply" and "Reset" buttons. The bottom section, titled "QoS Rules", features a table with the following columns: "#", "Source IP Address", "Max Bandwidth(Kbps)" (subdivided into "Up Ceiling" and "Down Ceiling"), and "Delete". At the bottom of this section are "Add", "Select All", and "Delete" buttons.

The following table describes the labels in this screen.

Table 43 Management > Bandwidth MGMT > Advanced

LABEL	DESCRIPTION
QoS Setup	
Total Bandwidth (0, Unlimited)	This field shows the maximum number of data in kbps the NBG6615 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 NBG6615.
Down Stream	Type the Down Stream or maximum incoming transmission data rate (kbps) that is allowed to go through the source interface on the NBG6615.
Apply	Click Apply to save your changes back to the NBG6615.
Reset	Click Reset to begin configuring this screen afresh.
QoS Rules	

Table 43 Management > Bandwidth MGMT > Advanced (continued)

LABEL	DESCRIPTION
#	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 (kpbs) that is allowed to go through the source interface on the NBG6615.
Down Ceiling	This field shows the maximum outgoing transmission data rate (kpbs) that is allowed to go through the source interface on the NBG6615.
Delete	Click the Delete check box to select the QoS rule you want to delete.
Add	Click Add button to add the QoS rule.
Select All	Click to select all entries.
Delete	Click Delete to remove the QoS rule.

CHAPTER 17

System

17.1 Overview

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

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

17.2 What You Can Do

- Use the **General** screen to enter a name to identify the NBG6615 in the network and set the password ([Section 17.3 on page 121](#)).
- Use the **Time Setting** screen to change your NBG6615's time and date ([Section 17.4 on page 122](#)).

17.3 System General Screen

Use this screen to enter a name to identify the NBG6615 in the network and set the password. Click **Maintenance > System**. The following screen will be displayed.

Figure 82 Maintenance > System > General

The screenshot shows a web interface for system configuration. It is divided into two main sections: 'System Setup' and 'Password Setup'. The 'System Setup' section contains three input fields: 'System Name' with the value 'NBG6615', 'Domain Name' with the value 'zyxel.com', and 'Administrator Inactivity Timer' with the value '5' and a note '(minutes, 0 means no timeout)'. The 'Password Setup' section contains three password input fields: 'Old Password', 'New Password', and 'Retype to Confirm', each represented by a box of dots. At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels on this screen.

Table 44 Maintenance > System > General

LABEL	DESCRIPTION
System Setup	
System Name	System Name is a unique name to identify the NBG6615 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. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password Setup	Change your NBG6615'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 NBG6615.
Reset	Click Reset to begin configuring this screen afresh.

17.4 Time Setting Screen

To change your NBG6615's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown. Use this screen to configure the NBG6615's time based on your local time zone.

Figure 83 Maintenance > System > Time Setting

The following table describes the labels in this screen.

Table 45 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NBG6615. Each time you reload this page, the NBG6615 synchronizes the time with the time server.
Current Date	This field displays the date of your NBG6615. Each time you reload this page, the NBG6615 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.
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 .
Copy Your Computer's Time Settings	Click the Copy Your Computer's Time Settings button to copy your computer's time settings into the NBG6615's time and date setup.
Get from Time Server	Select the Get from time server radio button to have the NBG6615 get the time and date from the time server you specified below.
Auto	Select Auto to have the NBG6615 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).
Automatically Adjust for Daylight Saving	Daylight savings 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 NBG6615.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 18

Logs

18.1 Overview

This chapter contains information about configuring general log settings and viewing the NBG6615's logs.

The Web Configurator allows you to look at all of the NBG6615's logs in one location.

18.2 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 on the **View Log** screen. Alerts are displayed in red and logs are displayed 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.

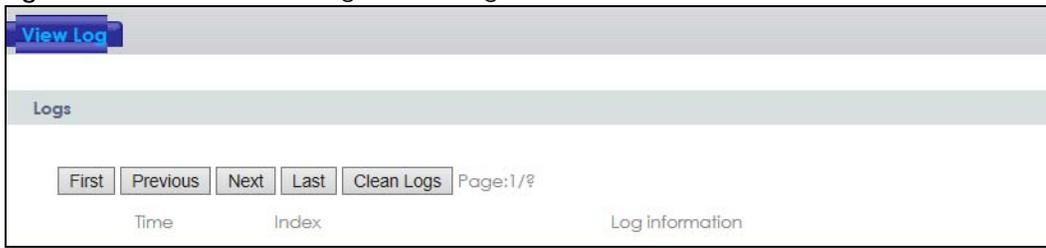
18.3 View Log Screen

Use the **View Log** screen to see the logged messages for the NBG6615. 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 84 Maintenance > Logs > View Log



The following table describes the labels on this screen.

Table 46 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.
Clean Logs	Click Clear Logs to delete all the logs.
Time	This field displays the time the log was recorded.
Index	This is the index number of the log.
Type	This field displays the type of the log.
Log information	This field states the reason for the log.

CHAPTER 19

Tools

19.1 Overview

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the NBG6615.

19.2 What You Can Do

- Use the **Firmware** screen to upload firmware to your NBG6615 ([Section 19.3 on page 126](#)).
- Use the **Configuration** screen to view information related to factory defaults, backup configuration, and restoring configuration ([Section 19.4 on page 128](#)).
- Use the **Restart** screen to have the NBG6615 reboot ([Section 19.5 on page 129](#)).

19.3 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., "NBG6615.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 NBG6615.

Figure 85 Maintenance > Tools > Firmware

The screenshot shows the 'Firmware Upgrade' screen. At the top, there is a title bar 'Firmware Upgrade'. Below it, a paragraph of text reads: 'To upgrade the internal router firmware, browse to the location of the binary (.bin) upgrade file and click Upload. Upgrade files can be downloaded from the Zyxel website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.bin) file. In some cases, you may need to reconfigure.' Below this text, there is a 'File Path:' label followed by a text input field and a 'Browse...' button. Underneath, there is a checkbox labeled 'Automatically reset default after firmware upgraded'. At the bottom of this section, there is a large 'Upload' button. Below the 'Upload' button, there is a section header 'On-line Firmware Upgrade' and a 'Check for Latest Firmware Now' button.

The following table describes the labels in this screen.

Table 47 Maintenance > Tools > Firmware

LABEL	DESCRIPTION
Browse	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 NBG6615 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 NBG6615 search for the latest firmware available online at ZyXEL's website.

Note: Do not turn off the NBG6615 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait for several minutes before logging into the NBG6615 again.

Figure 86 Upload Warning



The NBG6615 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 87 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 88 Upload Error Message



19.4 Configuration Screen

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

Figure 89 Maintenance > Tools > Configuration

The screenshot shows a web interface with three main sections:

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

19.4.1 Backup Configuration

Backup configuration allows you to back up (save) the NBG6615's current configuration to a file on your computer. Once your NBG6615 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 NBG6615's current configuration to your computer.

19.4.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG6615.

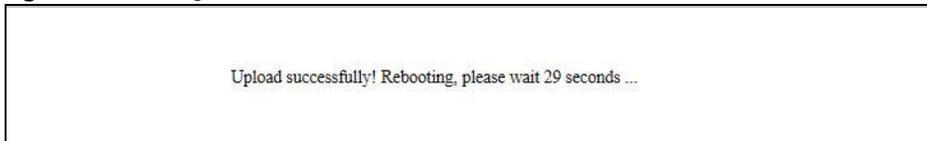
Table 48 Maintenance Restore Configuration

LABEL	DESCRIPTION
Browse	Click Browse 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 NBG6615 while configuration file upload is in progress.

After you see a "configuration upload successful" screen, you must then wait 30 seconds before logging into the NBG6615 again.

Figure 90 Configuration Restore Successful



The NBG6615 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 91 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 NBG6615 IP address (192.168.1.1 in router mode). See [Appendix C on page 158](#) 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 92 Configuration Restore Error



19.4.3 Back to Factory Defaults

Pressing the **Reset to default** button in this section clears all user-entered configuration information and returns the NBG6615 to its factory defaults.

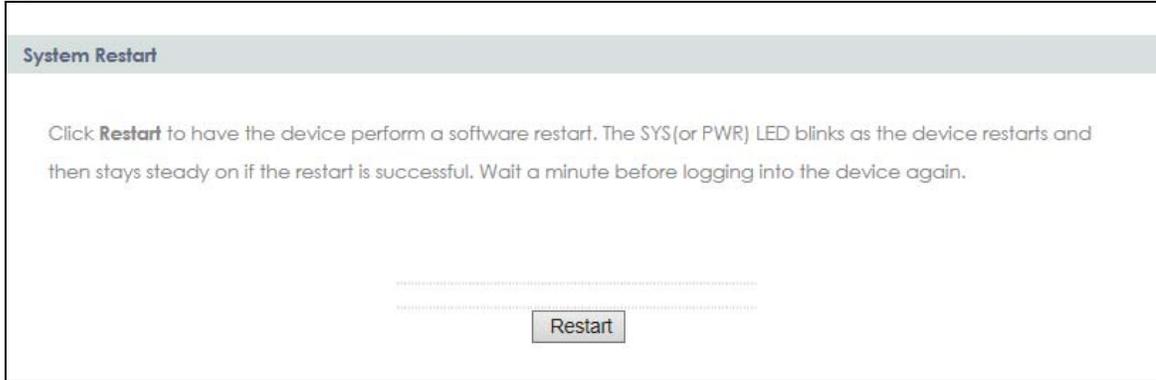
You can also press the **Reset** button on the rear panel to reset the factory defaults of your NBG6615. Refer to [Section 1.4.1 on page 14](#) for more information on the **Reset** button.

19.5 Restart Screen

System restart allows you to reboot the NBG6615 without turning the power off.

Click **Maintenance > Tools > Restart**. Click **Restart** to have the NBG6615 reboot. This does not affect the NBG6615's configuration.

Figure 93 Maintenance > Tools > Restart



CHAPTER 20

Sys OP Mode

20.1 Overview

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

See [Chapter 4 on page 28](#) for more information on which mode to choose.

20.2 General Screen

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

Figure 94 Maintenance > Sys OP Mode > General

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

Table 49 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 NBG6615 (N). The NBG6615 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.

Table 49 Maintenance > Sys Op Mode > General (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your settings.
Reset	Click Reset to return to the previous screen settings.

About the **Router** mode:

- 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 NBG6615 is set to 192.168.212.1.
- You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings.

About the **Access Point** mode:

- In AP mode, all Ethernet ports have the same IP address.
- All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port.
- The DHCP server on your device is disabled. In 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 NBG6615 is set to 192.168.1.2.

CHAPTER 21

Language

21.1 Language Screen

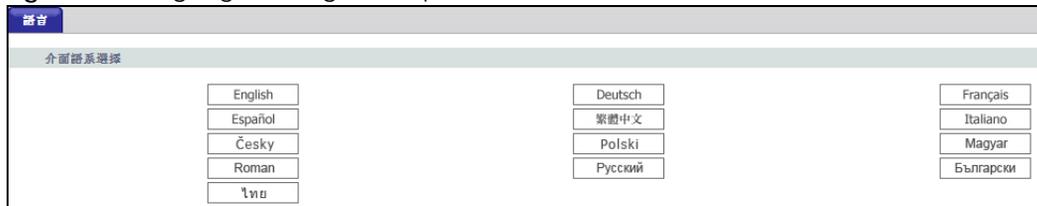
Use this screen to change the language for the Web Configurator display.

Click the language you prefer. The Web Configurator language changes after a while without restarting the NBG6615.

Figure 95 Language



Figure 96 Language Change Example



CHAPTER 22

Troubleshooting

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

- [Power, Hardware Connections, and LEDs](#)
- [NBG6615 Access and Login](#)
- [Internet Access](#)
- [Resetting the NBG6615 to Its Factory Defaults](#)
- [Wireless Problems](#)

22.1 Power, Hardware Connections, and LEDs

[The NBG6615 does not turn on. None of the LEDs turn on.](#)

- 1 Make sure you are using the power adaptor or cord included with the NBG6615.
- 2 Make sure the power adaptor or cord is connected to the NBG6615 and plugged into an appropriate power source. Make sure the power source is turned on.
- 3 Disconnect and re-connect the power adaptor or cord to the NBG6615.
- 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 13](#).
- 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 NBG6615.
- 5 If the problem continues, contact the vendor.

22.2 NBG6615 Access and Login

I don't know the IP address of my NBG6615.

- 1 The default web address in **Router Mode** is `http://192.168.1.1`.
- 2 The default IP address in router mode is **192.168.212.1** and in AP mode is **192.168.1.2**.
- 3 If you changed the IP address and have forgotten it, you might get the IP address of the NBG6615 in **Router Mode** by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter `cmd`, and then enter `ipconfig`. The IP address of the **Default Gateway** might be the IP address of the NBG6615 (it depends on the network), so enter this IP address in your Internet browser.
- 4 Reset your NBG6615 to change all settings back to their default. This means your current settings are lost. See [Section 22.4 on page 138](#) in the **Troubleshooting** for information on resetting your NBG6615.

I forget 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 22.4 on page 138](#).

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 192.168.212.1 (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 NBG6615](#).
- 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 149](#).
- 4 Make sure your computer is in the same subnet as the NBG6615. (If you know that there are routers between your computer and the NBG6615, 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 NBG6615.

- 5 Reset the device to its factory defaults, and try to access the NBG6615 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 NBG6615.

- 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 NBG6615.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 22.4 on page 138](#).

22.3 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 NBG6615), 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 13](#).
- 2 Reboot the NBG6615.
- 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 13](#). If the NBG6615 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 NBG6615 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 NBG6615.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

22.4 Resetting the NBG6615 to Its Factory Defaults

If you reset the NBG6615, you lose all of the changes you have made. The NBG6615 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 NBG6615,

- 1 Make sure the power LED is on.
- 2 Press the **WPS** button for longer than 10 second to reboot and restore factory-default configurations on the NBG6615.

If the NBG6615 restarts automatically, wait for the NBG6615 to finish restarting, and log in to the Web Configurator. The username is **admin** and password is **1234**.

If the NBG6615 does not restart automatically, disconnect and reconnect the NBG6615's power. Then, follow the directions above again.

22.5 Wireless Problems

I cannot access the NBG6615 or ping any computer from the WLAN.

- 1 Make sure the wireless LAN is enabled on the NBG6615.
- 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 NBG6615.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG6615.
- 5 Check that both the NBG6615 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 NBG6615.
- 7 Make sure you allow the NBG6615 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 158](#) for instructions on how to change your computer's IP address.

APPENDIX 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.

