NBG6503

Simultaneous Dual-band Wireless AC750 Home Router

Version 1.00
Edition 1, 03/2013

User's Guide

Default Details	
LAN IP Address	
- Router Mode (Default mode)	http://192.168.1.1
- AP Mode	http://192.168.1.2
User Name	admin
Password	1234
SSID	ZyXEL
Pre-shared Key	00000000

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the NBG6503 and access the Web Configurator wizards. It also contains a connection diagram and package contents list.

Note: It is recommended you use the Web Configurator to configure the NBG6503.

Contents Overview

Table of Contents

PART I
User's Guide

1

Getting to Know Your Router

1.1 Overview

This chapter introduces the main features and applications of the Router.

The Router upgrades the speed of your existing wireless network, providing faster network access to mobile users. Making use of IEEE 802.11AC technology, it not only upgrades your network to the next level but also eliminates dead spots, while offering backward compatibility with other IEEE 802.11b/g/n compatible devices.

A range of services such as a firewall and content filtering are also available for secure Internet computing. You can use media bandwidth management to efficiently manage traffic on your network. Bandwidth management features allow you to prioritize time-sensitive or highly important applications such as Voice over the Internet (VoIP).

1.2 Applications

Your can create the following networks using the Router:

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

1.3 Ways to Manage the Router

Use any of the following methods to manage the Router.

- Web Configurator. This is recommended for everyday management of the Router using a (supported) web browser.
- Wireless switch. You can use the built-in switch of the Router to turn the wireless function on and off without opening the Web Configurator.
- WPS (Wi-Fi Protected Setup) button. You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your Router.

1.4 Good Habits for Managing the Router

Do the following things regularly to make the Router more secure and to manage the Router 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 Router to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Router. You could simply restore your last configuration.

1.5 LEDs

Figure 1 Front Panel

The following table describes the LEDs and the WPS button.

Table 1 Front Panel LEDs and WPS Button

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The Router is receiving power and functioning properly.
		Off	The Router is not receiving power.
WAN	Green	On	The Router has a successful 10/100MB WAN connection.
		Blinking	The Router is sending/receiving data through the WAN.
		Off	The WAN connection is not ready, or has failed.
LAN 1-4	Green	On	The Router has a successful 10/100MB Ethernet connection.
		Blinking	The Router is sending/receiving data through the LAN.
		Off	The LAN is not connected.
WLAN 5 GHz	Green	On	The Router is ready, but is not sending/receiving data through the wireless LAN 5 GHz band.
		Blinking	The Router is sending/receiving data through the wireless LAN 5 GHz band.
		Off	The wireless LAN 5 GHz band is not ready or has failed.

Table 1 Front Panel LEDs and WPS Button (continued)

LED	COLOR	STATUS	DESCRIPTION
WLAN 2.4 GHz	Green	On	The Router is ready, but is not sending/receiving data through the wireless LAN 2.4 GHz band.
		Blinking	The Router is sending/receiving data through the wireless LAN 2.4 GHz band.
		Off	The wireless LAN 2.4 GHz band is not ready or has failed.
WPS	Green	On	WPS is enabled.
		Blinking	The Router is negotiating a WPS connection with a wireless client.
		Off	The wireless LAN is not ready or has failed.

1.6 The WPS Button

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

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

Depending on the devices you have, you can either press a button (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.

For more information on using WPS, see Section 9.3 on page 73.

1.7 Wall Mounting

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

Table 2 Wall Mounting Information

Distance between holes	11 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.

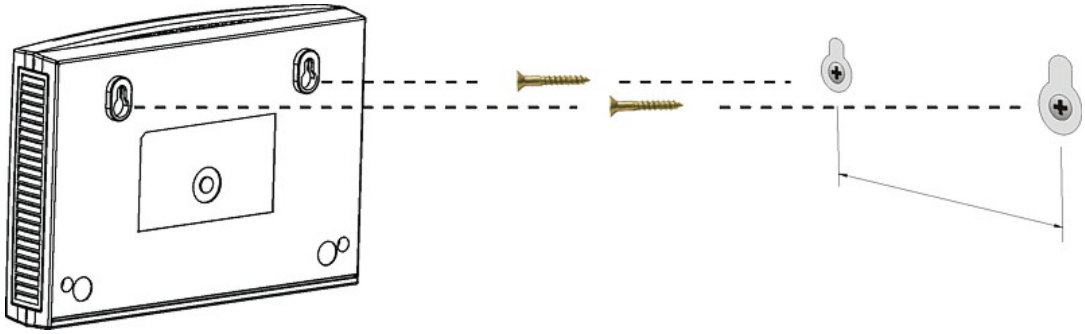
3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

   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 Router with the connection cables.

5 Align the holes on the back of the Router with the screws on the wall. Hang the Router on the screws.

Figure 2 Wall Mounting Example



2

Connection Wizard

2.1 Overview

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

The Web Configurator's wizard setup helps you configure your device to access the Internet. Refer to your ISP for your Internet account information. Leave a field blank if you don't have that information.

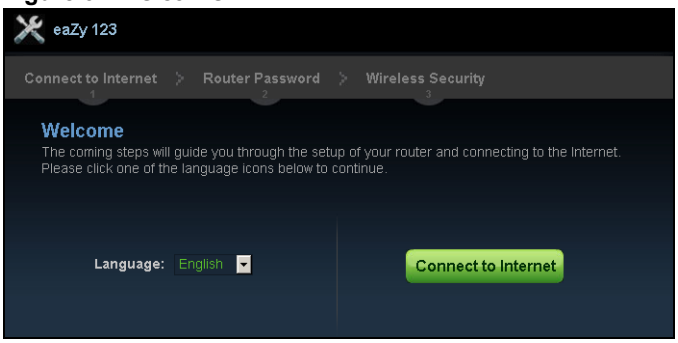
2.2 Accessing the Wizard

Launch your web browser and type "http://192.168.1.1" as the website address. Type "1234" (default) as the password and click **Login**.

Note: The Wizard appears when the Router is accessed for the first time or when you reset the Router to its default factory settings.

The Wizard screen opens. Choose your **Language** and click **Connect to Internet.**

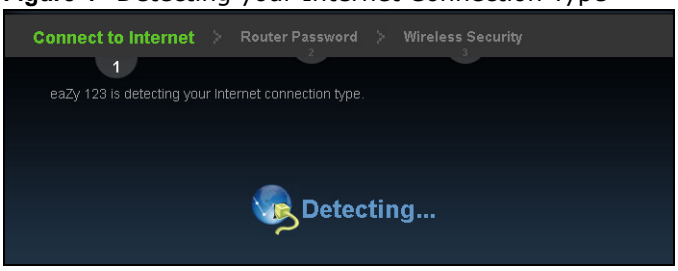
Figure 3 Welcome



2.3 Connect to Internet

The Router offers four Internet connection types. They are **Static IP**, **DHCP**, **PPPoE**, or **PPTP**. The wizard attempts to detect which WAN connection type you are using.

Figure 4 Detecting your Internet Connection Type

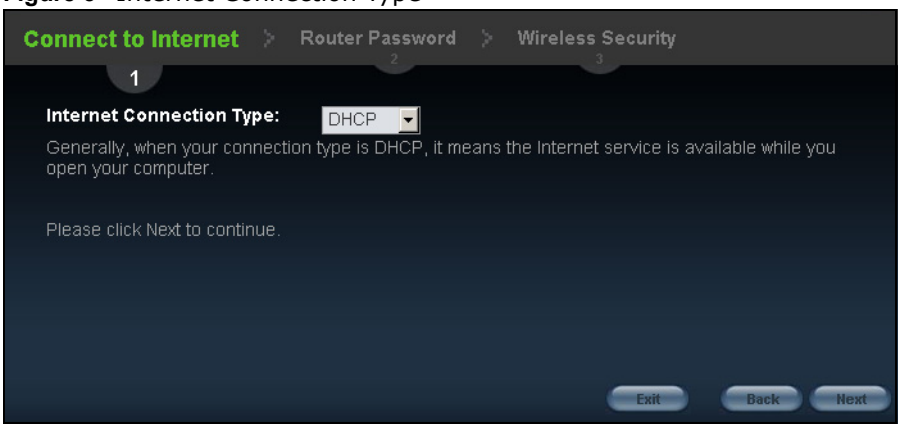


If the wizard does not detect a connection type, you must select one from the drop-down list box. Check with your ISP to make sure you use the correct type.

Note: If you get an error message, check your hardware connections. Make sure your Internet connection is up and running.

The following screen depends on your Internet connection type. Enter the details provided by your Internet Service Provider (ISP) in the fields (if any).

Figure 5 Internet Connection Type



Your Router detects the following Internet Connection type.

Table 3 Internet Connection Type

CONNECTION TYPE	DESCRIPTION
Static IP	Select the **Static IP** if an administrator assigns the IP address of your computer.
DHCP	Select the **DHCP** (Dynamic Host Configuration Protocol) option when the WAN port is used as a regular Ethernet.
PPPoE	Select the **PPPoE** (Point-to-Point Protocol over Ethernet) option for a dial-up connection.
PPTP	Select the **PPTP** (Point-to-Point Tunneling Protocol) option for a dial-up connection, and your ISP gave you an IP address and/or subnet mask.

2.3.1 Connection Type: DHCP

Choose **DHCP** as the **Internet Connection Type** when the WAN port is used as a regular Ethernet. Click **Next**.

Figure 6 Internet Connection Type: DHCP

Note: If you get an error screen after clicking **Next**, you might have selected the wrong Internet Connection type. Click **Back**, make sure your Internet connection is working and select the right Connection Type. Contact your ISP if you are not sure of your Internet Connection type.

2.3.2 Connection Type: Static IP

Choose **Static IP** as the **Internet Connection Type** if your ISP assigned an IP address for your Internet connection. Click **Next**.

Figure 7 Internet Connection Type: Static IP

The following table describes the labels in this screen.

Table 4 Internet Connection Type: Static IP

LABEL	DESCRIPTION
Internet Connection Type	Select the **Static IP** option.
IP Address	Enter the IP address provided by your ISP.

Table 4 Internet Connection Type: Static IP (continued)

LABEL	DESCRIPTION
Subnet Mask	Enter the IP subnet mask in this field.
Default Gateway	Enter the gateway IP address in this field.
Primary DNS	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The Router uses a system DNS server (in the order you specify here) to resolve domain names for DDNS and the time server. Enter the primary DNS server's IP address in the fields provided.
Secondary DNS	Enter the secondary DNS server's IP address in the fields provided.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

2.3.3 Connection Type: PPPoE

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.

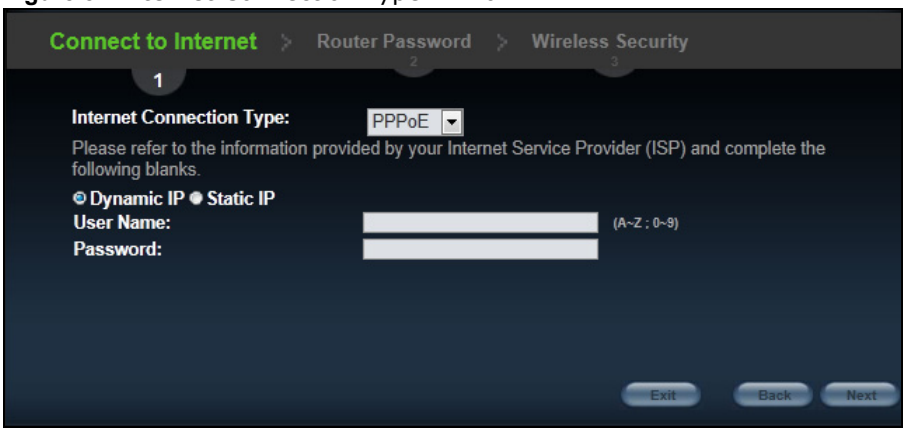
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, RADIUS).

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

Figure 8 Internet Connection Type: PPPoE



The following table describes the labels in this screen.

Table 5 Internet Connection Type: PPPoE

LABEL	DESCRIPTION
Internet Connection Type	Select the **PPPoE** option for a dial-up connection.
Dynamic IP	Select this radio button if your ISP did not assign you a fixed IP address.
Static IP	Select this radio button, provided by your ISP to give the Router a fixed, unique IP address.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

2.3.4 Connection Type: PPTP

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers 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.

Refer to the appendix for more information on PPTP.

The Router supports one PPTP server connection at any given time.

Figure 9 Internet Connection Type: PPTP

The following table describes the fields in this screen

Table 6 Internet Connection Type: PPTP

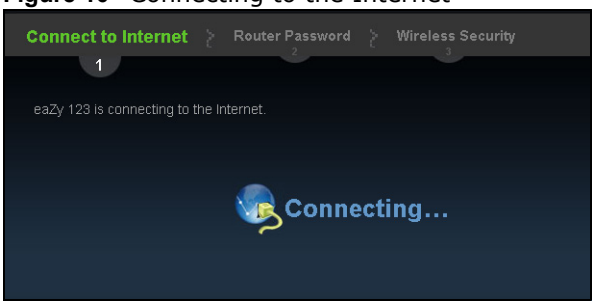
LABEL	DESCRIPTION
Internet Connection Type	Select **PPTP** from the drop-down list box. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
Dynamic IP	Select this radio button if your ISP did not assign you a fixed IP address.

Table 6 Internet Connection Type: PPTP (continued)

LABEL	DESCRIPTION
Static IP	Select this radio button, provided by your ISP to give the Router a fixed, unique IP address.
PPTP Address	Type the (static) IP address assigned to you by your ISP.
PPTP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
PPTP Gateway IP Address	Type the gateway IP address of the PPTP server.
PPTP Server IP Address	Type the server 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.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

The Router connects to the Internet.

Figure 10 Connecting to the Internet



Note: If the Wizard successfully connects to the Internet, it proceeds to the next step. If you get an error message, go back to the previous screen and make sure you have entered the correct information provided by your ISP.

2.4 Router Password

Change the login password in the following screen. Enter the new password and retype it to confirm. Click **Next** to proceed with the **Wireless Security** screen**.**

Figure 11 Router Password

2.5 Wireless Security

Configure Wireless Settings. Configure the wireless network settings on your Router in the following screen. The fields that show up depend on the kind of security you select.

2.5.1 Wireless Security: No Security

Choose **No Security** in the Wireless Security screen to let wireless devices within range access your wireless network.

Figure 12 Wireless Security: No Security

The following table describes the labels in this screen.

Table 7 Wireless Security: No Security

LABEL	DESCRIPTION
Wireless Radio	Select a wireless radio from the drop-down list box. Choose **2.4G Hz** to set the security setting for the wireless 2.4G band. Choose **5G Hz** to set the security setting for the wireless 5G band.
Wireless Network 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 Router, make sure all wireless stations use the same SSID in order to access the network.
Security mode	Select a **Security** level from the drop-down list box. Choose **None** to have no wireless LAN security configured. If you do not enable any wireless security on your Router, your network is accessible to any wireless networking device that is within range.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

2.5.2 Wireless Security: WPA-PSK/WPA2-PSK

Choose **WPA-PSK** or **WPA2-PSK** security in the Wireless Security screen to set up a password for your wireless network.

Figure 13 Wireless Security: WPA-PSK/WPA2-PSK

The following table describes the labels in this screen.

Table 8 Wireless Security: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Wireless Radio	Select a wireless radio from the drop-down list box. Choose **2.4G Hz** to set the security setting for the wireless 2.4G band. Choose **5G Hz** to set the security setting for the wireless 5G band.
Wireless Network 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 Router, make sure all wireless stations use the same SSID in order to access the network.

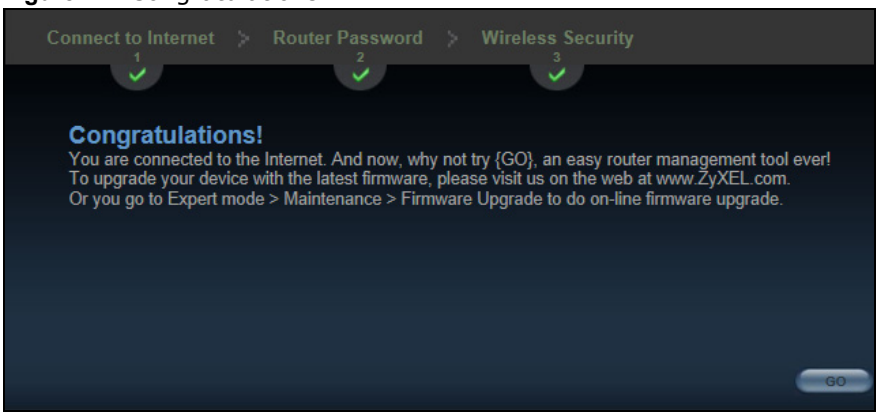
Table 8 Wireless Security: WPA-PSK/WPA2-PSK (continued)

LABEL	DESCRIPTION
Security mode	Select a **Security** level from the drop-down list box. Choose **WPA-PSK** or **WPA2-PSK** security to configure a Pre-Shared Key. Choose this option only if your wireless clients support WPA-PSK or WPA2-PSK respectively.
Wireless password	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens.
Verify Password	Retype the password to confirm.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

Congratulations! Open a web browser, such as Internet Explorer, to visit your favorite website.

Note: If you cannot access the Internet when your computer is connected to one of the Router's LAN ports, check your connections. Then turn the Router off, wait for a few seconds then turn it back on. If that does not work, log in to the web configurator again and check you have typed all information correctly. See the User's Guide for more suggestions.

Figure 14 Congratulations



You can also click **GO** to open the **Easy Mode** Web Configurator of your Router.

You have successfully set up your Router to operate on your network and access the Internet. You are now ready to connect wirelessly to your Router and access the Internet.

3

Introducing the Web Configurator

3.1 Overview

This chapter describes how to access the Router 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 Router via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions or Safari 2.0 or later versions. The recommended screen resolution is 1024 by 768 pixels.

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

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

Refer to the Troubleshooting chapter (Chapter 23 on page 165) to see how to make sure these functions are allowed in Internet Explorer.

3.2 Accessing the Web Configurator

1. Make sure your Router hardware is properly connected and prepare your computer or computer network to connect to the Router (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "http://192.168.1.1" as the website address.

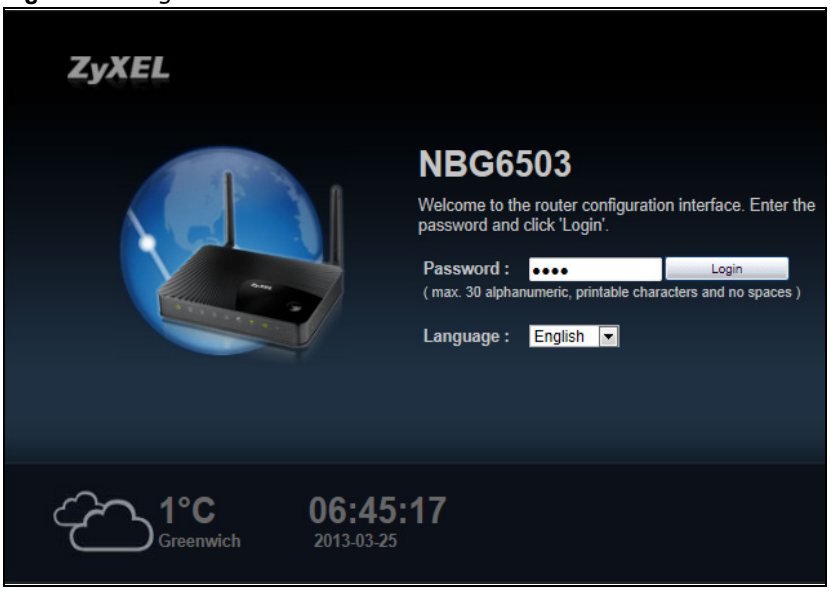
   Your computer must be in the same subnet in order to access this website address.

3.2.1 Login Screen

Note: If this is the first time you are accessing the Web Configurator, you may be redirected to the Wizard. Refer to Chapter 2 on page 21 for the Connection Wizard screens.

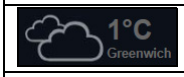
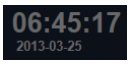
The Web Configurator initially displays the following login screen.

Figure 15 Login screen



The following table describes the labels in this screen.

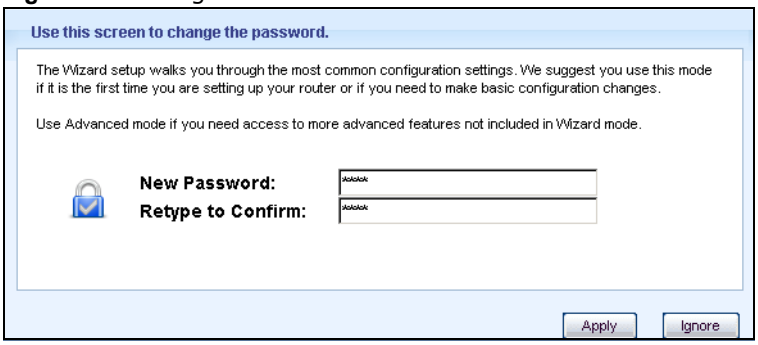
Table 9 Login screen

LABEL	DESCRIPTION
Password	Type "1234" (default) as the password.
Language	Select the language you want to use to configure the Web Configurator. Click **Login**.
	This shows the current weather, either in celsius or fahrenheit, of the city you specify in Section 3.2.3.1 on page 34.
	This shows the time (hh:mm:ss) and date (yyyy:mm:dd) of the timezone you select in Section 3.2.3.2 on page 34 or Section 22.5 on page 157. The time is in 24-hour format, for example 15:00 is 3:00 PM.

3.2.2 Password Screen

You should see a screen asking you to change your password (highly recommended) as shown next.

Figure 16 Change Password Screen



The following table describes the labels in this screen.

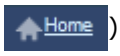
Table 10 Change Password Screen

LABEL	DESCRIPTION
New Password	Type a new password.
Retype to Confirm	Retype the password for confirmation.
Apply	Click **Apply** to save your changes back to the Router.
Ignore	Click **Ignore** if you do not want to change the password this time.

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to Chapter 22 on page 155 to change this). Simply log back into the Router if this happens.

3.2.3 Home Screen

If you have previously logged into the Web Configurator but did not click **Logout**, you may be redirected to the Home screen.

You can also open this screen by clicking **Home** ( or ) in the Easy Mode or Expert mode screens.

The Home screen displays as follows.

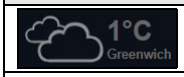
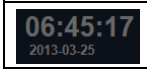
Figure 17 Home Screen

The following table describes the labels in this screen.

Table 11 Home Screen

LABEL	DESCRIPTION
Go	Click this to open the Easy mode Web Configurator.
Language	Select a language to go to the Easy mode Web Configurator in that language and click **Login**.

Table 11 Home Screen (continued)

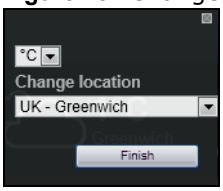
LABEL	DESCRIPTION
	(This is just an example). This shows the current weather, either in celsius or fahrenheit, of the city you specify in Section 3.2.3.1 on page 34.
	(This is just an example). This shows the time (hh:mm:ss) and date (yyyy:mm:dd) of the timezone you select in Section 3.2.3.2 on page 34 or Section 22.5 on page 157.

3.2.3.1 Weather Edit

You can change the temperature unit and select the location for which you want to know the weather.

Click the  icon to change the Weather display.

Figure 18 Change Weather



The following table describes the labels in this screen.

Table 12 Change Weather

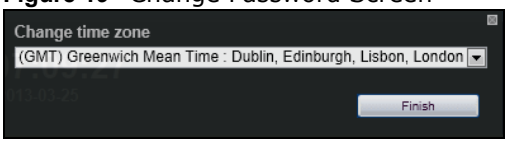
LABEL	DESCRIPTION
°C or °F	Choose which temperature unit you want the Router to display.
Change Location	Select the location for which you want to know the weather. If the city you want is not listed, choose one that is closest to it.
Finish	Click this to apply the settings and refresh the date and time display.

3.2.3.2 Time/Date Edit

One timezone can cover more than one country. You can choose a particular country in which the Router is located and have the Router display and use the current time and date for its logs.

Click the  icon to change the Weather display.

Figure 19 Change Password Screen



The following table describes the labels in this screen.

Table 13 Change Password Screen

LABEL	DESCRIPTION
Change time zone	Select the specific country whose current time and date you want the Router to display.
Finish	Click this to apply the settings and refresh the weather display.

Note: You can also edit the timezone in Section 22.5 on page 157.

3.3 Resetting the Router

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 Router to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to "1234" and the IP address will be reset to "192.168.1.1".

3.3.1 Procedure to Use the Reset Button

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

4

Monitor

4.1 Overview

This chapter discusses read-only information related to the device state of the Router.

Note: To access the Monitor screens, you can also click the links in the Summary table of the Status screen to view the bandwidth consumed, packets sent/received as well as the status of clients connected to the Router.

4.2 What You Can Do

- Use the **Log** (Section 4.3 on page 37) screen to see the logs for the activity on the Router.
- Use the **BW MGMT Monitor** screen (Section 4.4 on page 39) to view the amount of network bandwidth that applications running in the network are using.
- Use the **DHCP Table** screen (Section 4.5 on page 39) to view information related to your DHCP status.
- Use the **Packet Statistics** screen (Section 4.6 on page 40) to view port status, packet specific statistics, the "system up time" and so on.
- Use the **WLAN 2.4G Station Status** screen (Section 4.7 on page 41) to view the wireless stations that are currently associated to the Router through the wireless 2.4G network.
- Use the **WLAN 5G Station Status** screen (Section 4.8 on page 41) to view the wireless stations that are currently associated to the Router through the wireless 5G network.

4.3 The Log Screen

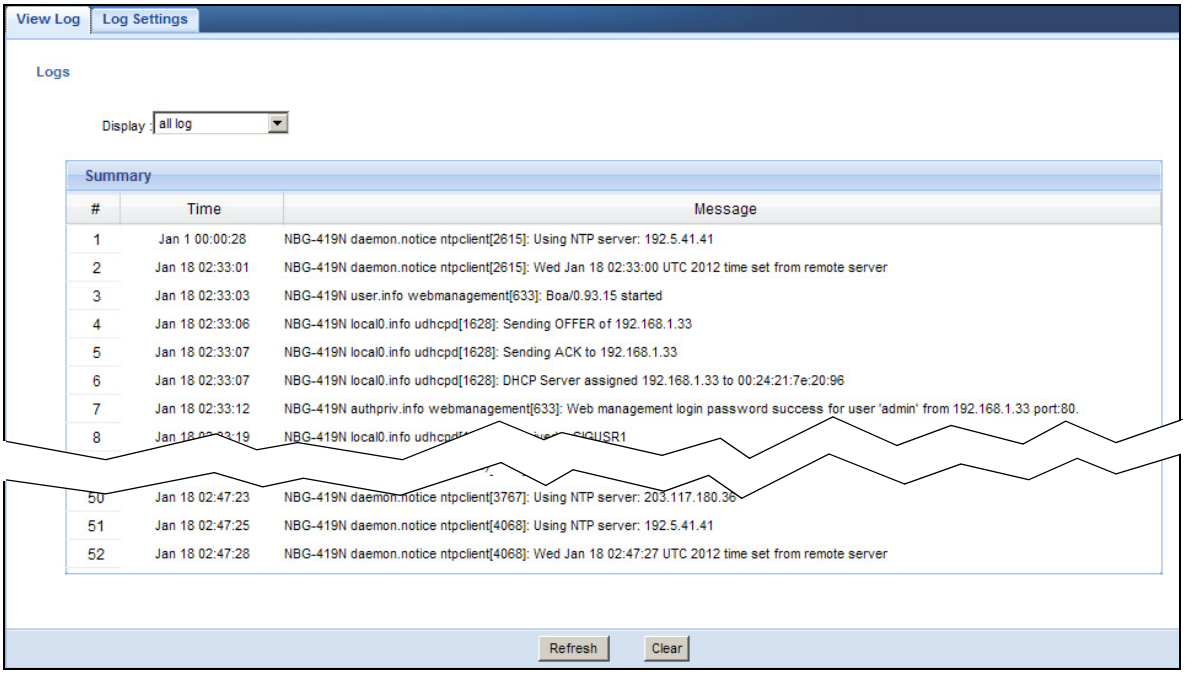
The Web Configurator allows you to look at all of the Router's logs in one location.

4.3.1 View Log

Use the **View Log** screen to see the logged messages for the Router. The log wraps around and deletes the old entries after it fills. Select what logs you want to see from the **Display** drop list. The

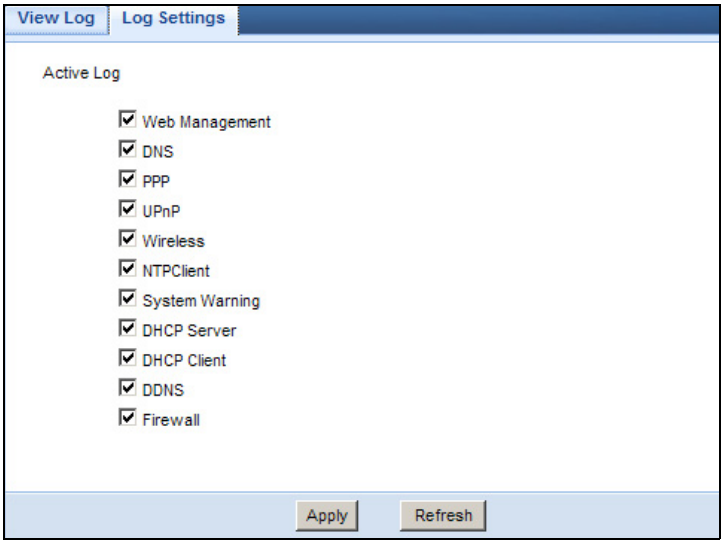
log choices depend on your settings in the **Log Settings** screen. Click **Refresh** to renew the log screen. Click **Clear** to delete all the logs.

Figure 20 View Log



You can configure which logs to display in the **View Log** screen. Go to the **Log Settings** screen and select the logs you wish to display. Click **Apply** to save your settings. Click **Refresh** to start the screen afresh.

Figure 21 Log Settings



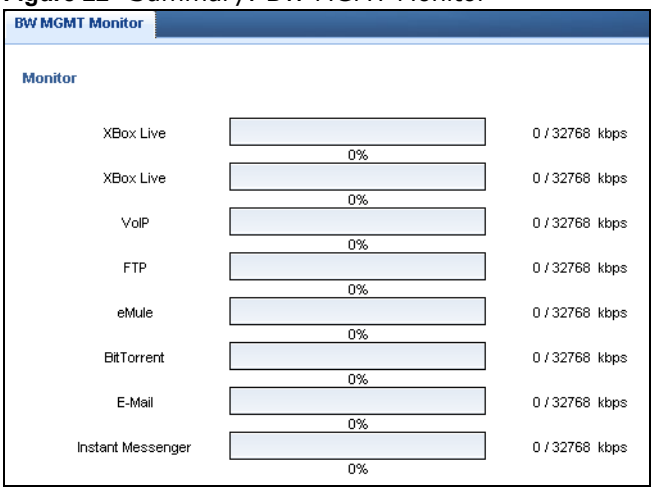
4.4 BW MGMT Monitor

The Bandwidth Management (BW MGMT) Monitor allows you to view the amount of network bandwidth that applications running in the network are using.

The bandwidth is measured in kilobits per second (kbps).

The monitor shows what kinds of applications are running in the network, the maximum kbps that each application can use, as well as the percentage of bandwidth it is using.

Figure 22 Summary: BW MGMT Monitor

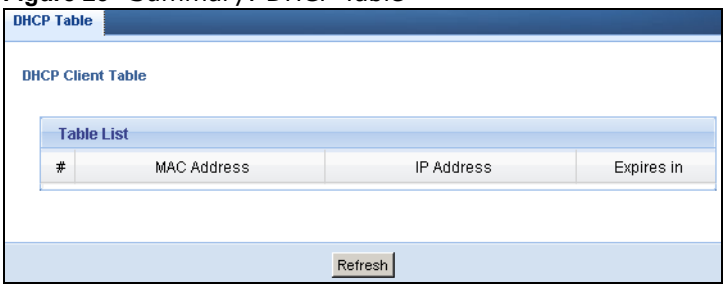


4.5 DHCP Table

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

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

Figure 23 Summary: DHCP Table



The following table describes the labels in this screen.

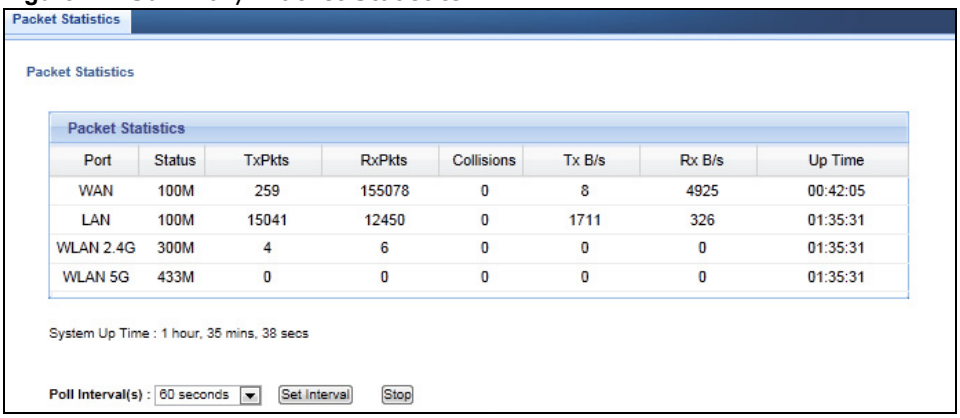
Table 14 Summary: DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
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.
IP Address	This field displays the IP address relative to the # field listed above.
Expires in	This field displays the time when the IP address and MAC address association ends.
Refresh	Click **Refresh** to renew the screen.

4.6 Packet Statistics

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

Figure 24 Summary: Packet Statistics



The following table describes the labels in this screen.

Table 15 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the Router's port type.
Status	For the LAN ports, this displays the port speed and duplex setting or **Down** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays **Down** when the line is disconnected. For WLAN 2.4G/5G, it displays the maximum transmission rate when the WLAN 2.4G/5G is enabled and **Down** when the WLAN 2.4G/5G is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.

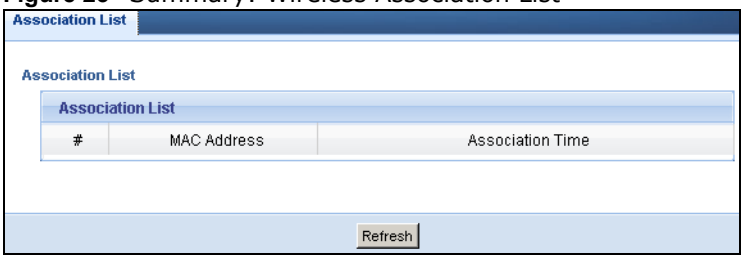
Table 15 Summary: Packet Statistics (continued)

LABEL	DESCRIPTION
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total time the Router has been for each session.
System Up Time	This is the total time the Router has been on.
Poll Interval(s)	Enter the time interval in seconds for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

4.7 WLAN 2.4G Station Status

Click the **WLAN 2.4G Station Status (Details...)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the Router in the **Association List**. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Figure 25 Summary: Wireless Association List



The following table describes the labels in this screen.