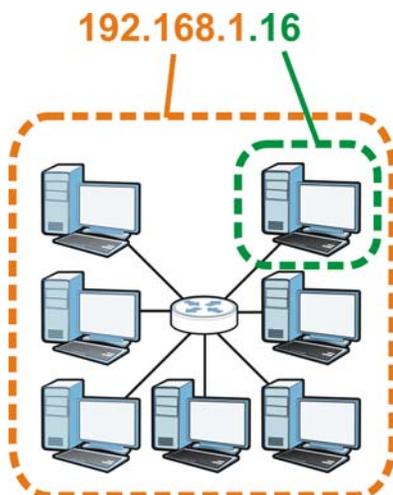
Structure

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 97 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 50 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 51 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 52 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 53 Alternative Subnet Mask Notation

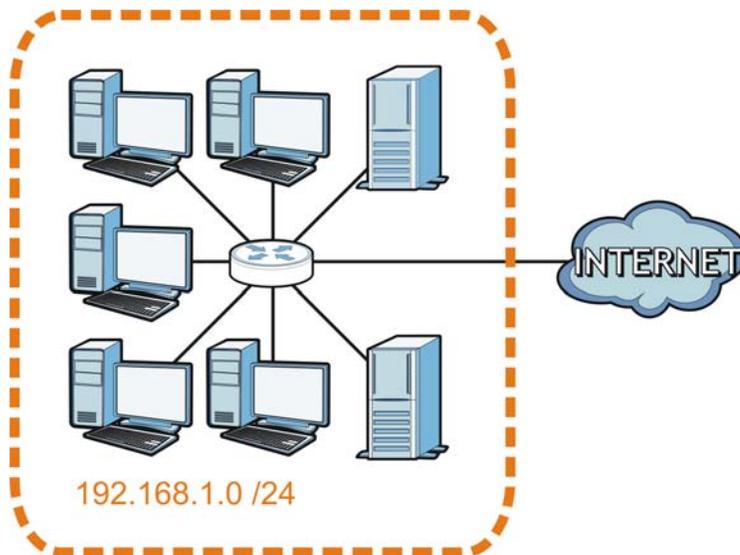
SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	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.

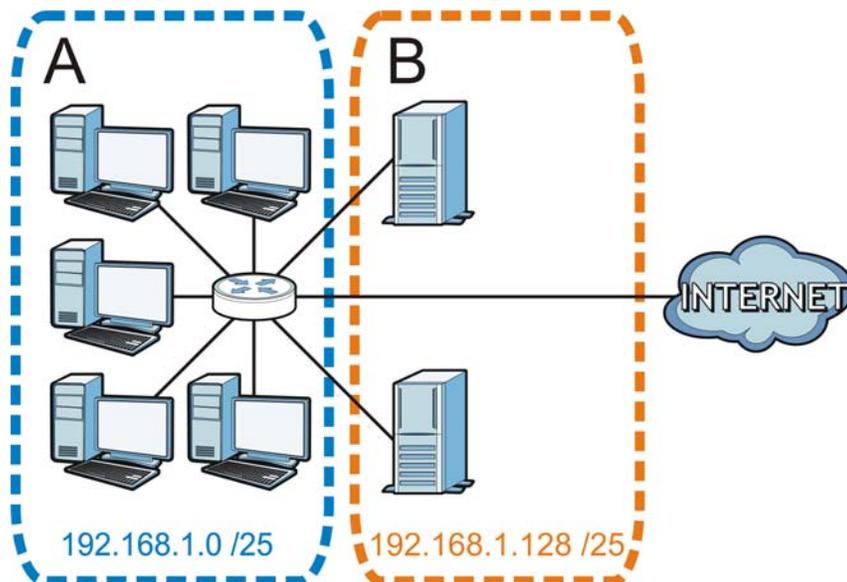
The following figure shows the company network before subnetting.

Figure 98 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 99 Subnetting Example: After Subnetting

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

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

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

Example: Four Subnets

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

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

Table 54 Subnet 1

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

Table 55 Subnet 2

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

Table 56 Subnet 3

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

Table 57 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000

Table 57 Subnet 4 (continued)

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

Example: Eight Subnets

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

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

Table 58 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
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 59 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 60 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

Table 60 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
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 NBG6615.

Once you have decided on the network number, pick an IP address for your NBG6615 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 NBG6615 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 NBG6615 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.

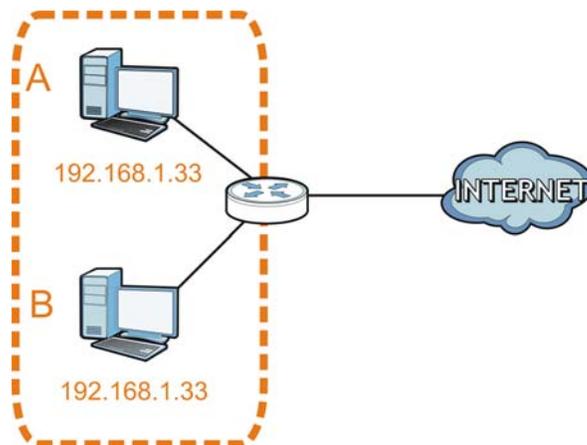
IP Address Conflicts

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

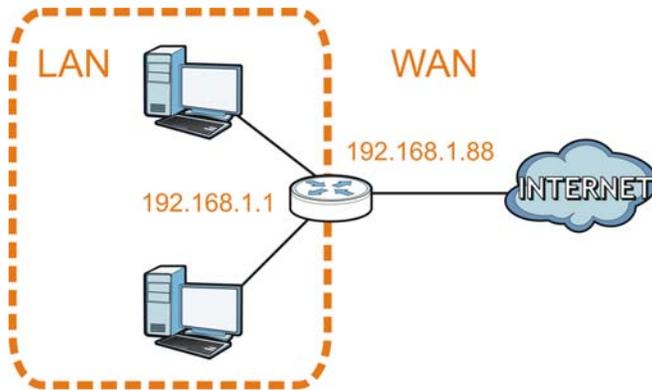
More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

Figure 100 Conflicting Computer IP Addresses Example



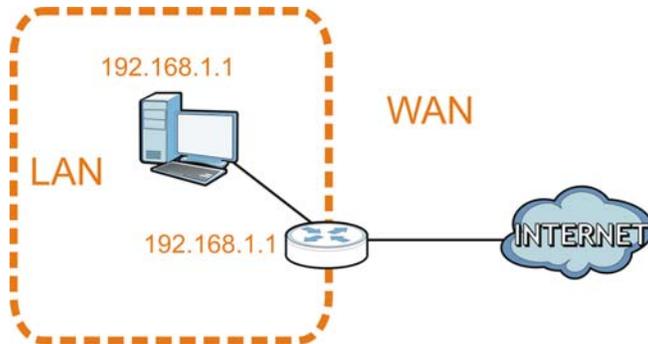
Conflicting Router IP Addresses Example

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 101 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 102 Conflicting Computer and Router IP Addresses Example

APPENDIX 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 103 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 104 Internet Options: Privacy



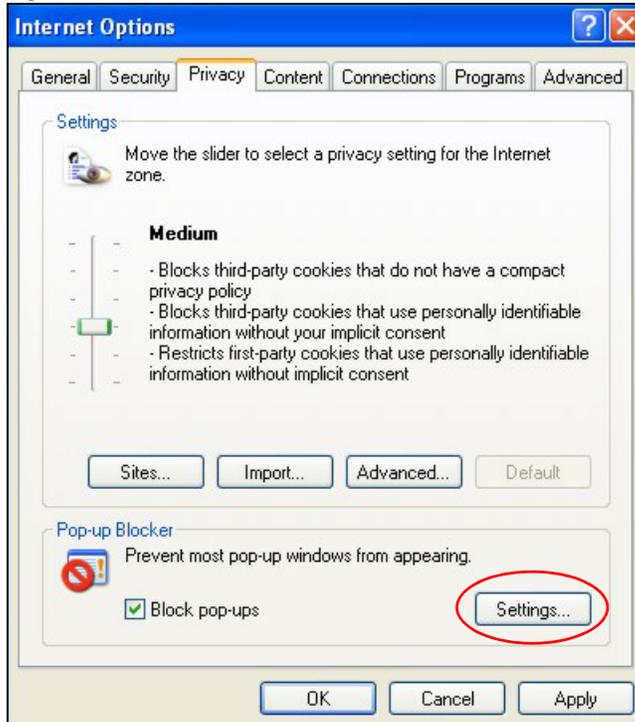
- 3 Click **Apply** to save this setting.

Enable Pop-up Blockers with Exceptions

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

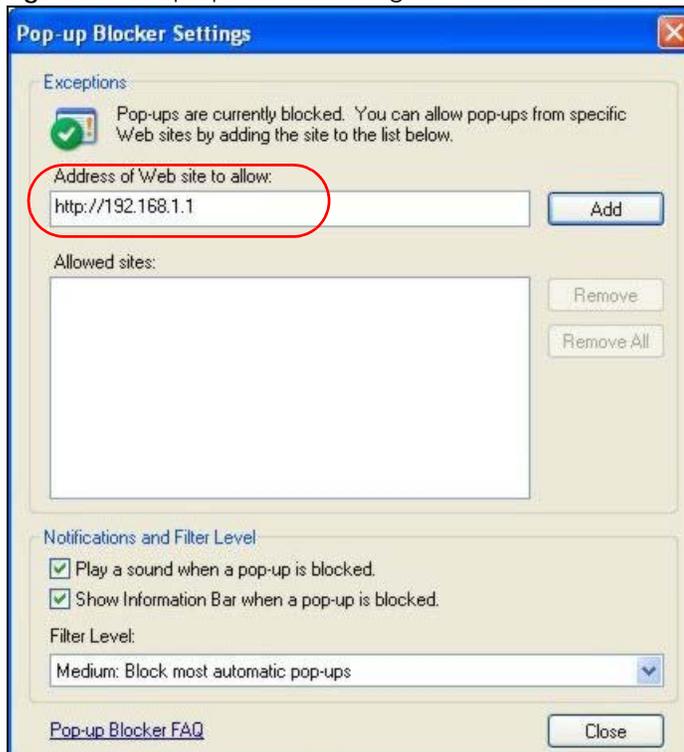
- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

Figure 105 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 106 Pop-up Blocker Settings



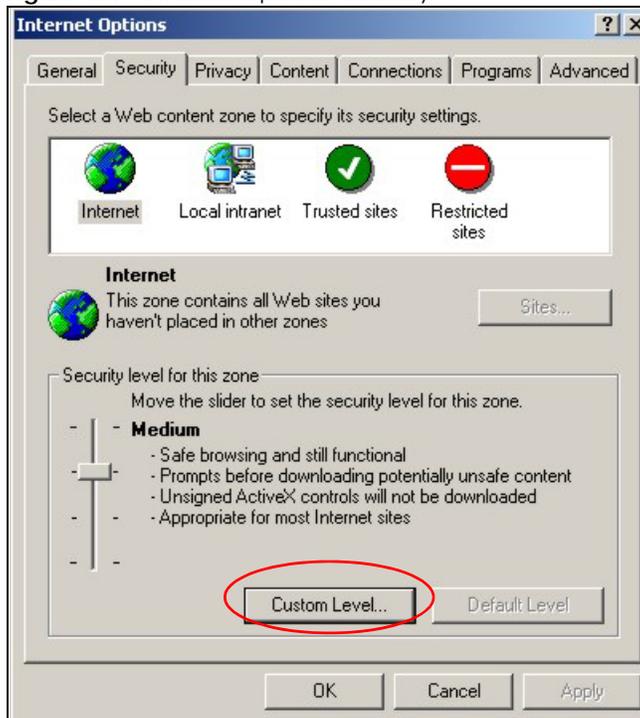
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

JavaScripts

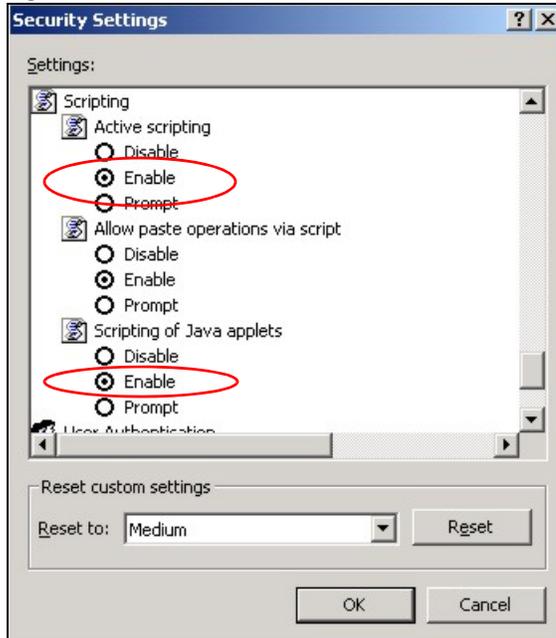
If pages of the Web Configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

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

Figure 107 Internet Options: Security



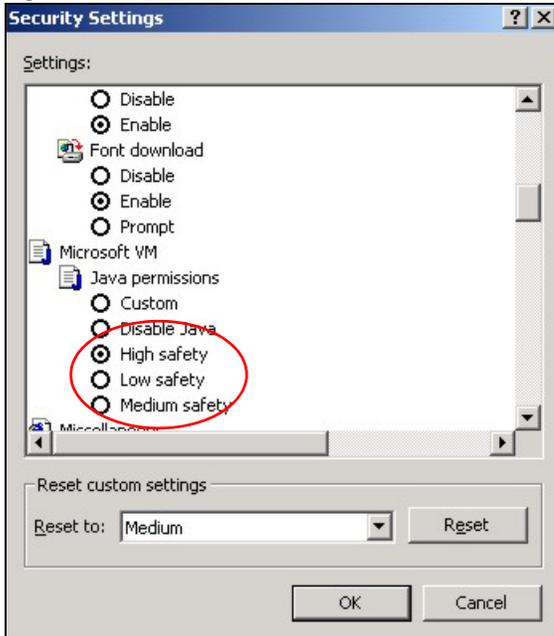
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6 Click **OK** to close the window.

Figure 108 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.

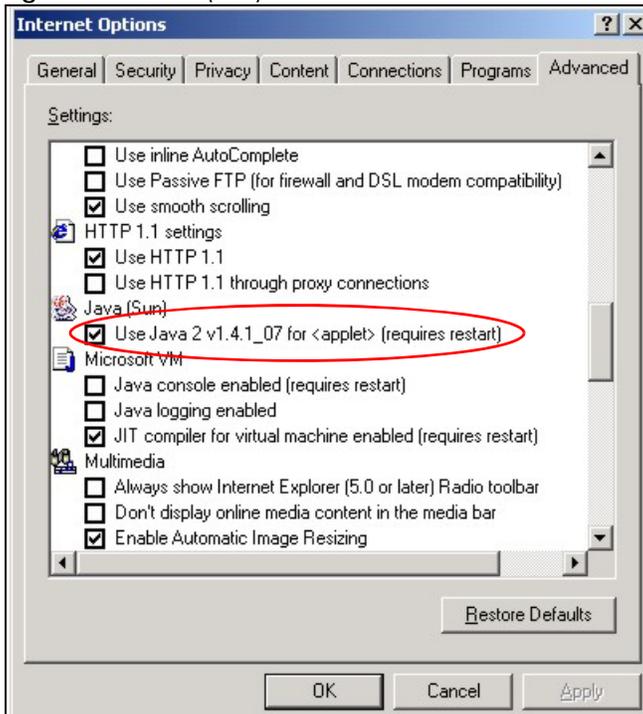
Figure 109 Security Settings - Java



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 110 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.