Table 16 Summary: Wireless Association List

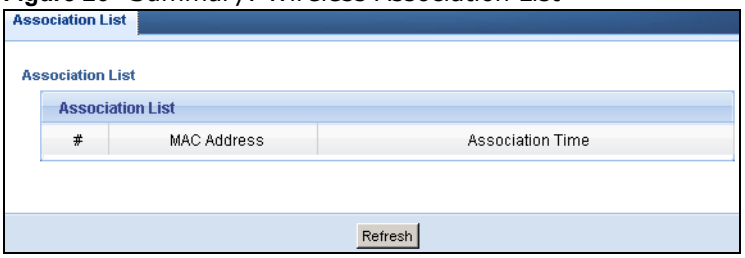
LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the Router's WLAN network.
Refresh	Click **Refresh** to reload the list.

4.8 WLAN 5G Station Status

Click the **WLAN 5G Station Status (Details...)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the Router in the **Association List**. Association means that a wireless client (for example, your network or computer with a wireless network card) has

connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Figure 26 Summary: Wireless Association List



The following table describes the labels in this screen.

Table 17 Summary: Wireless Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the Router's WLAN network.
Refresh	Click **Refresh** to reload the list.

5

Router Modes

5.1 Overview

This chapter introduces the different modes available on your Router. First, the term "mode" refers to two things in this User's Guide.

- **Web Configurator mode**. This refers to the Web Configurator interface you want to use for editing Router features.
- **Device mode**. This is the operating mode of your Router, or simply how the Router is being used in the network.

5.1.1 Web Configurator Modes

This refers to the configuration interface of the Web Configurator, which has two modes:

- **Easy**. The Web Configurator shows this mode by default. Refer to Chapter 6 on page 45 for more information on the screens in this mode. This interface may be sufficient for users who just want to use the device.
- **Expert**. Advanced users can change to this mode to customize all the functions of the Router. Click **Expert Mode** after logging into the Web Configurator. The User's Guide Chapter 3 on page 31 through Chapter 22 on page 155 discusses the screens in this mode.

5.1.2 Device Modes

This refers to the operating mode of the Router, which can act as a:

- **Router**. This is the default device mode of the Router. Use this mode to connect the local network to another network, like the Internet. Go to Section 7.3 on page 58 to view the **Status** screen in this mode.
- **Access Point**. Use this mode if you want to extend your network by allowing network devices to connect to the Router wirelessly. Go to Section 8.4 on page 68 view the **Status** screen in this mode.

For more information on these modes and to change the mode of your Router, refer to Section 22.10 on page 163.

The menu for changing device modes is available in **Expert** mode only.

Note: Choose your Device Mode carefully to avoid having to change it later.

When changing to another mode, the IP address of the Router changes. The running applications and services of the network devices connected to the Router can be interrupted.

6

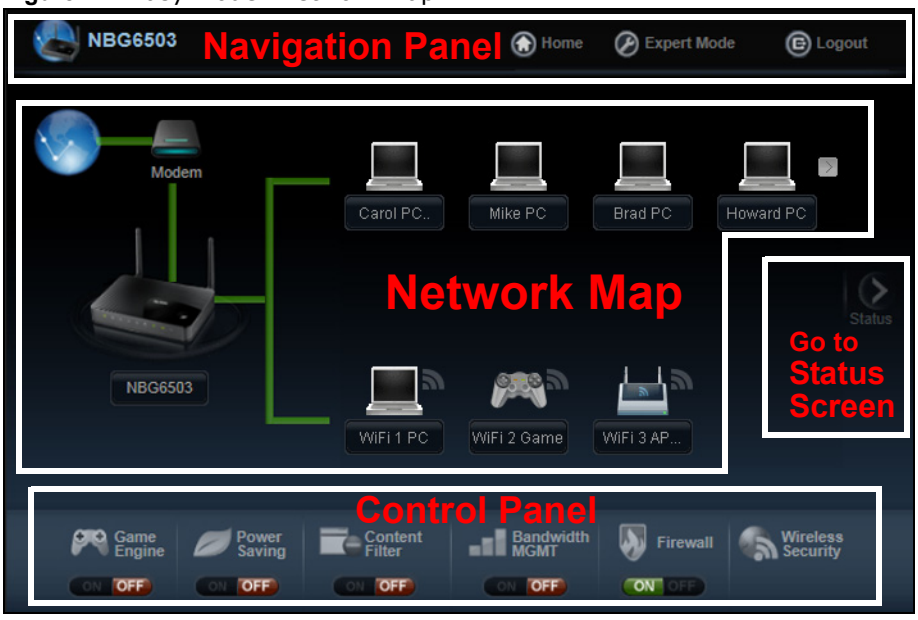
Easy Mode

6.1 Overview

The Web Configurator is set to **Easy Mode** by default. You can configure several key features of the Router in this mode. This mode is useful to users who are not fully familiar with some features that are usually intended for network administrators.

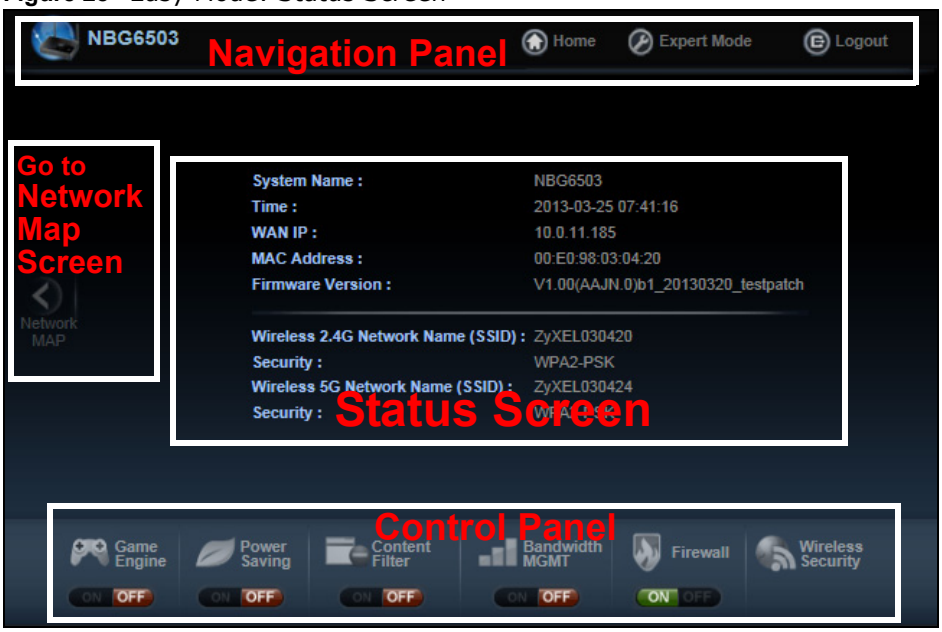
When you log in to the Web Configurator, the following screen opens.

Figure 27 Easy Mode: Network Map



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

Figure 28 Easy Mode: Status Screen



6.2 What You Can Do

You can do the following in this mode:

- Use this **Navigation Panel** (Section 6.4 on page 47) to opt out of the **Easy** mode.
- Use the **Network Map** screen (Section 6.5 on page 47) to check if your Router can ping the gateway and whether it is connected to the Internet.
- Use the **Control Panel** (Section 6.6 on page 48) to configure and enable Router features, including wireless security, wireless scheduling and bandwidth management and so on.
- Use the **Status Screen** screen (Section 6.7 on page 55) to view read-only information about the Router, including the WAN IP, MAC Address of the Router and the firmware version.

6.3 What You Need to Know

Between the different device modes, the Control Panel (Section 6.6 on page 48) changes depending on which features are applicable to the mode:

- **Router Mode**: All Control Panel features are available.
- **Access Point Mode**: Only **Power Saving** and **Wireless Security** are available.

6.4 Navigation Panel

Use this navigation panel to opt out of the **Easy** mode.

Figure 29 Navigation Panel

The following table describes the labels in this screen.

Table 18 Navigation Panel

ITEM	DESCRIPTION
Home	Click this to go to the **Login** page.
Expert Mode	Click this to change to **Expert** mode and customize features of the Router.
Logout	Click this to end the Web Configurator session.

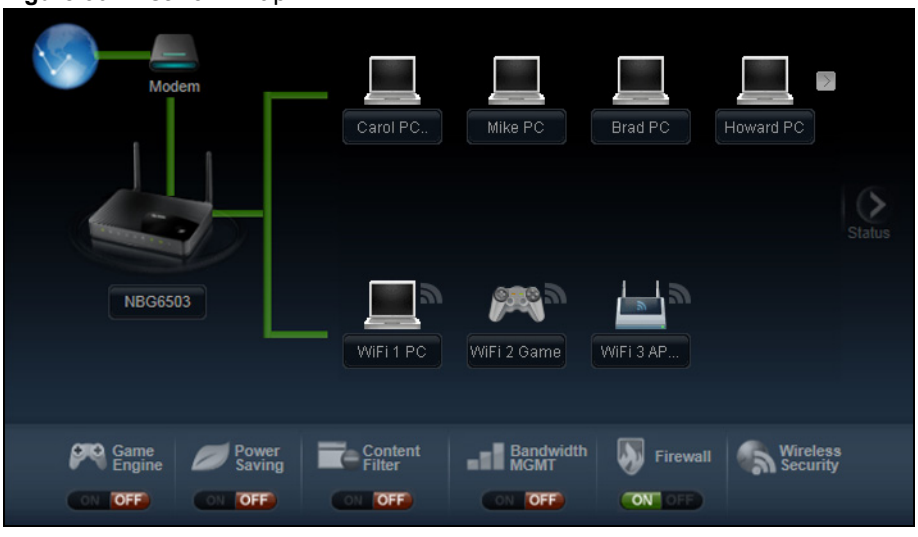
6.5 Network Map

Note: The Network MAP is viewable by Windows XP (need to install patch), Windows Vista and Windows 7 users only. For Windows XP (Service Pack 2) users, you can see the network devices connected to the Router by downloading the LLTD (Link Layer Topology Discovery) patch from the Microsoft Website.

Note: Don't worry if the Network Map does not display in your web browser. This feature may not be supported by your system. You can still configure the Control Panel (Section 6.6 on page 48) in the Easy Mode and the Router features that you want to use in the Expert Mode.

When you log into the Network Configurator, the Network Map is shown as follows.

Figure 30 Network Map



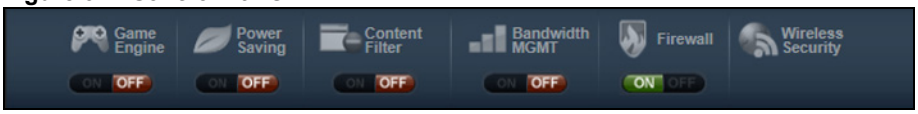
The line connecting the Router to the gateway becomes green when the Router is able to ping the gateway. It becomes red when the ping initiating from the Router does not get a response from the gateway. The same rule applies to the line connecting the gateway to the Internet.

You can also view the devices (represented by icons indicating the kind of network device) connected to the Router, including those connecting wirelessly. Right-click on the Router icon to refresh the network map and go to the Wizard. Right click on the other icons to view information about the device.

6.6 Control Panel

The features configurable in **Easy Mode** are shown in the **Control Panel**.

Figure 31 Control Panel



Switch **ON** to enable the feature. Otherwise, switch **OFF**. If the feature is turned on, the green light flashes. If it is turned off, the red light flashes.

Additionally, click the feature to open a screen where you can edit its settings.

The following table describes the labels in this screen.

Table 19 Control Panel

ITEM	DESCRIPTION
Game Engine	Switch **ON** to maximize bandwidth for gaming traffic in your network. Otherwise, switch **OFF**. Refer to Section 6.6.1 on page 49 to see this screen.
Power Saving	Click this to schedule the wireless feature of the Router. Disabling the wireless function helps lower the energy consumption of the Router. Switch **ON** to apply wireless scheduling. Otherwise, switch **OFF**. Refer to Section 6.6.2 on page 49 to see this screen.
Content Filter	Click this to restrict access to certain websites, based on keywords contained in URLs, to which you do not want users in your network to open. Switch **ON** to apply website filtering. Otherwise, switch **OFF**. Refer to Section 6.6.3 on page 51 to see this screen.
Bandwidth MGMT	Click this to edit bandwidth management for predefined applications. Switch **ON** to have the Router management bandwidth for uplink and downlink traffic according to an application or service. Otherwise, switch **OFF**. Refer to Section 6.6.4 on page 51 to see this screen.

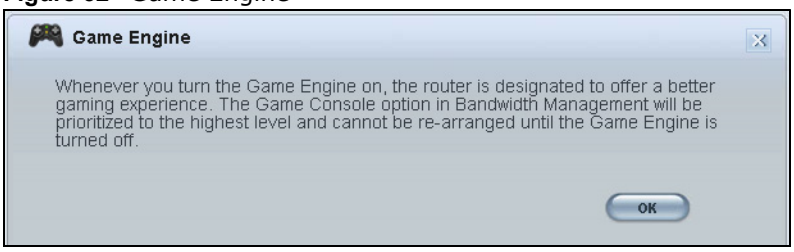
Table 19 Control Panel (continued)

ITEM	DESCRIPTION
Firewall	Switch **ON** to ensure that your network is protected from Denial of Service (DoS) attacks. Otherwise, switch **OFF**. Refer to Section 6.6.5 on page 52 to see this screen.
Wireless Security	Click this to configure the wireless security, such as SSID, security mode and WPS key on your Router. Refer to Section 6.6.6 on page 52 to see this screen.

6.6.1 Game Engine

When this feature is enabled, the Router maximizes the bandwidth for gaming traffic that it forwards out through an interface.

Figure 32 Game Engine



Note: When this is switched on, the **Game Console** tab in the **Bandwidth MGMT** screen is automatically positioned on top.

Turn this off if your network is not using gaming.

Click **OK** to close this screen.

6.6.2 Power Saving

Use this screen to set the day of the week and time of the day when your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default.

Disabling the wireless capability lowers the energy consumption of the of the Router.

Figure 33 Power Saving

The following table describes the labels in this screen.

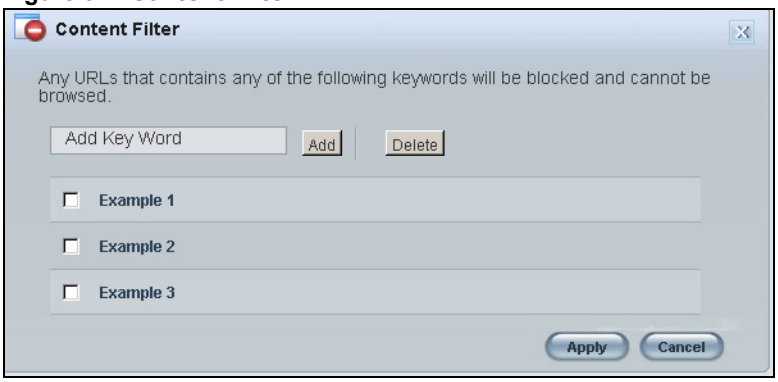
Table 20 Power Saving

LABEL	DESCRIPTION
Wireless Radio	Select the wireless radio to set its power saving settings.
WLAN Status	Select **On** or **Off** to specify whether the Wireless LAN is turned on or off (depending on what you selected in the **WLAN Status** field). This field works in conjunction with the **Day** and **Except for the following times** fields.
Day	Select **Everyday** or the specific days to turn the Wireless LAN on or off. If you select **Everyday** you can not select any specific days. This field works in conjunction with the **Except for the following times** field.
For the following times (24-Hour Format)	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 on between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields. In this time format, midnight is 00:00 and progresses up to 24:00. For example, 6:00 PM is 18:00.
Apply	Click **Apply** to save your changes back to the Router.
Reset	Click **Reset** to begin configuring this screen afresh.

6.6.3 Content Filter

Use this screen to restrict access to certain websites, based on keywords contained in URLs, to which you do not want users in your network to open.

Figure 34 Content Filter



The following table describes the labels in this screen.

Table 21 Content Filter

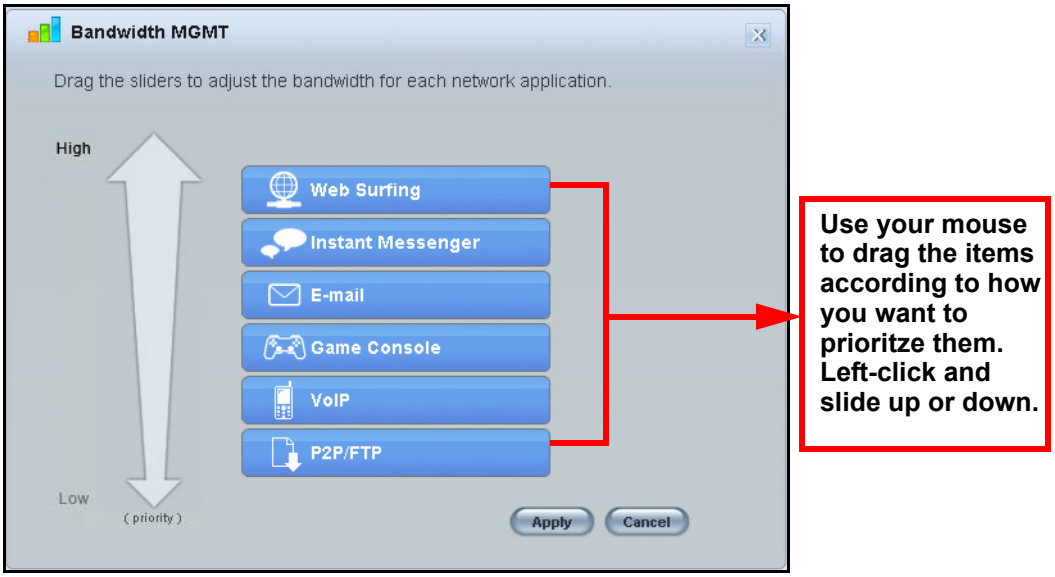
LABEL	DESCRIPTION
Add	Click **Add** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. Note: The Router does not recognize wildcard characters as keywords. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the text box and click **Delete** to remove it. The keyword disappears from the text box after you click **Apply**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to close this screen without saving any changes.

6.6.4 Bandwidth MGMT

Use this screen to set bandwidth allocation to pre-defined services and applications for bandwidth allocation.

The Router uses bandwidth management for incoming and outgoing traffic. Rank the services and applications by dragging them accordingly from **High** to **Low** and click **Apply**. Click **Cancel** to close the screen.

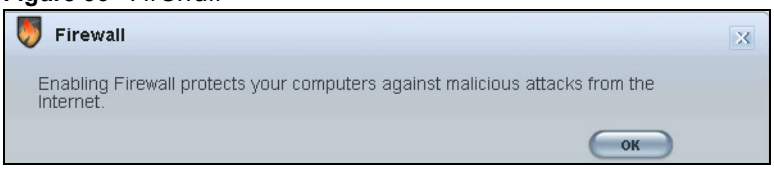
Figure 35 Bandwidth MGNT



6.6.5 Firewall

Enable this feature to protect the network from Denial of Service (DoS) attacks. The Router blocks repetitive pings from the WAN that can otherwise cause systems to slow down or hang.

Figure 36 Firewall



Click **OK** to close this screen.

6.6.6 Wireless Security

Use this screen to configure security for your the Wireless LAN. You can enter the SSID and select the wireless security mode in the following screen.

Note: You can enable the Wireless function of your Router by first turning on the switch in the back panel.

Figure 37 Wireless Security

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

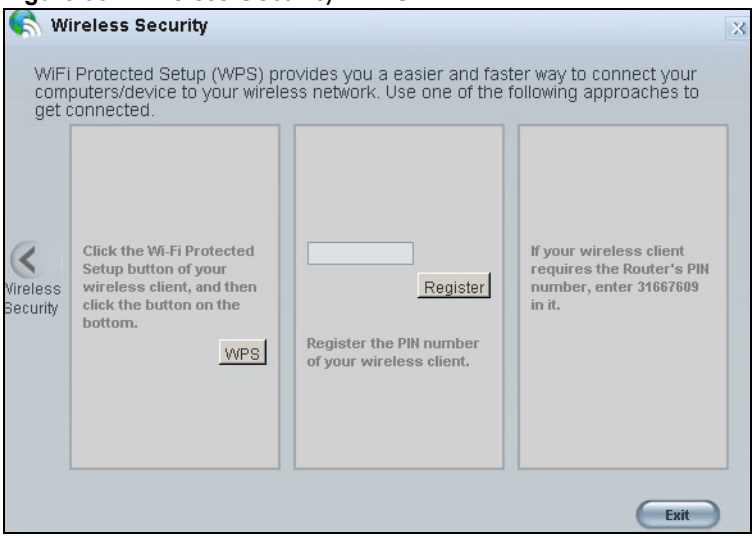
Table 22 Wireless Security

LABEL	DESCRIPTION
Wireless Radio	Select the wireless radio to set its security setting.
Wireless Network Name (SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 keyboard characters) for the wireless LAN.
Security mode	Select **WPA-PSK** or **WPA2-PSK** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. Select **No Security** to allow any client to connect to this network without authentication.
Wireless password	This field appears when you choose wither **WPA-PSK** or **WPA2-PSK** as the security mode. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Verify password	Type the password again to confirm.
Apply	Click **Apply** to save your changes back to the Router.
Cancel	Click **Cancel** to close this screen.
WPS	Click this to configure the WPS screen. You can transfer the wireless settings configured here (**Wireless Security** screen) to another wireless device that supports WPS.

6.6.7 WPS

Use this screen to add a wireless station to the network using WPS. Click **WPS** in the **Wireless Security** to open the following screen.

Figure 38 Wireless Security: WPS



The following table describes the labels in this screen.

Table 23 Wireless Security: WPS

LABEL	DESCRIPTION
Wireless Security	Click this to go back to the Wireless Security screen.
WPS	Create a secure wireless network simply by pressing a button. The Router scans for a WPS-enabled device within the range and performs wireless security information synchronization. Note: After you click the **WPS** 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.
Register	Create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the Router's interface and pushing this button. Type the same PIN number generated in the wireless station's utility. Then click **Register** to associate to each other and perform the wireless security information synchronization.
Exit	Click **Exit** to close this screen.

6.7 Status Screen in Easy Mode

In the Network Map screen, click **Status** to view read-only information about the Router.

Figure 39 Status Screen in Easy Mode

The following table describes the labels in this screen.

Table 24 Status Screen in Easy Mode

ITEM	DESCRIPTION
Name	This is the name of the Router in the network. You can change this in the **Maintenance > General** screen in Section 22.3 on page 155.
Time	This is the current system date and time. The date is in YYYY:MM:DD (Year-Month-Day) format. The time is in HH:MM:SS (Hour:Minutes:Seconds) format.
WAN IP	This is the IP address of the WAN port.
MAC Address	This is the MAC address of the Router.
Firmware Version	This shows the firmware version of the Router. The firmware version format shows the trunk version, model code and release number.
Wireless 2.4G Network Name	This shows the SSID of the wireless 2.4G network. You can configure this in the Wireless Security screen (Section 6.6.6 on page 52; Section 10.3.1.1 on page 84).
Security	This shows the wireless security used by the Router for the 2.4G wireless radio.
Wireless 5G Network Name	This shows the SSID of the wireless 5G network. You can configure this in the Wireless Security screen (Section 6.6.6 on page 52; Section 10.3.1.1 on page 84).
Security	This shows the wireless security used by the Router for the 5G wireless radio.

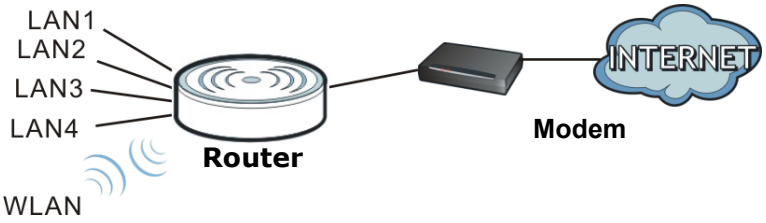
7

Router Mode

7.1 Overview

The Router is set to router mode by default. Routers are used to connect the local network to another network (for example, the Internet). In the figure below, the Router connects the local network (**LAN1** ~ **LAN4**) to the Internet.

Figure 40 Router Network



Note: The Status screen is shown after changing to the Expert mode of the Web Configurator. It varies depending on the device mode of your Router.

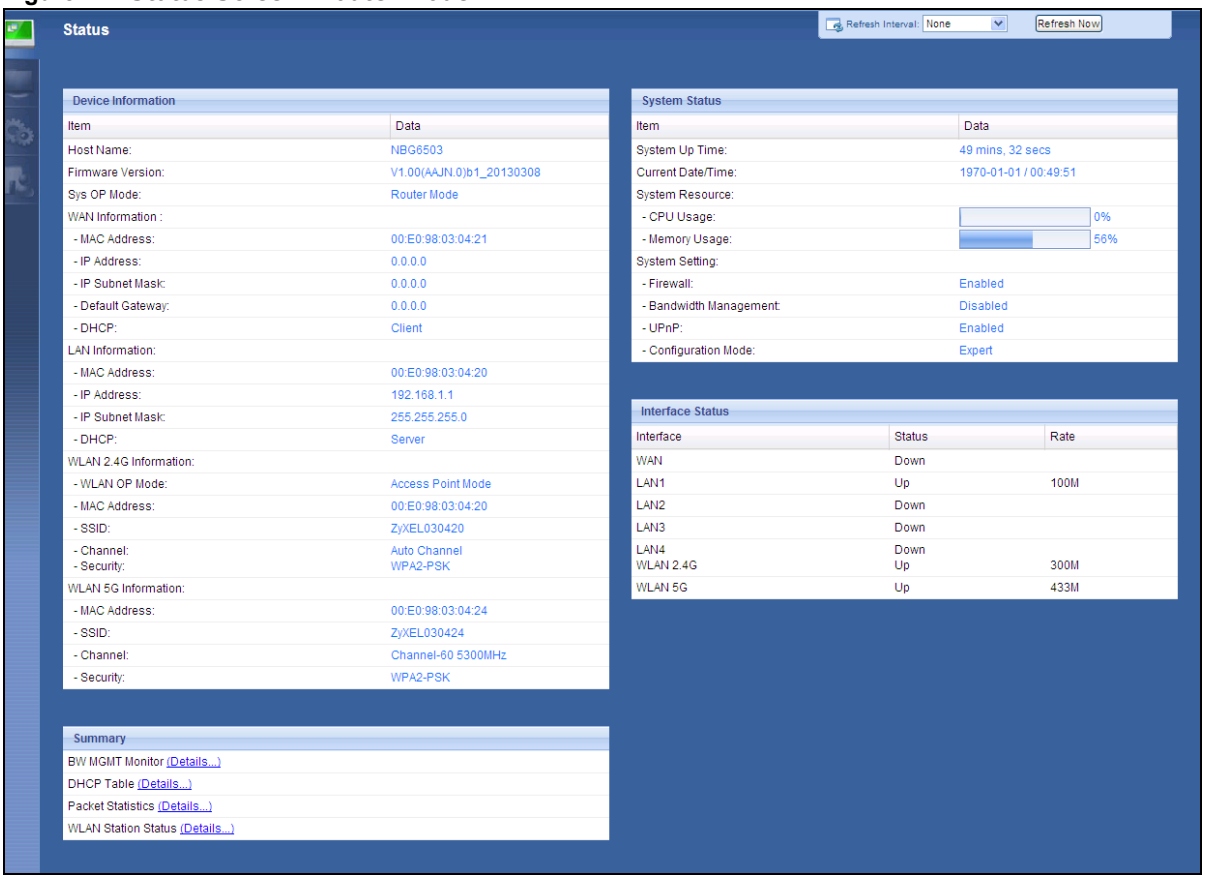
7.2 What You Can Do

Use the **Status** screen (Section 7.3 on page 58) to view read-only information about your Router.

7.3 Status Screen

Click  to open the status screen.

Figure 41 Status Screen: Router Mode



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

Table 25 Status Screen Icon Key: Router Mode

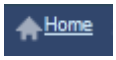
ICON	DESCRIPTION
	Click this icon to view copyright and a link for related product information.
	Click this icon to go to Easy Mode. See Chapter 6 on page 45.
	Click this to go to the Home page. See Chapter 4 on page 37.
	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
	Click this button to refresh the status screen statistics.
	Click this icon to see the Status page. The information in this screen depends on the device mode you select.
	Click this icon to see the **Monitor** navigation menu.

Table 25 Status Screen Icon Key: Router Mode (continued)

ICON	DESCRIPTION
	Click this icon to see the **Configuration** navigation menu.
	Click this icon to see the **Maintenance** navigation menu.

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

Table 26 Status Screen: Router Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the **System Name** you enter in the **Maintenance** > **General** screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the Router is set - **Router Mode**.
WAN Information	
- MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the WAN port's IP address.
- IP Subnet Mask	This shows the WAN port's subnet mask.
- Default Gateway	This shows the WAN port's gateway IP address.
- DHCP	This shows the LAN port's DHCP role - **Client** or **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	This shows the LAN port's DHCP role - **Server** or **None**.
WLAN 2.4G Information	
- WLAN OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the Router's wireless LAN is set - **Access Point Mode**.
- MAC Address	This shows the wireless adapter MAC Address of your device.
- SSID	This shows a descriptive name used to identify the Router in the wireless LAN.
- Channel	This shows the channel number which the Router is currently using over the wireless LAN..
- Security	This shows the level of wireless security the Router is using.
WLAN 5G Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- SSID	This shows a descriptive name used to identify the Router in the wireless LAN.
- Channel	This shows the channel number which the Router is currently using over the wireless LAN..
- Security	This shows the level of wireless security the Router is using.
System Status	
Item	This column shows the type of data the Router is recording.
Data	This column shows the actual data recorded by the Router.
System Up Time	This is the total time the Router has been on.

Table 26 Status Screen: Router Mode (continued)

LABEL	DESCRIPTION
Current Date/Time	This field displays your Router's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the Router's processing ability is currently used. When this percentage is close to 100%, the Router is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.)
- Memory Usage	This shows what percentage of the heap memory the Router is using.
System Setting	
- Firewall	This shows whether the firewall is enabled or not.
- Bandwidth Management	This shows whether the bandwidth management is enabled or not.
- UPnP	This shows whether UPnP is enabled or not.
- Configuration Mode	This shows the web configurator mode you are viewing - **Expert**.
Interface Status	
Interface	This displays the Router port types. The port types are: **WAN**, **LAN** and **WLAN**.
Status	For the LAN and WAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or **N/A** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
Summary	
BW MGMT Monitor	Click **Details...** to go to the **Monitor > BW MGMT Monitor** screen (Section 4.4 on page 39). Use this screen to view the amount of network bandwidth that applications running in the network are using.
DHCP Table	Click **Details...** to go to the **Monitor > DHCP Table** screen (Section 4.5 on page 39). Use this screen to view current DHCP client information.
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen (Section 4.6 on page 40). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click **Details...** to go to the **Monitor > WLAN 2.4G / 5G Station Status** screen (Section 4.8 on page 41). Use this screen to view the wireless stations that are currently associated to the Router.

7.3.1 Navigation Panel

Use the sub-menus on the navigation panel to configure Router features.

Figure 42 Navigation Panel: Router Mode

The following table describes the sub-menus.

Table 27 Navigation Panel: Router Mode

LINK	TAB	FUNCTION
Status		This screen shows the Router's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
MONITOR		
Log		Use this screen to view the list of activities recorded by your Router.
BW MGMT		Use this screen to view the amount of network bandwidth that applications running in the network are using.
DHCP Table		Use this screen to view current DHCP client information.
Packet Statistics		Use this screen to view port status and packet specific statistics.
WLAN 2.4G Station Status		Use this screen to view the wireless stations that are currently associated to the Router through the wireless 2.4G network.
WLAN 5G Station Status		Use this screen to view the wireless stations that are currently associated to the Router through the wireless 5G network.
CONFIGURATION		
Network		

Table 27 Navigation Panel: Router Mode (continued)

LINK	TAB	FUNCTION
Wireless LAN 2.4G	General	Use this screen to configure wireless 2.4G LAN.
	MAC Filter	Use the MAC filter screen to configure the Router to block access to devices or block the devices from accessing the Router.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
	WDS	Use this screen to set up Wireless Distribution System (WDS) on your Router.
Wireless LAN 5G	General	Use this screen to configure wireless 5G LAN.
	MAC Filter	Use the MAC filter screen to configure the Router to block access to devices or block the devices from accessing the Router.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
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 other advanced properties.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
	IP Alias	Use this screen to have the Router apply IP alias to create LAN subnets.
DHCP Server	General	Use this screen to enable the Router's DHCP server.
	Advanced	Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
NAT	General	Use this screen to enable NAT.
	Application	Use this screen to configure servers behind the Router.
	Advanced	Use this screen to change your Router's port triggering settings.
DDNS	General	Use this screen to set up dynamic DNS.
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	This screen shows a summary of the firewall rules, and allows you to edit/ add a firewall rule.
Content Filter		Use this screen to block certain web features and sites containing certain keywords in the URL.
Management		

Table 27 Navigation Panel: Router Mode (continued)

LINK	TAB	FUNCTION
Bandwidth Management	General	Use this screen to enable bandwidth management.
	Advanced	Use this screen to set the upstream bandwidth and edit a bandwidth management rule.
	Monitor	Use this screen to view the amount of network bandwidth that applications running in the network are using.
Remote Management	WWW	Use this screen to be able to access the Router from the LAN, WAN or both.
UPnP	General	Use this screen to enable UPnP on the Router.
MAINTENANCE		
General		Use this screen to view and change administrative settings such as system and domain names.
Password	Password Setup	Use this screen to change the password of your Router.
Time	Time Setting	Use this screen to change your Router's time and date.
Firmware Upgrade		Use this screen to upload firmware to your Router.
Backup/ Restore		Use this screen to backup and restore the configuration or reset the factory defaults to your Router.
Restart		This screen allows you to reboot the Router without turning the power off.
Sys OP Mode		This screen allows you to select whether your device acts as a Router or a Access Point.

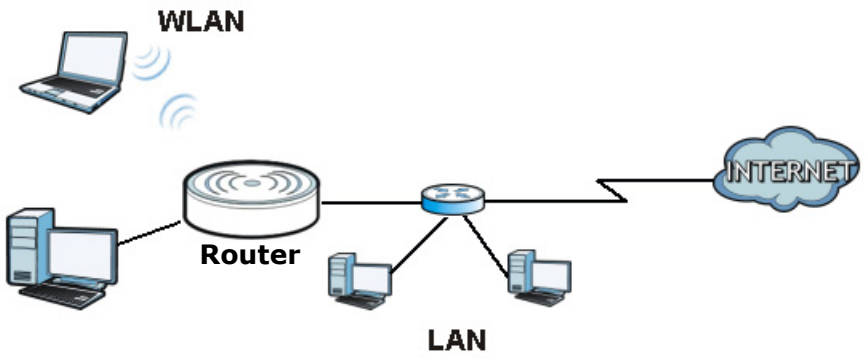
8

Access Point Mode

8.1 Overview

Use your Router as an access point (AP) if you already have a router or gateway on your network. In this mode your Router bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 43 Wireless Internet Access in Access Point Mode



Many screens that are available in Router mode are not available in Access Point mode, such as bandwidth management and firewall.

Note: See Chapter 9 on page 73 for an example of setting up a wireless network in Access Point mode.

8.2 What You Can Do

- Use the **Status** screen (Section 8.4 on page 68) to view read-only information about your Router.
- Use the **LAN** screen (Section 8.5 on page 70) to set the IP address for your Router acting as an access point.

8.3 What You Need to Know

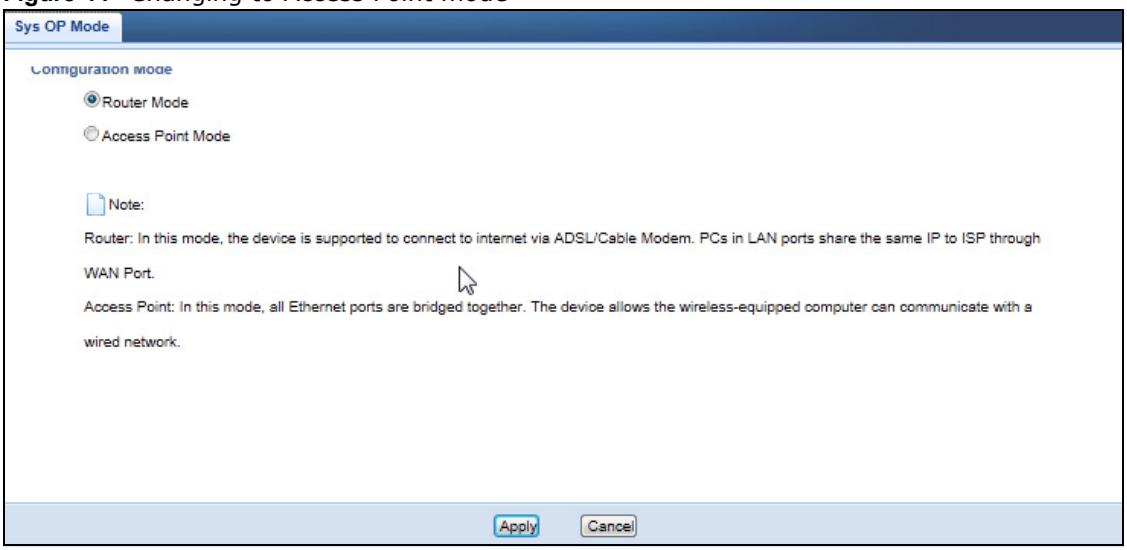
See Chapter 9 on page 73 for a tutorial on setting up a network with the Router as an access point.

8.3.1 Setting your Router to AP Mode

1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.

2 To use your Router as an access point, go to **Maintenance > Sys OP Mode** and select **Access Point mode.**

Figure 44 Changing to Access Point mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your Router is already in Access Point mode.

3 When you select **Access Point Mode**, the following pop-up message window appears.

Figure 45 Pop up for Access Point mode

Click **OK**.

4 Click **Apply**. The Web Configurator refreshes once the change to Access Point mode is successful.

8.3.2 Accessing the Web Configurator in Access Point Mode

Log in to the Web Configurator in Access Point mode, do the following:

1 Connect your computer to the LAN port of the Router.

2 The default IP address of the Router is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix B on page 181 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 "192.168.1.2" as the web address in your web browser.

Note: After clicking Login, the Easy mode appears. Refer to page 45 for the Easy mode screens. Change to Expert mode to see the screens described in the sections following this.

8.3.3 Configuring your WLAN, Bandwidth Management and Maintenance Settings

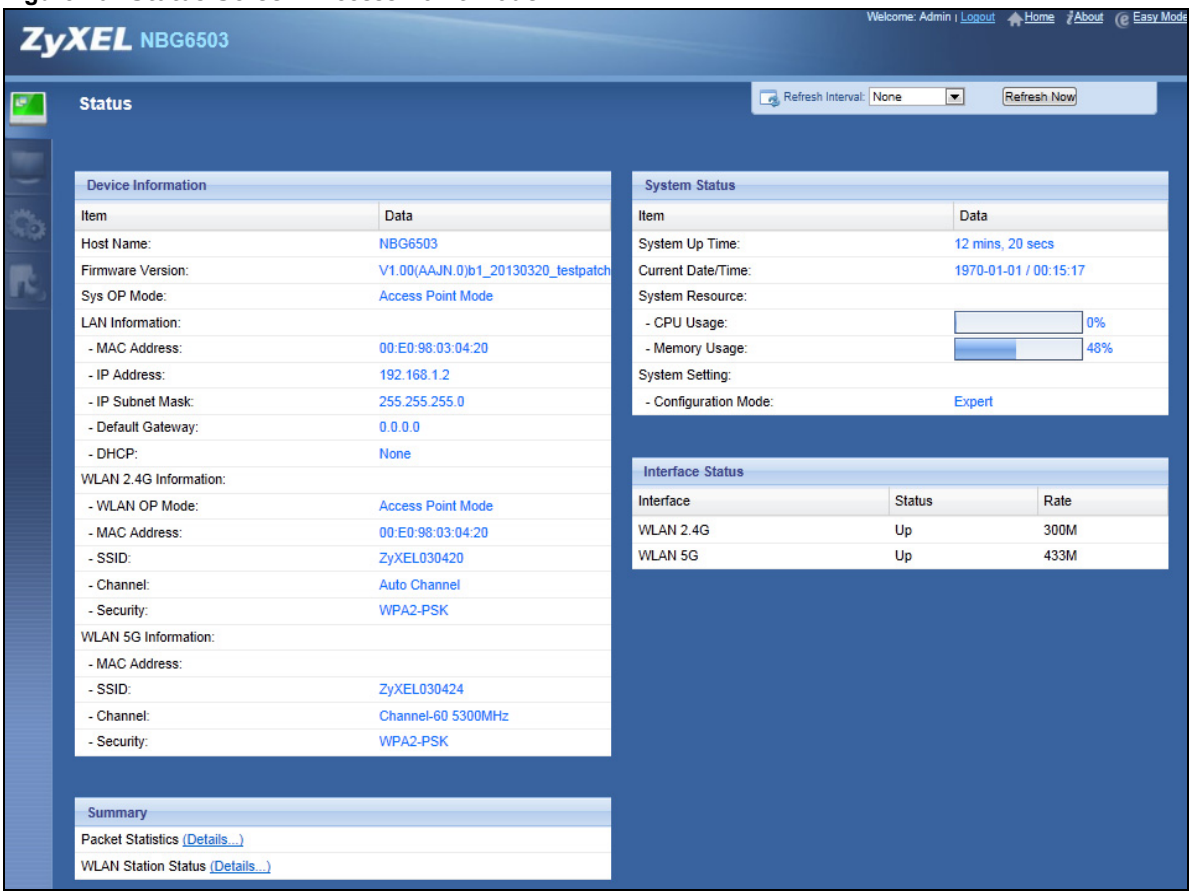
The configuration of wireless, bandwidth management and maintenance settings in **Access Point** mode is the same as for **Router Mode**.

- See Chapter 10 on page 83 for information on the configuring your wireless network.
- See Chapter 19 on page 137 for information on configuring your Bandwidth Management screen.
- See Chapter 22 on page 155 to Chapter 22 on page 155 for information on configuring your Maintenance settings.

8.4 AP Mode Status Screen

Click  to open the **Status** screen.

Figure 46 Status Screen: Access Point Mode



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

Table 28 Status Screen: Access Point Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the **System Name** you enter in the **Maintenance** > **General** screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the Router is set - **Access Point Mode**.
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.
- Default Gateway	This shows the LAN Ethernet default gateway of your device.
- DHCP	This shows the LAN port's DHCP role - **Server, Client or None.**

Table 28 Status Screen: Access Point Mode (continued)

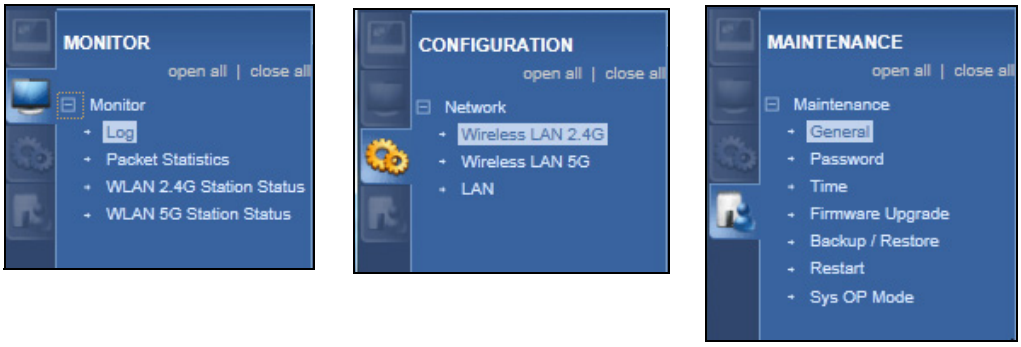
LABEL	DESCRIPTION
WLAN 2.4G Information	
- WLAN OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the Router's wireless LAN is set - **Access Point Mode**.
- MAC Address	This shows the wireless adapter MAC Address of your device.
- SSID	This shows a descriptive name used to identify the Router in the wireless 2.4G LAN.
- Channel	This shows the channel number which you select manually.
- Security	This shows the level of wireless security the Router is using.
WLAN 5G Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- SSID	This shows a descriptive name used to identify the Router in the wireless 5G LAN.
- Channel	This shows the channel number which you select manually.
- Security	This shows the level of wireless security the Router is using.
System Status	
Item	This column shows the type of data the Router is recording.
Data	This column shows the actual data recorded by the Router.
System Up Time	This is the total time the Router has been on.
Current Date/Time	This field displays your Router's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the Router's processing ability is currently used. When this percentage is close to 100%, the Router is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.
- Memory Usage	This shows what percentage of the heap memory the Router is using.
System Setting	
- Configuration Mode	This shows the web configurator mode you are viewing - **Expert**.
Interface Status	
Interface	This displays the Router port types. The port types are: **LAN**, **WLAN 2.4G**, and **WLAN 5G**.
Status	For the LAN and WAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or **N/A** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
Summary	
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen (Section 4.6 on page 40). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click **Details...** to go to the **Monitor > WLAN 2.4G / 5G Station Status** screen (Section 4.8 on page 41). Use this screen to view the wireless stations that are currently associated to the Router.

8.4.0.1 Navigation Panel

Use the menu in the navigation panel to configure Router features in Access Point mode.

The following screen and table show the features you can configure in Access Point mode.

Figure 47 Menu: Access Point Mode



Refer to Table 27 on page 61 for descriptions of the labels shown in the **Navigation** panel.

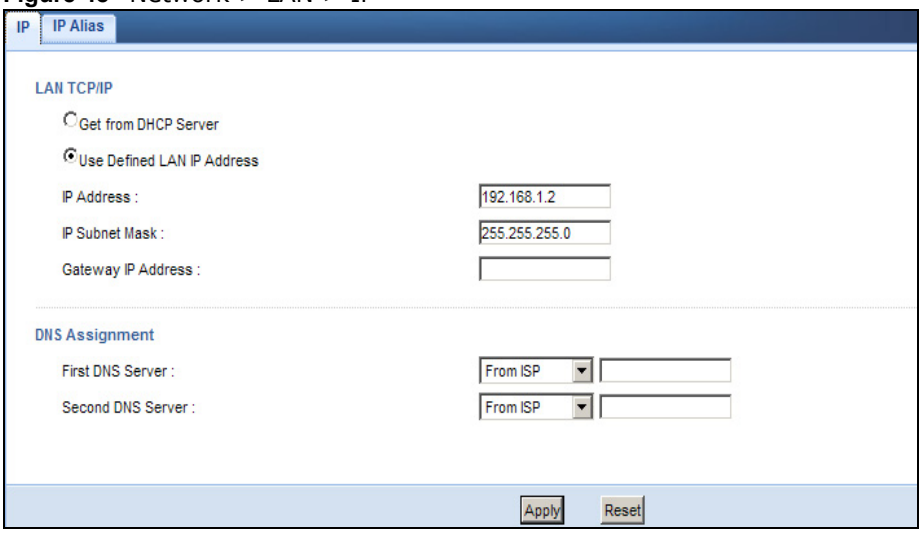
8.5 LAN Screen

Use this section to configure your LAN settings while in **Access Point** mode.

Click **Network > LAN** to see the screen below.

Note: If you change the IP address of the Router in the screen below, you will need to log into the Router again using the new IP address.

Figure 48 Network > LAN > IP



The table below describes the labels in the screen.

Table 29 Network > LAN > IP

LABEL	DESCRIPTION
Get from DHCP Server	Click this to deploy the Router as an access point in the network. When you enable this, the Router gets its IP address from the network's DHCP server (for example, your ISP). Users connected to the Router can now access the network (i.e., the Internet if the IP address is given by the ISP). The Web Configurator may no longer be accessible unless you know the IP address assigned by the DHCP server to the Router. You need to reset the Router to be able to access the Web Configurator again (see Section 22.7 on page 160 for details on how to reset the Router). Also when you select this, you cannot enter an IP address for your Router in the field below.
Use Defined LAN IP Address	Click this if you want to specify the IP address of your Router. Or if your ISP or network administrator gave you a static IP address to access the network or the Internet.
IP Address	Type the IP address in dotted decimal notation. The default setting is 192.168.1.2. If you change the IP address you will have to log in again with the new IP address.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your Router 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 Router.
Gateway IP Address	Enter a **Gateway IP Address** (if your ISP or network administrator gave you one) in this field.
DNS Assignment	
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Router's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes to the Router.
Reset	Click **Reset** to reload the previous configuration for this screen.

9

Tutorials

9.1 Overview

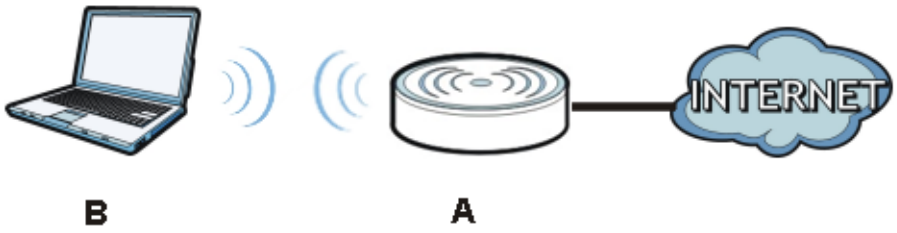
This chapter provides tutorials for your Router as follows:

- Connecting to the Internet from an Access Point
- Configuring Wireless Security Using WPS
- Enabling and Configuring Wireless Security (No WPS)
- If your connection is successful, open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

9.2 Connecting to the Internet from an Access Point

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 access point wirelessly.

Figure 49 Wireless Access Point Connection to the Internet



9.3 Configuring Wireless Security Using WPS

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

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

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

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 9.3.1 on page 74.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 Router's interface. See Section 9.3.2 on page 75. This is the more secure method, since one device can authenticate the other.

9.3.1 Push Button Configuration (PBC)

1. Make sure that your Router 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 Router's Web Configurator and press the **Push Button** button in the **Network** > **Wireless LAN 2.4G** or **Wireless LAN 5G** > **WPS Station** screen.

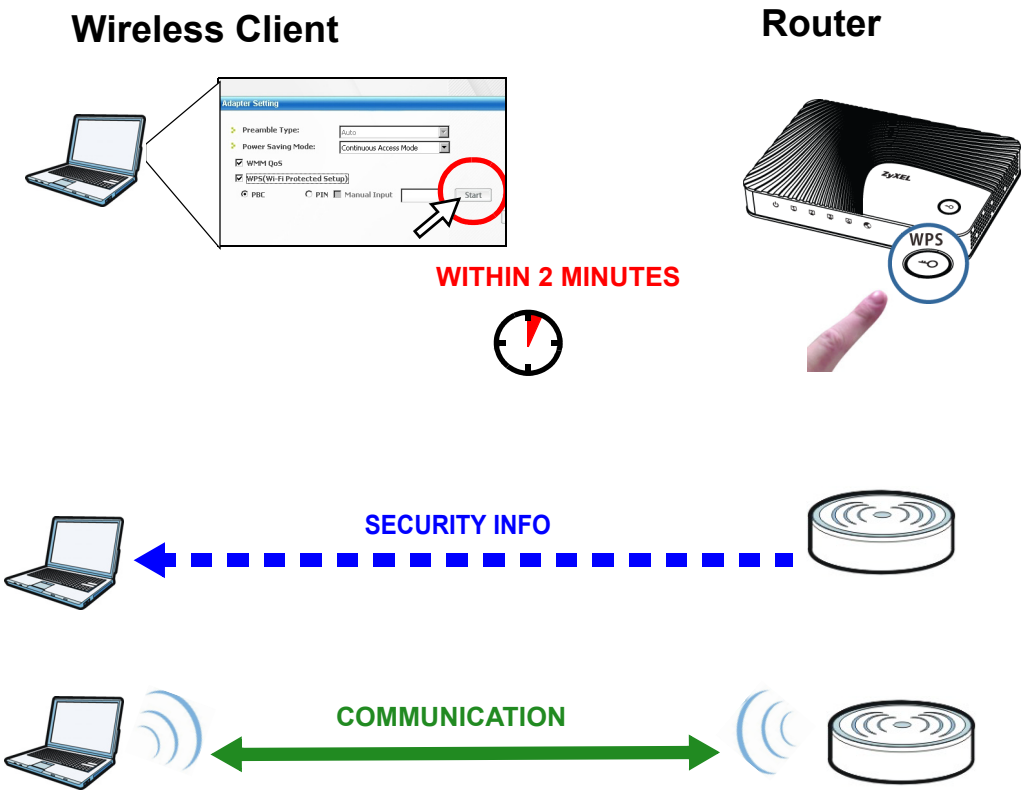
   Note: Your Router has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

   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 Router 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 Router securely.

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

Figure 50 Example WPS Process: PBC Method



9.3.2 PIN Configuration

When you use the PIN configuration method, you need to use both Router'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.

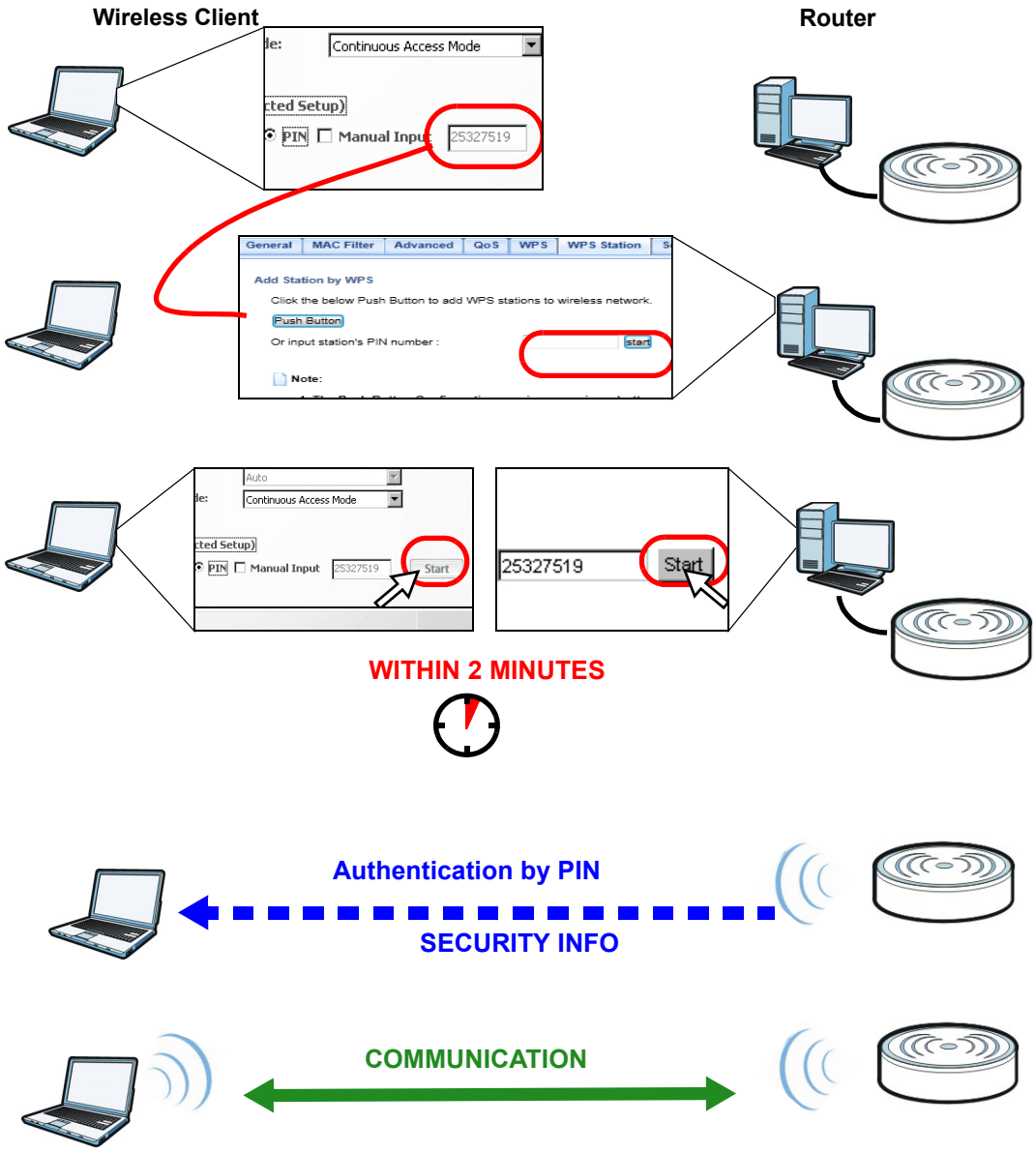
2 Enter the PIN number to the **PIN** field in the **Network** > **Wireless LAN 2.4G** or **Wireless LAN 5G** > **WPS Station** screen on the Router.

3 Click **Start** button (or button next to the PIN field) on both the wireless client utility screen and the Router's **WPS Station** screen within two minutes.

The Router 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 Router securely.

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

Figure 51 Example WPS Process: PIN Method



9.4 Enabling and Configuring Wireless Security (No WPS)

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

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

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

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 3.2 on page 31).

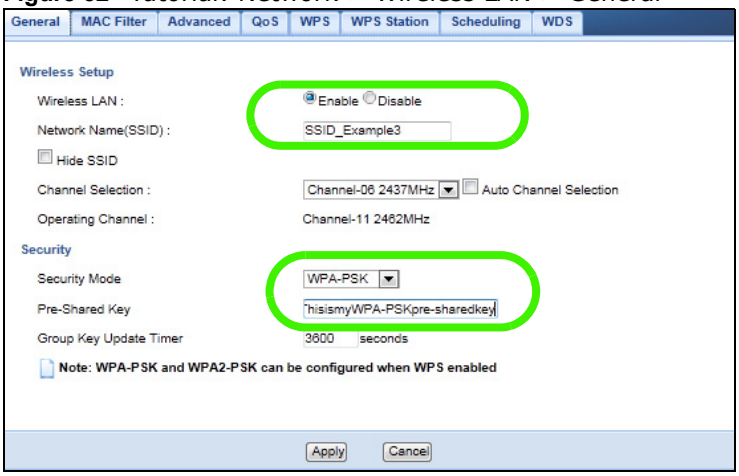
1 Open the **Wireless LAN > General** screen in the AP's Web Configurator.

2 Enable **Wireless LAN**.

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

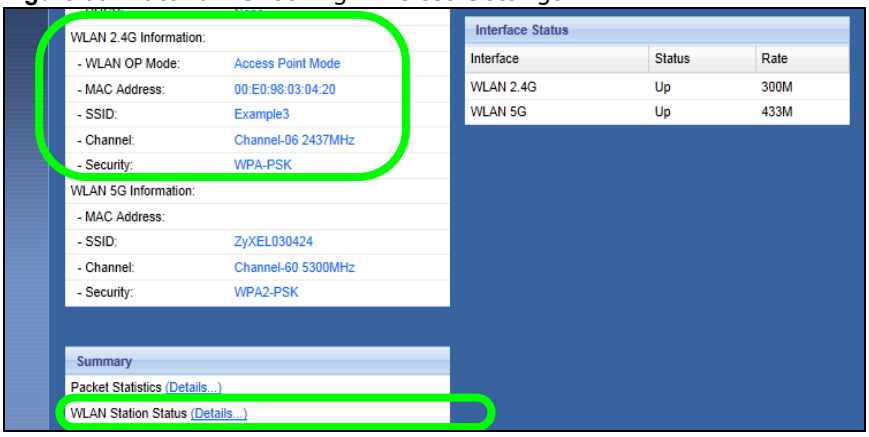
4 Set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Figure 52 Tutorial: Network > Wireless LAN > General



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

Figure 53 Tutorial: Checking Wireless Settings



9.4.1 Configure Your Notebook

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.

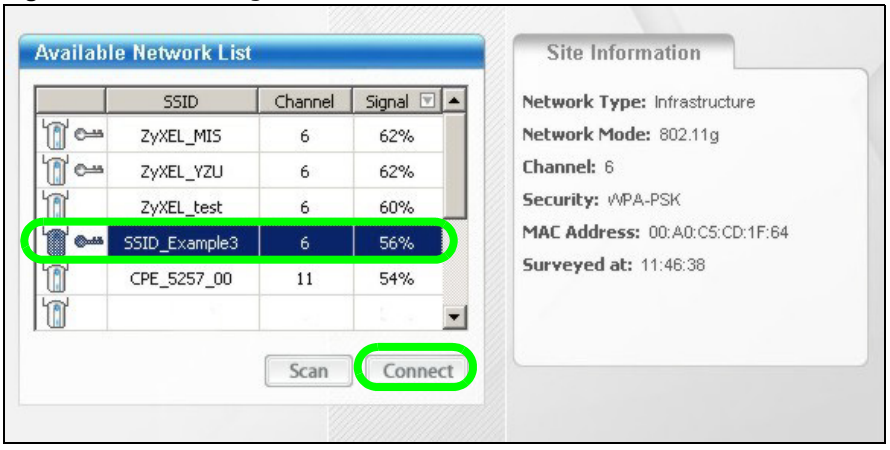
1 The Router supports IEEE 802.11b, IEEE 802.11g, IEEE 802.11n and IEEE 802.11ac wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

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.

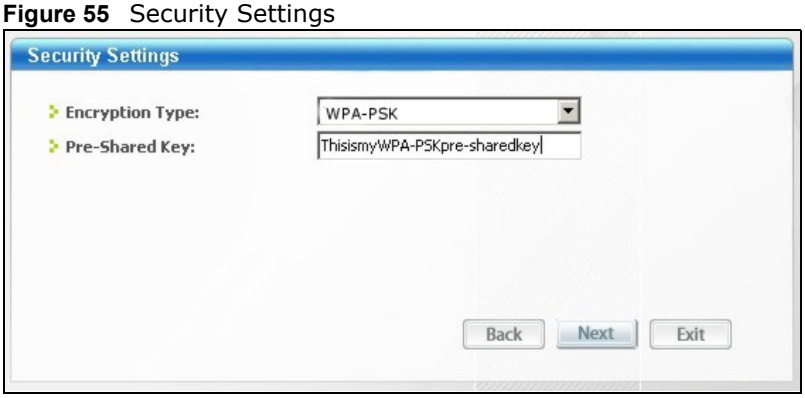
4 Select SSID_Example3 and click **Connect**.

Figure 54 Connecting a Wireless Client to a Wireless Network t



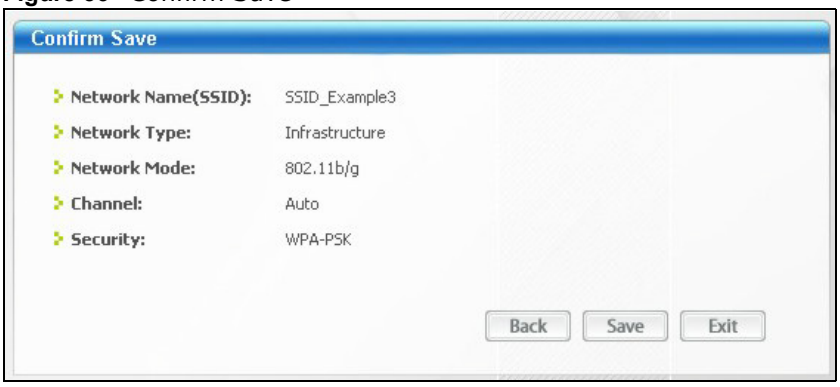
5 Select WPA-PSK and type the security key in the following screen. Click **Next**.

Figure 55 Security Settings



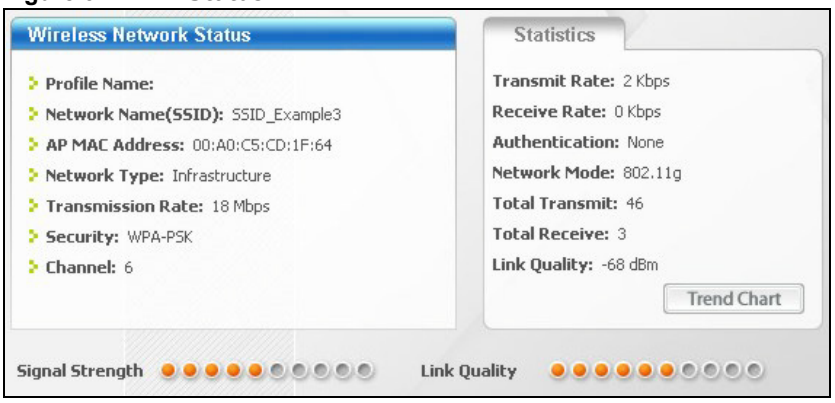
6 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 56 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 57 Link Status



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

PART II
Technical Reference

10

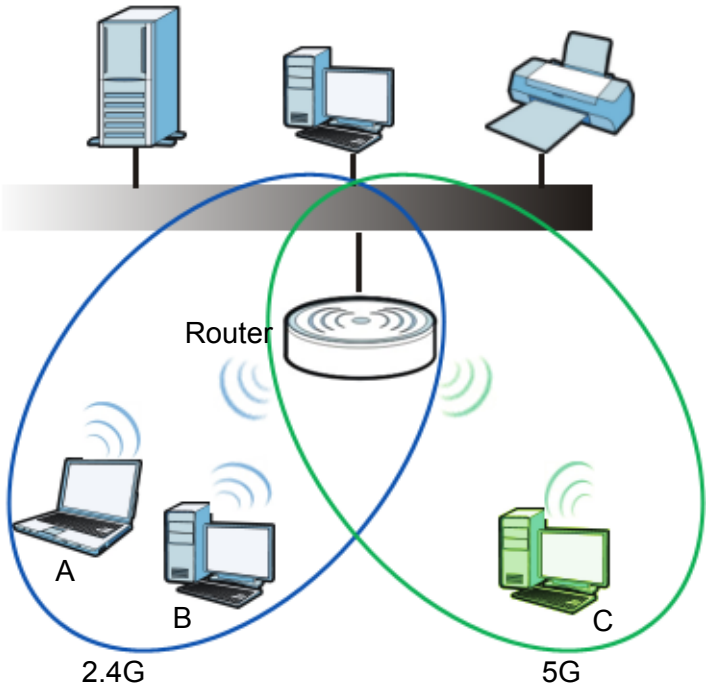
Wireless LAN

10.1 Overview

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

The following figure provides an example of a wireless network.

Figure 58 Example of a Wireless Network



The wireless 2.4G network is the part in the blue circle and wireless 5G network is the part in the green circle. In these wireless networks, devices A, B and C 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.

10.2 What You Can Do

- Use the **General** screen (Section 10.4 on page 86) to enable the Wireless LAN, enter the SSID and select the wireless security mode.
- Use the **MAC Filter** screen (Section 10.5 on page 90) to allow or deny wireless stations based on their MAC addresses from connecting to the Router.

- Use the **Advanced** screen (Section 10.6 on page 91) to allow wireless advanced features, such as intra-BSS networking and set the RTS/CTS Threshold.
- Use the **QoS** screen (Section 10.7 on page 93) to set priority levels to services, such as e-mail, VoIP, chat, and so on.
- Use the **WPS** screen (Section 10.8 on page 94) to quickly set up a wireless network with strong security, without having to configure security settings manually.
- Use the **WPS Station** screen (Section 10.9 on page 95) to add a wireless station using WPS.
- Use the **Scheduling** screen (Section 10.10 on page 96) to set the times your wireless LAN is turned on and off.
- Use the **WDS** screen (Section 10.11 on page 97) to configure Wireless Distribution System on your Router.

10.3 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.

10.3.1 Wireless Security Overview

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

10.3.1.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

10.3.1.2 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or

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.

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.

10.3.1.3 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.

The types of encryption you can choose depend on the type of user authentication.

Table 30 Types of Encryption for Each Type of Authentication

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

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

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

When you select **WPA2-PSK** in your Router, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** (depending on the type of wireless network login) and select the **WPA Compatible** option in the Router.

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.

10.3.1.4 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 9.3 on page 73.

10.3.1.5 WDS

Wireless Distribution System or WDS security is used between bridged APs. It is independent of the security between the wired networks and their respective APs. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key.

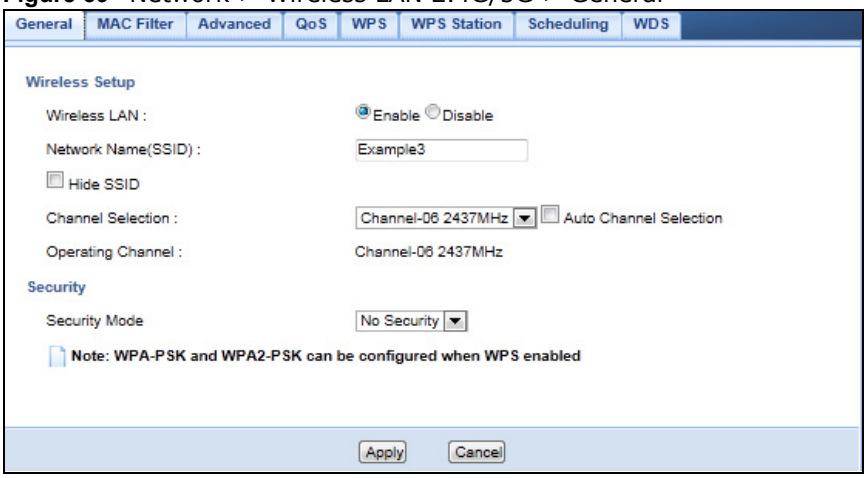
10.4 General Wireless LAN 2.4G/5G Screen

Use this screen to enable the Wireless LAN 2.4G or 5G, enter the SSID and select the wireless security mode.

Note: If you are configuring the Router from a computer connected to the wireless LAN and you change the Router'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 Router's new settings.

Click **Network** > **Wireless LAN 2.4G** or **Wireless LAN 5G** to open the **General** screen.

Figure 59 Network > Wireless LAN 2.4G/5G > General



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

Table 31 Network > Wireless LAN 2.4G/5G > General

LABEL	DESCRIPTION
Wireless Setup	
Wireless LAN	Select the radio button to **Enable** or **Disable Wireless LAN**. You can turn the wireless LAN on or off using the switch at the rear panel of the Router.
Network Name(SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the Router must have the same SSID. Enter a descriptive name (up to 32 keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.