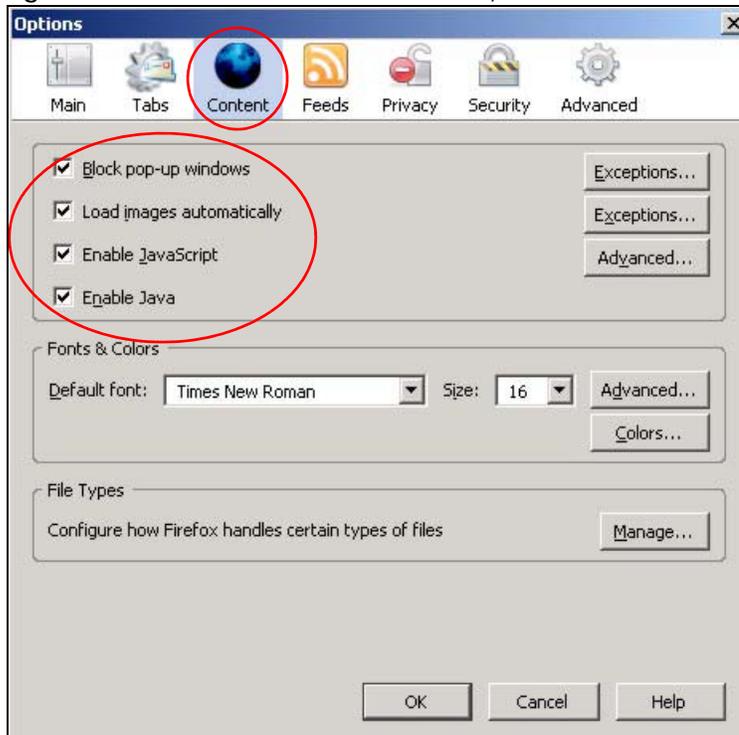
You can enable Java, JavaScripts and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

Figure 111 Mozilla Firefox: TOOLS > Options



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

Figure 112 Mozilla Firefox Content Security



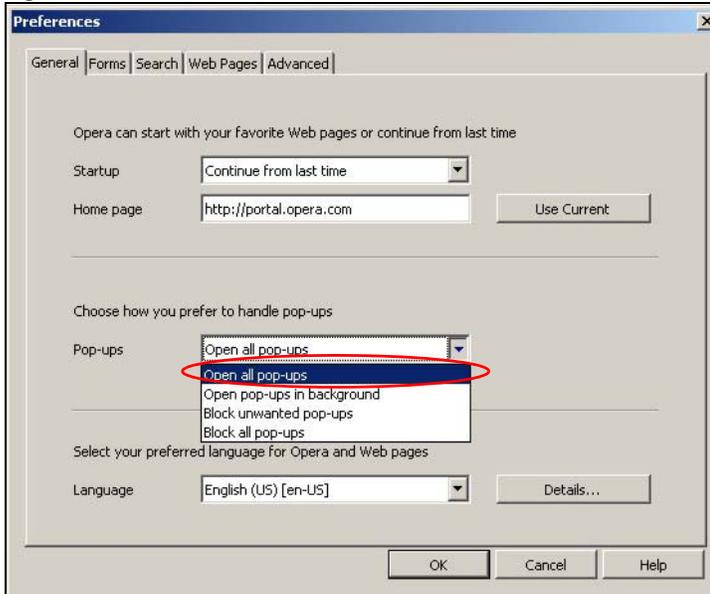
Opera

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**.

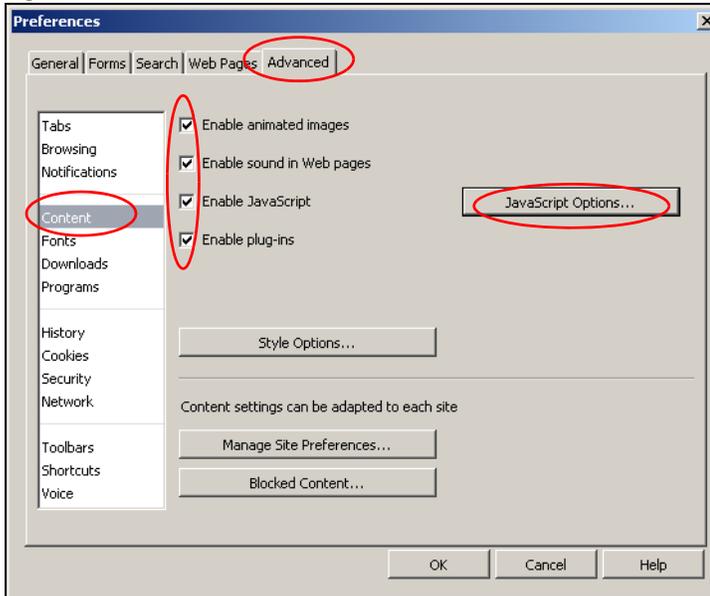
Figure 113 Opera: Allowing Pop-Ups



Enabling Java

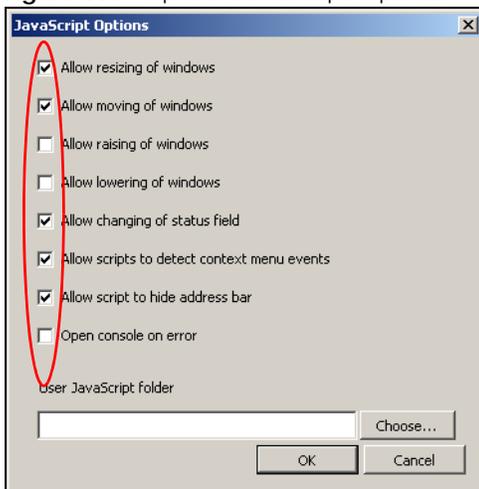
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 114 Opera: Enabling Java



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

Figure 115 Opera: JavaScript Options



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

APPENDIX C

Setting Up Your Computer's IP Address

Note: Your specific NBG6615 may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

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

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

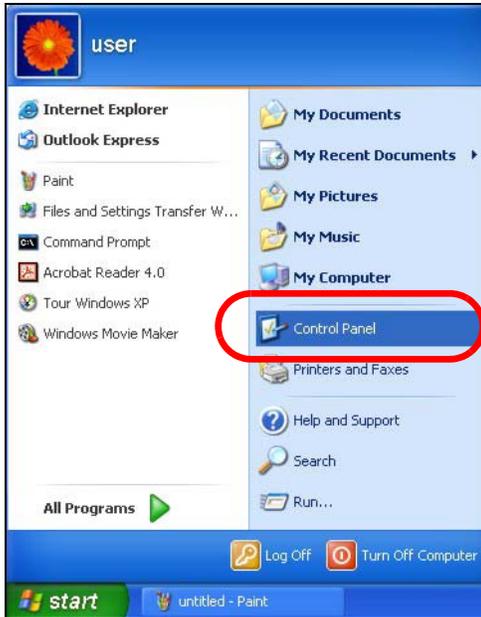
In this appendix, you can set up an IP address for:

- [Windows XP/NT/2000](#) on [page 158](#)
- [Windows Vista](#) on [page 161](#)
- [Windows 7](#) on [page 164](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 169](#)
- [Mac OS X: 10.5 and 10.6](#) on [page 172](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 175](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 179](#)

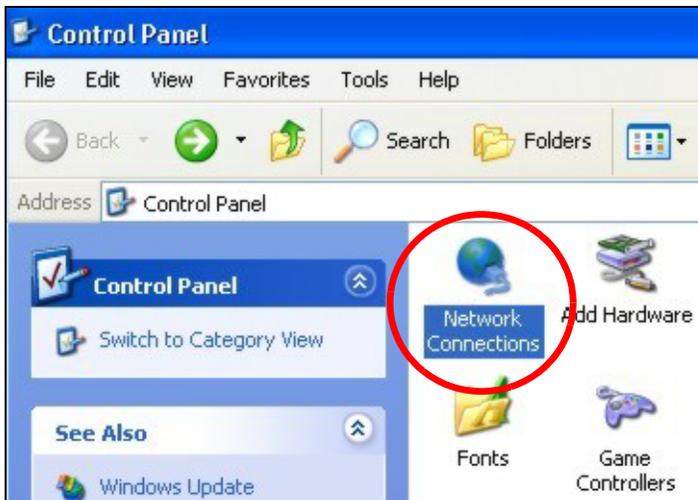
Windows XP/NT/2000

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

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



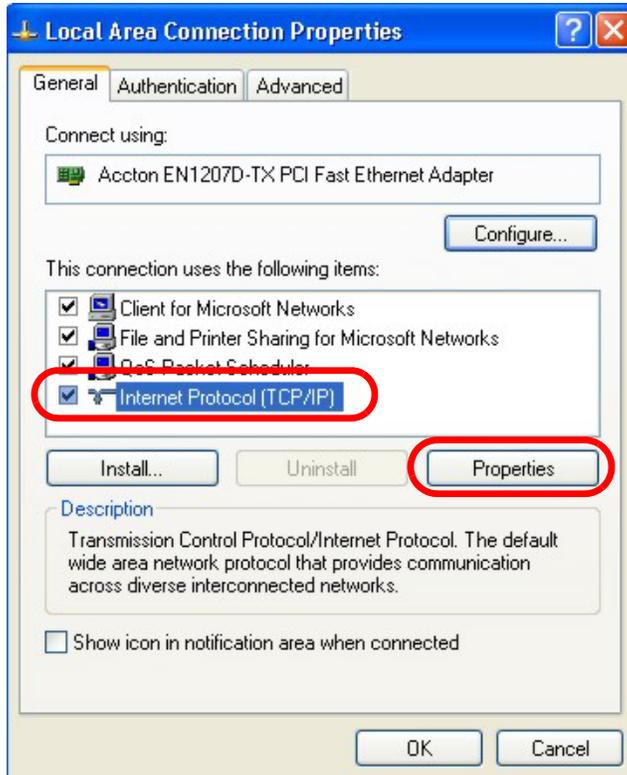
- 2 In the **Control Panel**, click the **Network Connections** icon.



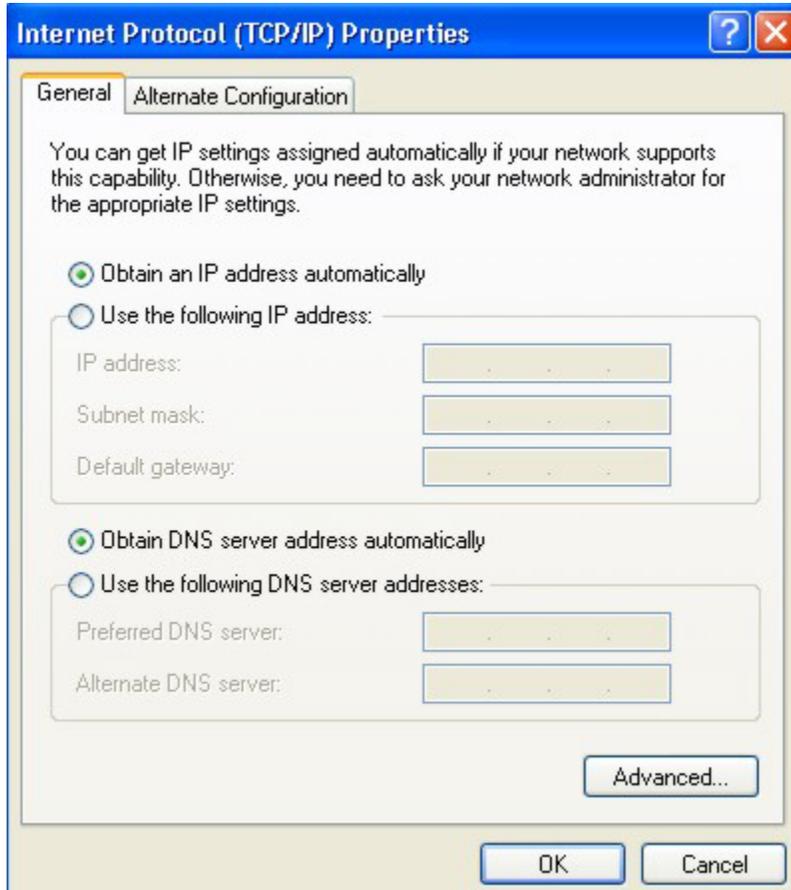
- 3 Right-click **Local Area Connection** and then select **Properties**.



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



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



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

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

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

Verifying Settings

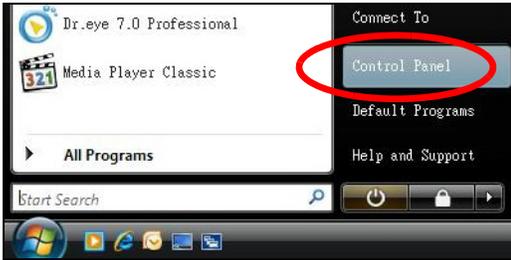
- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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

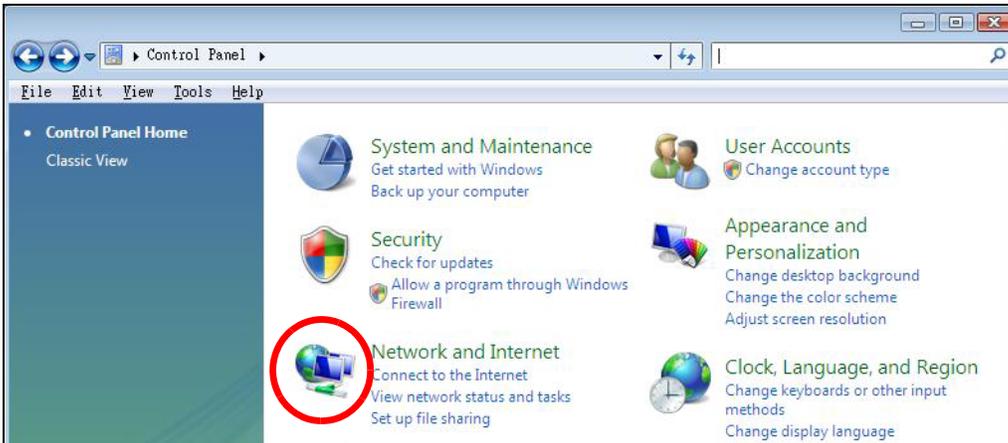
Windows Vista

This section shows screens from Windows Vista Professional.

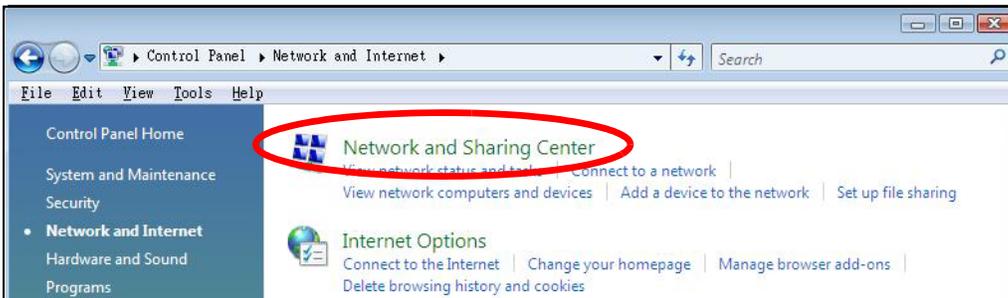
- 1 Click **Start > Control Panel**.