Table 31 Network > Wireless LAN 2.4G/5G > General (continued)

LABEL	DESCRIPTION
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels. This option is only available if **Auto Channel Selection** is disabled.
Operating Channel	This displays the channel the Router is currently using.
Security	
Security Mode	Select **WEP**, **WPA**, **WPA2**, **WPA-PSK** or **WPA2-PSK** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Router. After you select to use a security, additional options appears in this screen. See 10.4.2, and 10.4.3 sections. Or you can select **No Security** to allow any client to associate this network without authentication. Note: If you enable the WPS function, only **No Security**, **Static WEP**, **WPA-PSK** and **WPA2-PSK** are available in this field.
Apply	Click **Apply** to save your changes back to the Router.
Reset	Click **Reset** to reload the previous configuration for this screen.

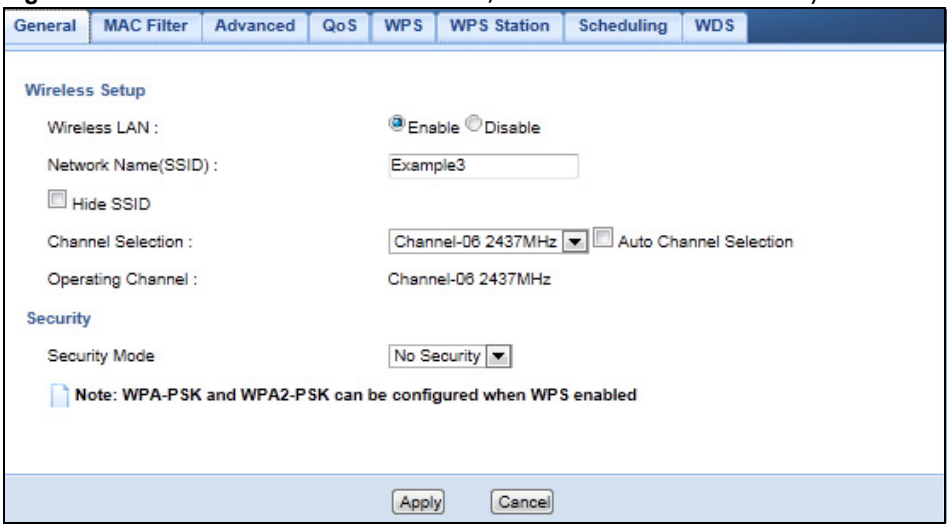
See the rest of this chapter for information on the other labels in this screen.

10.4.1 No Security

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

Note: If you do not enable any wireless security on your Router, your network is accessible to any wireless networking device that is within range.

Figure 60 Network > Wireless LAN 2.4G/5G > General: No Security



The following table describes the labels in this screen.

Table 32 Network > Wireless LAN 2.4G/5G > General: No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the Router.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

Refer to Table 31 on page 86 for descriptions of the other labels in this screen.

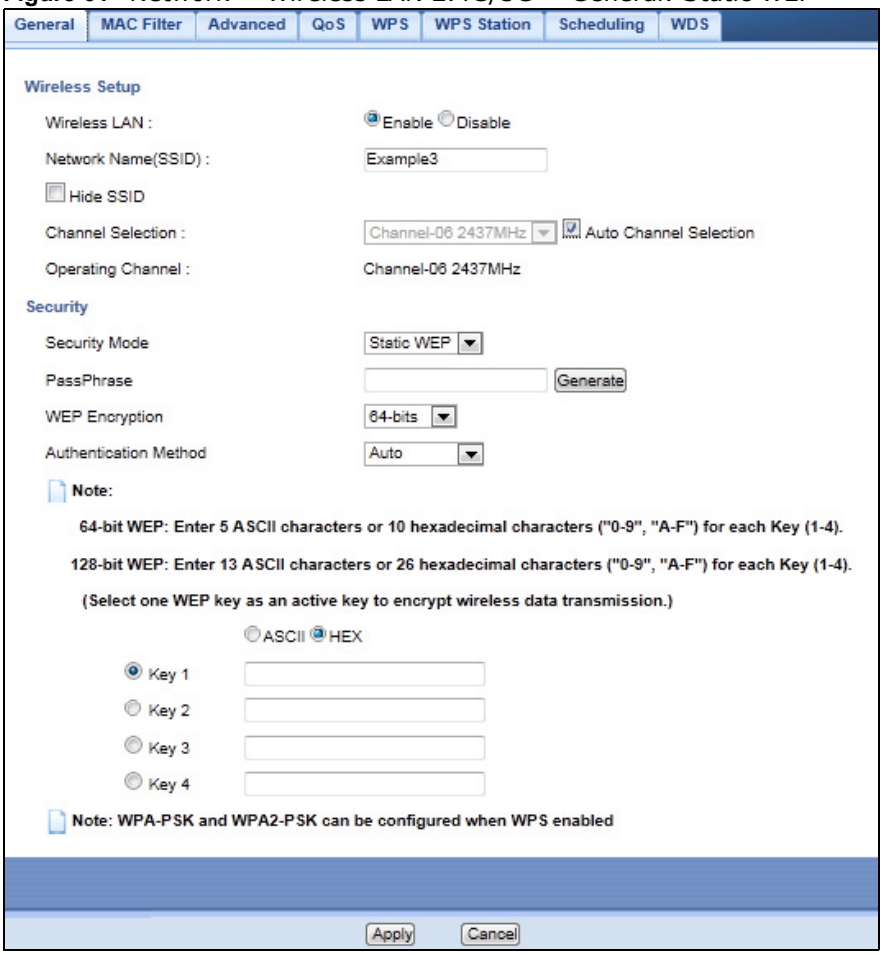
10.4.2 WEP Encryption

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

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

In order to configure and enable WEP encryption, click **Network** > **Wireless LAN 2.4G** or **Wireless LAN 5G** to display the **General** screen. Select **Static WEP** from the **Security Mode** list.

Figure 61 Network > Wireless LAN 2.4G/5G > General: Static WEP



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

Table 33 Network > Wireless LAN 2.4G/5G > General: Static WEP

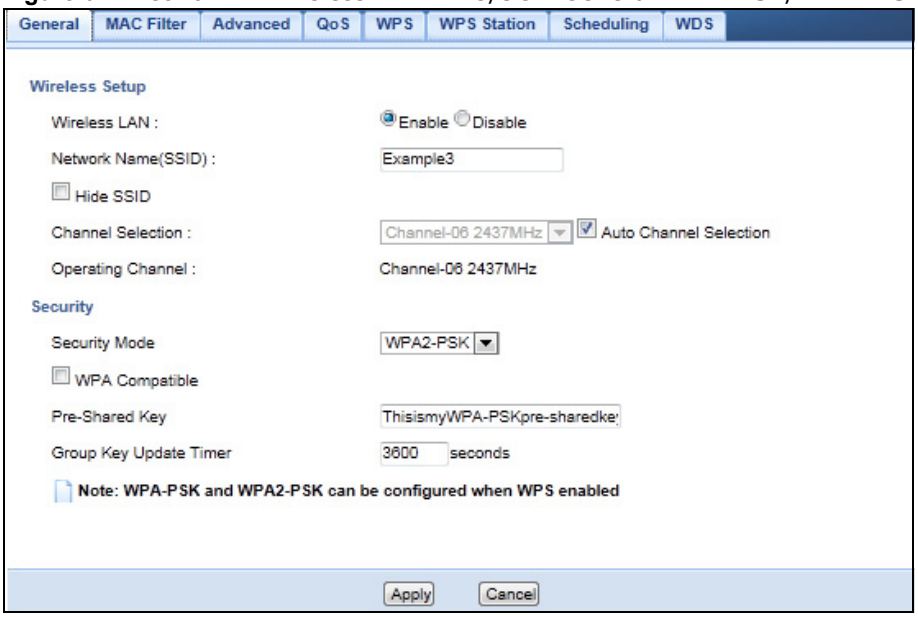
LABEL	DESCRIPTION
Security Mode	Select **Static WEP** to enable data encryption.
PassPhrase	Enter a Passphrase (up to 26 printable characters) and click Generate. A passphrase functions like a password. In WEP security mode, it is further converted by the Router into a complicated string that is referred to as the "key". This key is requested from all devices wishing to connect to a wireless network.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP**. This dictates the length of the security key that the network is going to use.
Authentication Method	Select **Auto** or **Shared Key** from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Keep this setting at **Auto** unless you want to force a key verification before communication between the wireless client and the Router occurs. Select **Shared Key** to force the clients to provide the WEP key prior to communication.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the Router and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time.
Apply	Click **Apply** to save your changes back to the Router.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

Refer to Table 31 on page 86 for descriptions of the other labels in this screen.

10.4.3 WPA-PSK/WPA2-PSK

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

Figure 62 Network > Wireless LAN 2.4G/5G> General: WPA-PSK/WPA2-PSK



The following table describes the labels in this screen.

Table 34 Network > Wireless LAN 2.4G/5G > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Security Mode	Select **WPA-PSK** or **WPA2-PSK** to enable data encryption.
WPA-PSK Compatible	This field appears when you choose **WPA-PSK2** as the **Security Mode**. Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your Router.
Pre-Shared Key	**WPA-PSK/WPA2-PSK** uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients.
Apply	Click **Apply** to save your changes back to the Router.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

Refer to Table 31 on page 86 for descriptions of the other labels in this screen.

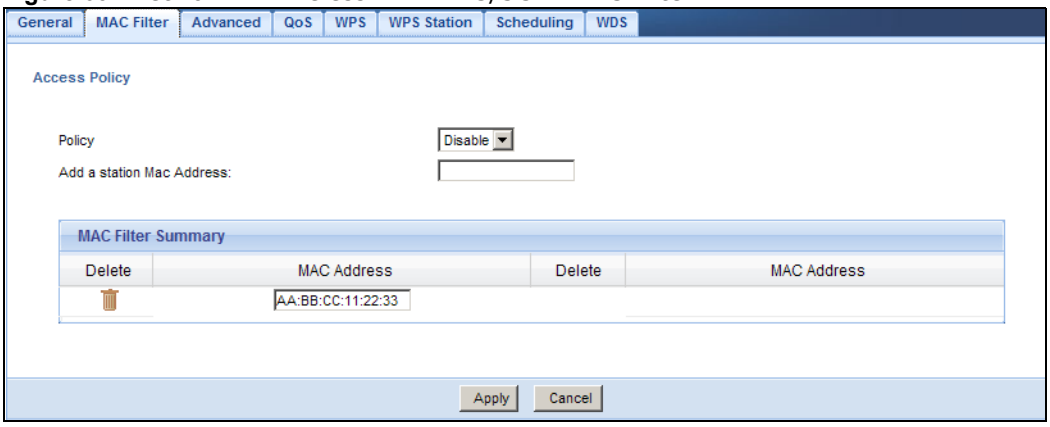
10.5 MAC Filter

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

Figure 63 Network > Wireless LAN 2.4G/5G > MAC Filter



The following table describes the labels in this menu.

Table 35 Network > Wireless LAN 2.4G/5G > MAC Filter

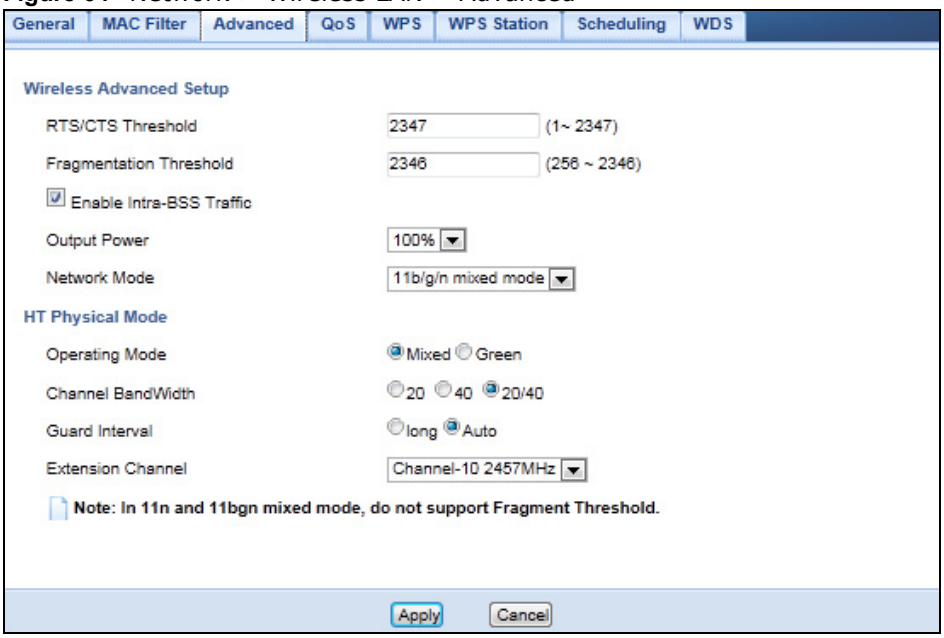
LABEL	DESCRIPTION
Access Policy	
Policy	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Allow** to permit access to the Router, MAC addresses not listed will be denied access to the Router. Select **Reject** to block access to the Router, MAC addresses not listed will be allowed to access the Router
Add a station Mac Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the Router in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. Click **Add**.
MAC Filter Summary	
Delete	Click the delete icon to remove the MAC address from the list.
MAC Address	This is the MAC address of the wireless station that are allowed or denied access to the Router.
Apply	Click **Apply** to save your changes back to the Router.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.6 Wireless LAN Advanced Screen

Use this screen to allow wireless advanced features, such as intra-BSS networking and set the RTS/CTS Threshold

Click **Network** > **Wireless LAN 2.4G** or **Wireless LAN 5G** > **Advanced**. The screen appears as shown.

Figure 64 Network > Wireless LAN > Advanced



The following table describes the labels in this screen.

Table 36 Network > Wireless LAN 2.4G/5G > Advanced

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number.
Enable Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.
Output Power	Set the output power of the Router in this field. If there is a high density of APs in an area, decrease the output power of the Router to reduce interference with other APs. Select one of the following **100%**, **90%**, **75%**, **50%**, **25%**, **10%** or **Minimum**. See the product specifications for more information on your Router's output power.
Network Mode (Wireless LAN 2.4G)	Select **11b/g mixed mode** to allow IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the Router. Select **11b only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Router. Select **11g only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Router. Select **11n only** to allow only IEEE 802.11n compliant WLAN devices to associate with the Router. Select **11b/g/n mixed mode** to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the Router.

Table 36 Network > Wireless LAN 2.4G/5G > Advanced (continued)

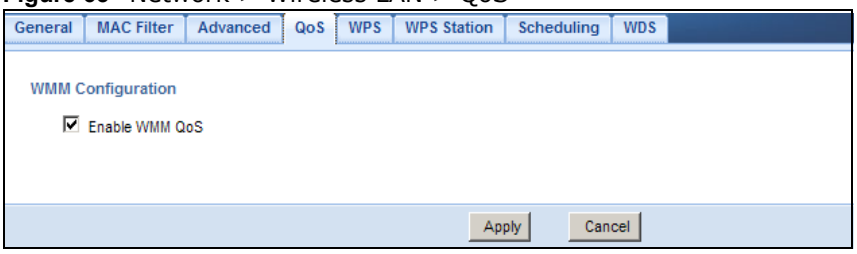
LABEL	DESCRIPTION
Network Mode (Wireless LAN 5G)	Select **11a/n mixed mode** to allow IEEE802.11a and IEEE802.11n compliant WLAN devices to associate with the Router. Select **11a only** to allow only IEEE 802.11a compliant WLAN devices to associate with the Router. Select **11a/an/ac** to allow only IEEE 802.11a, IEEE802.11an and IEEE802.11ac compliant WLAN devices to associate with the Router.
HT (High Throughput) Physical Mode - Use the fields below to configure the 802.11 wireless environment of your Router.	
Operating Mode	Choose this according to the wireless mode(s) used in your network. **Mixed Mode** - Select this if the wireless clients in your network use different wireless modes (for example, IEEE 802.11b/g and IEEE 802.1n modes) **Green Mode** - Select this if the wireless clients in your network uses only one type of wireless mode (for example, IEEEE 802.11 n only)
Channel Bandwidth	Select the channel bandwidth you want to use for your wireless network. It is recommended that you select **20/40** (20, 40, 20/40 MHz). Select 20 MHz if you want to lessen radio interference with other wireless devices in your neighborhood.
Guard Interval	Select **Auto** to increase data throughput. However, this may make data transfer more prone to errors. Select **Long** to prioritize data integrity. This may be because your wireless network is busy and congested or the Router is located in an environment prone to radio interference.
Extension Channel	This is set to **Auto** by default. If you select **20/40** as your **Channel Bandwidth**, the extension channel enables the Router to get higher data throughput. This also lowers radio interference and traffic.
Apply	Click **Apply** to save your changes back to the Router.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.7 Quality of Service (QoS) Screen

The QoS screen allows you to automatically give a service (such as VoIP and video) a priority level.

Click **Network** > **Wireless LAN 2.4G** or **Wireless LAN 5G** > **QoS**. The following screen appears.

Figure 65 Network > Wireless LAN > QoS



The following table describes the labels in this screen.

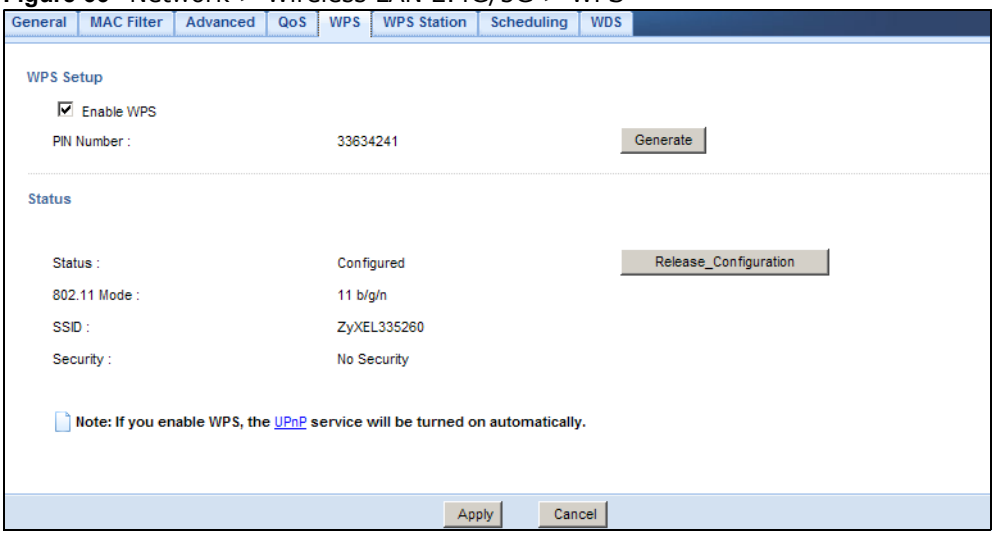
Table 37 Network > Wireless LAN 2.4G/5G > QoS

LABEL	DESCRIPTION
Enable WMM QoS	Check this to have the Router automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Apply	Click **Apply** to save your changes to the Router.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.8 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 2.4G** or **Wireless LAN 5G** > **WPS** tab.

Figure 66 Network > Wireless LAN 2.4G/5G > WPS



The following table describes the labels in this screen.

Table 38 Network > Wireless LAN 2.4G/5G > WPS

LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select this to enable the WPS feature.
PIN Number	This displays a PIN number last time system generated. Click **Generate** to generate a new PIN number.
Status	
Status	This displays **Configured** when the Router 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 Router or you click **Release_Configuration** to remove the configured wireless and wireless security settings.

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

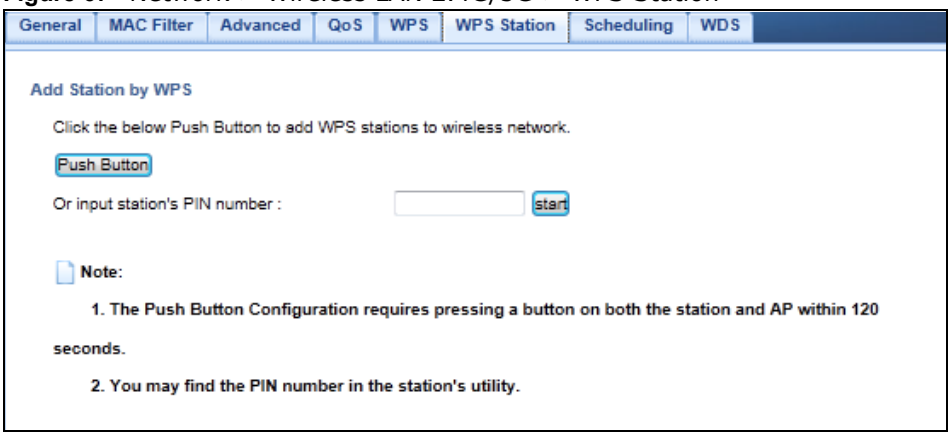
LABEL	DESCRIPTION
Release Configuration	This button is only available when the WPS status displays **Configured**. Click this button to remove all configured wireless and wireless security settings for WPS connections on the Router.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the Router.
SSID	This is the name of the wireless network.
Security	This is the type of wireless security employed by the network.
Apply	Click **Apply** to save your changes back to the Router.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.9 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** or **Wireless LAN 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 67 Network > Wireless LAN 2.4G/5G > WPS Station



The following table describes the labels in this screen.

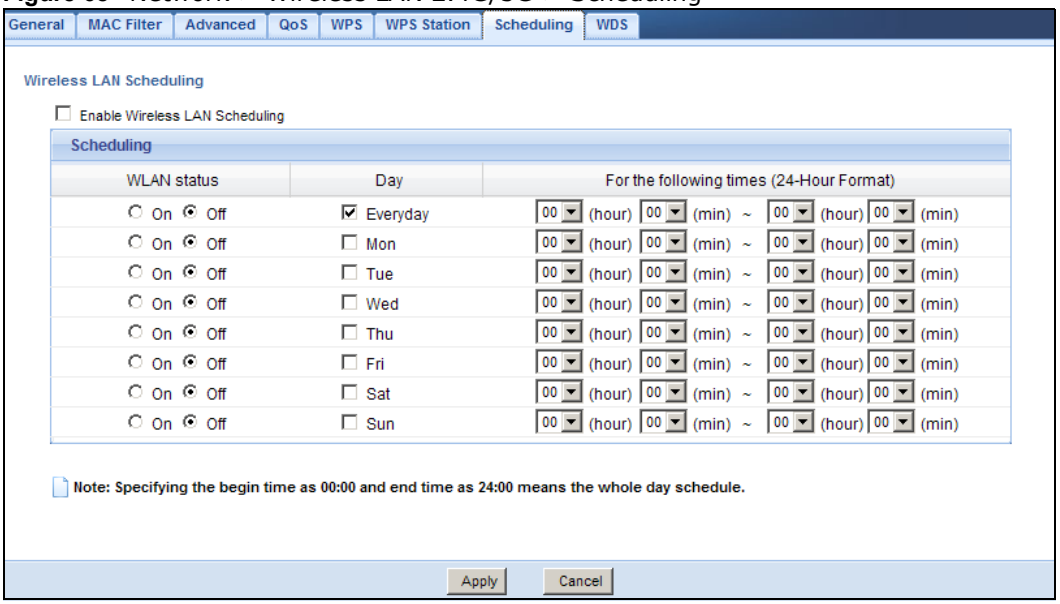
Table 39 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. See Section 9.3.1 on page 74. 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 9.3.2 on page 75. 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.

10.10 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** or **Wireless LAN 5G** > **Scheduling** tab.

Figure 68 Network > Wireless LAN 2.4G/5G > Scheduling



The following table describes the labels in this screen.

Table 40 Network > Wireless LAN 2.4G/5G > Scheduling

LABEL	DESCRIPTION
Wireless LAN Scheduling	
Enable Wireless LAN Scheduling	Select this to enable Wireless LAN scheduling.
Scheduling	

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

LABEL	DESCRIPTION
WLAN Status	Select **On** or **Off** to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the **Day** and **Except for the following times** fields.
Day	Select **Everyday** or the specific days to turn the Wireless LAN on or off. If you select **Everyday** you can not select any specific days. This field works in conjunction with the **Except for the following times** field.
For the following times (24-Hour Format)	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 on between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields.
Apply	Click **Apply** to save your changes back to the Router.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.11 WDS Screen

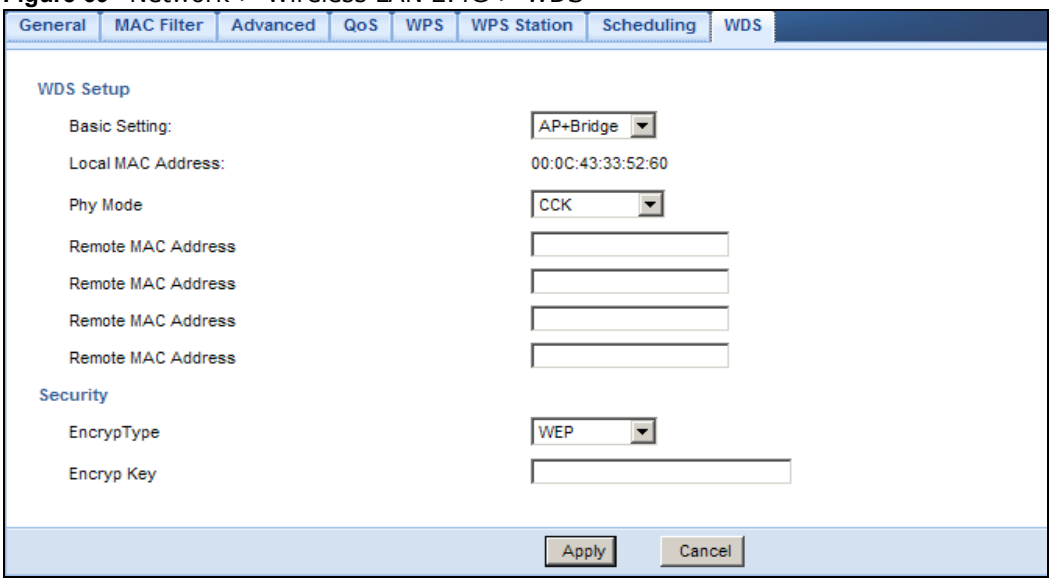
A Wireless Distribution System is a wireless connection between two or more APs. Use this screen to set the operating mode of your Router to **AP + Bridge** or **Bridge Only** and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

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

The WDS feature is only available in wireless 2.4G network.

Click **Network** > **Wireless LAN 2.4G** > **WDS** tab. The following screen opens with the **Basic Setting** set to **AP+Bridge**, and **Security Mode** set to **WEP**.

Figure 69 Network > Wireless LAN 2.4G > WDS



The following table describes the labels in this screen.

Table 41 Network > Wireless LAN 2.4G > WDS

LABEL	DESCRIPTION
WDS Setup	
Basic Settings	Select the operating mode for your Router. • **AP + Bridge -** The Router functions as a bridge and access point simultaneously. • **Bridge** - The Router acts as a wireless network bridge and establishes wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode. The Router can establish up to five wireless links with other APs.
Local MAC Address	This is the MAC address of your Router.
Phy Mode	Select the Phy mode you want the Router to use. This dictates the maximum size of packets during data transmission.
Remote MAC Address	This is the MAC address of the peer device that your Router wants to make a bridge connection with. You can connect to up to 4 peer devices.
Security	
EncrypType	Select whether to use **WEP**, **TKIP** or **AES** encryption for your WDS connection in this field. Otherwise, select **No Security**.
EncrypKey	The Encryp key is used to encrypt data. Peers must use the same key for data transmission.
Apply	Click **Apply** to save your changes to Router.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

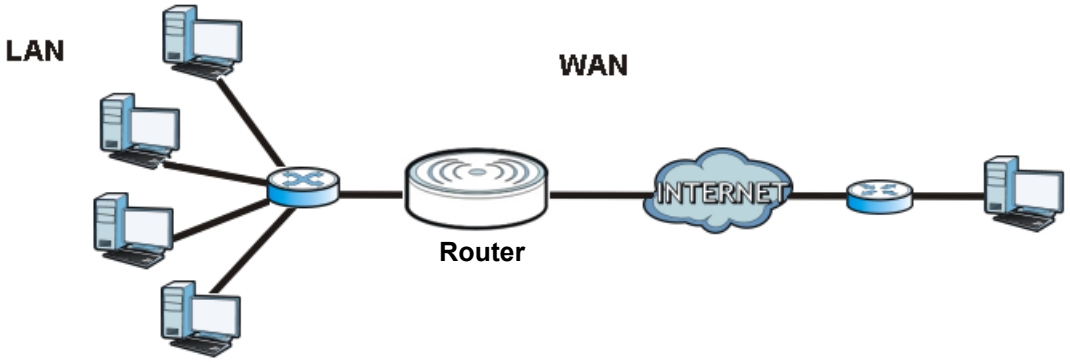
11 WAN

11.1 Overview

This chapter discusses the Router's **WAN** screens. Use these screens to configure your Router 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 70 LAN and WAN



11.2 What You Can Do

- Use the **Internet Connection** screen (Section 11.4 on page 102) to enter your ISP information and set how the computer acquires its IP, DNS and WAN MAC addresses.
- Use the **Advanced** screen (Section 11.5 on page 108) to enable multicasting, configure Windows networking and bridge.

11.3 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 Router.

11.3.1 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 Router, which makes it accessible from an outside network. It is used by the Router to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the Router 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 Router 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 Router's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

WAN MAC Address

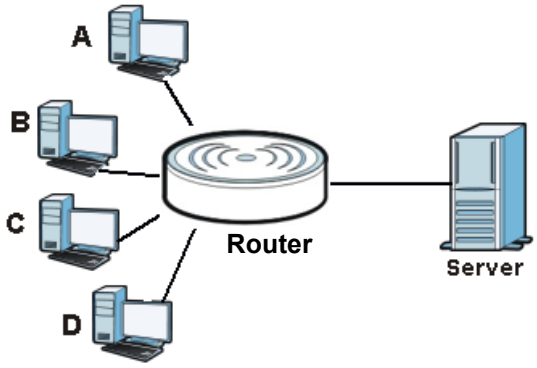
The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

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.

11.3.2 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Figure 71 Multicast Example



In the multicast example above, systems A and D comprise one multicast group. In multicasting, the server only needs to send one data stream and this is delivered to systems A and D.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. The Router supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**).

At start up, the Router queries all directly connected networks to gather group membership. After that, the Router periodically updates this information. IP multicasting can be enabled/disabled on the Router LAN and/or WAN interfaces in the Web Configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

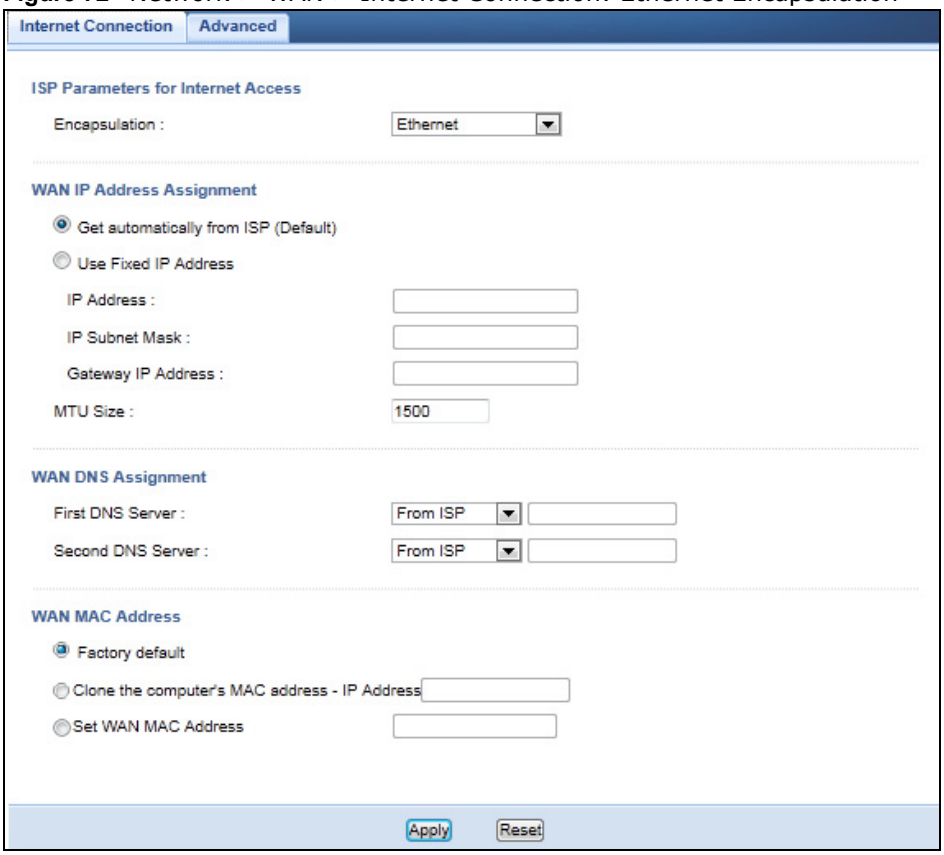
11.4 Internet Connection

Use this screen to change your Router's Internet access settings. Click **WAN** from the Configuration menu. The screen differs according to the encapsulation you choose.

11.4.1 Ethernet Encapsulation

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

Figure 72 Network > WAN > Internet Connection: Ethernet Encapsulation



The following table describes the labels in this screen.

Table 42 Network > WAN > Internet Connection: Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet.
WAN IP Address Assignment	
Get automatically from ISP (Default)	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.

Table 42 Network > WAN > Internet Connection: Ethernet Encapsulation (continued)

LABEL	DESCRIPTION
IP Subnet Mask	Enter the **IP Subnet Mask** in this field.
Gateway IP Address	Enter a **Gateway IP Address** (if your ISP gave you one) in this field.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your Router can receive and process.
WAN DNS Assignment	
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Router's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the Router's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning.
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 Router.
Reset	Click **Reset** to begin configuring this screen afresh.

11.4.2 PPPoE Encapsulation

The Router 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).

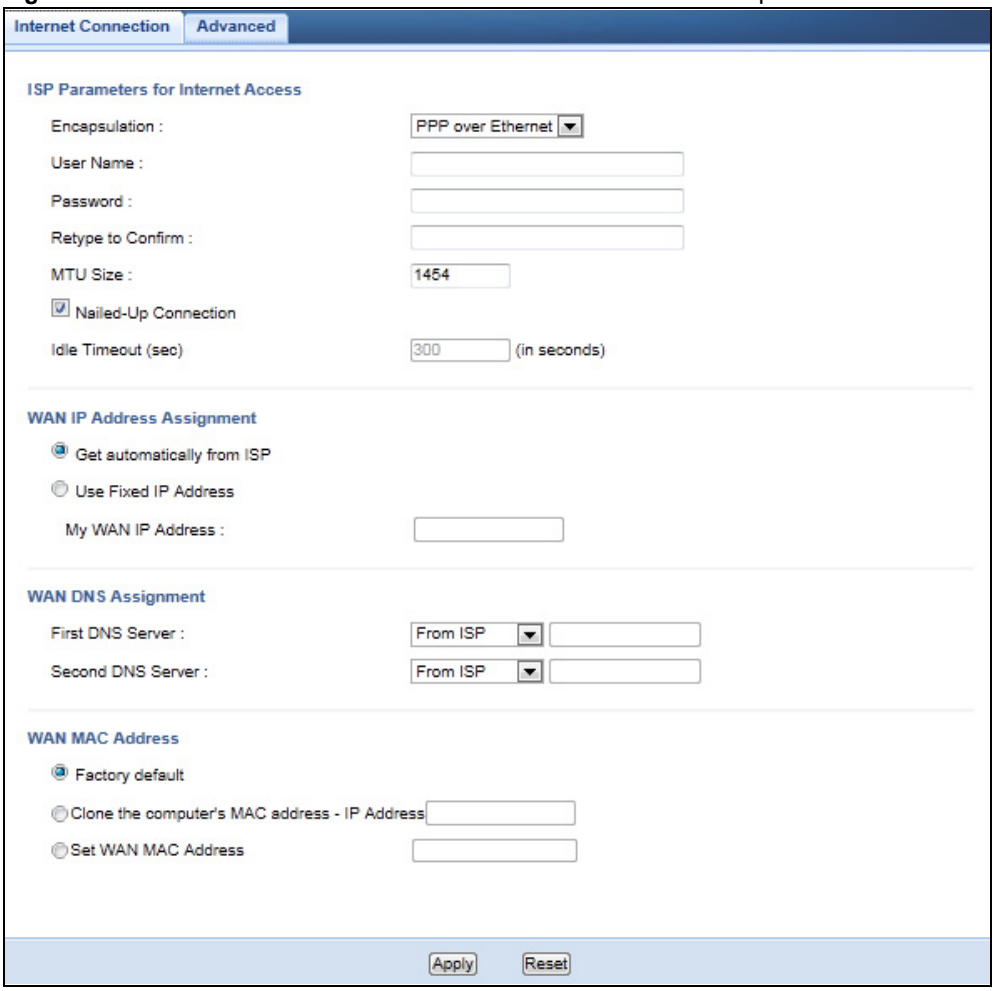
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

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 Router (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Router 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 73 Network > WAN > Internet Connection: PPPoE Encapsulation



The following table describes the labels in this screen.

Table 43 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	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.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your Router can receive and process.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout (sec)	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.
WAN IP Address Assignment	

Table 43 Network > WAN > Internet Connection: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
WAN DNS Assignment	
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Router's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the Router's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning.
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 Router.
Reset	Click **Reset** to begin configuring this screen afresh.

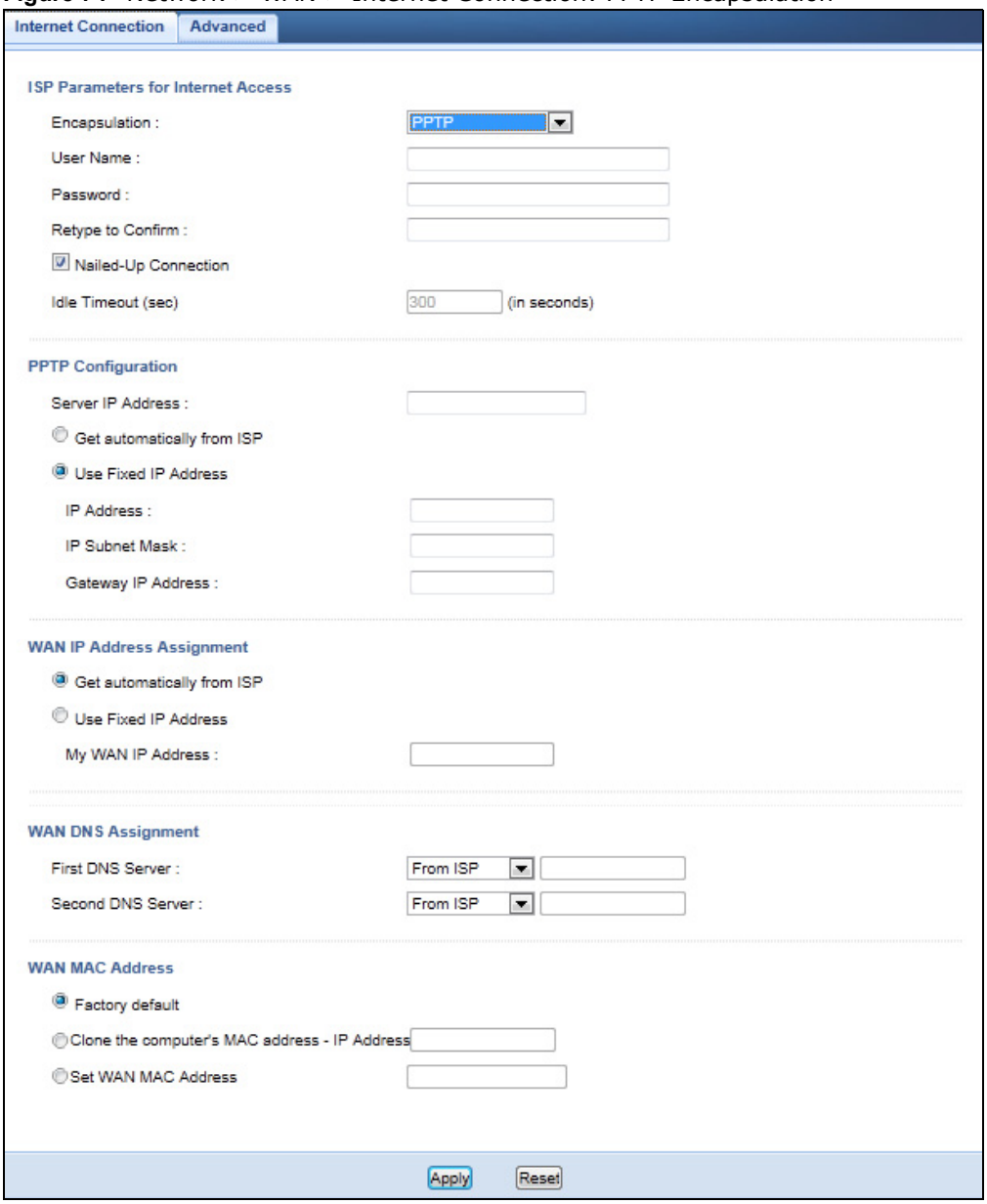
11.4.3 PPTP Encapsulation

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 74 Network > WAN > Internet Connection: PPTP Encapsulation



The following table describes the labels in this screen.

Table 44 Network > WAN > Internet Connection: PPTP Encapsulation

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.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.

Table 44 Network > WAN > Internet Connection: PPTP Encapsulation (continued)

LABEL	DESCRIPTION
Nailed-up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in minutes that elapses before the Router automatically disconnects from the PPTP server.
PPTP Configuration	
Server IP Address	Type the IP address of the PPTP server.
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
IP Subnet Mask	Your Router 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 Router.
Gateway IP Address	Enter a **Gateway IP Address** (if your ISP gave you one) in this field.
WAN IP Address Assignment	
Get automatically from ISP	Select this to get your WAN IP address from your ISP.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
WAN DNS Assignment	
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Router's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the Router's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning.
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 Router.
Reset	Click **Reset** to begin configuring this screen afresh.

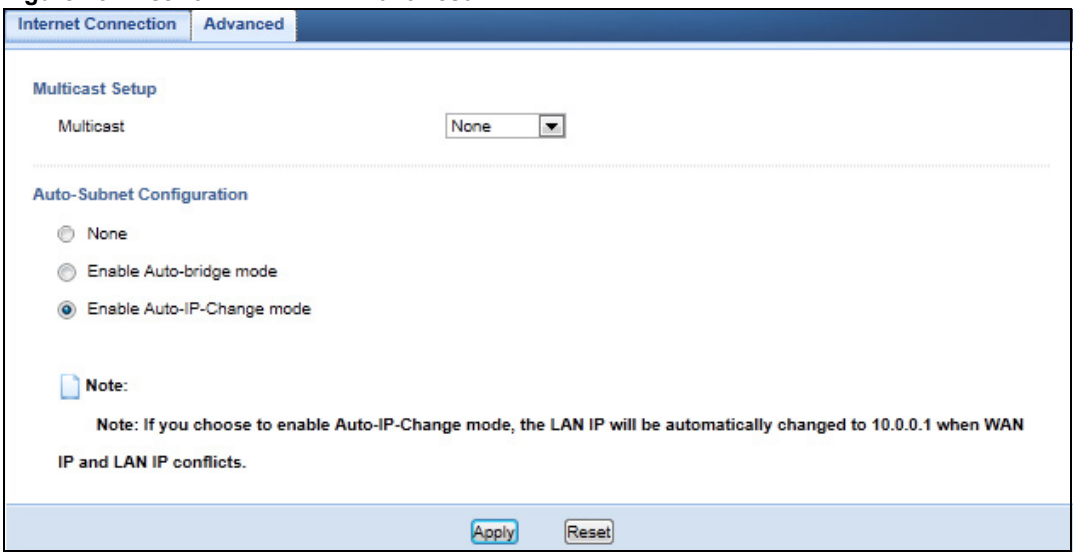
11.5 Advanced WAN Screen

Use this screen to enable **Multicast** and enable **Auto-bridge**.

Note: The categories shown in this screen are independent of each other.

To change your Router's advanced WAN settings, click **Network** > **WAN** > **Advanced**. The screen appears as shown.

Figure 75 Network > WAN > Advanced



The following table describes the labels in this screen.

Table 45 Network > WAN > Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast	Select **IGMPv1/v2** to enable multicasting. This applies to traffic routed from the WAN to the LAN. Select **None** to disable this feature. This may cause incoming traffic to be dropped or sent to all connected network devices.
Auto-Subnet Setup	
None	Select this option to have the Router do nothing when it gets a WAN IP address in the range of 192.168.x.y (where x and y are from zero to nine) or in the same subnet as the LAN IP address.
Enable Auto-bridge mode	Select this option to have the Router switch to bridge mode automatically when the Router gets a WAN IP address in the range of 192.168.x.y (where x and y are from zero to nine) no matter what the LAN IP address is.
Enable Auto-IP-Change mode	Select this option to have the Router change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the Router gets a dynamic WAN IP address in the same subnet as the LAN IP address 192.168.1.1 or 10.0.0.1. The NAT, DHCP server and firewall functions on the Router are still available in thismode.
Apply	Click **Apply** to save your changes back to the Router.
Reset	Click **Reset** to begin configuring this screen afresh.

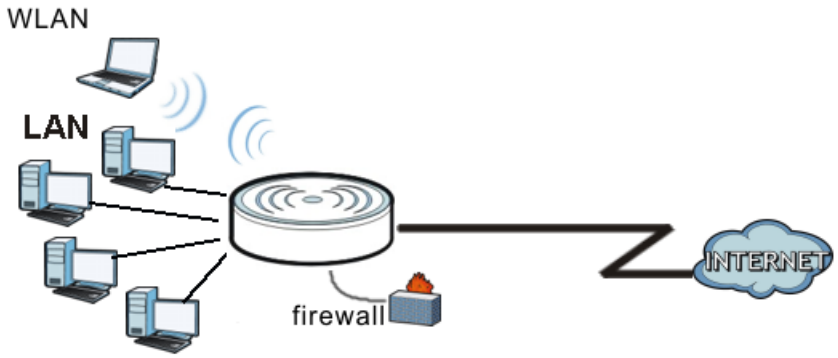
12 LAN

12.1 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 76 LAN Example



The LAN screens can help you manage IP addresses.

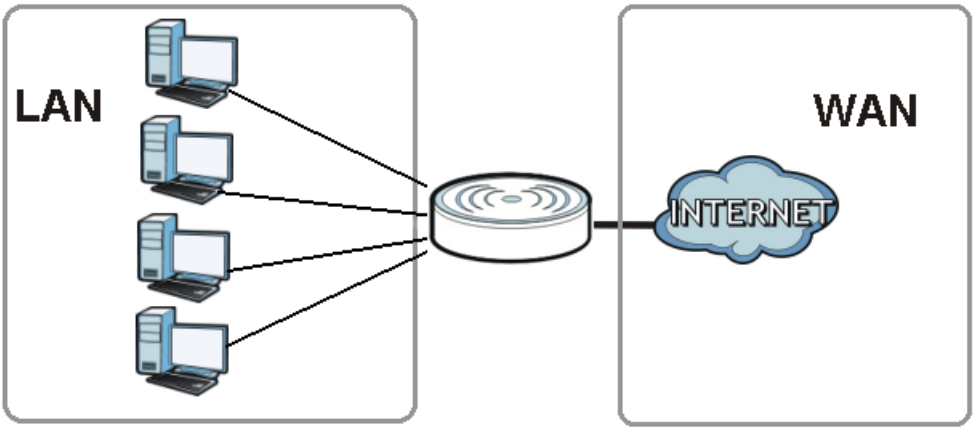
12.2 What You Can Do

- Use the **IP** screen (Section 12.4 on page 111) to change the IP address for your Router.
- Use the **IP Alias** screen (Section 12.5 on page 111) to have the Router apply IP alias to create LAN subnets.

12.3 What You Need To Know

The actual physical connection determines whether the Router 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 77 LAN and WAN IP Addresses



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

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

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

12.3.1 IP Pool Setup

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

12.3.2 LAN TCP/IP

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

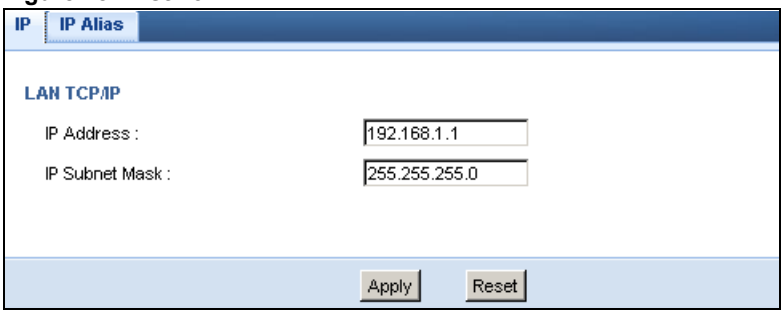
12.3.3 IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Router supports three logical LAN interfaces via its single physical Ethernet interface with the Router itself as the gateway for each LAN network.

12.4 LAN IP Screen

Use this screen to change the IP address for your Router. Click **Network > LAN > IP**.

Figure 78 Network > LAN > IP



The following table describes the labels in this screen.

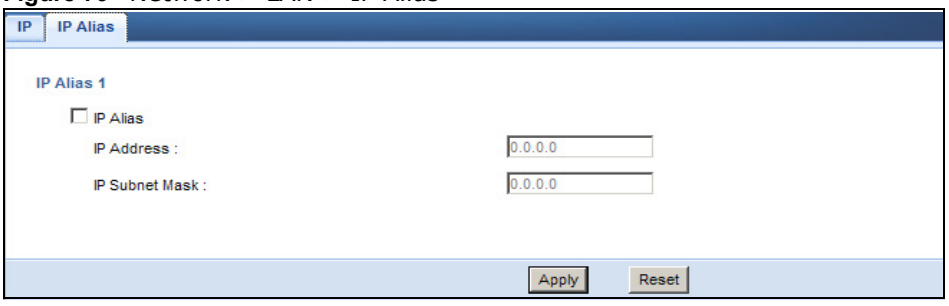
Table 46 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your Router in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your Router 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 Router.
Apply	Click **Apply** to save your changes back to the Router.
Reset	Click **Reset** to begin configuring this screen afresh.

12.5 IP Alias Screen

Use this screen to have the Router apply IP alias to create LAN subnets. Click **LAN > IP Alias**.

Figure 79 Network > LAN > IP Alias



The following table describes the labels in this screen.

Table 47 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias	Check this to enable IP alias.
IP Address	Type the IP alias address of your Router in dotted decimal notation.

Table 47 Network > LAN > IP Alias (continued)

LABEL	DESCRIPTION
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your Router 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 Router.
Apply	Click **Apply** to save your changes back to the Router.
Reset	Click **Reset** to begin configuring this screen afresh.

13

DHCP Server

13.1 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 Router's LAN as a DHCP server or disable it. When configured as a server, the Router 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.

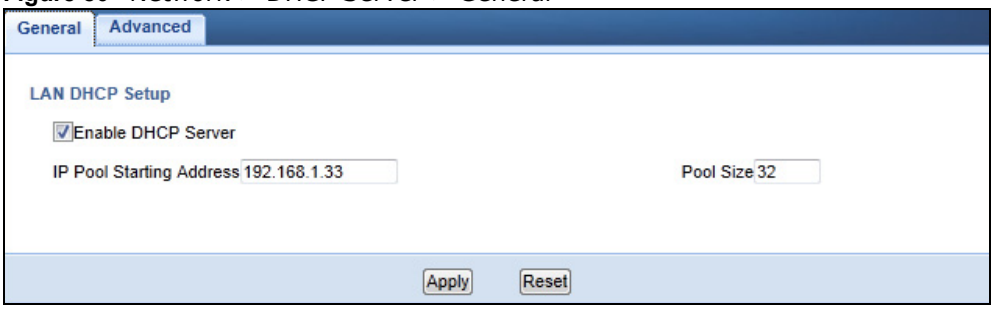
13.2 What You Can Do

- Use the **General** (Section 13.3 on page 113) screen to enable the DHCP server.
- Use the **Advanced** (Section 13.4 on page 114) screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

13.3 General Screen

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

Figure 80 Network > DHCP Server > General



The following table describes the labels in this screen.

Table 48 Network > DHCP Server > General

LABEL	DESCRIPTION
Enable DHCP Server	Enable or Disable DHCP for LAN.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool for LAN.

Table 48 Network > DHCP Server > General (continued)

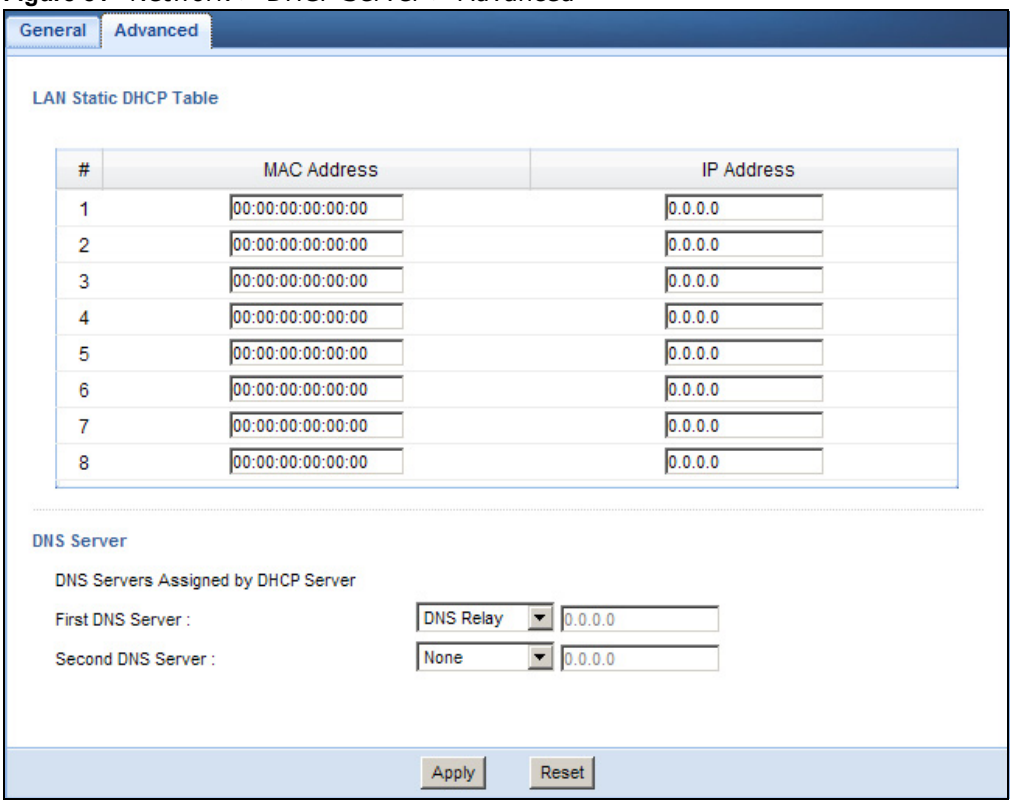
LABEL	DESCRIPTION
Pool Size	This field specifies the size, or count of the IP address pool for LAN.
Apply	Click **Apply** to save your changes back to the Router.
Reset	Click **Reset** to begin configuring this screen afresh.

13.4 Advanced Screen

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

To change your Router's static DHCP settings, click **Network** > **DHCP Server** > **Advanced**. The following screen displays.

Figure 81 Network > DHCP Server > Advanced



The following table describes the labels in this screen.

Table 49 Network > DHCP Server > Advanced

LABEL	DESCRIPTION
LAN Static DHCP Table	
#	This is the index number of the static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.

Table 49 Network > DHCP Server > Advanced (continued)

LABEL	DESCRIPTION
IP Address	Type the LAN IP address of a computer on your LAN.
DNS Server	
DNS Servers Assigned by DHCP Server	The Router passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The Router only passes this information to the LAN DHCP clients when you select the **Enable DHCP Server** check box. When you clear the **Enable DHCP Server** check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Router's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the Router act as a DNS proxy. The Router's LAN IP address displays in the field to the right (read-only). The Router tells the DHCP clients on the LAN that the Router itself is the DNS server. When a computer on the LAN sends a DNS query to the Router, the Router forwards the query to the Router's system DNS server (configured in the **WAN > Internet Connection** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the Router.
Reset	Click **Reset** to begin configuring this screen afresh.

14

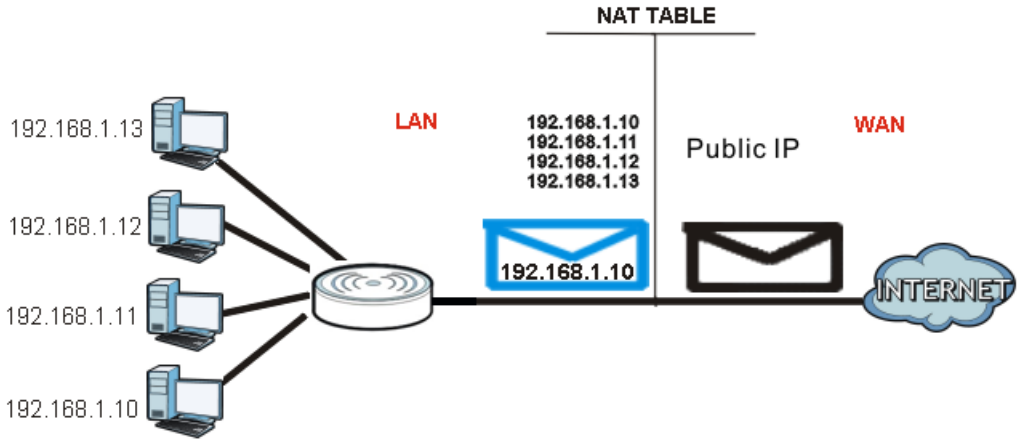
Network Address Translation (NAT)

14.1 Overview

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 Router 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 82 NAT Example



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

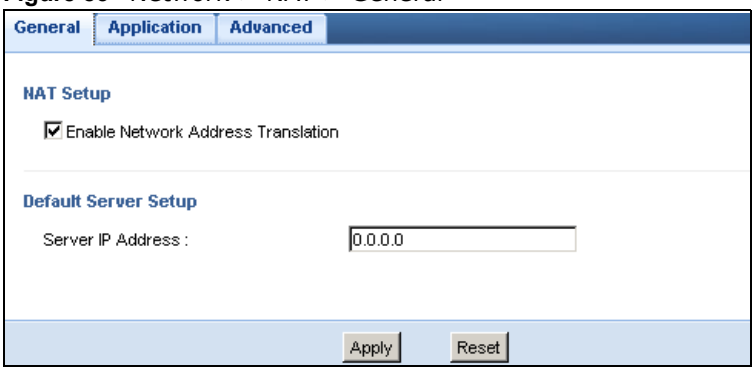
14.2 What You Can Do

- Use the **General** screen (Section 14.3 on page 118) to enable NAT and set a default server.
- Use the **Application** screen (Section 14.4 on page 118) o forward incoming service requests to the server(s) on your local network.
- Use the **Advanced** screen (Section 14.5 on page 120) to change your Router's trigger port settings.

14.3 General NAT Screen

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

Figure 83 Network > NAT > General



The following table describes the labels in this screen.

Table 50 Network > NAT > General

LABEL	DESCRIPTION
NAT Setup	
Enable Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select the check box to enable NAT.
Default Server Setup	
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 Router 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 Router.
Reset	Click **Reset** to begin configuring this screen afresh.

14.4 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.

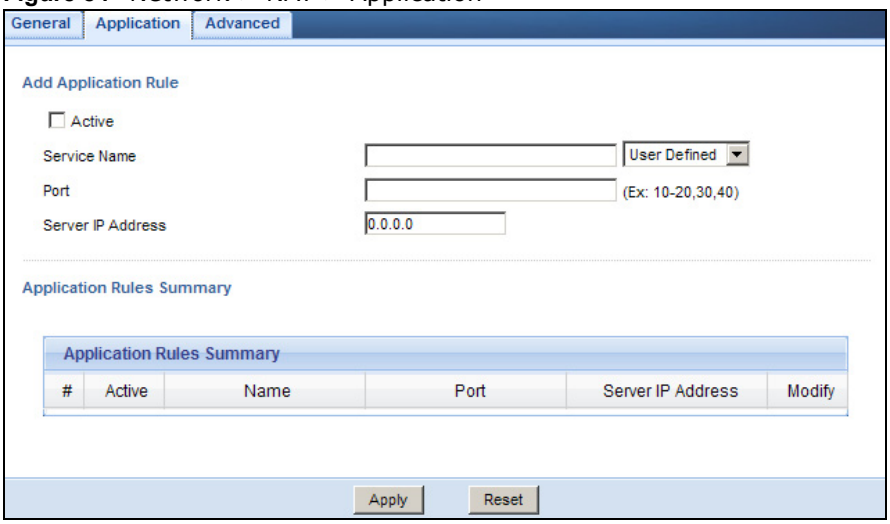
Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your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

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your Router'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 Router discards all packets received for ports that are not specified in this screen or remote management.

Refer to Appendix D on page 223 for port numbers commonly used for particular services.

Figure 84 Network > NAT > Application



The following table describes the labels in this screen.

Table 51 Network > NAT > Application

LABEL	DESCRIPTION
Add Application Rule	
Active	Select the check box to enable this rule and the requested service can be forwarded to the host with a specified internal IP address. Clear the checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Service Name	Type a name (of up to 31 printable characters) to identify this rule in the first field next to **Service Name**. Otherwise, select a predefined service in the second field next to **Service Name**. The predefined service name and port number(s) will display in the **Service Name** and **Port** fields.
Port	Type a port number(s) to define the service to be forwarded to the specified server. To specify a range of ports, enter a hyphen (-) between the first port and the last port, such as 10-20. To specify two or more non-consecutive port numbers, separate them by a comma without spaces, such as 123,567.
Server IP Address	Type the IP address of the server on your LAN that receives packets from the port(s) specified in the **Port** field.

Table 51 Network > NAT > Application (continued)

LABEL	DESCRIPTION
Application Rules Summary	
#	This is the number of an individual port forwarding server entry.
Active	This icon is turned on when the rule is enabled.
Name	This field displays a name to identify this rule.
Port	This field displays the port number(s).
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the **Edit** icon to display and modify an existing rule setting in the fields under **Add Application Rule**. Click the **Remove** icon to delete a rule.
Apply	Click **Apply** to save your changes back to the Router.
Reset	Click **Reset** to begin configuring this screen afresh.

14.5 NAT Advanced Screen

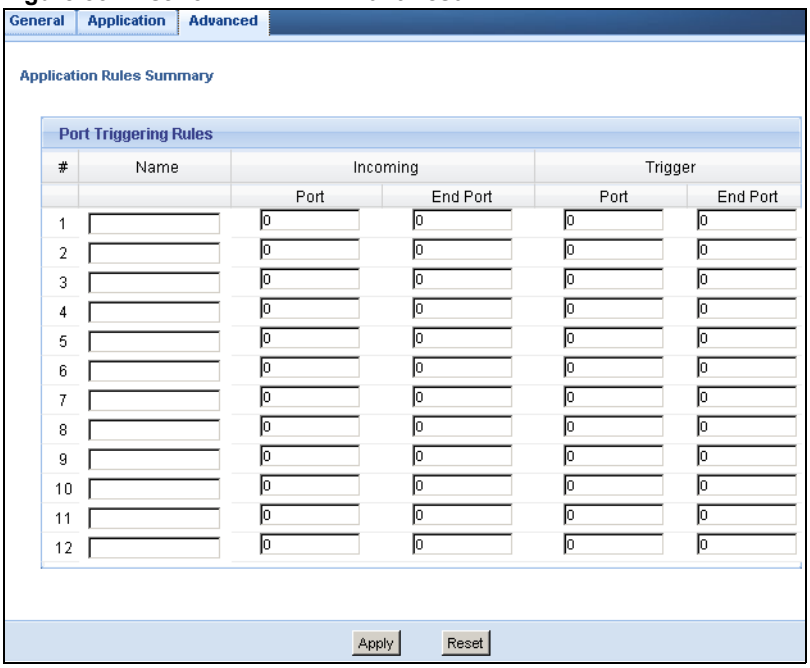
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem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

To change your Router’s trigger port settings, click **Network > NAT** > **Advanced**. The screen appears as shown.

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

Figure 85 Network > NAT > Advanced



The following table describes the labels in this screen.

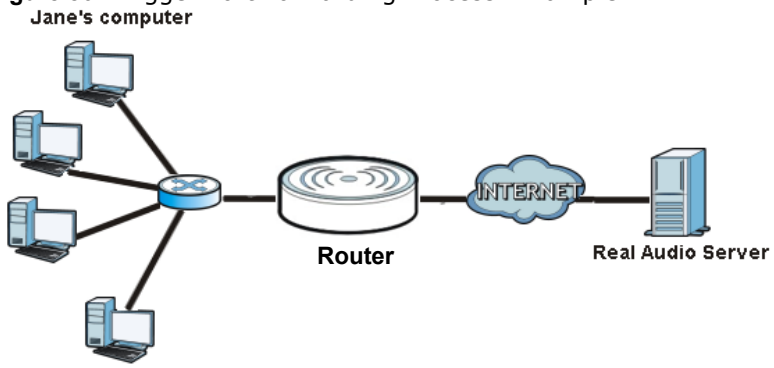
Table 52 Network > NAT > Advanced

LABEL	DESCRIPTION
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Router forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the Router to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click **Apply** to save your changes back to the Router.
Reset	Click **Reset** to begin configuring this screen afresh.

14.5.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 86 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 Router to record Jane’s computer IP address. The Router 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 Router 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 Router times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

14.5.2 Two Points To Remember About Trigger Ports

1. Trigger events only happen on data that is going coming from inside the Router 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.

15

Dynamic DNS

15.1 Overview

Dynamic DNS (DDNS) services let you use a domain name with a dynamic IP address.

15.2 What You Can Do

Use the **Dynamic DNS** screen (Section 15.4 on page 123) to enable DDNS and configure the DDNS settings on the Router.

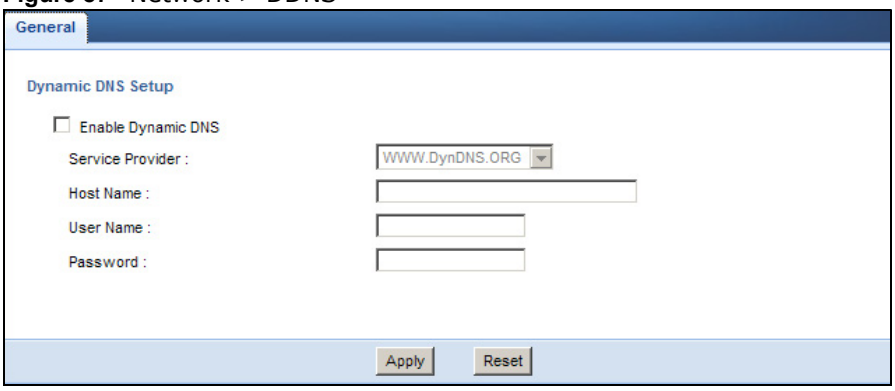
15.3 What You Need To Know

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

15.4 Dynamic DNS Screen

To change your Router's DDNS, click **Network > DDNS**. The screen appears as shown.

Figure 87 Network > DDNS



The following table describes the labels in this screen.

Table 53 Network > DDNS

LABEL	DESCRIPTION
Enable Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Enter a host names in the field provided. You can specify up to two host names in the field separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Apply	Click **Apply** to save your changes back to the Router.
Reset	Click **Reset** to begin configuring this screen afresh.

16

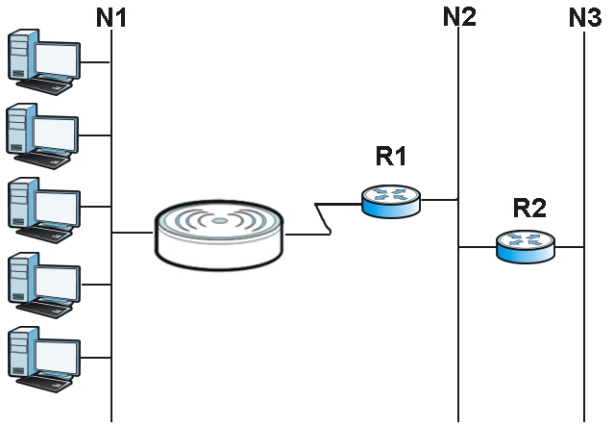
Static Route

16.1 Overview

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

Each remote node specifies only the network to which the gateway is directly connected, and the Router has no knowledge of the networks beyond. For instance, the Router knows about network N2 in the following figure through remote node Router 1. However, the Router is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the Router about the networks beyond the remote nodes.