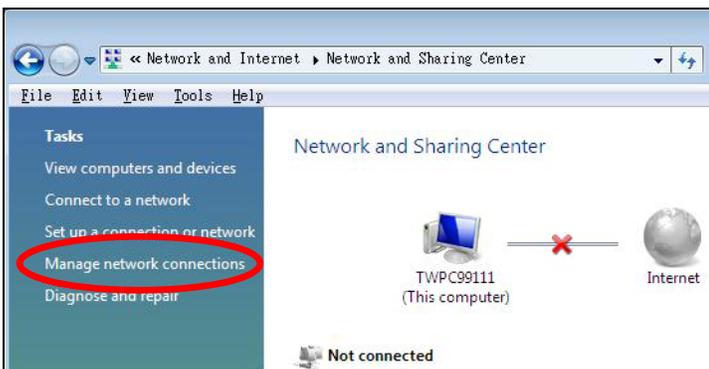
- 2 In the **Control Panel**, click the **Network and Internet** icon.



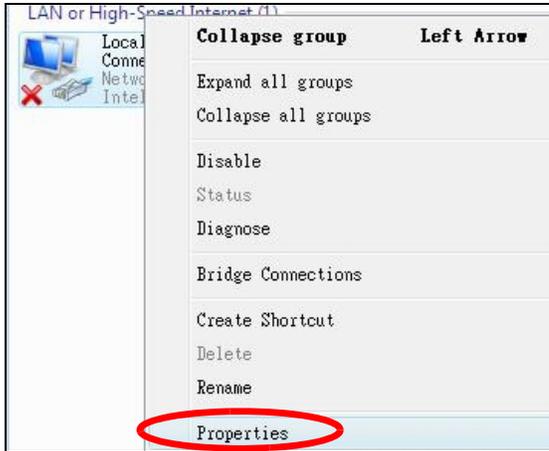
- 3 Click the **Network and Sharing Center** icon.



- 4 Click **Manage network connections**.

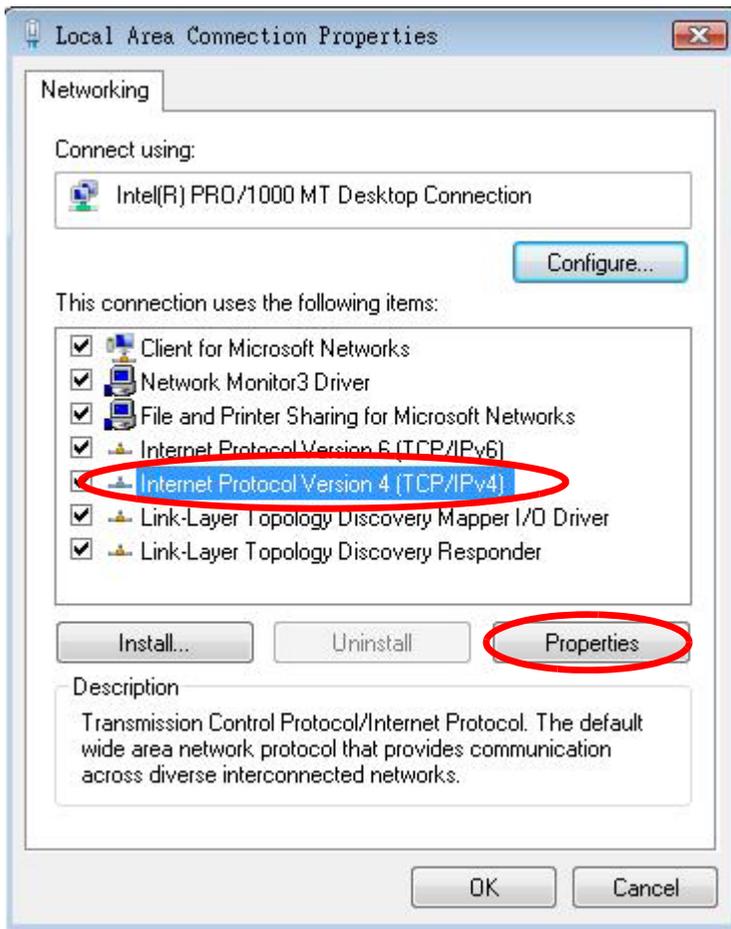


- 5 Right-click **Local Area Connection** and then select **Properties**.

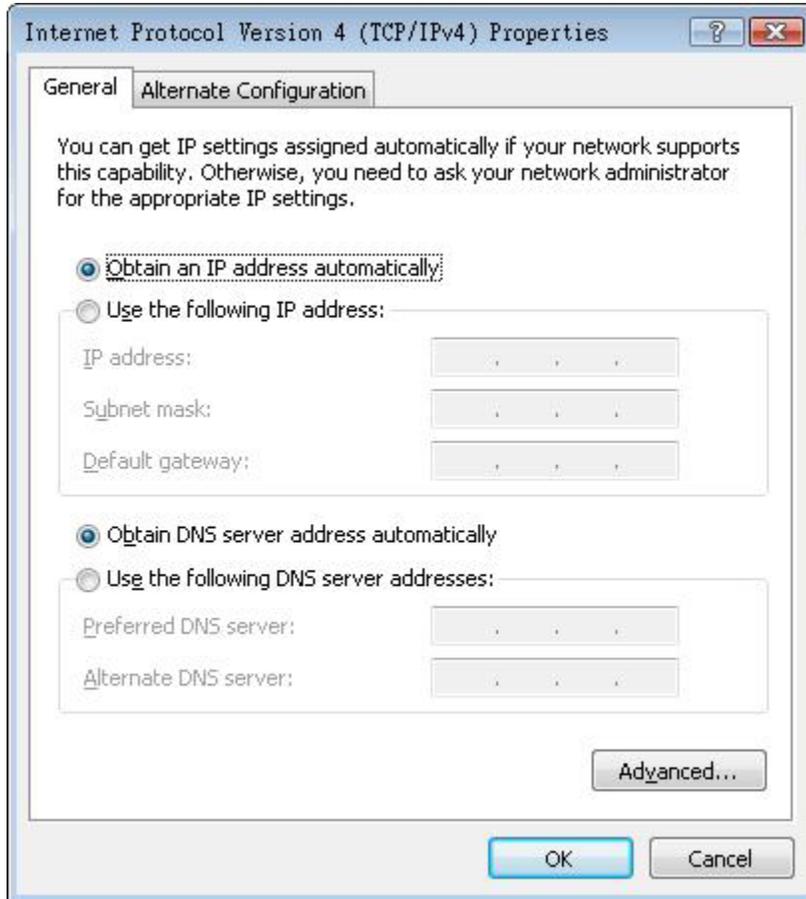


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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



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



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

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

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

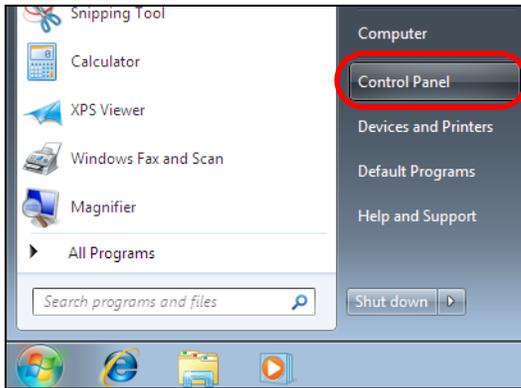
Verifying Settings

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

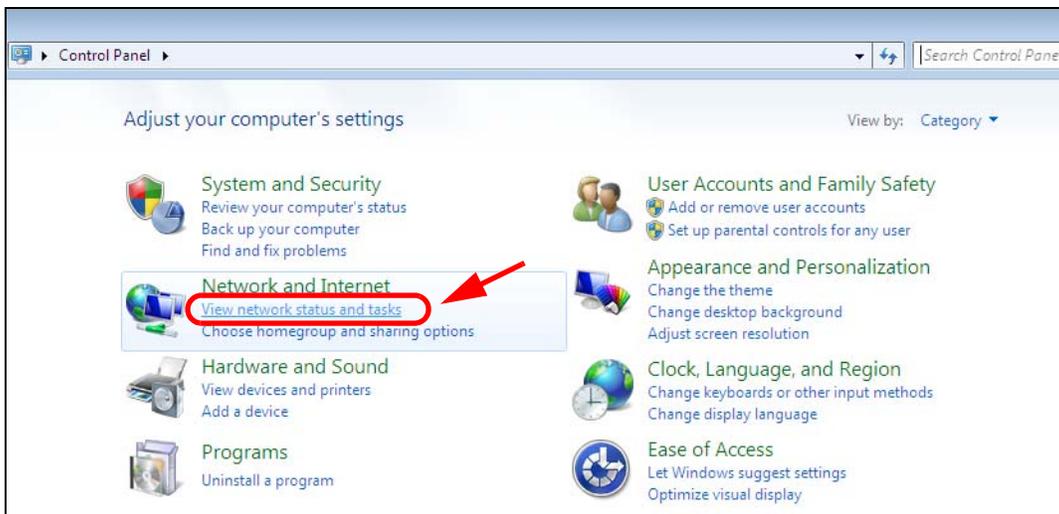
Windows 7

This section shows screens from Windows 7 Enterprise.

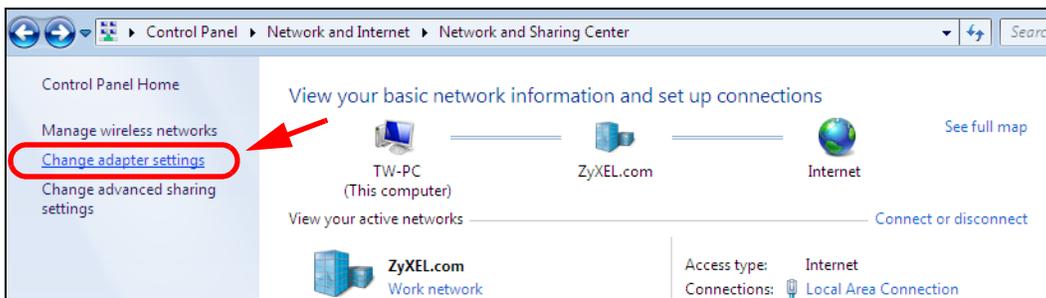
- 1 Click **Start > Control Panel**.



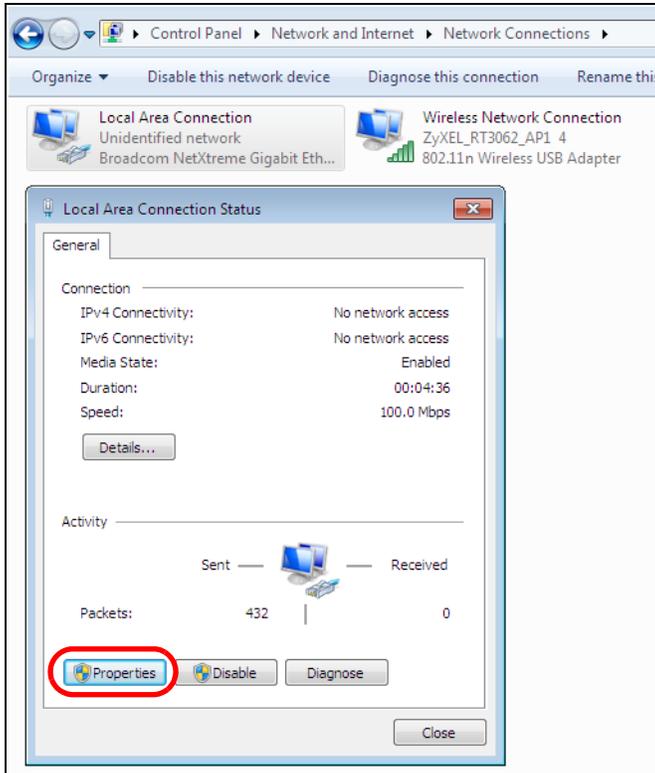
- 2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.



- 3 Click **Change adapter settings**.

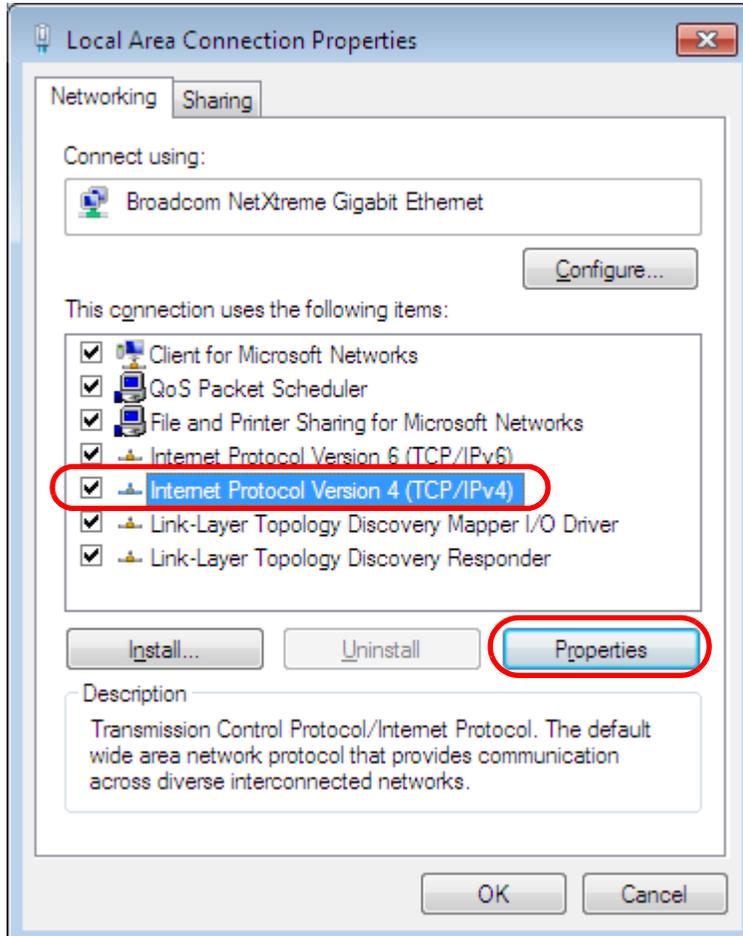


- 4 Double click **Local Area Connection** and then select **Properties**.

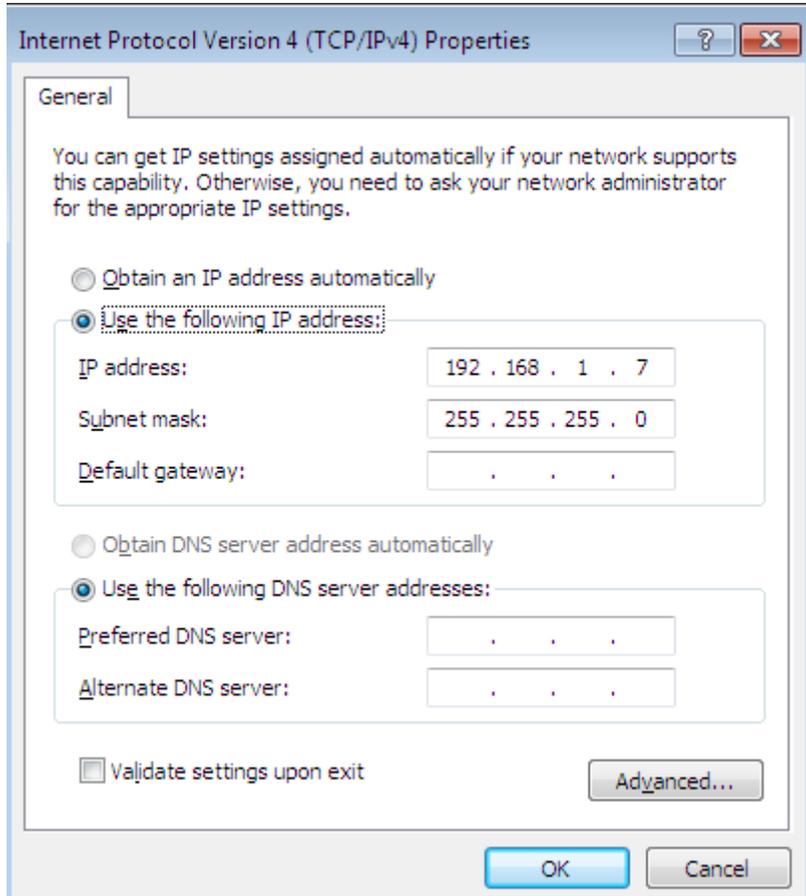


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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



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



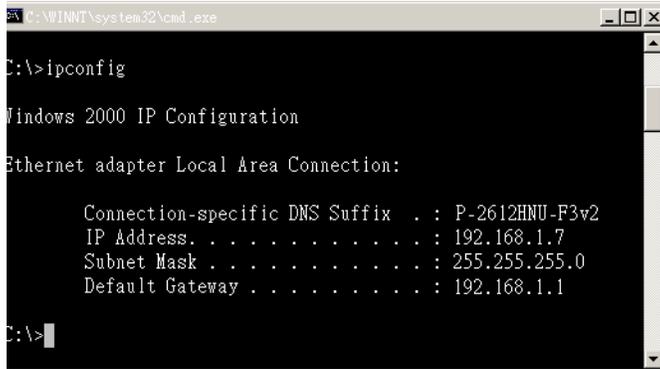
- 7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