Figure 88 Example of Static Routing Topology



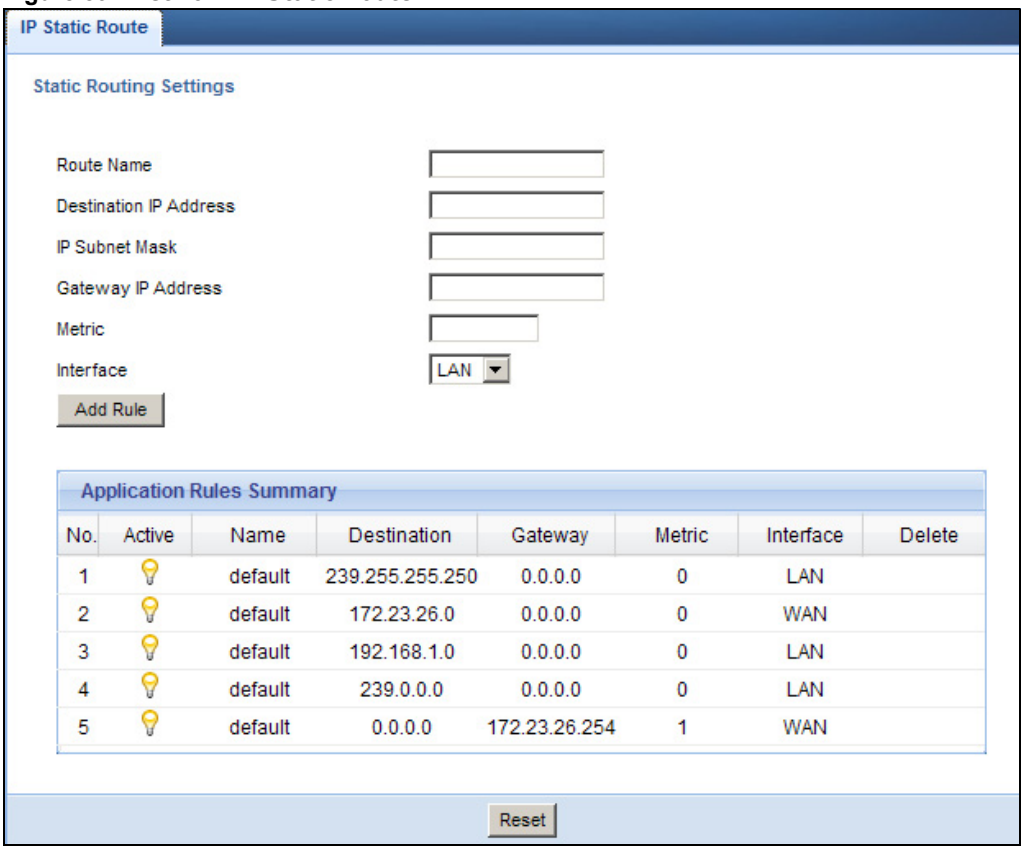
16.2 What You Can Do

Use the **IP Static Route** screen (Section 16.3 on page 126) to view, add and delete routes.

16.3 IP Static Route Screen

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

Figure 89 Network > Static Route



The following table describes the labels in this screen.

Table 54 Network > Static Route

LABEL	DESCRIPTION
Static Routing Settings	
Route Name	Enter a the name that describes or identifies this route.
Destination IP Address	Enter the IP network address of the final destination.
IP Subnet Netmask	This is the subnet to which the route's final destination belongs.
Gateway IP Address	Enter the the IP address of the gateway.
Metric	Assign a number to identify the route.
Add Rule	Click this to add the IP static route.
Application Rules Summary	
No.	This is the number of an individual static route.
Active	The rules are always on and this is indicated by the icon.
Name	This is the name that describes or identifies this route.

Table 54 Network > Static Route

LABEL	DESCRIPTION
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	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.
Metric	This is the number assigned to the route.
Delete	Click the Delete icon to remove a static route from the Router. A window displays asking you to confirm that you want to delete the route.

17

Firewall

17.1 Overview

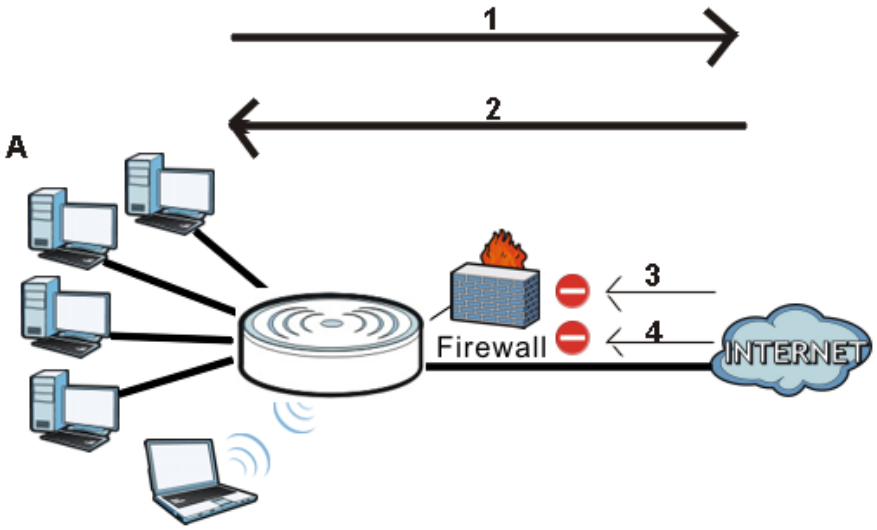
This chapter shows you how to enable and configure the firewall that protects your Router and your LAN from unwanted or malicious traffic.

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 90 Default Firewall Action



17.2 What You Can Do

- Use the **General** (Section 17.4 on page 130) screen to enable or disable the Router's firewall.
- Use the **Services** screen (Section 17.5 on page 131) screen enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

17.3 What You Need To Know

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

It is designed to protect against Denial of Service (DoS) attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The Router's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The Router 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 Router 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 Router 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.

17.4 General Firewall Screen

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

Figure 91 Security > Firewall > General

The following table describes the labels in this screen.

Table 55 Security > Firewall > General

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

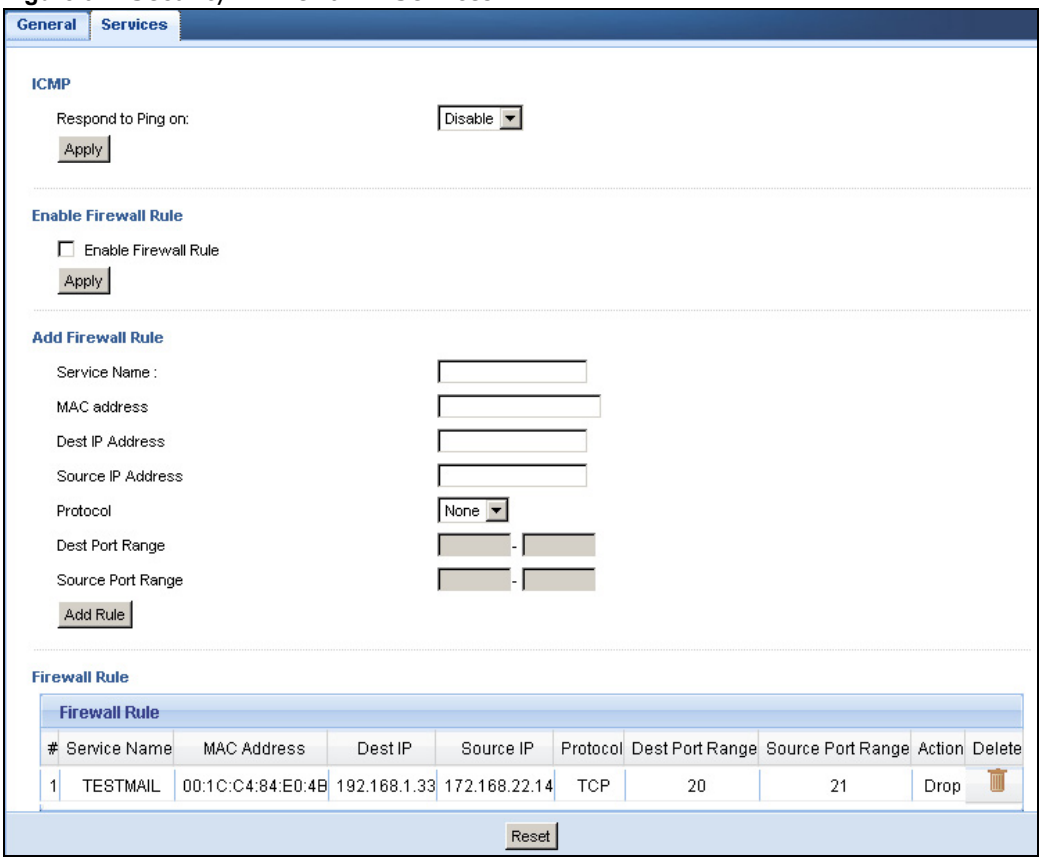
17.5 Services Screen

If an outside user attempts to probe an unsupported port on your Router, an ICMP response packet is automatically returned. This allows the outside user to know the Router exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your Router when unsupported ports are probed.

You can also use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

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

Figure 92 Security > Firewall > Services



The following table describes the labels in this screen.

Table 56 Security > Firewall > Services

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol 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	The Router will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to all incoming LAN and WAN Ping requests.
Apply	Click **Apply** to save the settings.

Table 56 Security > Firewall > Services (continued)

LABEL	DESCRIPTION
Enable Firewall Rule	
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see **Add Firewall Rule** below)
Apply	Click **Apply** to save the settings.
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest IP Address	Enter the IP address of the computer to which traffic for the application or service is entering. The Router applies the firewall rule to traffic initiating from this computer.
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service. The Router applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol (**TCP**, **UDP**, **ICMP** or **None**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click **Add** to save the firewall rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Service Name	This is a name that identifies or describes the firewall rule.
MAC Address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP Address	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP Address	This is the IP address of the computer from which traffic for the application or service is initialized.
Protocol	This is the protocol (**TCP**, **UDP**, **ICMP** or **None**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Action	**Drop** - Traffic matching the conditions of the firewall rule are stopped.
Delete	Click this to remove the firewall rule.
Reset	Click **Reset** to start configuring this screen again.

See Appendix D on page 223 for commonly used services and port numbers.

18

Content Filter

18.1 Overview

This chapter provides a brief overview of content filtering using the embedded web GUI.

Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering is the ability to block certain web features or specific URL keywords.

18.2 What You Can Do

Use the **Content Filter** (Section 18.4 on page 134) screen to restrict web features, add keywords for blocking and designate a trusted computer.

18.3 What You Need To Know

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages.

18.3.1 Content Filtering Profiles

A content filtering profile conveniently stores your custom settings for the following features.

Restrict Web Features

The Router can disable web proxies and block web features such as ActiveX controls, Java applets and cookies.

Keyword Blocking URL Checking

The Router 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.

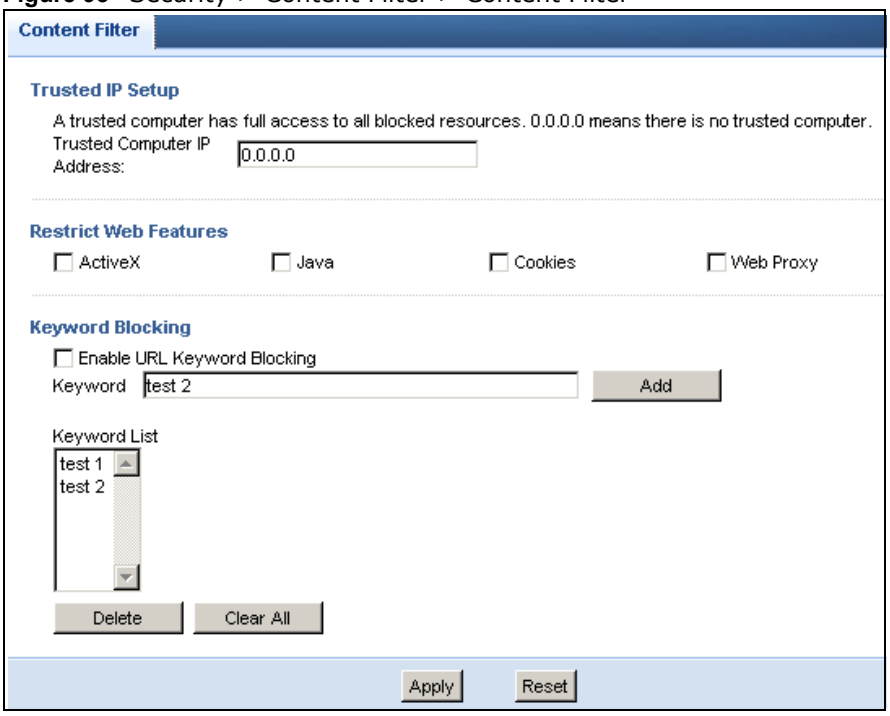
Since the Router checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the Router would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file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

18.4 Content Filter Screen

Use this screen to restrict web features, add keywords for blocking and designate a trusted computer.

Click **Security** > **Content Filter** to open the **Content Filter** screen.

Figure 93 Security > Content Filter > Content Filter



The following table describes the labels in this screen.

Table 57 Security > Content Filter > Content Filter

LABEL	DESCRIPTION
Trusted IP Setup	To enable this feature, type an IP address of any one of the computers in your network that you want to have as a trusted computer. This allows the trusted computer to have full access to all features that are configured to be blocked by content filtering. Leave this field blank to have no trusted computers.
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.

Table 57 Security > Content Filter > Content Filter (continued)

LABEL	DESCRIPTION
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	The Router 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 this check box to enable this feature.
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.
Keyword List	This list displays the keywords already added.
Add	Click **Add** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. 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.
Delete	Highlight a keyword in the lower box and click **Delete** to remove it. The keyword disappears from the text box after you click **Apply**.
Clear All	Click this button to remove all of the listed keywords.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh

19

Bandwidth Management

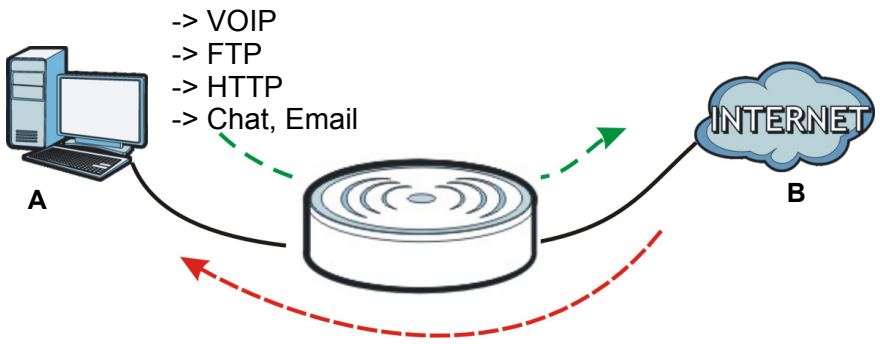
19.1 Overview

This chapter contains information about configuring bandwidth management and editing rules.

ZyXEL's Bandwidth Management allows you to specify bandwidth management rules based on an application.

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 94 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).

19.2 What You Can Do

- Use the **General** screen (Section 19.4 on page 138) to enable bandwidth management and assign bandwidth values.
- Use the **Advanced** screen (Section 19.5 on page 138) to configure bandwidth managements rule for the pre-defined services and applications.
- Use the **Monitor** screen (Section 19.6 on page 143) to view the amount of network bandwidth that applications running in the network are using.

19.3 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 (Section 19.5 on page 138).

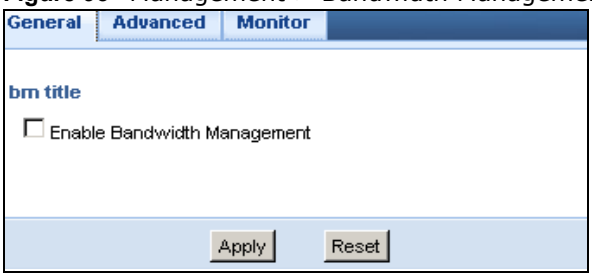
The sum of the bandwidth allotments that apply to the LAN interface (WAN to LAN, WAN to WLAN) must be less than or equal to the **Downstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen Section 19.5 on page 138.

19.4 General Screen

Use this screen to have the Router apply bandwidth management.

Click **Management > Bandwidth Management** to open the bandwidth management **General** screen.

Figure 95 Management > Bandwidth Management > General



The following table describes the labels in this screen.

Table 58 Management > Bandwidth Management > General

LABEL	DESCRIPTION
Enable Bandwidth Management	This field allows you to have Router apply bandwidth management. Enable bandwidth management to give traffic that matches a bandwidth rule priority over traffic that does not match a bandwidth rule. Enabling bandwidth management also allows you to control the maximum or minimum amounts of bandwidth that can be used by traffic that matches a bandwidth rule.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

19.5 Advanced Screen

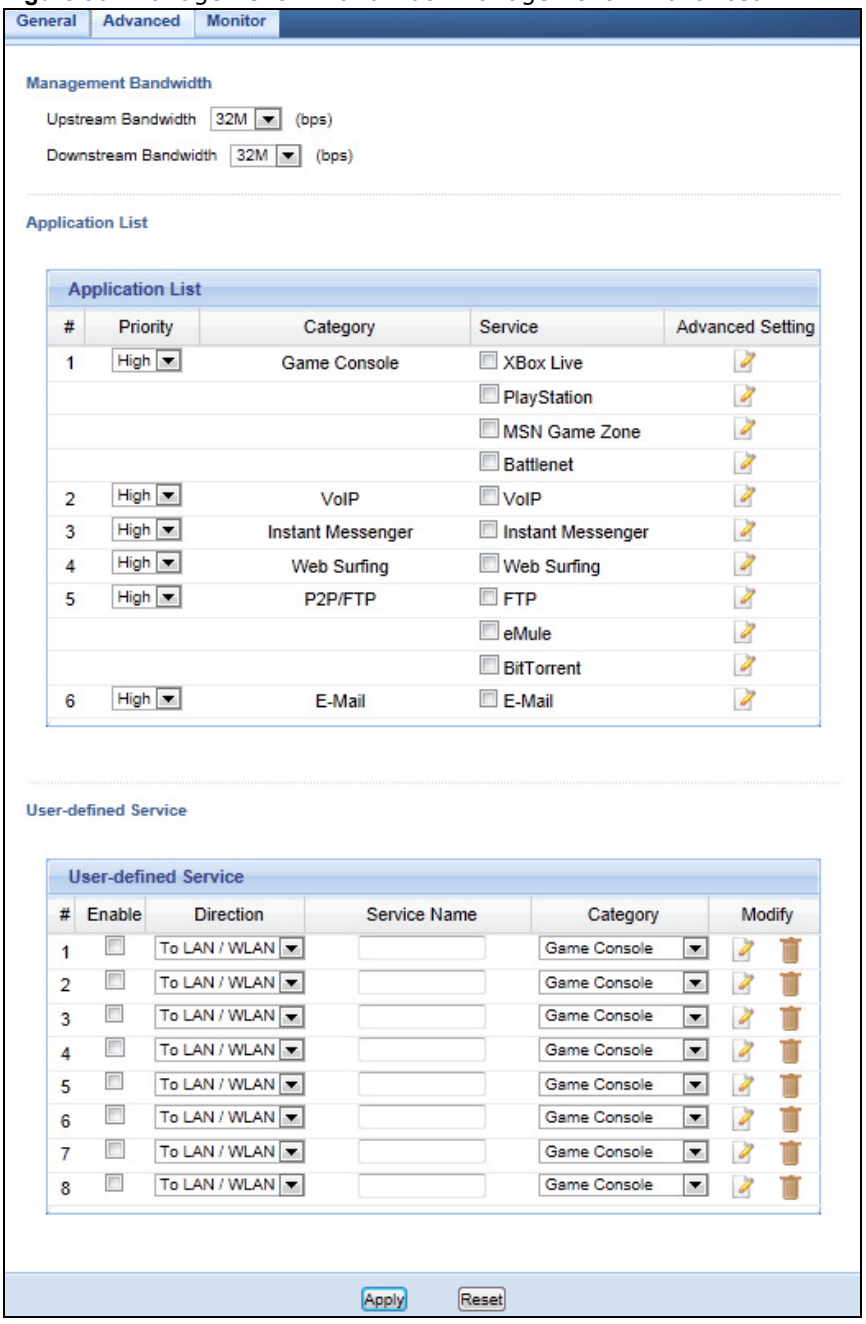
Use this screen to configure bandwidth management rules for the pre-defined services or applications.

You can also use this screen to configure bandwidth management rule for other services or applications that are not on the pre-defined list of Router. Additionally, you can define the source and destination IP addresses and port for a service or application.

Note: The two tables shown in this screen can be configured and applied at the same time.

Click **Management** > **Bandwidth Management** > **Advanced** to open the bandwidth management **Advanced** screen.

Figure 96 Management > Bandwidth Management > Advanced



The following table describes the labels in this screen.

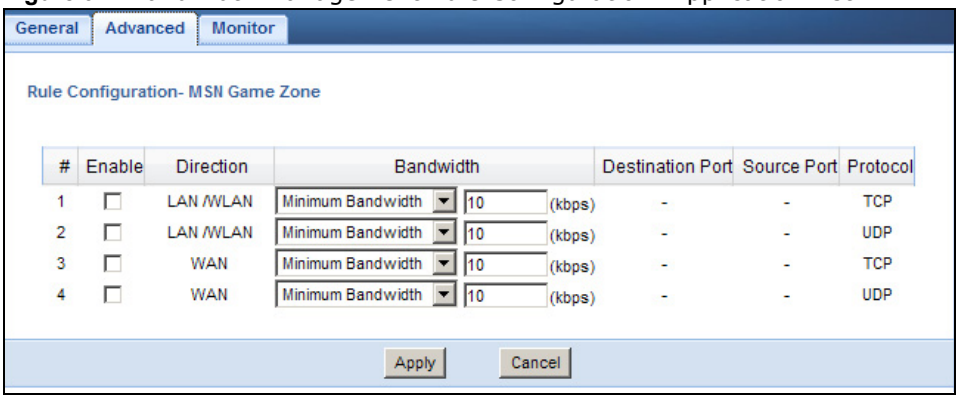
Table 59 Management > Bandwidth Management > Advanced

LABEL	DESCRIPTION
Management Bandwidth	
Upstream Bandwidth	Select the total amount of bandwidth (from 64 Kilobits to 50 Megabits) that you want to dedicate to uplink traffic. This is traffic from LAN/WLAN to WAN.
Downstream Bandwidth	Select the total amount of bandwidth (from 64 Kilobits to 50 Megabits) that you want to dedicate to uplink traffic. This is traffic from WAN to LAN/WLAN.
Application List	Use this table to allocate specific amounts of bandwidth based on a pre-defined service.
#	This is the number of an individual bandwidth management rule.
Priority	Select a priority from the drop down list box. Choose **High**, **Mid** or **Low**. • **High** - Select this for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay). • **Mid** - Select this for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay. • **Low** - Select this for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Category	This is the category where a service belongs.
Service	This is the name of the service. Select the check box to have the Router apply this bandwidth management rule.
Advanced Setting	Click the **Edit** icon to open the **Rule Configuration** screen where you can modify the rule.
User-defined Service	Use this table to allocate specific amounts of bandwidth to specific applications or services you specify.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the Router apply this bandwidth management rule.
Direction	Select **TO LAN/WLAN** to apply bandwidth management to traffic from WAN to LAN/WLAN. Select **TO WAN** to apply bandwidth management to traffic from LAN/WLAN to WAN.
Service Name	Enter a descriptive name for the bandwidth management rule.
Category	This is the category where a service belongs.
Modify	Click the **Edit** icon to open the **Rule Configuration** screen. Modify an existing rule or create a new rule in the **Rule Configuration** screen. See Section 19.5.2 on page 142 for more information. Click the **Remove** icon to delete a rule.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

19.5.1 Rule Configuration: Application Rule Configuration

If you want to edit a bandwidth management rule for a pre-defined service or application, click the **Edit** icon in the **Application List** table of the **Advanced** screen. The following screen displays.

Figure 97 Bandwidth Management Rule Configuration: Application List



The following table describes the labels in this screen.

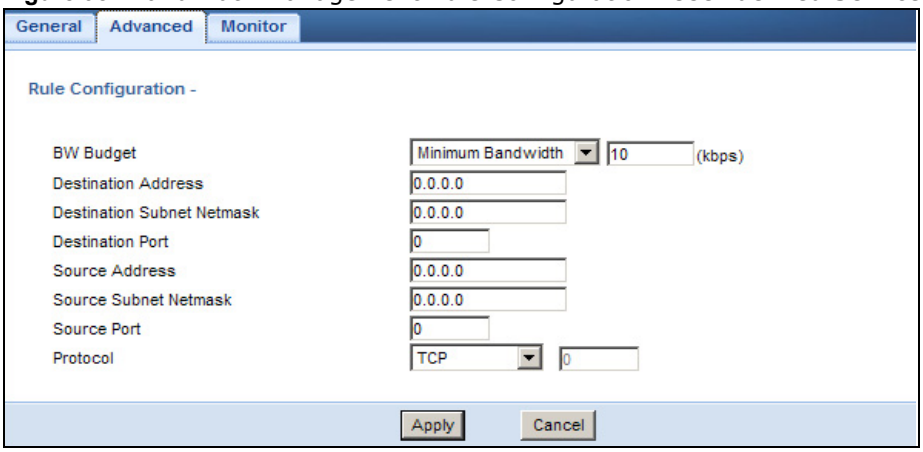
Table 60 Bandwidth Management Rule Configuration: Application List

LABEL	DESCRIPTION
#	This is the number of an individual bandwidth management rule.
Enable	Select an interface's check box to enable bandwidth management on that interface.
Direction	These read-only labels represent the physical interfaces. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the Router and be managed by bandwidth management.
Bandwidth	Select **Maximum Bandwidth** or **Minimum Bandwidth** and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Port	This is the port number of the destination that define the traffic type, for example TCP port 80 defines web traffic. See Appendix D on page 223 for some common services and port numbers.
Source Port	This is the port number of the source that define the traffic type, for example TCP port 80 defines web traffic. See Appendix D on page 223 for some common services and port numbers.
Protocol	This is the protocol (**TCP**, **UDP** or user-defined) used for the service.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to exit this screen without saving.

19.5.2 Rule Configuration: User Defined Service Rule Configuration

If you want to edit a bandwidth management rule for other applications or services, click the **Edit** icon in the **User-defined Service** table of the **Advanced** screen. The following screen displays.

Figure 98 Bandwidth Management Rule Configuration: User-defined Service



The following table describes the labels in this screen

Table 61 Bandwidth Management Rule Configuration: User-defined Service

LABEL	DESCRIPTION
BW Budget	Select **Maximum Bandwidth** or **Minimum Bandwidth** and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Address	Enter the IP address of the destination computer. The Router applies bandwidth management to the service or application that is entering this computer.
Destination Subnet Netmask	Enter the subnet netmask of the destination of the traffic for which the bandwidth management rule applies.
Destination Port	This is the port number of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Address	Enter the IP address of the computer that initializes traffic for the application or service. The Router applies bandwidth management to traffic initiating from this computer.
Source Subnet Netmask	Enter the subnet netmask of the computer initiating the traffic for which the bandwidth management rule applies.
Source Port	This is the port number of the source that define the traffic type, for example TCP port 80 defines web traffic.
Protocol	Select the protocol (**TCP**, **UDP**, **User defined**) for which the bandwidth management rule applies. If you select **User-defined**, enter the protocol for which the bandwidth management rule applies. For example, ICMP for ping traffic.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to exit this screen without saving.

See Appendix D on page 223 for commonly used services and port numbers.

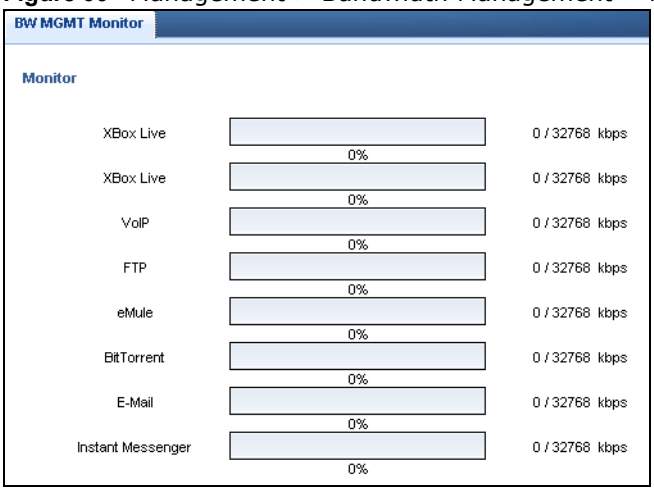
19.6 Monitor Screen

Use this screen to view the amount of network bandwidth that applications running in the network are using.

The bandwidth is measured in kilobits per second (kbps).

The monitor shows what kinds of applications are running in the network, the maximum kbps that each application can use, as well as the percentage of bandwidth it is using.

Figure 99 Management > Bandwidth Management > Monitor



19.6.1 Predefined Bandwidth Management Services

The following is a description of some services that you can select and to which you can apply media bandwidth management in the **Management** > **Bandwidth Management** > **Advanced** screen.

Table 62 Media Bandwidth Management Setup: Services

SERVICE	DESCRIPTION
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail.
WWW	The World Wide Web (WWW) is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.
E-Mail	Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail:
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is transported primarily over UDP but can also be transported over TCP.

Table 62 Media Bandwidth Management Setup: Services (continued)

SERVICE	DESCRIPTION
BitTorrent	BitTorrent is a free P2P (peer-to-peer) sharing tool allowing you to distribute large software and media files. BitTorrent requires you to search for a file with a searching engine yourself. It distributes files by corporation and trading, that is, the client downloads the file in small pieces and share the pieces with other peers to get other half of the file.
Gaming	Online gaming services lets you play multiplayer games on the Internet via broadband technology. As of this writing, your Router supports Xbox, Playstation, Battlenet and MSN Game Zone.

20

Remote Management

20.1 Overview

This chapter provides information on the Remote Management screens.

Remote Management allows you to manage your Router from a remote location through the following interfaces:

- LAN and WAN
- LAN only
- WAN only

Note: The Router is managed using the Web Configurator.

20.2 What You Can Do

Use the **WWW** screen (Section 20.4 on page 146) to define the interface/s from which the Router can be managed remotely and specify a secure client that can manage the Router.

20.3 What You Need to Know

Remote management over LAN or WAN will not work when:

1. The IP address in the **Secured Client IP Address** field (Section 20.4 on page 146) does not match the client IP address. If it does not match, the Router will disconnect the session immediately.
2. There is already another remote management session. You may only have one remote management session running at one time.
3. There is a firewall rule that blocks it.

20.3.1 Remote Management and NAT

When NAT is enabled:

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

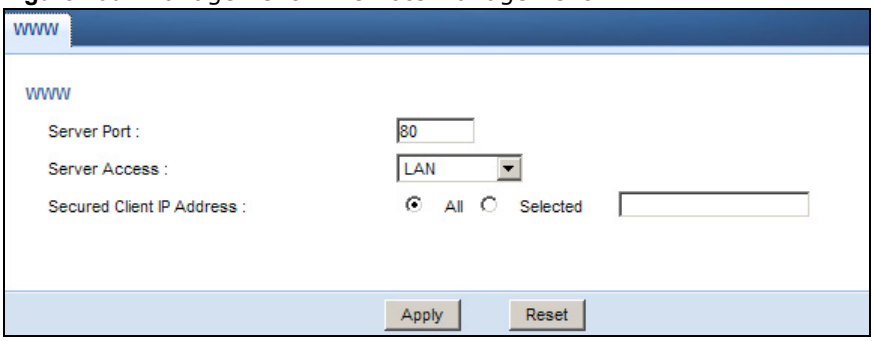
20.3.2 System Timeout

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

20.4 WWW Screen

To change your Router's remote management settings, click **Management > Remote Management > WWW**.

Figure 100 Management > Remote Management > WWW



The following table describes the labels in this screen

Table 63 Management > Remote Management > WWW

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the Router using this service.
Secured Client IP Address	Select **All** to allow all computes to access the Router. Otherwise, check **Selected** and specify the IP address of the computer that can access the Router.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

21

Universal Plug-and-Play (UPnP)

21.1 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.

21.2 What You Can Do

Use the UPnP screen (Section 21.4 on page 148) to enable UPnP on your Router.

21.3 What You Need to Know

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.

21.3.1 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.

21.3.2 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 Router allows multicast messages on the LAN only.

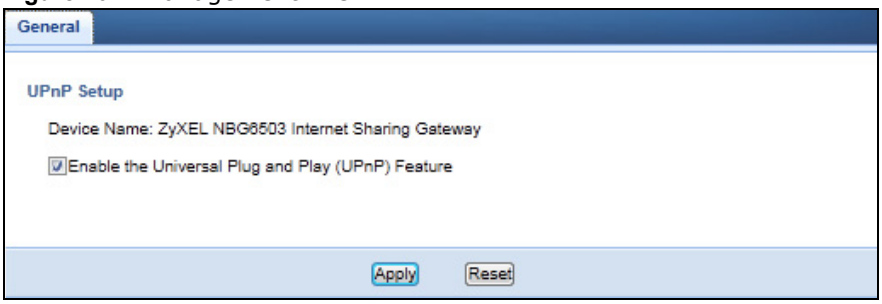
All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

21.4 UPnP Screen

Use this screen to enable UPnP on your Router.

Click **Management > UPnP** to display the screen shown next.

Figure 101 Management > UPnP



The following table describes the fields in this screen.

Table 64 Management > UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Router's IP address (although you must still enter the password to access the web configurator).
Apply	Click **Apply** to save the setting to the Router.
Reset	Click **Reset** to return to the previously saved settings.

21.5 Technical Refereance

The sections show examples of using UPnP.

21.5.1 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 Router.