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

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

Verifying Settings

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



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

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

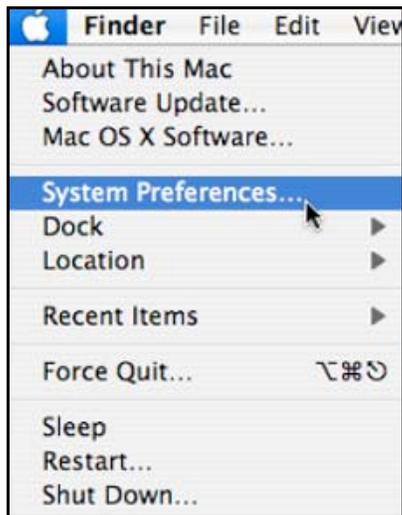
    Connection-specific DNS Suffix  . : P-2612HNU-F3v2
    IP Address. . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\>
```

Mac OS X: 10.3 and 10.4

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

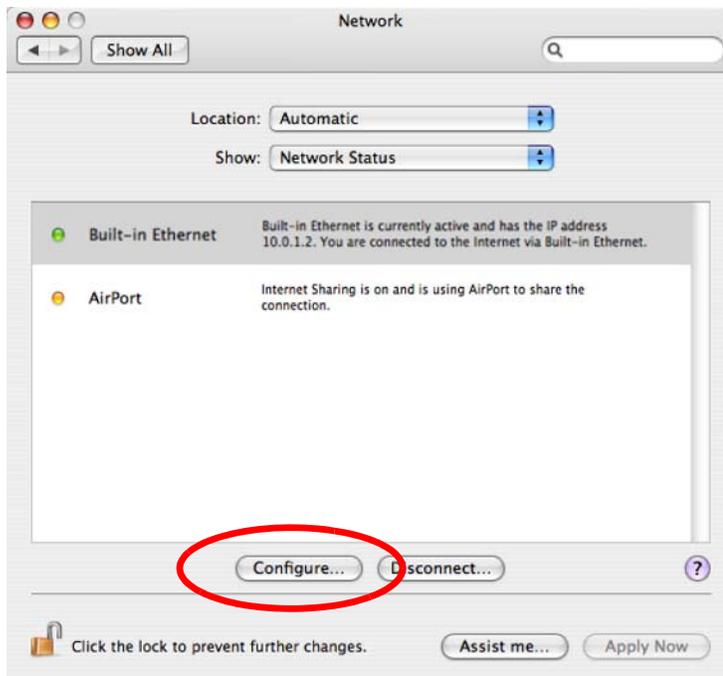
- 1 Click **Apple > System Preferences**.



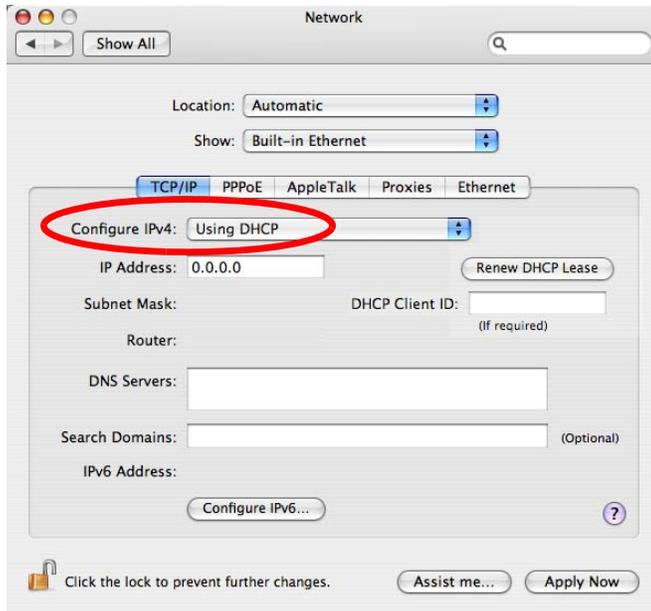
- 2 In the **System Preferences** window, click the **Network** icon.



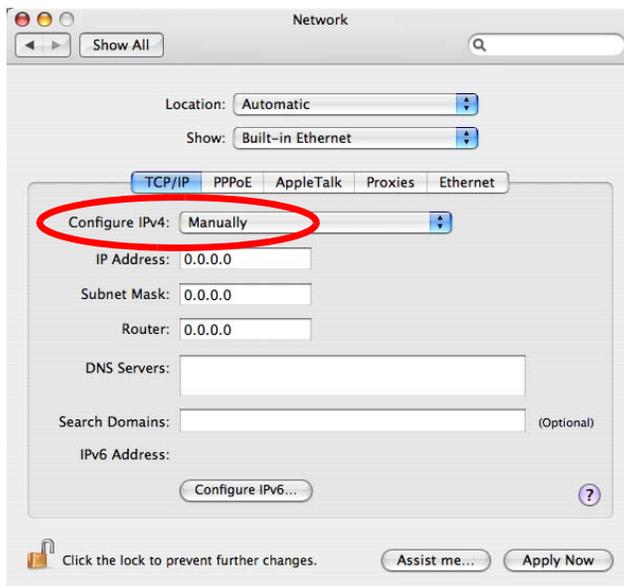
- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.



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



- 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.

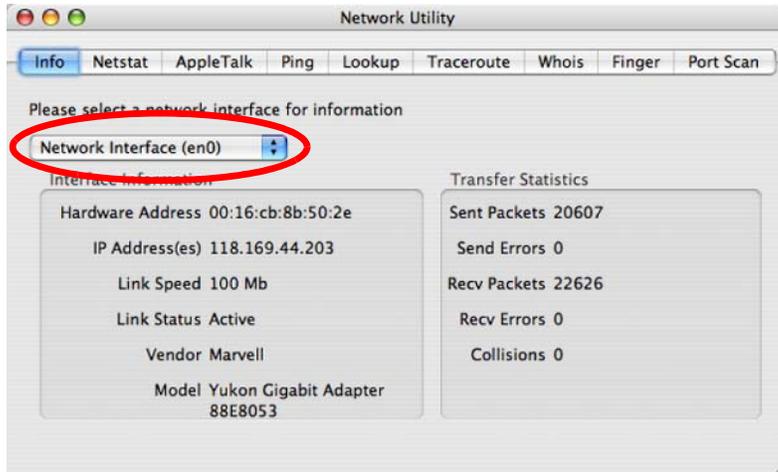


- Click **Apply Now** and close the window.

Verifying Settings

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

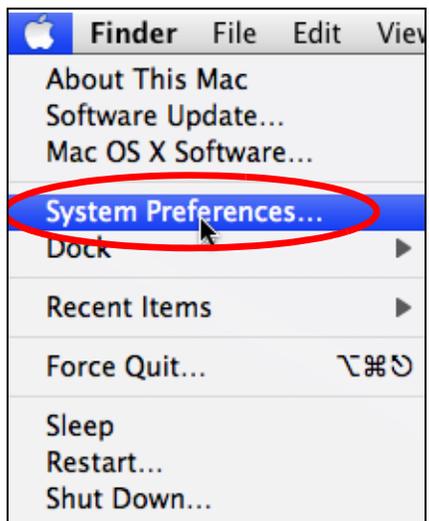
Figure 116 Mac OS X 10.4: Network Utility



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.

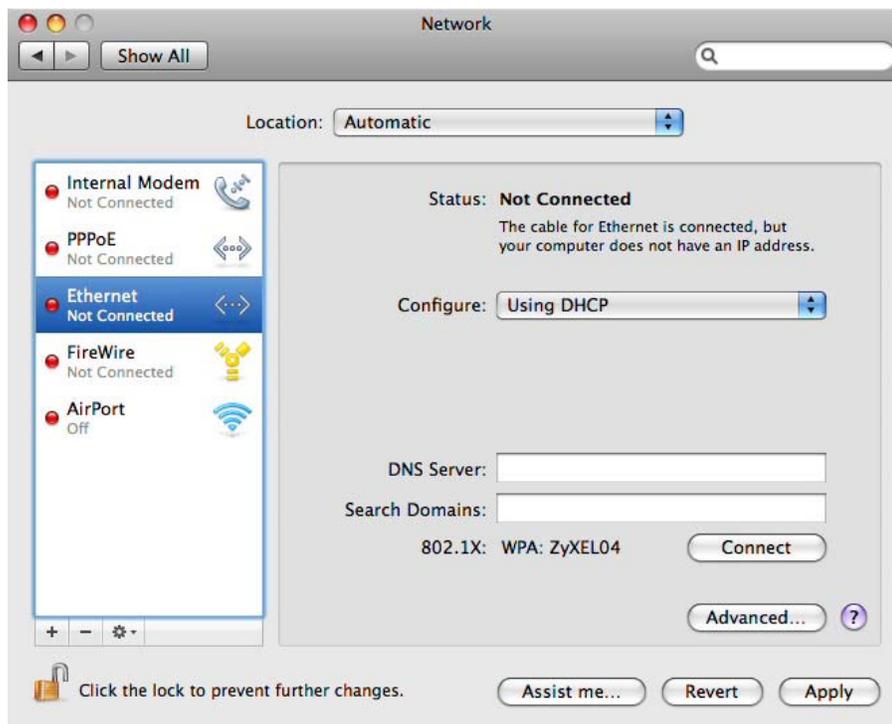
- 1 Click **Apple > System Preferences**.



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

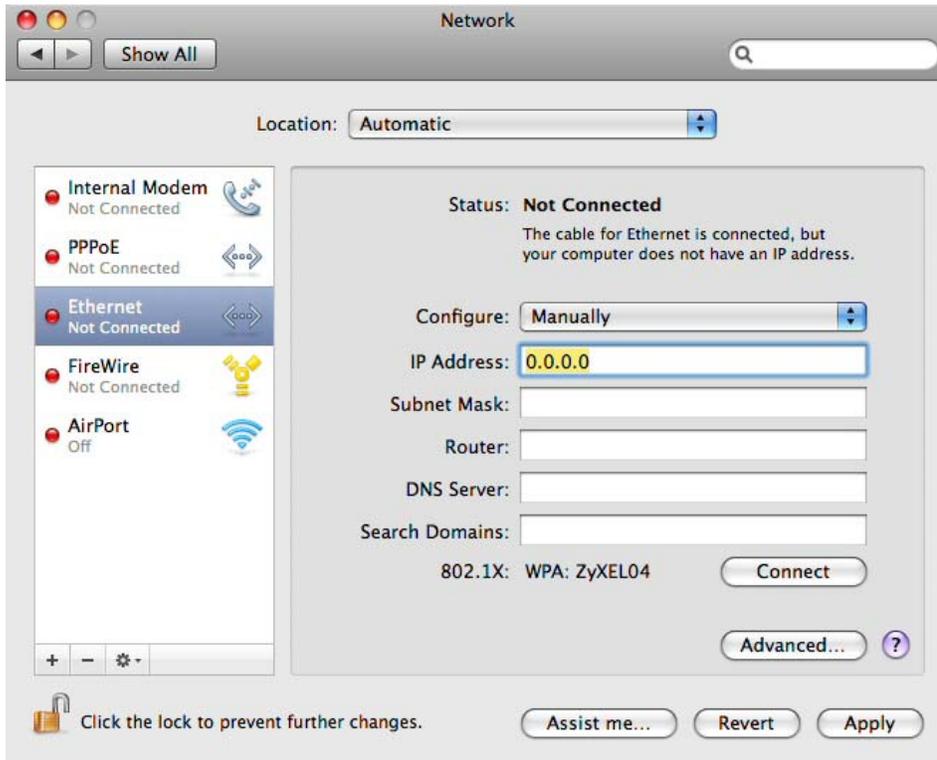


- 3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.



- 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 NBG6615.

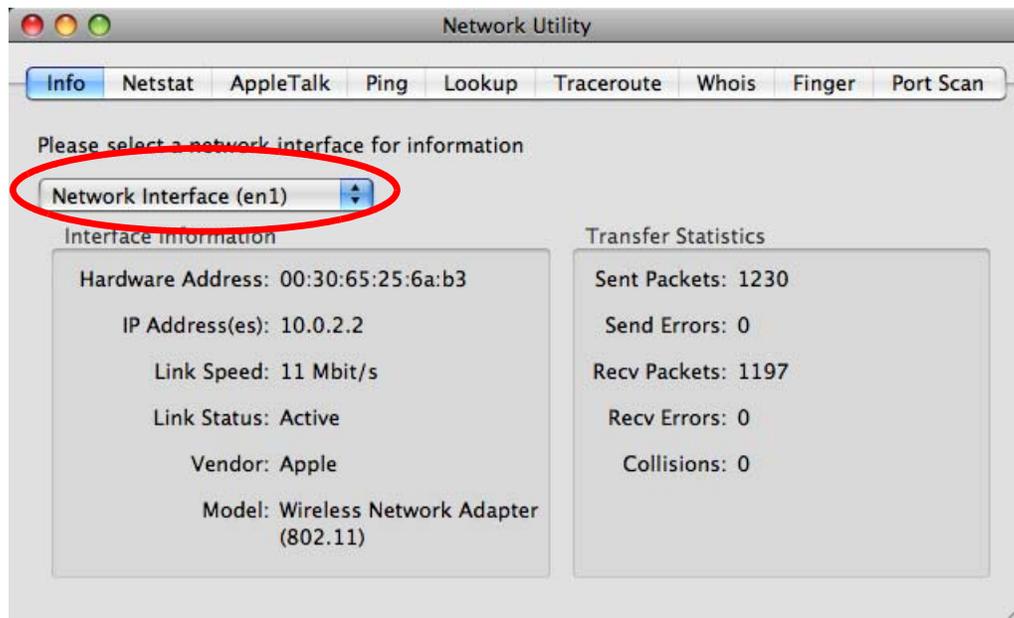


- 6 Click **Apply** and close the window.

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 117 Mac OS X 10.5: Network Utility



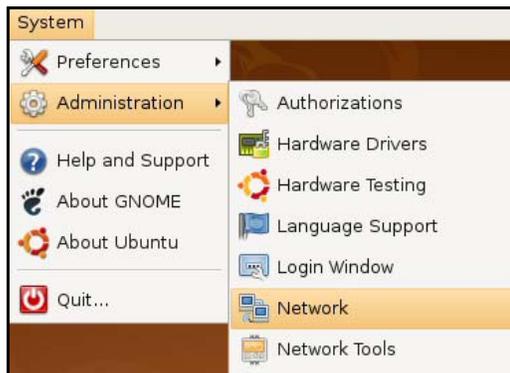
Linux: Ubuntu 8 (GNOME)

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.

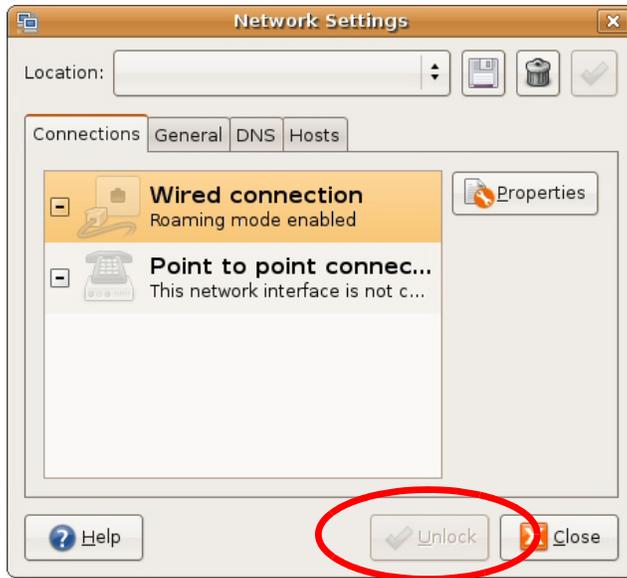
Note: Make sure you are logged in as the root administrator.

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

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



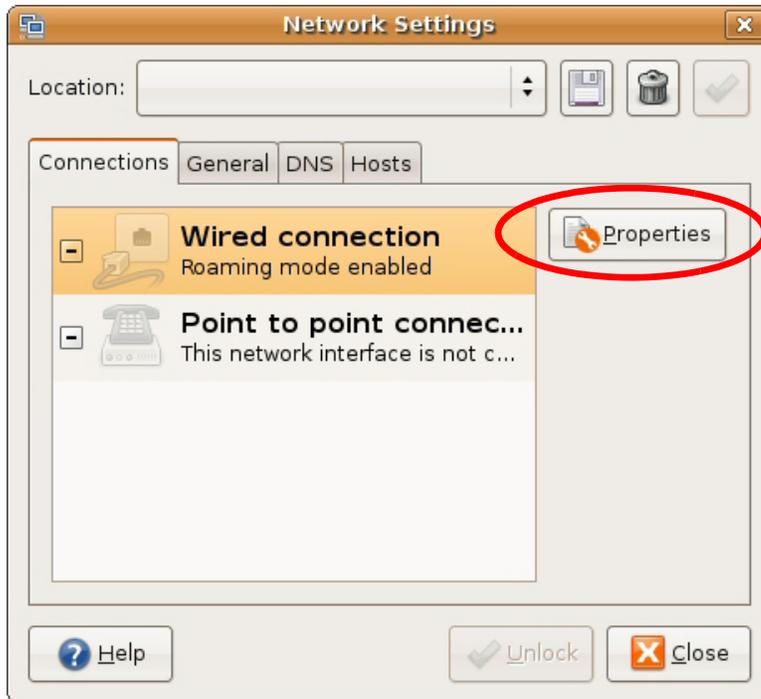
- 2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.



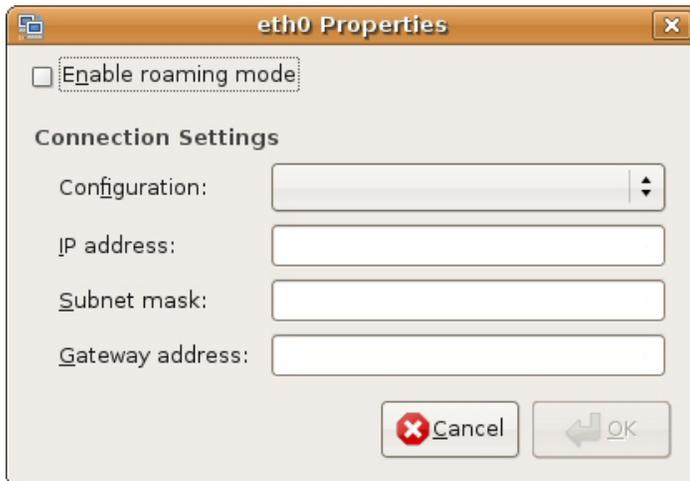
- 3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.



- 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.

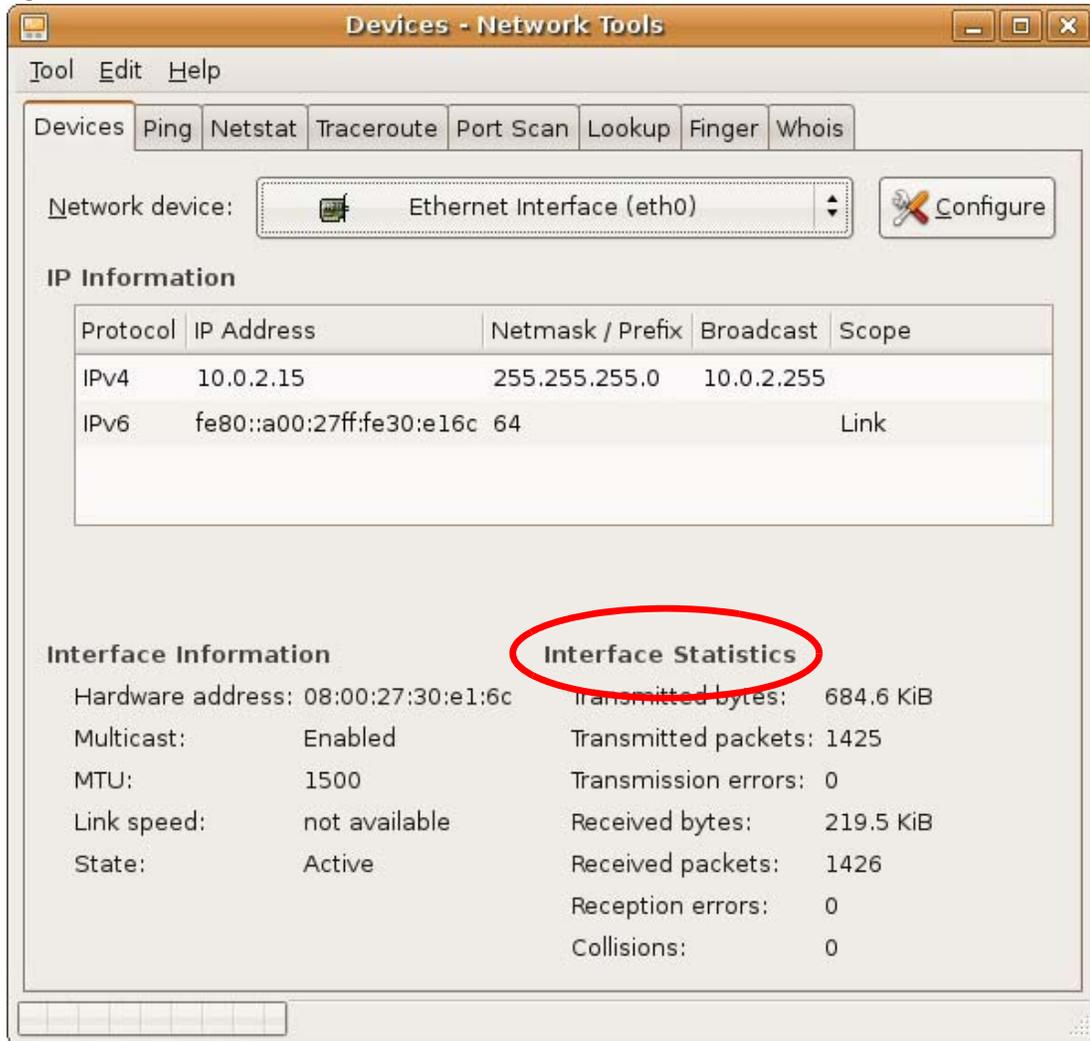


- 8 Click the **Close** button to apply the changes.

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 118 Ubuntu 8: Network Tools



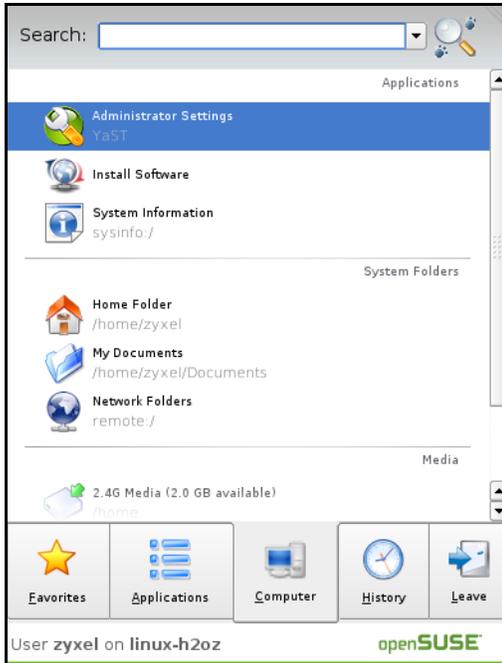
Linux: openSUSE 10.3 (KDE)

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:

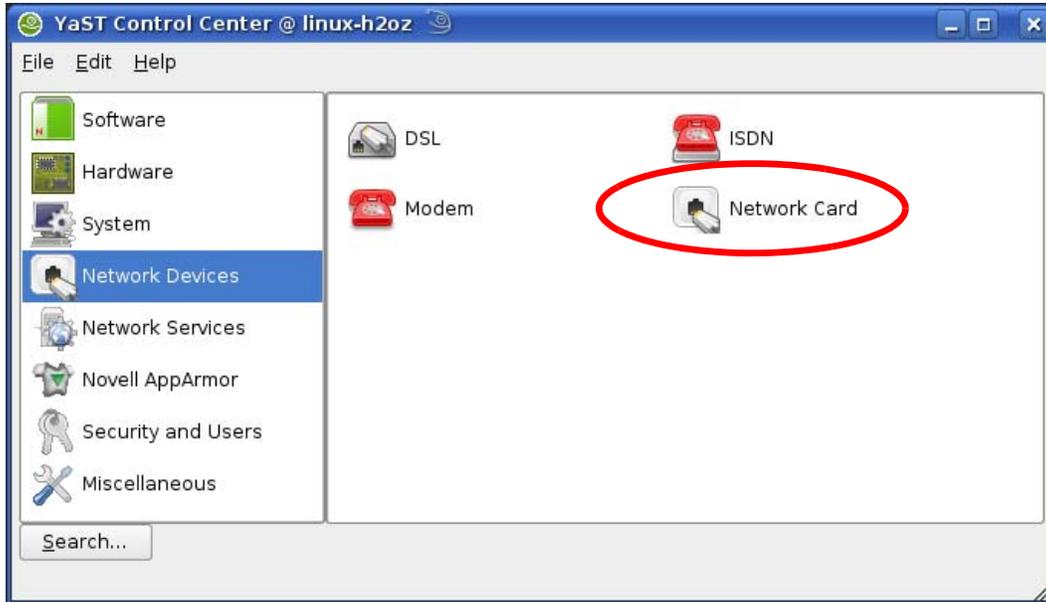
- 1 Click **K Menu > Computer > Administrator Settings (YaST)**.



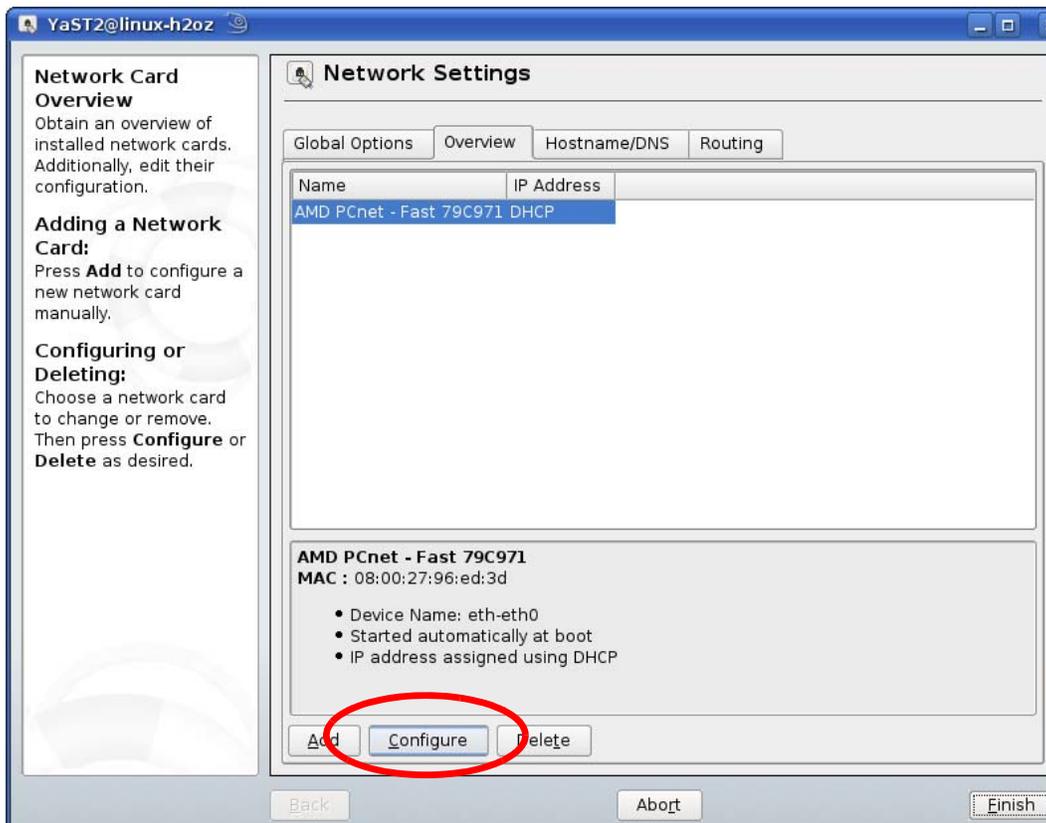
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.



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

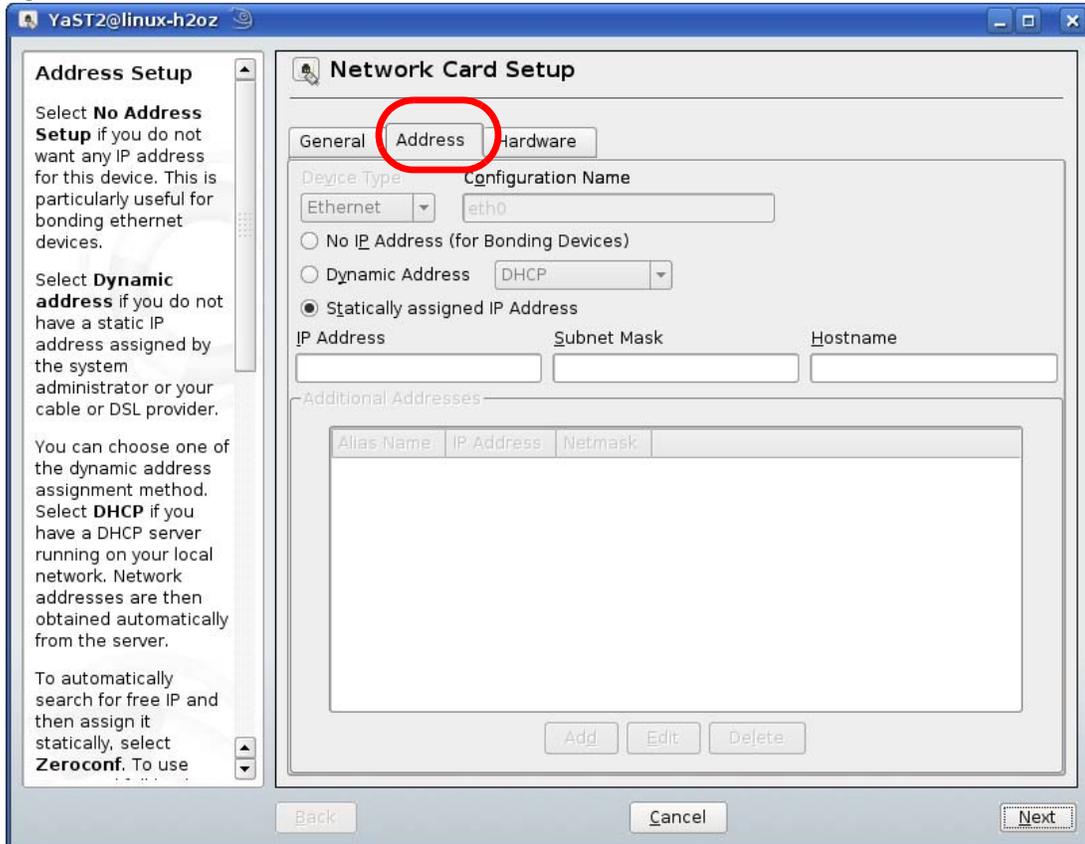


- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

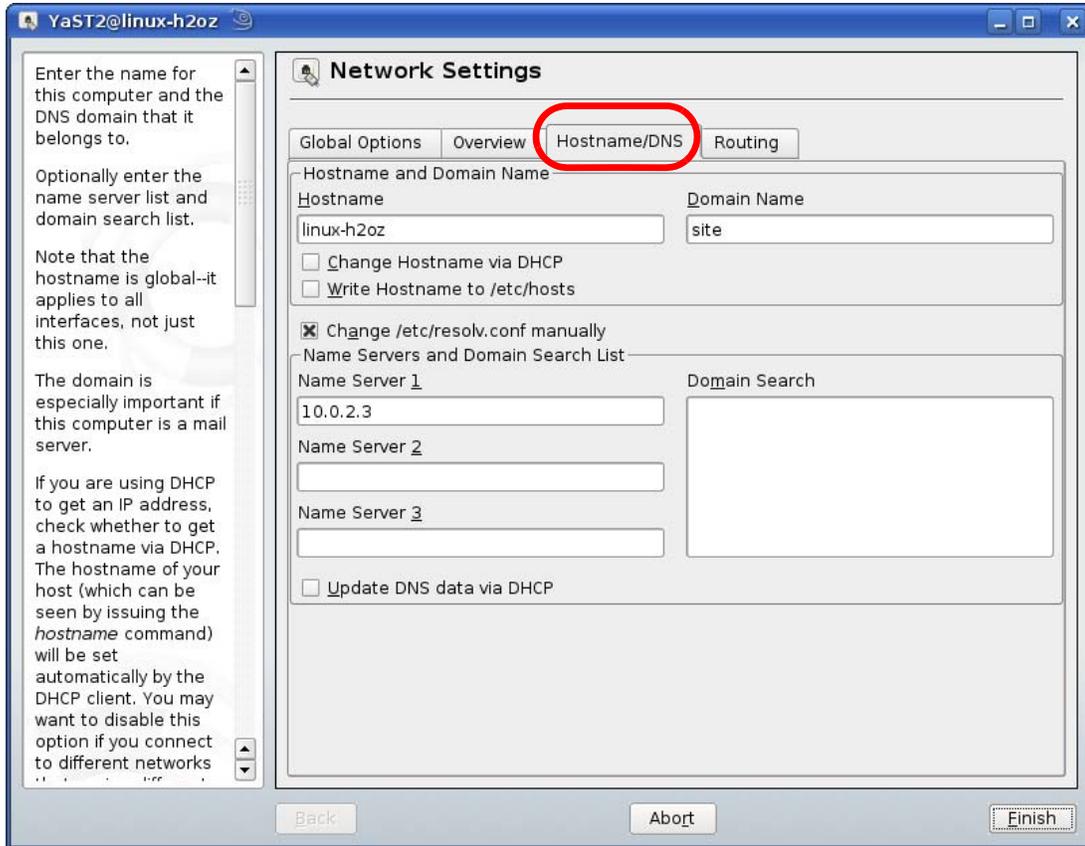


- 5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 119 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.

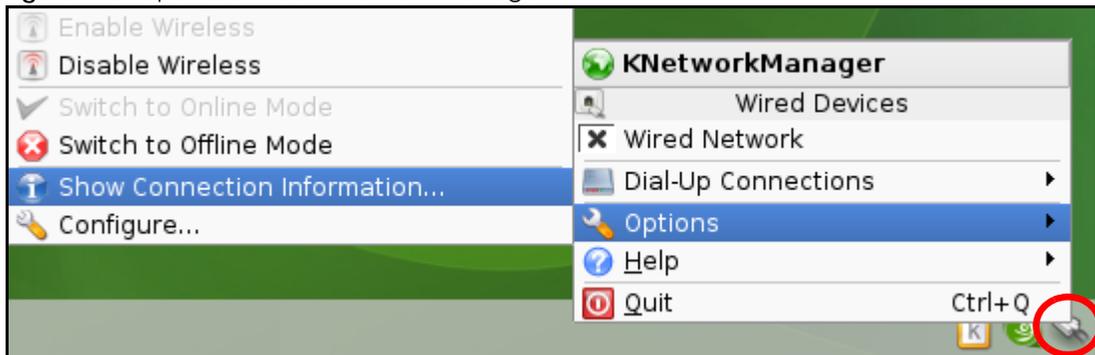


- 9 Click **Finish** to save your settings and close the window.

Verifying Settings

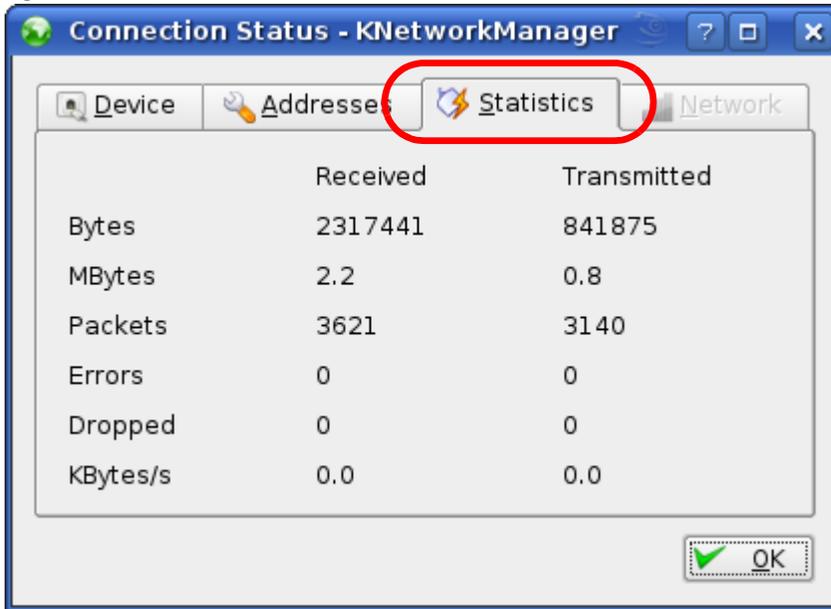
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 120 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 121 openSUSE: Connection Status - KNetwork Manager



APPENDIX D

Wireless LANs

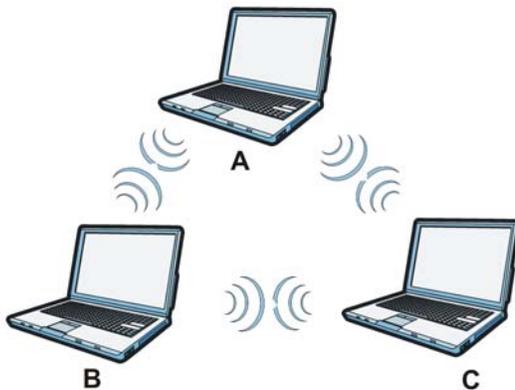
Wireless LAN Topologies

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

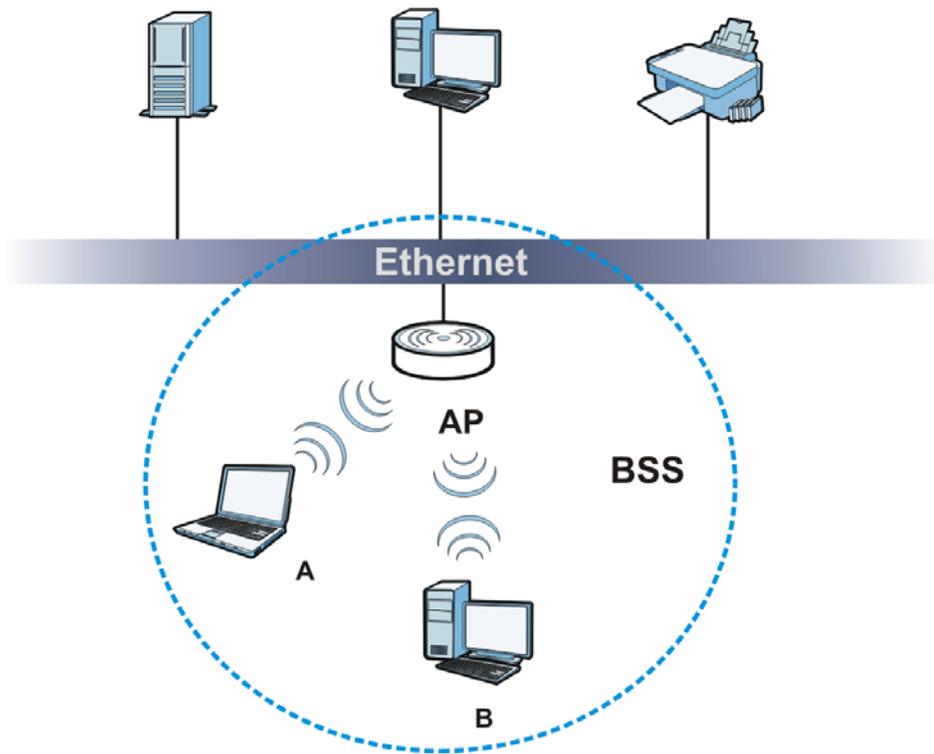


BSS

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 123 Basic Service Set



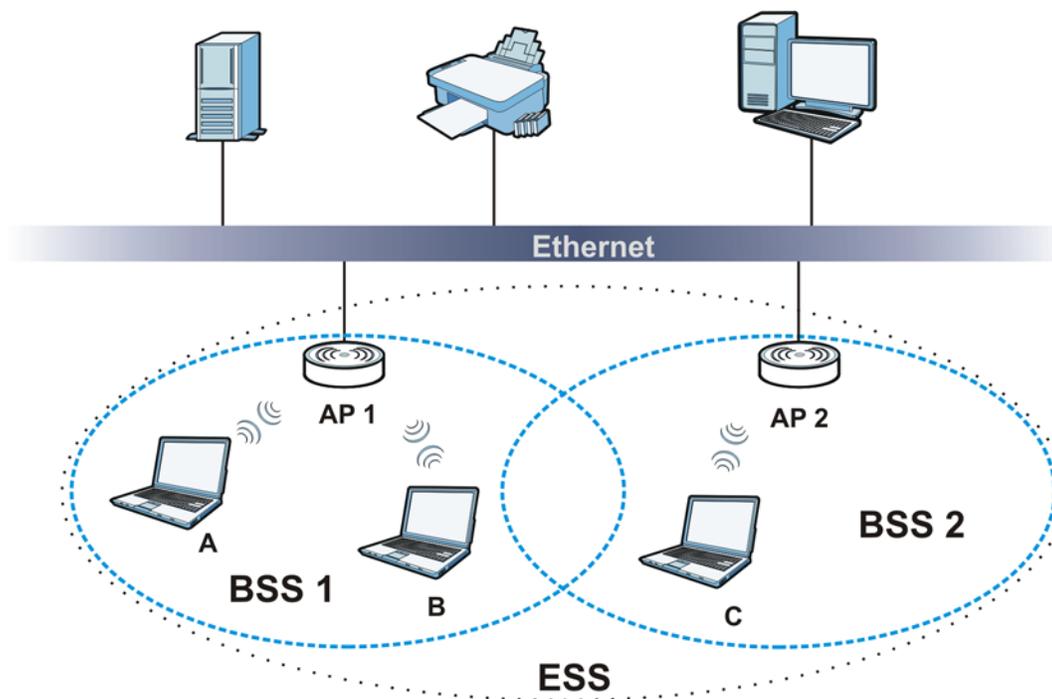
ESS

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 124 Infrastructure WLAN



Channel

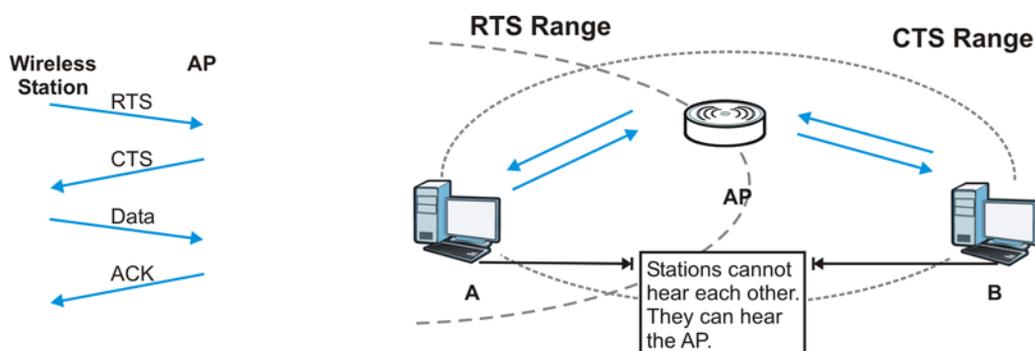
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference 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 125 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 NBG6615 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 61 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 NBG6615 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NBG6615 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your NBG6615.

Table 62 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 NBG6615 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 63 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.

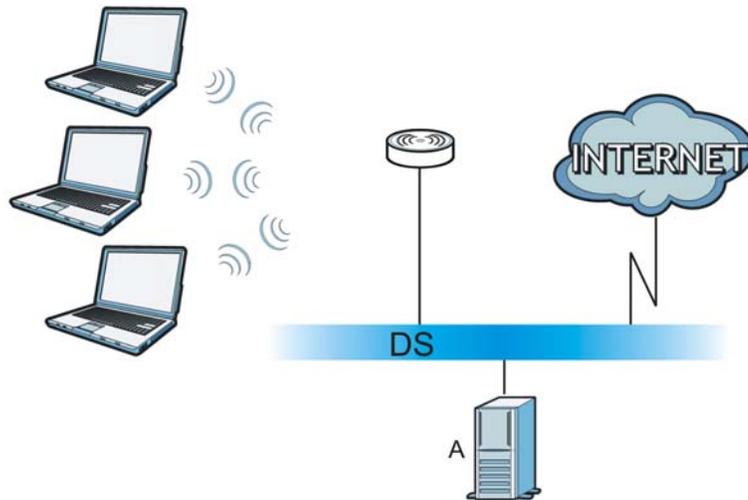
WPA(2) with RADIUS Application Example

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 126 WPA(2) with RADIUS Application Example

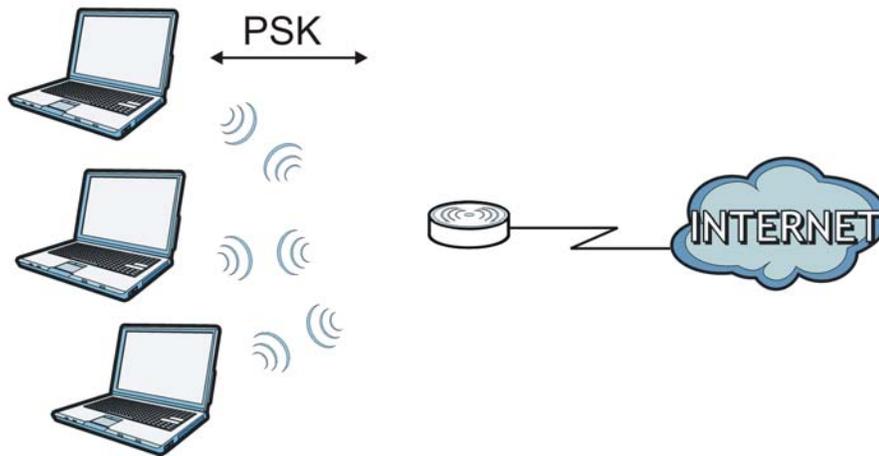


WPA(2)-PSK Application Example

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 127 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 64 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.

APPENDIX 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 65 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.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.

Table 65 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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).
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.

Table 65 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.

APPENDIX F

Legal Information

Copyright

Copyright © 2018 by Zyxel Communications Corporation.

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

Published by Zyxel Communications Corporation. All rights reserved.

Disclaimer

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

Regulatory Notice and Statement

UNITED STATES of AMERICA



The following information applies if you use the product within USA area.

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference, and
 - (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications 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 according to 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 or television reception, which is found 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:
 - Reorient or relocate the receiving antenna