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

21.5.1.1 Auto-discover Your UPnP-enabled Network Device

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

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

Figure 102 Network Connections

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

Figure 103 Internet Connection Properties

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

Figure 104 Internet Connection Properties: Advanced Settings

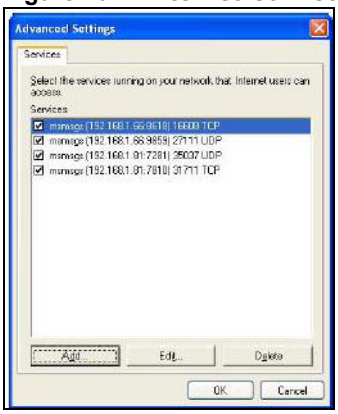
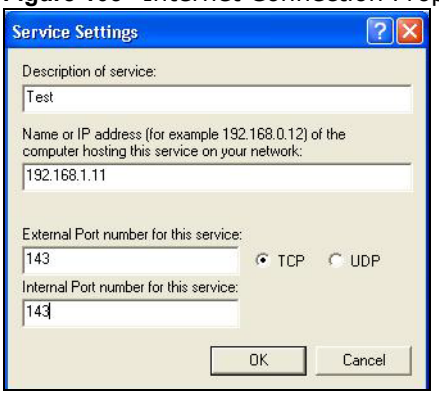


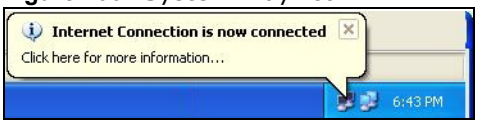
Figure 105 Internet Connection Properties: Advanced Settings: Add



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 106 System Tray Icon



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

Figure 107 Internet Connection Status

21.5.2 Web Configurator Easy Access

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

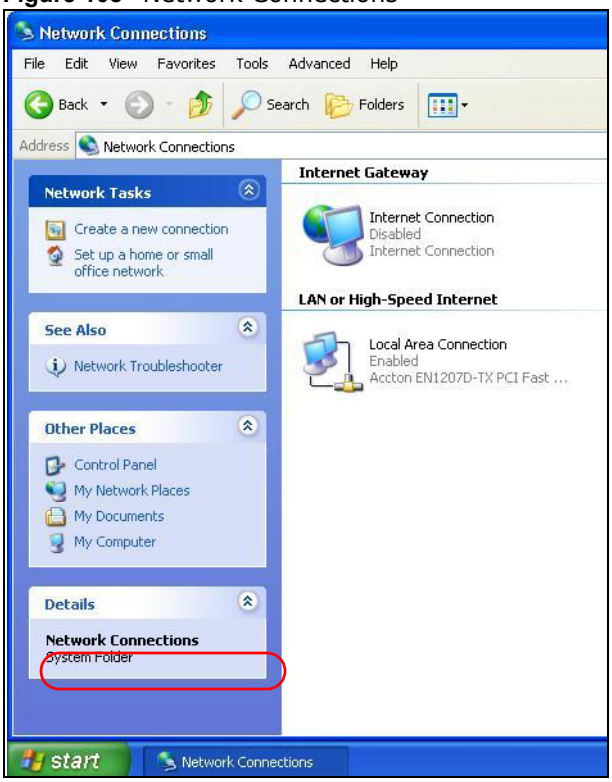
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

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

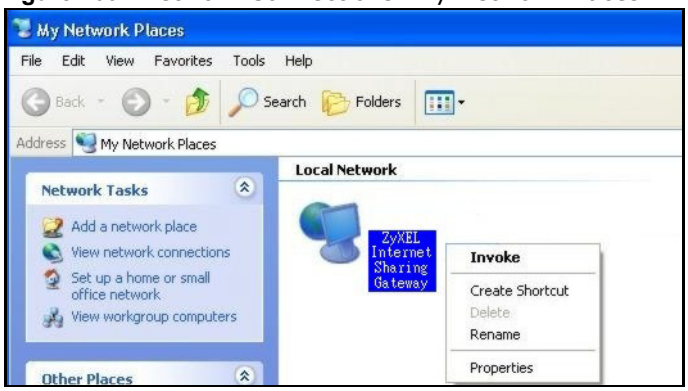
Figure 108 Network Connections



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

5 Right-click on the icon for your Router and select **Invoke**. The web configurator login screen displays.

Figure 109 Network Connections: My Network Places



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

Figure 110 Network Connections: My Network Places: Properties: Example

22

Maintenance

22.1 Overview

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

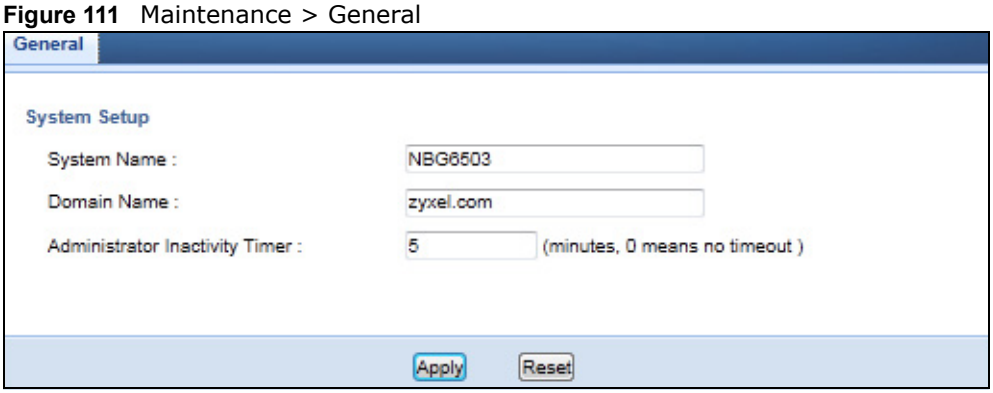
22.2 What You Can Do

- Use the **General** screen to configure system and domain name. You can also set the timeout period of the management session (Section 22.3 on page 155).
- Use the **Password** screen to change your Router's system password (Section 22.4 on page 156).
- Use the **Time** screen to change your Router's time and date (Section 22.5 on page 157).
- Use the **Firmware Upgrade** screen to upload firmware to your Router (Section 22.6 on page 158).
- Use the **Backup/Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration (Section 22.8 on page 161).
- Use the **Restart** screen to reboot the Router without turning the power off (Section 22.8 on page 161).
- Use the **Sys OP Mode** screen to select how you want to use your Router (Section 22.10 on page 163).

22.3 General Screen

Use this screen to set the configure system and domain name as well as management session timeout period. Click **Maintenance** > **General**. The following screen displays.

Figure 111 Maintenance > General



The following table describes the labels in this screen.

Table 65 Maintenance > General

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

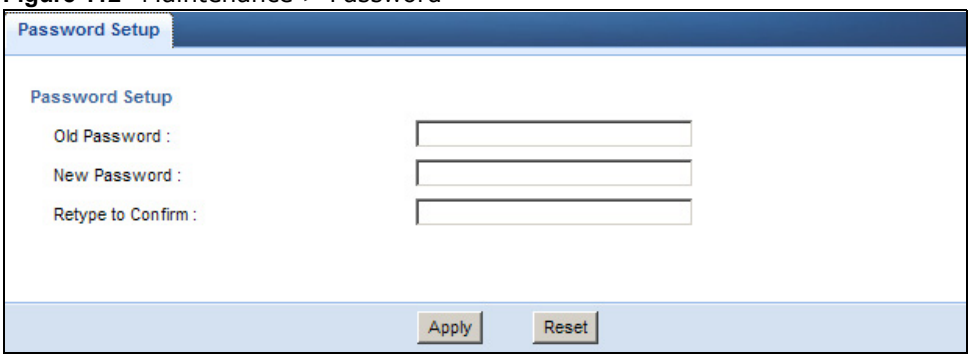
22.4 Password Screen

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

If you forget your Router's password (or IP address), you will need to reset the device. See Section 22.8 on page 161 for details.

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

Figure 112 Maintenance > Password



The following table describes the labels in this screen.

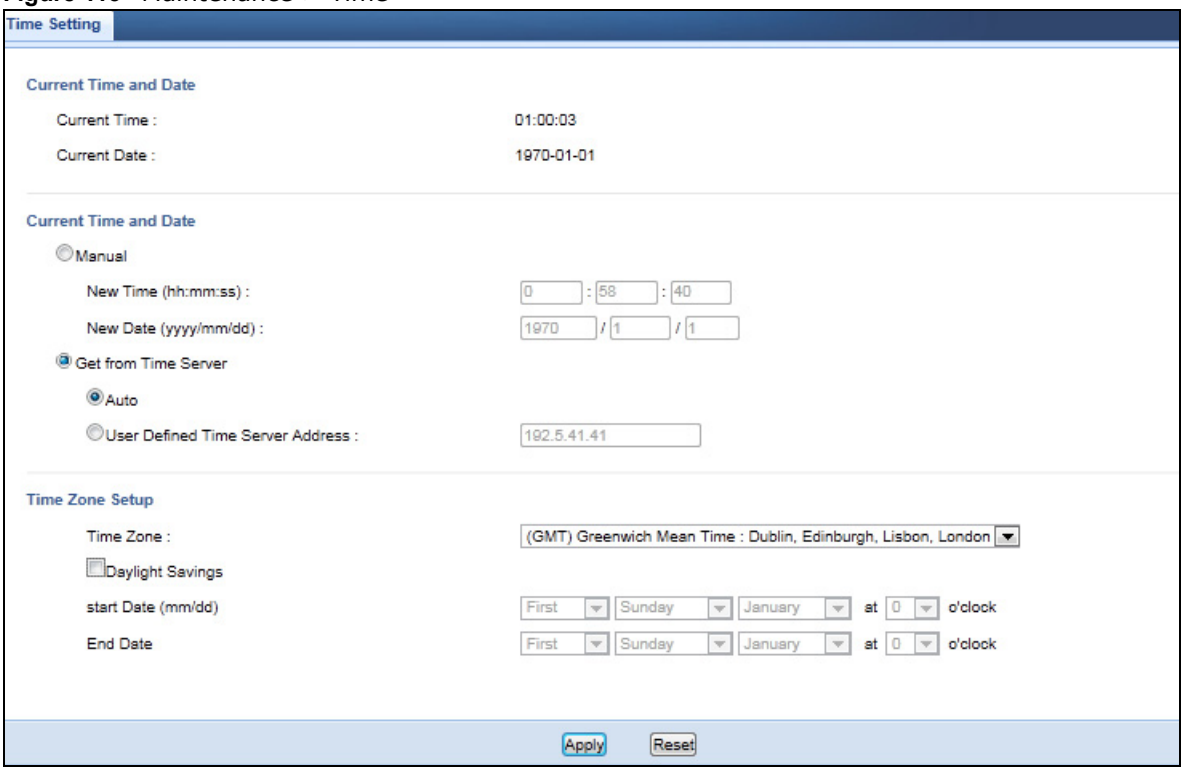
Table 66 Maintenance > Password

LABEL	DESCRIPTION
Password Setup	Change your Router'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 Router.
Reset	Click **Reset** to begin configuring this screen afresh.

22.5 Time Setting Screen

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

Figure 113 Maintenance > Time



The following table describes the labels in this screen.

Table 67 Maintenance > Time

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

Table 67 Maintenance > Time (continued)

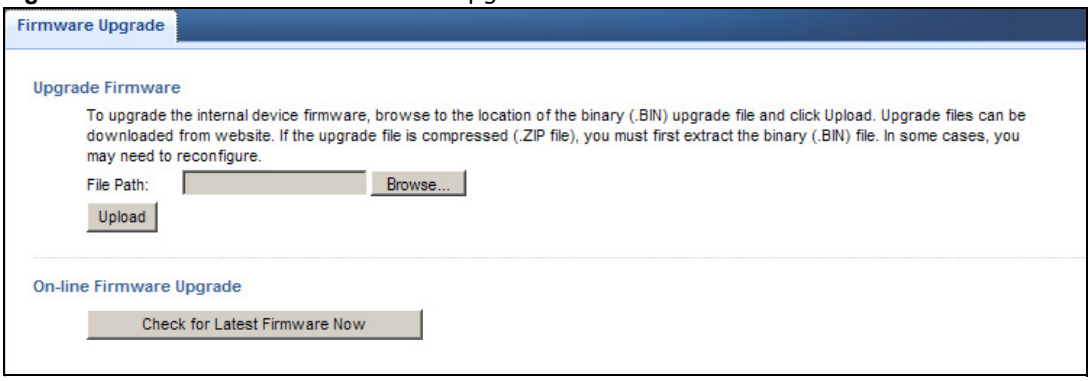
LABEL	DESCRIPTION
Get from Time Server	Select this radio button to have the Router get the time and date from the time server you specified below.
Auto	Select **Auto** to have the Router automatically search for an available time server and synchronize the date and time with the time server after you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

22.6 Firmware Upgrade Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "Router.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

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

Figure 114 Maintenance > Firmware Upgrade



The following table describes the labels in this screen.

Table 68 Maintenance > Firmware Upgrade

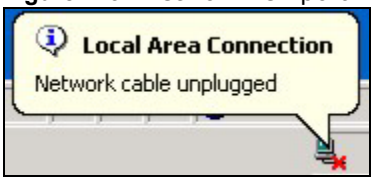
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload**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

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

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

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

Figure 115 Network Temporarily Disconnected



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

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

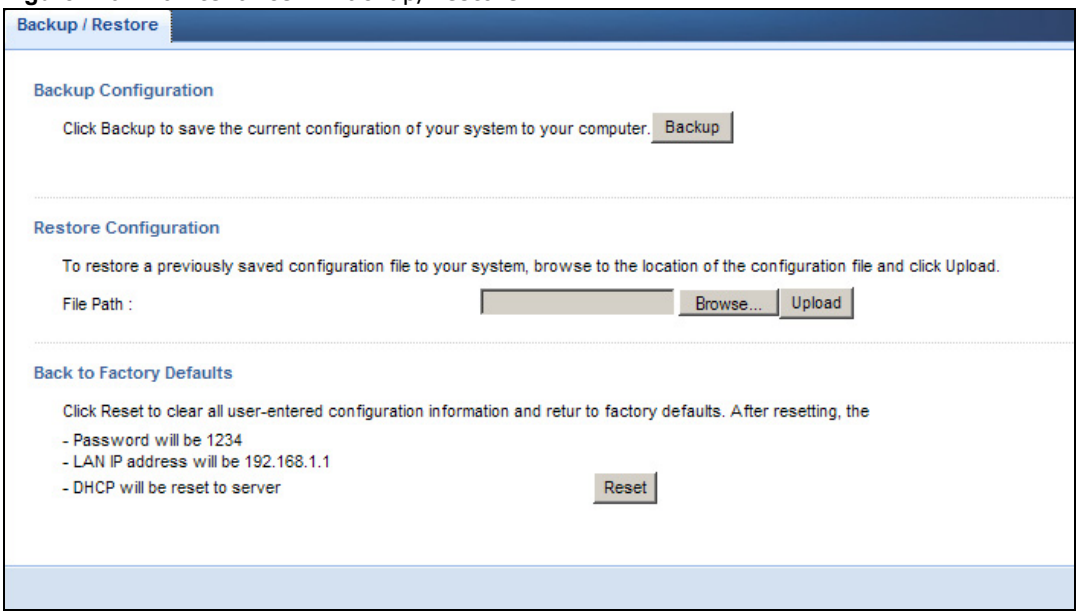
22.7 Configuration Backup/Restore Screen

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

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

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

Figure 116 Maintenance > Backup/Restore



The following table describes the labels in this screen.

Table 69 Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup	Click **Backup** to save the Router's current configuration to your computer.
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.

Table 69 Maintenance > Backup/Restore (continued)

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

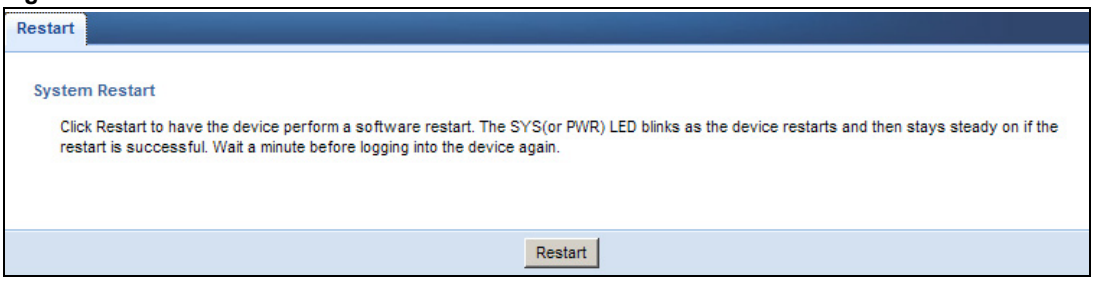
Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default Router IP address (192.168.1.2). See Appendix B on page 181 for details on how to set up your computer's IP address.

22.8 Restart Screen

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

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

Figure 117 Maintenance > Restart



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

22.9 System Operation Mode Overview

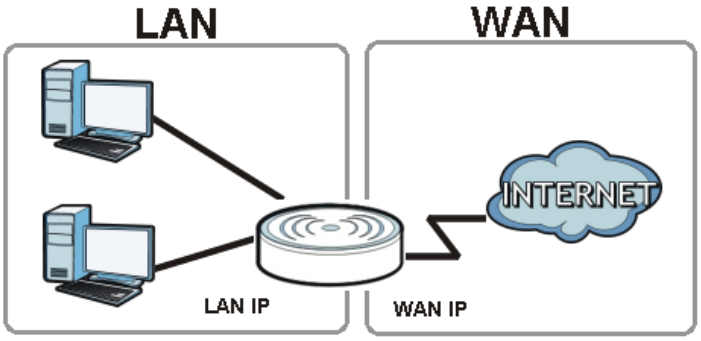
The **Sys OP Mode** (System Operation Mode) function lets you configure your Router as an access point, wireless client or both at the same time. You can choose between **Router** and **Access Point Mode** depending on your network topology and the features you require from your device.

The following describes the device modes available in your Router.

Router

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

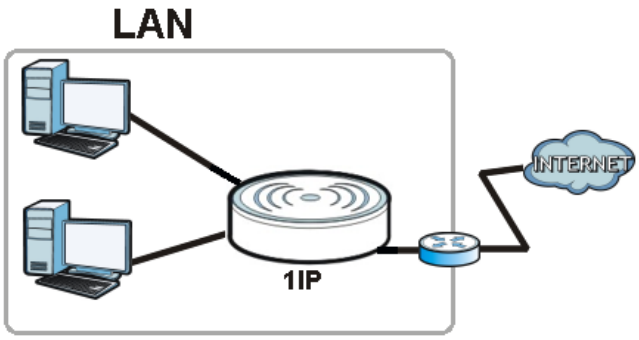
Figure 118 LAN and WAN IP Addresses in Router Mode



Access Point

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

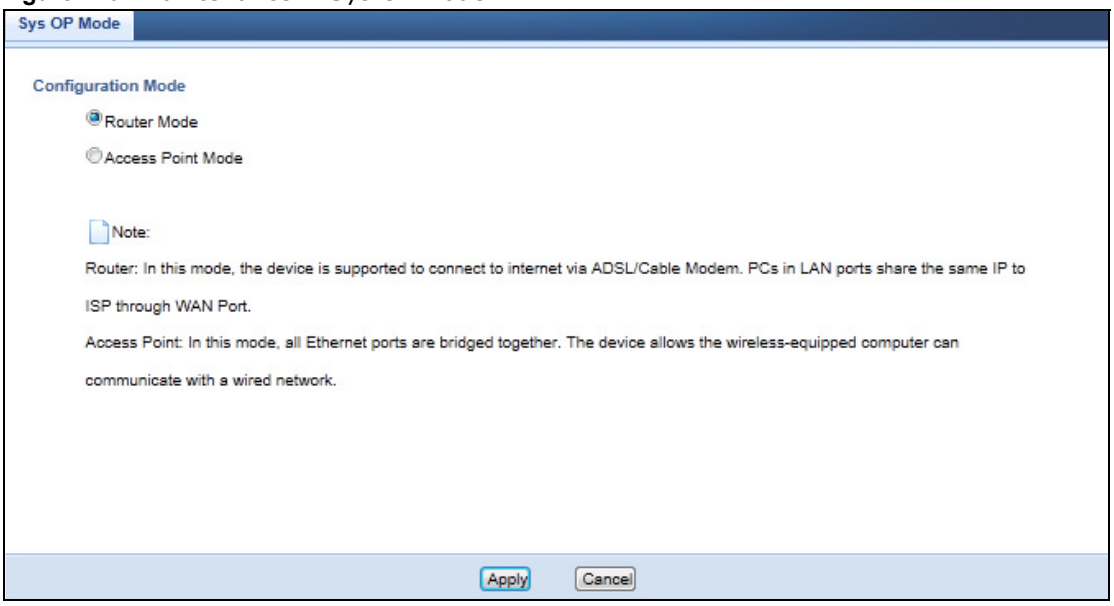
Figure 119 Access Point Mode



22.10 Sys OP Mode Screen

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

Figure 120 Maintenance > Sys OP Mode



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

Table 70 Maintenance > Sys OP Mode

LABEL	DESCRIPTION
System Operation Mode	
Router	Select **Router Mode** if your device routes traffic between a local network and another network such as the Internet. This mode offers services such as a firewall or bandwidth management. You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings.
Access Point	Select **Access Point Mode** if your device bridges traffic between clients on the same network. • In **Access Point 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. • The IP address of the device on the local network is set to 192.168.1.2.
Apply	Click **Apply** to save your settings.
Cancel	Click **Cancel** to return your settings to the default (**Router**).

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

23

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
- Router Access and Login
- Internet Access
- Resetting the Router to Its Factory Defaults
- Wireless Router/AP Troubleshooting

23.1 Power, Hardware Connections, and LEDs

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

1. Make sure you are using the power adaptor or cord included with the Router.
2. Make sure the power adaptor or cord is connected to the Router and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the Router.
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 1.5 on page 17.
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 Router.
5. If the problem continues, contact the vendor.

23.2 Router Access and Login

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

1 The default IP address is **192.168.1.1**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the Router 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 Router (it depends on the network), so enter this IP address in your Internet browser.Set your device to **Router Mode**, login (see the Quick Start Guide for instructions) and go to the **Device Information** table in the **Status** screen. Your Router's IP address is available in the **Device Information** table.

- If the **DHCP** setting under **LAN information** is **None**, your device has a fixed IP address.
- If the **DHCP** setting under **LAN information** is **Client**, then your device receives an IP address from a DHCP server on the network.

3 If your Router is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.

4 Reset your Router to change all settings back to their default. This means your current settings are lost. See Section 23.4 on page 169 in the **Troubleshooting** for information on resetting your Router.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 23.4 on page 169.

I cannot see or access the **Login** screen in the Web Configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address (Section 12.4 on page 111), 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 Router.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix A on page 173.

4 Make sure your computer is in the same subnet as the Router. (If you know that there are routers between your computer and the Router, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Appendix B on page 181.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the Router. See Appendix B on page 181.

5 Reset the device to its factory defaults, and try to access the Router with the default IP address. See Section 3.3 on page 35.

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

Advanced Suggestion

- 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 Router.

1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.

2 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.

3 Disconnect and re-connect the power adaptor or cord to the Router.

4 If this does not work, you have to reset the device to its factory defaults. See Section 23.4 on page 169.

23.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.

- Go to **Network > Wireless LAN 2.4G > General > WDS** and check if the Router is set to bridge mode. Select **Disable** and try to connect to the Internet again.

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**. Check your System Operation Mode setting.

- Select **Router** if your device routes traffic between a local network and another network such as the Internet.
- Select **Access Point** if your device bridges traffic between clients on the same network.

6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the Router), 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 1.5 on page 17.

2 Reboot the Router.

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 1.5 on page 17. If the Router 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 Router 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 Router.

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

Advanced Suggestions

- Check the settings for bandwidth management. If it is disabled, you might consider activating it. If it is enabled, you might consider changing the allocations.

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

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

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

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

23.4 Resetting the Router to Its Factory Defaults

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

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

To reset the Router,

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

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

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

23.5 Wireless Router/AP Troubleshooting

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

1. Make sure the wireless LAN is enabled on the Router

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 Router.

4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the Router.

5 Check that both the Router 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 Router.

7 Make sure you allow the Router to be remotely accessed through the WLAN interface. Check your remote management settings.

- See the chapter on Wireless LAN in the User's Guide for more information.

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

192.168.1.1 is the default IP in Router mode (the default mode). In AP mode the default IP is 192.168.1.2. So, when you switch from Router mode to AP mode, you need to use the AP mode IP to log in.

My 5G network doesn't work.

Make sure you connect the correct antenna (5G antenna) to the **2.4G / 5G** connector. See the Quick Start Guide for details.

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.

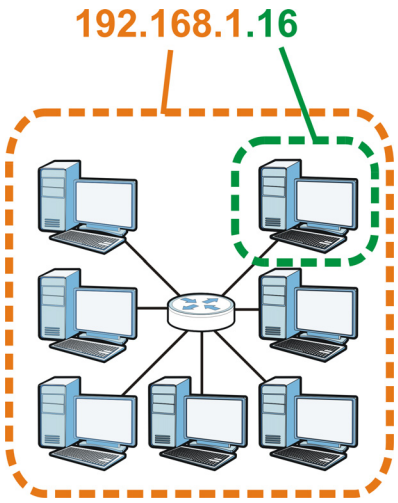
Structure

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 121 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 71 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 72 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 73 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 74 Alternative Subnet Mask Notation

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

Table 74 Alternative Subnet Mask Notation (continued)

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

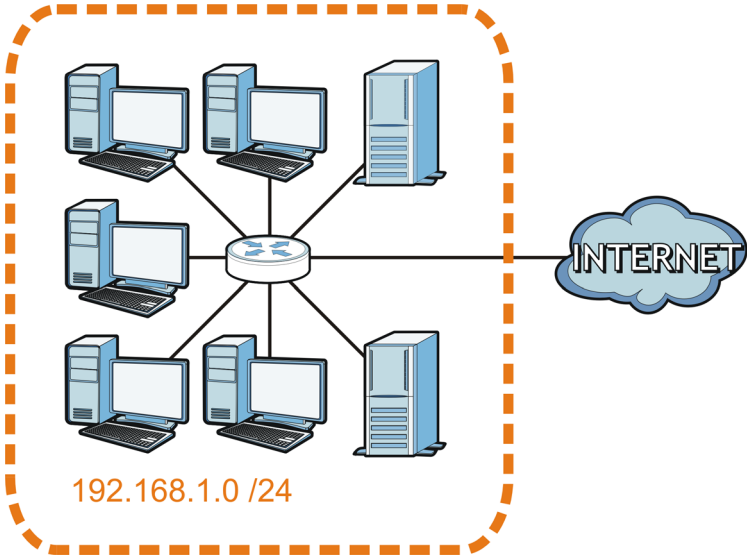
Subnetting

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

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

The following figure shows the company network before subnetting.

Figure 122 Subnetting Example: Before Subnetting

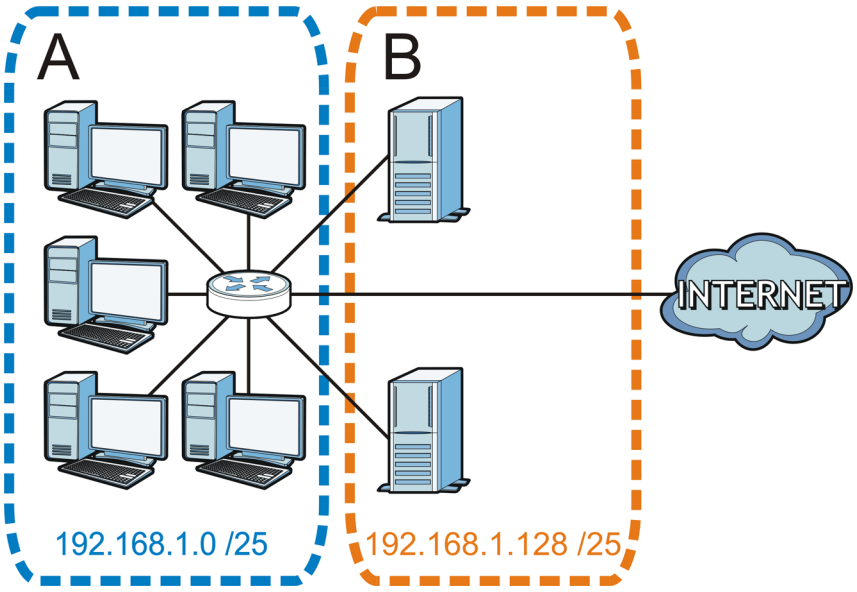


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 123 Subnetting Example: After Subnetting



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

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

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

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

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

Table 75 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000

Table 75 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
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 76 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 77 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 78 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

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

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

Table 79 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 80 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 81 16-bit Network Number Subnet Planning

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

Table 81 16-bit Network Number Subnet Planning (continued)

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

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

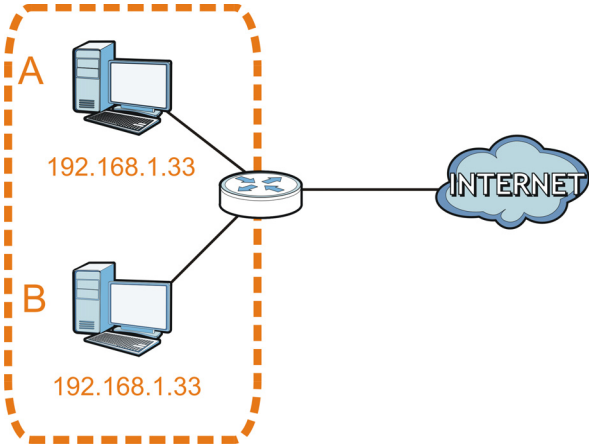
IP Address Conflicts

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.

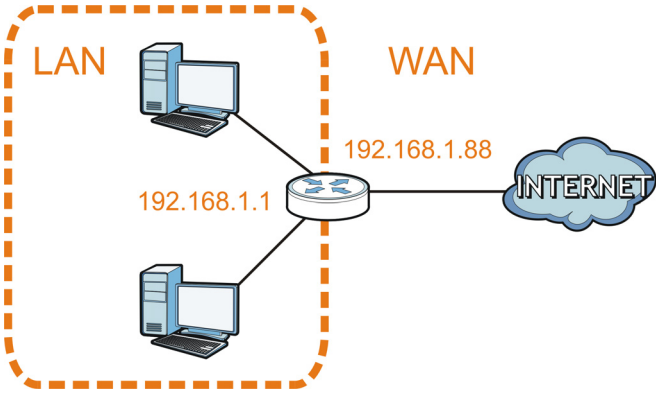
Figure 124 Conflicting Computer IP Addresses Example



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.

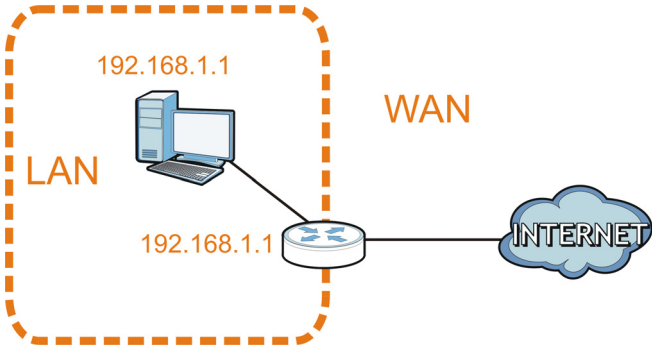
Figure 125 Conflicting Router IP Addresses Example



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 126 Conflicting Computer and Router IP Addresses Example



B

Setting Up Your Computer's IP Address

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

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

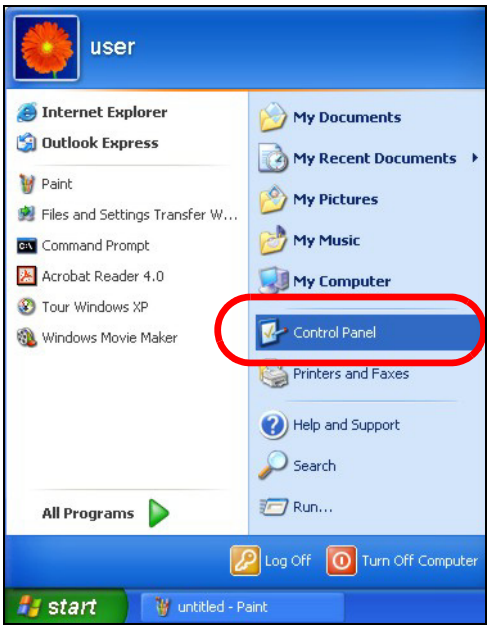
If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

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

Windows XP/NT/2000

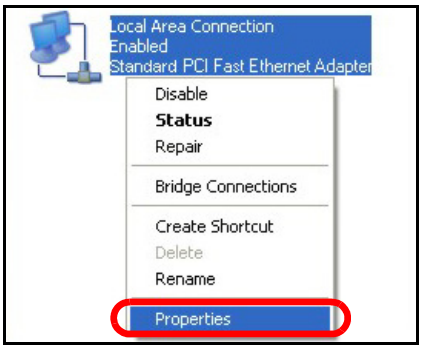
The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

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

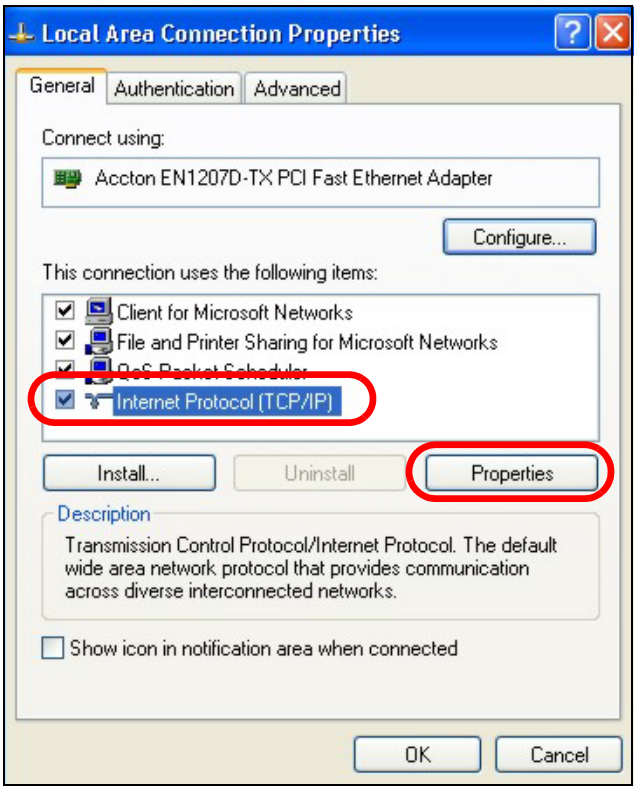


2 In the **Control Panel**, click the **Network Connections** icon.

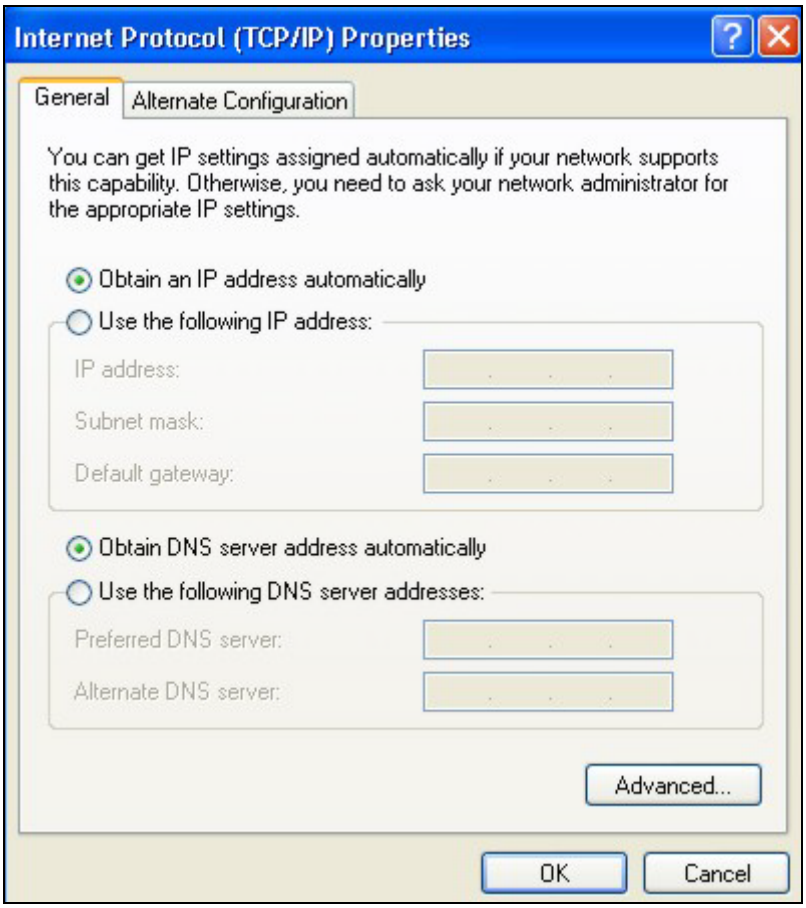
3 Right-click **Local Area Connection** and then select **Properties**.