 - Increase the separation between the devices
 - Connect the equipment to an outlet other than the receiver's
 - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment.

CANADA

The following information applies if you use the product within Canada area.

Industry Canada ICES Statement

CAN ICES-3 (B)/NMB-3(B)

Industry Canada RSS-GEN & RSS-247 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.
- This radio transmitter 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.

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid.

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- The worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
- Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. 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 radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio de modèle s'il fait partie du matériel de catégoriel) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'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 strictement interdits pour l'exploitation de l'émetteur.

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3) du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes.

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

Industry Canada radiation exposure statement

This device complies with IC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

EUROPEAN UNION



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

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz 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 the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20cm between the radio equipment and your body.
- The maximum RF power operating for each band as follows:
 - the band 2,400 to 2,483.5 MHz is 88.51 mW,
 - the bands 5,150 MHz to 5,350 MHz is 175.79 mW,

- the 5,470 MHz to 5,725 MHz is 682.34 mW.

Български (Bulgarian)	<p>С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> 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.
Español (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 2014/53/UE..
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	<p>Undertegnede Zyxel erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΙΑ Ζyxel ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΤΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.
Italiano (Italian)	<p>Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> 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 alle 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.
Latviešu valoda (Latvian)	<p>Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details. 2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: http://www.esd.lv.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoją, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-htġġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.

Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteen tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53/EU.

Notes:

- Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
- 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	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

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 obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- 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.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- 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.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. 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.

- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device.
 - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
 - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive)" as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless setting, please refer to "Wireless" chapter for more detail.)

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣



以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 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，指依電信法規定作業之無線電通信。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。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中

- 使用無線產品時，應避免影響附近雷達系統之操作。
- 若使用高增益指向性天線，該產品僅應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
 - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
 - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
 - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
 - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

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

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to

proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

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

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

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

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.

APPENDIX 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.

See <http://www.zyxel.com/homepage.shtml> and also http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml for the latest information.

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

- ZyxelPhilippines
- <http://www.zyxel.com.ph>

Singapore

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com/tw/zh/>

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/>
- <http://www.zyxel.com/be/fr/>

Bulgaria

- Zyxel България
- <http://www.zyxel.com/bg/bg/>

Czech Republic

- Zyxel Communications Czech s.r.o
- <http://www.zyxel.cz>

Denmark

- ZyxelCommunications 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>

Italy

- Zyxel Communications Italy
- <http://www.zyxel.it/>

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 Communications ES Ltd
- <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/>

Brazil

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

Ecuador

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

Middle East

Israel

- Zyxel Communication Corporation
- <http://il.zyxel.com/homepage.shtml>

Middle East

- Zyxel Communication Corporation
- <http://www.zyxel.com/me/en/>

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- <http://www.zyxel.com/us/en/>

Oceania

Australia

- Zyxel Communications Corporation
- <http://www.zyxel.com/au/en/>

Africa

South Africa

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

Index

A

Address Assignment [69](#)
Advanced Encryption Standard
 See AES.
AES [193](#)
Alert [124](#)
alternative subnet mask notation [142](#)
antenna
 directional [197](#)
 gain [197](#)
 omni-directional [197](#)
AP (access point) [187](#)
AP Mode
 menu [33, 37](#)
 overview [28](#)
 status screen [29, 35](#)

B

Backup configuration [128](#)
Basic Service Set, See BSS [185](#)
BSS [185](#)

C

CA [192](#)
Certificate Authority
 See CA.
certifications [204](#)
 viewing [206](#)
Channel [31, 37](#)
channel [56, 187](#)
 interference [187](#)
Client table [31](#)
Configuration
 backup [128](#)
 reset the factory defaults [129](#)

 restore [128](#)
contact information [208](#)
copyright [201](#)
CTS (Clear to Send) [188](#)
customer support [208](#)

D

Daylight saving [123](#)
DDNS
 service providers [95](#)
device mode [11, 28](#)
DHCP [82](#)
 see also Dynamic Host Configuration Protocol
DHCP client information [84](#)
DHCP client list [84](#)
DHCP server [79, 82](#)
DHCP table [84](#)
disclaimer [201](#)
DNS [79](#)
 DNS server
 see also Domain name system
DNS Server [69](#)
Domain Name System. See DNS.
Dynamic DNS [95](#)
Dynamic Host Configuration Protocol [82](#)
dynamic WEP key exchange [192](#)
DynDNS [95](#)
DynDNS see also DDNS [95](#)

E

EAP Authentication [191](#)
encryption [57, 193](#)
 key [57](#)
ESS [186](#)
ESSID [139](#)

Extended Service Set, See ESS [186](#)

F

Factory LAN defaults [82](#)

Firewall

ICMP packets [102](#), [105](#)

ZyXEL device firewall [101](#)

firewall

stateful inspection [100](#)

Firmware upload [126](#)

file extension

using HTTP

firmware version [30](#), [36](#)

fragmentation threshold [188](#)

G

General wireless LAN screen [57](#)

H

hidden node [187](#)

I

IANA [146](#), [147](#)

IBSS [185](#)

IEEE 802.11g [189](#)

Independent Basic Service Set

See IBSS [185](#)

initialization vector (IV) [193](#)

Internet Assigned Numbers Authority

See IANA [146](#)

IP Address [77](#), [80](#), [89](#)

IP address [79](#)

dynamic

IP Pool [83](#)

L

LAN [78](#)

IP pool setup [80](#)

LAN overview [78](#)

LAN setup [78](#)

LAN TCP/IP [80](#)

Language [133](#)

Local Area Network [78](#)

Log [124](#)

M

MAC [60](#)

MAC address [56](#), [69](#)

cloning [69](#)

MAC address filter [56](#)

MAC address filtering [60](#)

MAC filter [60](#)

managing the device

good habits [12](#)

MBSSID [56](#)

Media access control [60](#)

Message Integrity Check (MIC) [193](#)

mode [11](#)

Multiple BSS, see MBSSID

N

NAT [86](#), [89](#), [146](#)

global [87](#)

how it works [86](#), [88](#)

inside [87](#)

local [87](#)

outside [87](#)

overview [86](#)

port forwarding [93](#)

see also Network Address Translation

server [87](#)

server sets [93](#)

NAT traversal [110](#)

Navigation Panel [33](#), [37](#)

navigation panel [33](#), [37](#)

Network Address Translation [86, 89](#)

O

operating mode [11](#)

operation mode [28, 131](#)

access point [28](#)

client [29](#)

router [28](#)

overview [11](#)

P

Pairwise Master Key (PMK) [193, 195](#)

Point-to-Point Protocol over Ethernet [23, 24, 72](#)

Point-to-Point Tunneling Protocol [74](#)

Pool Size [83](#)

Port forwarding [89, 93](#)

default server [89, 93](#)

example [93](#)

local server [89](#)

port numbers

services

Port Trigger [91](#)

PPPoE [23, 24, 72](#)

benefits [23](#)

dial-up connection

see also Point-to-Point Protocol over Ethernet [23, 24](#)

PPTP [74](#)

preamble mode [189](#)

PSK [194](#)

Q

Quality of Service (QoS) [62](#)

R

RADIUS [190](#)

message types [191](#)

messages [191](#)

shared secret key [191](#)

Remote management

and NAT [108](#)

and the firewall [107](#)

limitations [108](#)

system timeout [108](#)

Reset button [18, 129](#)

Reset the device [18](#)

Restore configuration [128](#)

Roaming [61](#)

RTS (Request To Send) [188](#)

threshold [187, 188](#)

RTS/CTS Threshold [55, 61](#)

S

Scheduling [64](#)

screw anchor [14](#)

Service Set [58](#)

Service Set IDentification [58](#)

Service Set IDentity. See SSID.

SSID [31, 37, 55, 58](#)

MBSSID [56](#)

stateful inspection firewall [100](#)

Static DHCP [83](#)

Static Route [97](#)

subnet [140](#)

Subnet Mask [81](#)

subnet mask [79, 141](#)

subnetting [142](#)

Summary

Packet statistics [32](#)

Sys Op Mode [131](#)

System General Setup [118, 119, 121](#)

System Name [122](#)

System restart [129](#)

T

TCP/IP configuration [82](#)

Temporal Key Integrity Protocol (TKIP) [193](#)

- Time setting [122](#)
 - trigger port [94](#)
 - Trigger port forwarding [94](#)
 - example [94](#)
 - process [94](#)
- ## U
- Universal Plug and Play [110](#)
 - application [110](#)
 - universal repeater [11](#)
 - UPnP [110](#)
 - example [117](#)
 - installation [117](#)
 - security issues [110](#)
- ## V
- VPN [74](#)
- ## W
- wall mounting [14](#)
 - WAN (Wide Area Network) [68](#)
 - WAN MAC address [69](#)
 - warranty [206](#)
 - note [207](#)
 - Web Configurator
 - how to access [16](#)
 - Overview [16](#)
 - Wi-Fi Protected Access [193](#)
 - wireless channel [139](#)
 - wireless client WPA supplicants [194](#)
 - wireless LAN [139](#)
 - MBSSID [56](#)
 - wireless LAN scheduling [64](#)
 - Wireless network
 - basic guidelines [55](#)
 - channel [56](#)
 - encryption [57](#)
 - example [54](#)
 - MAC address filter [56](#)
 - overview [54](#)
 - security [56](#)
 - SSID [55](#)
 - Wireless security [56](#)
 - overview [56](#)
 - type [56](#)
 - wireless security [139, 189](#)
 - Wireless tutorial [39](#)
 - WPS [39](#)
 - Wizard setup [20](#)
 - WLAN
 - interference [187](#)
 - security parameters [196](#)
 - WPA [193](#)
 - key caching [194](#)
 - pre-authentication [194](#)
 - user authentication [194](#)
 - vs WPA-PSK [194](#)
 - wireless client supplicant [194](#)
 - with RADIUS application example [194](#)
 - WPA2 [193](#)
 - user authentication [194](#)
 - vs WPA2-PSK [194](#)
 - wireless client supplicant [194](#)
 - with RADIUS application example [194](#)
 - WPA2-Pre-Shared Key [193](#)
 - WPA2-PSK [193, 194](#)
 - application example [195](#)
 - WPA-PSK [193, 194](#)
 - application example [195](#)
 - WPS [13](#)
 - WPS button [13](#)