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



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



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

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

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

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

Verifying Settings

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

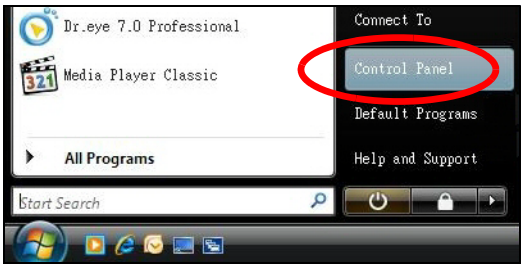
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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

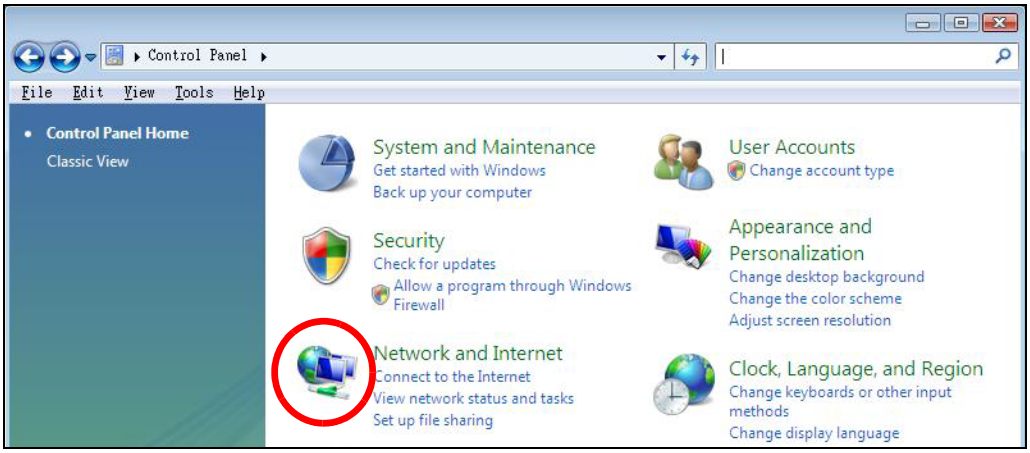
Windows Vista

This section shows screens from Windows Vista Professional.

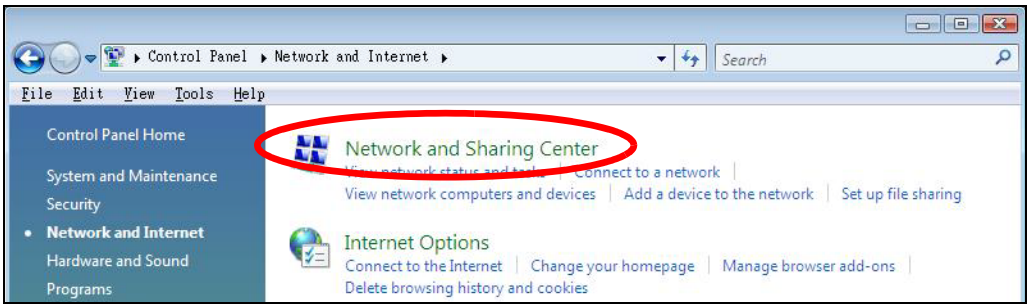
1 Click **Start** > **Control Panel**.



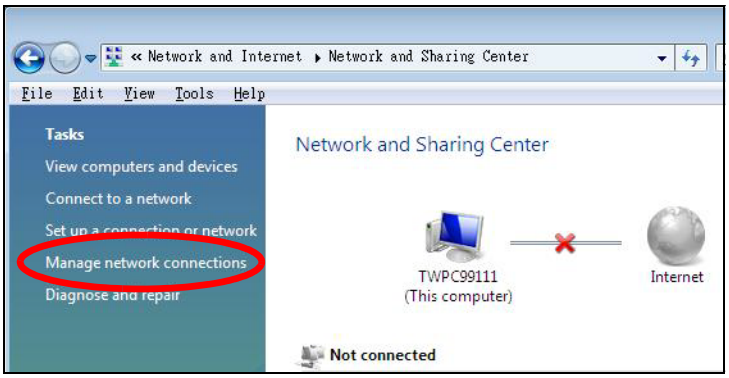
2 In the **Control Panel**, click the **Network and Internet** icon.



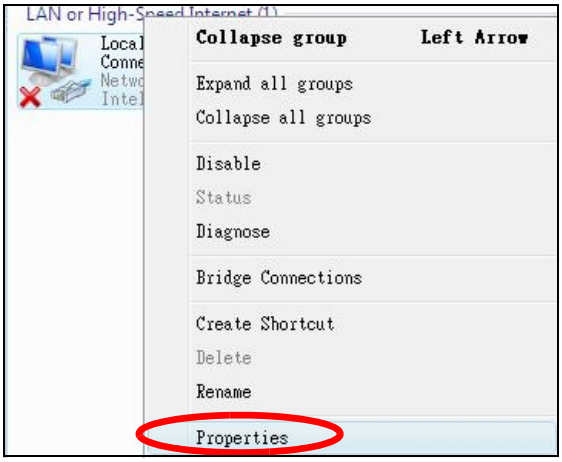
3 Click the **Network and Sharing Center** icon.



4 Click **Manage network connections**.

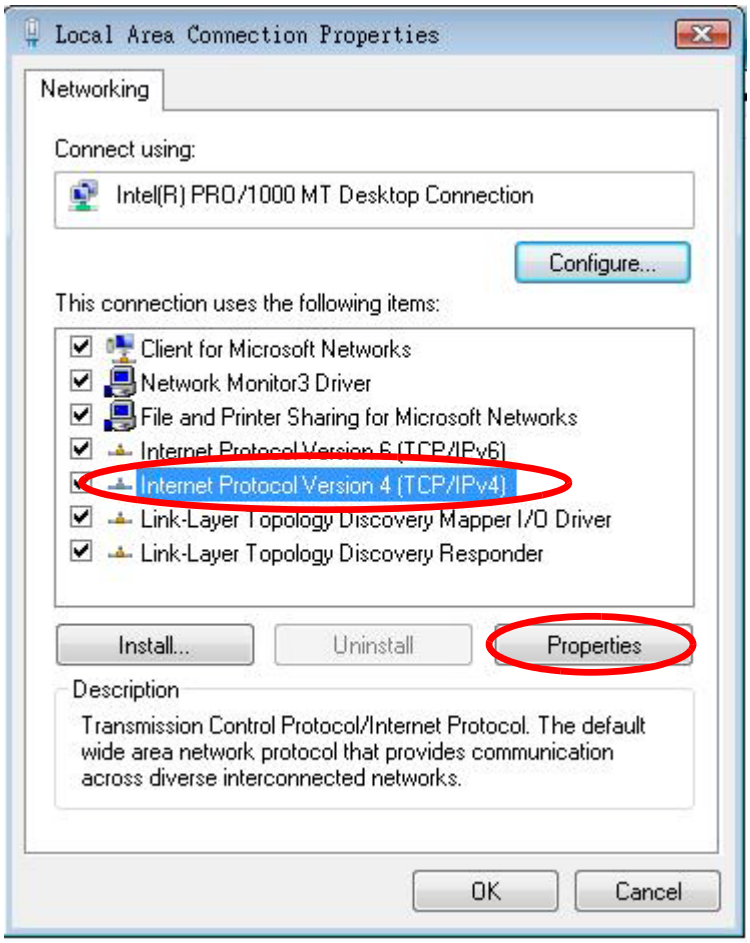


5 Right-click **Local Area Connection** and then select **Properties**.

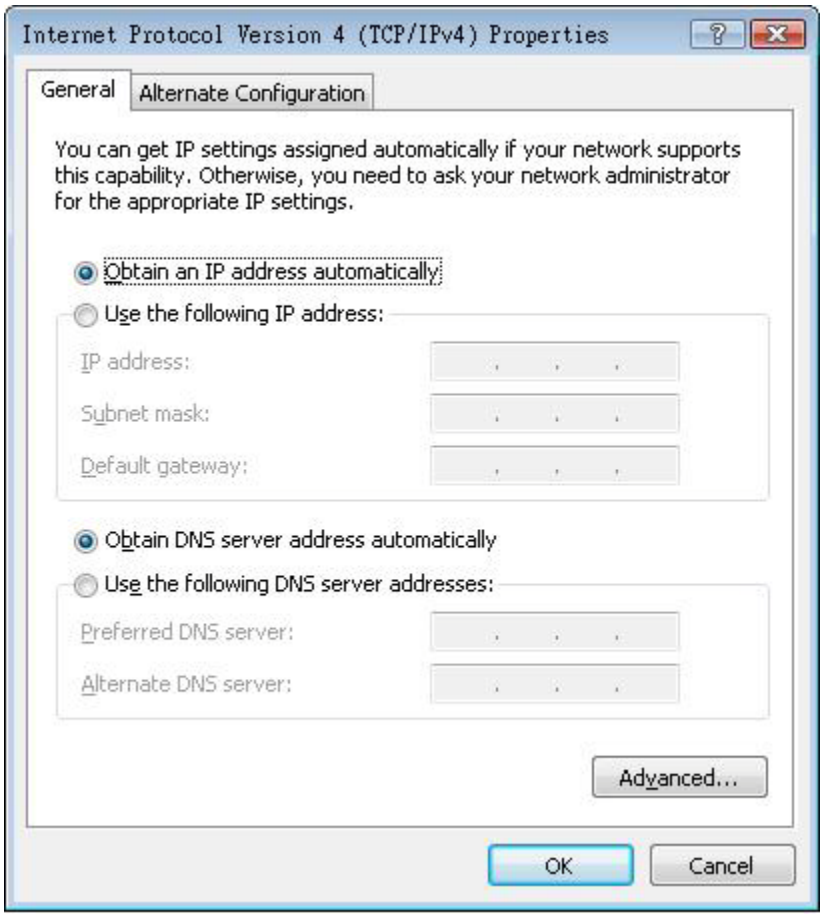


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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



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



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

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

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

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

Verifying Settings

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

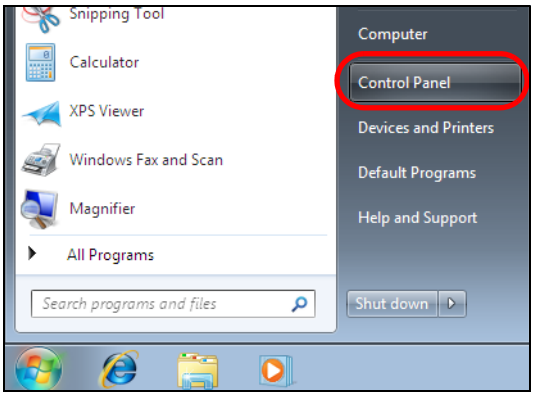
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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

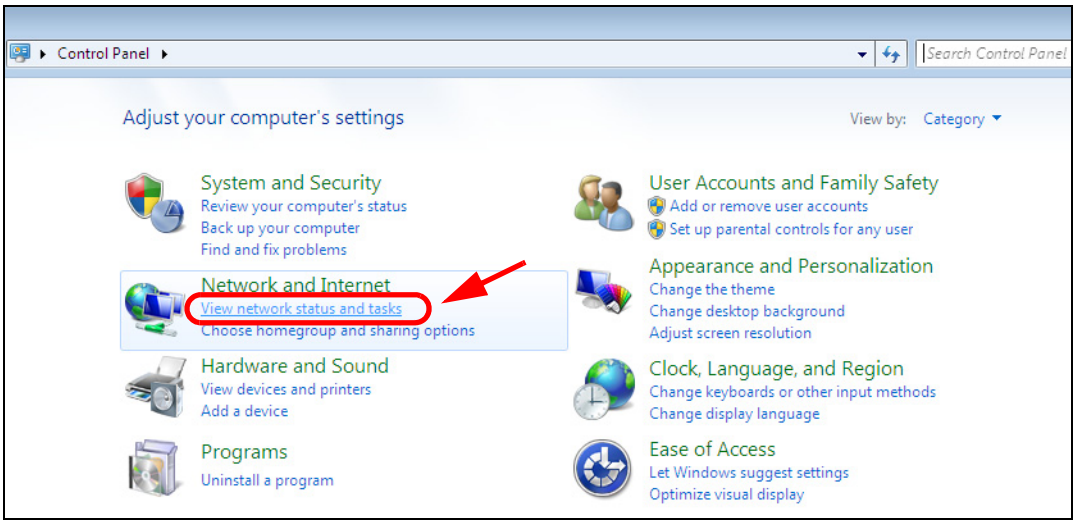
Windows 7

This section shows screens from Windows 7 Enterprise.

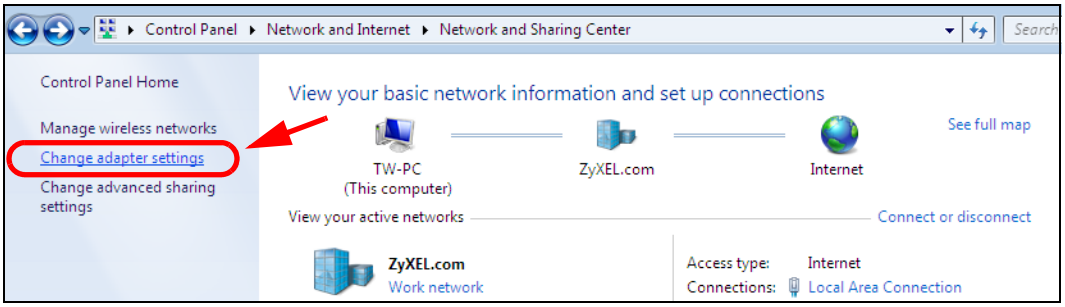
1 Click **Start** > **Control Panel**.



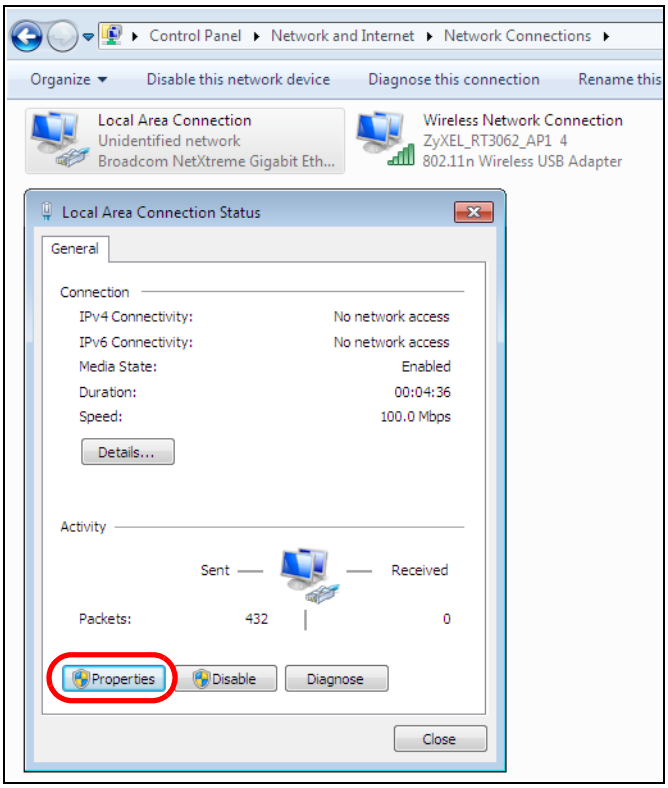
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.



3 Click **Change adapter settings**.

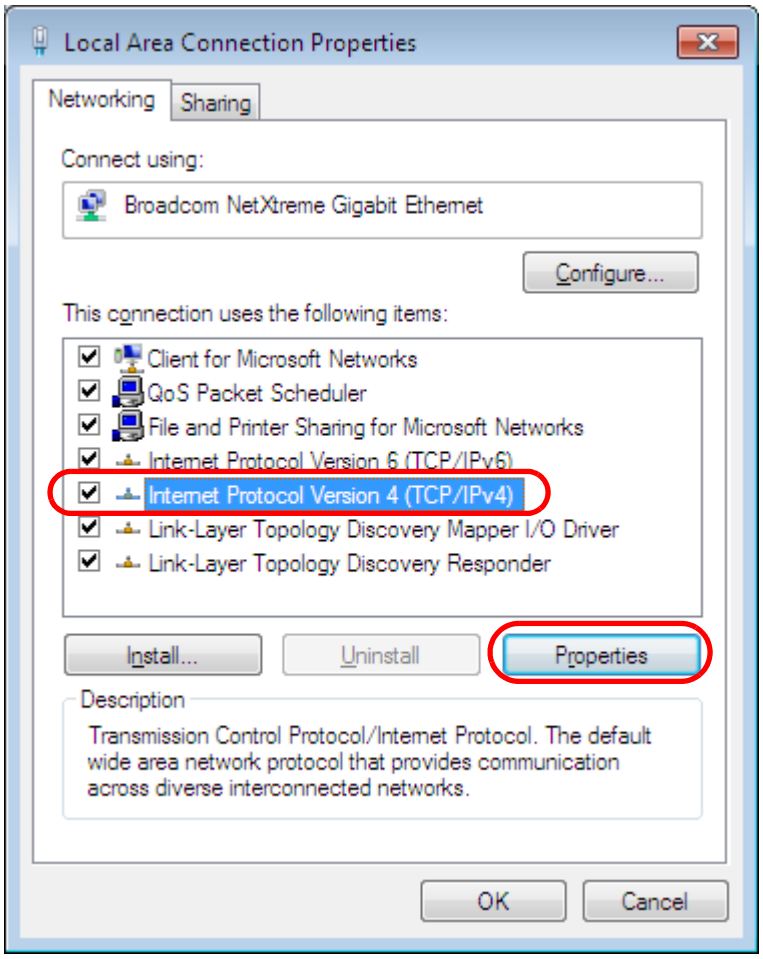


4 Double click **Local Area Connection** and then select **Properties**.

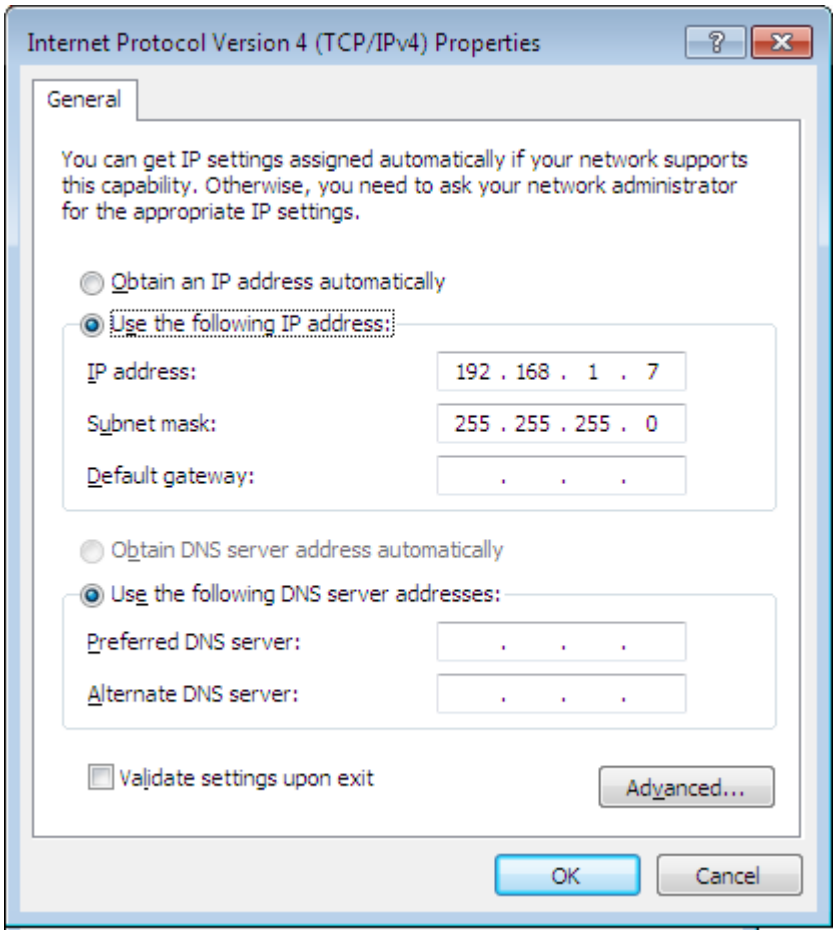


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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



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



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

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

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

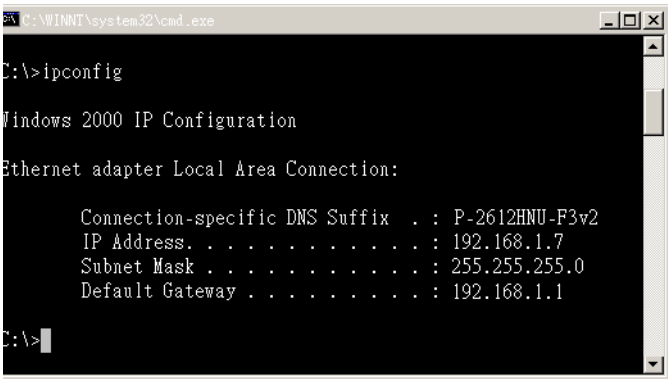
9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

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

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

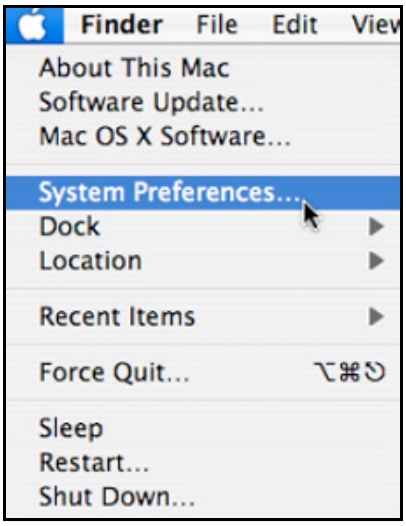
3 The IP settings are displayed as follows.



Mac OS X: 10.3 and 10.4

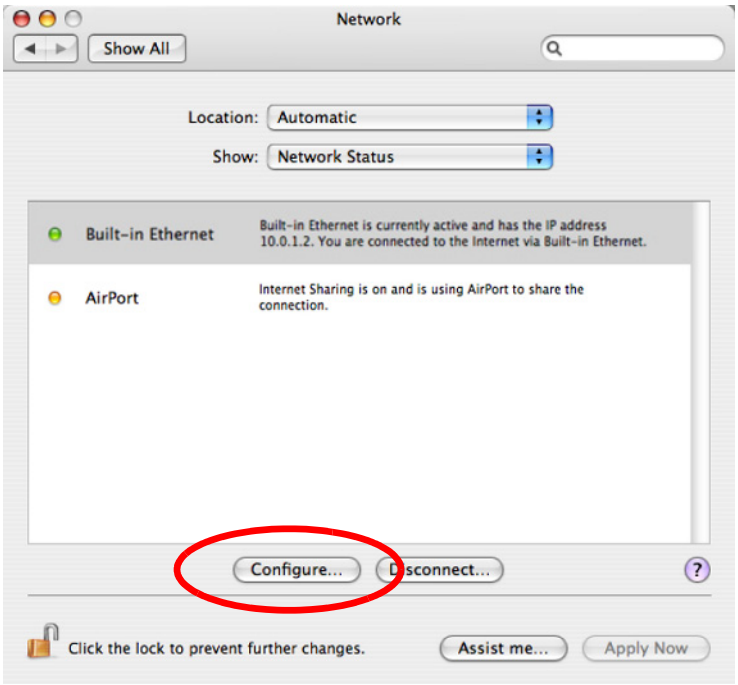
The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

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

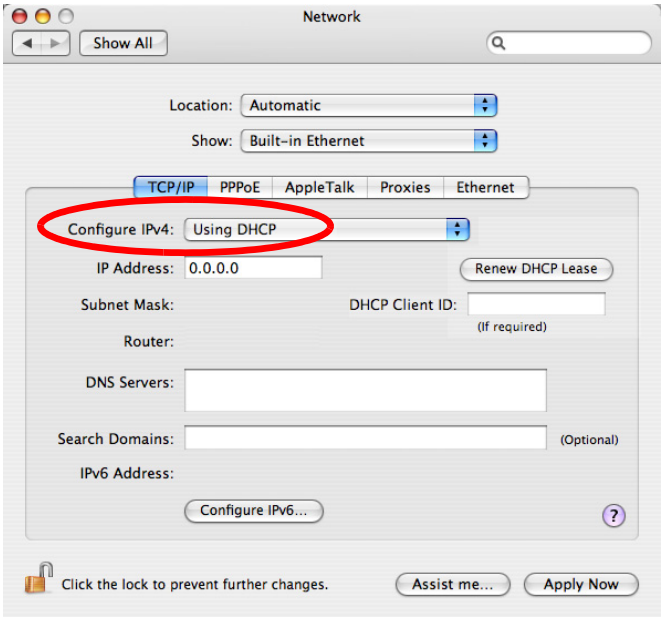


2 In the **System Preferences** window, click the **Network** icon.

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

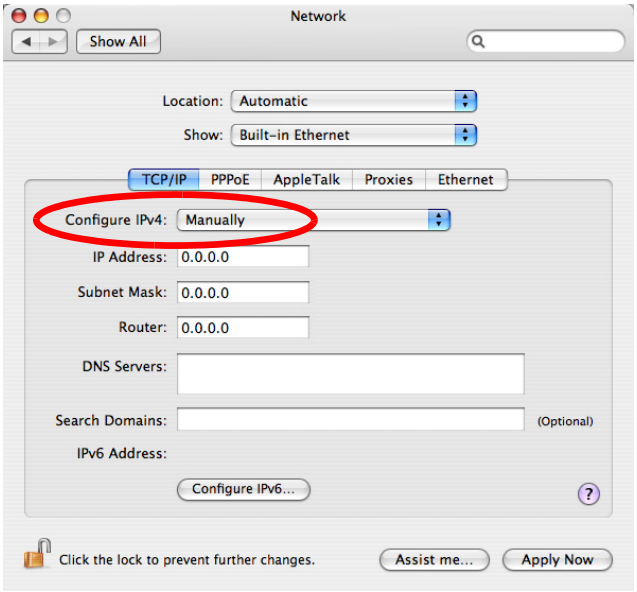


4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.



5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.

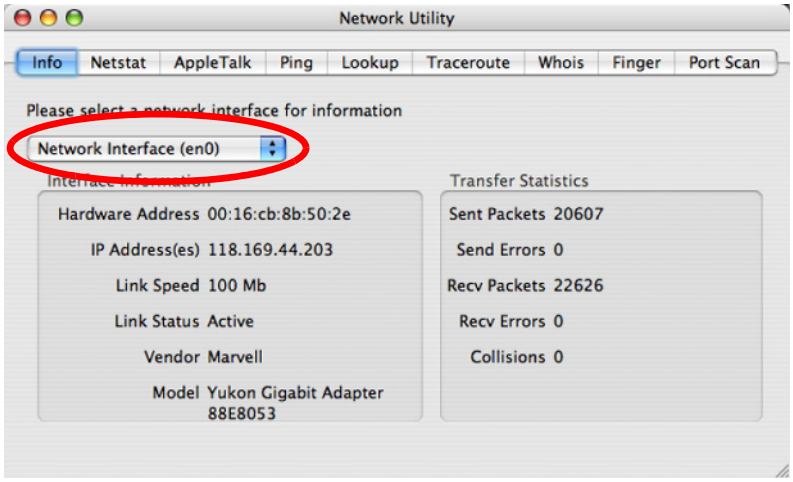


6 Click **Apply Now** and close the window.

Verifying Settings

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

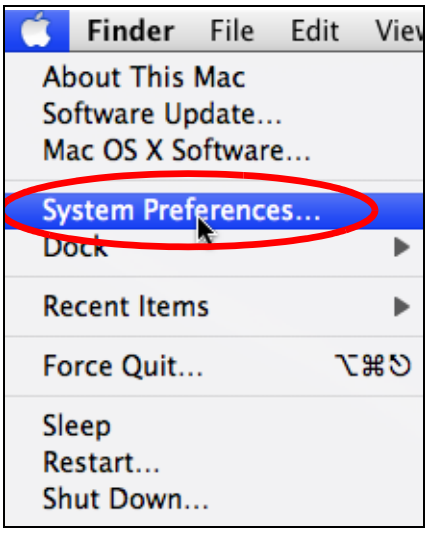
Figure 127 Mac OS X 10.4: Network Utility



Mac OS X: 10.5 and 10.6

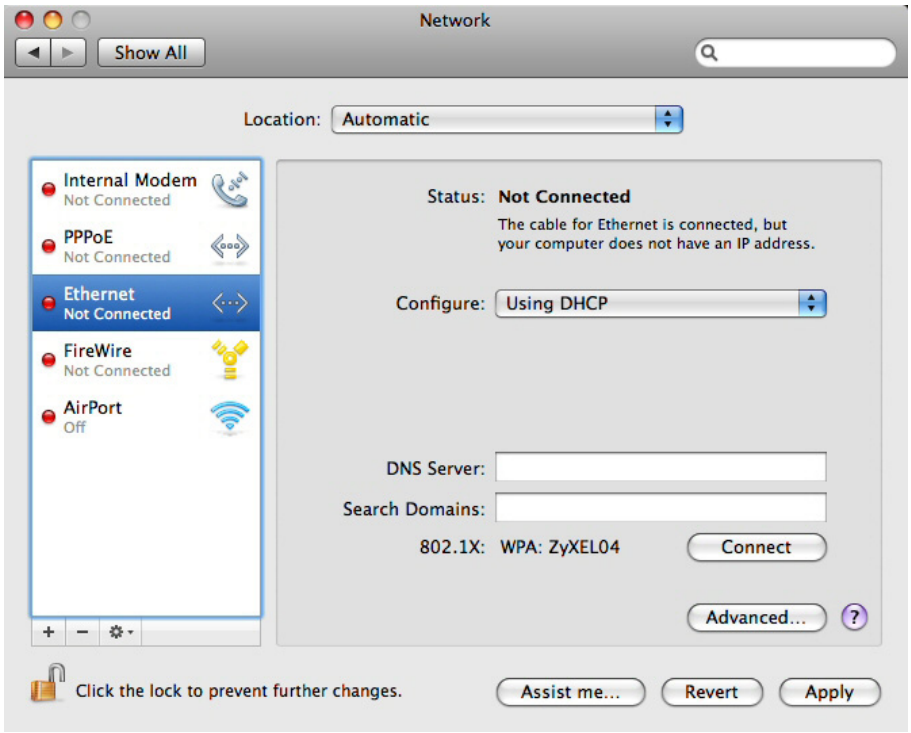
The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

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



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

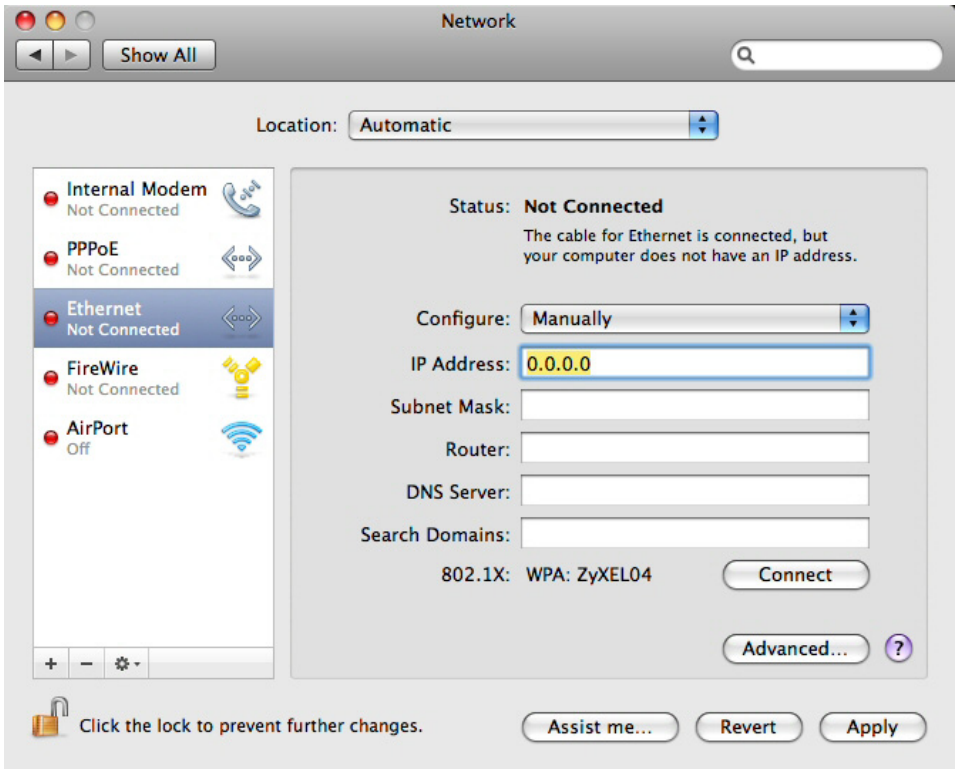
3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.



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

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your Router.

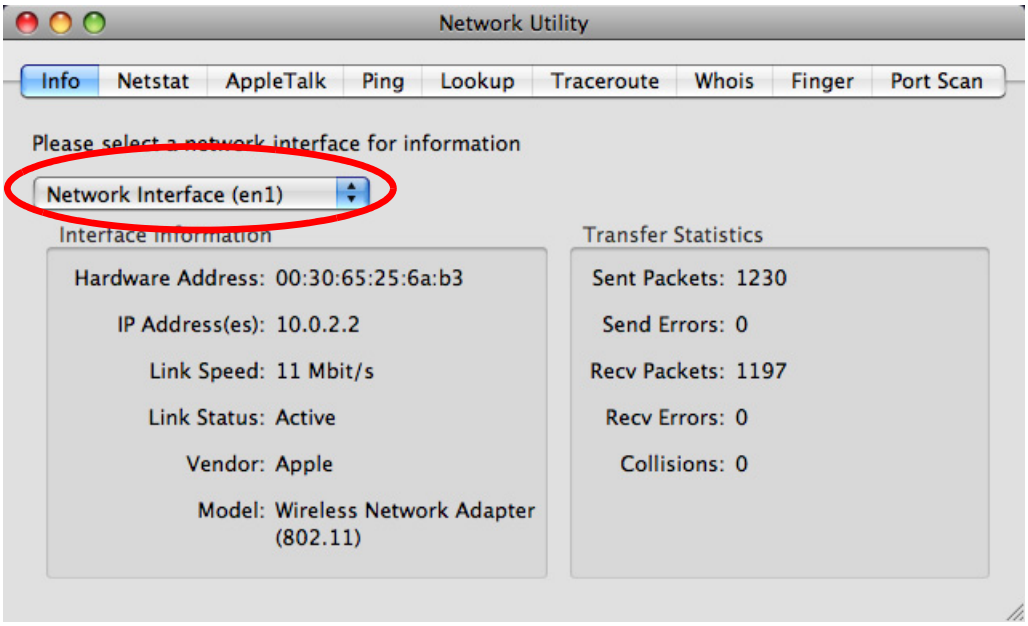


6 Click **Apply** and close the window.

Verifying Settings

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

Figure 128 Mac OS X 10.5: Network Utility



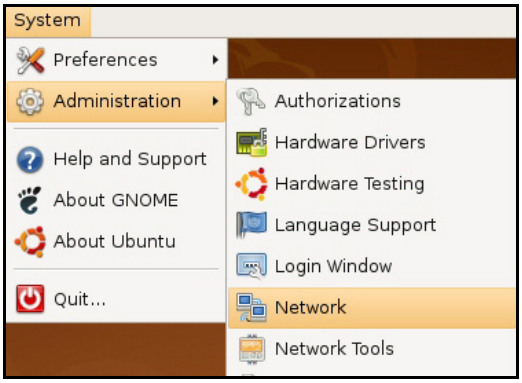
Linux: Ubuntu 8 (GNOME)

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

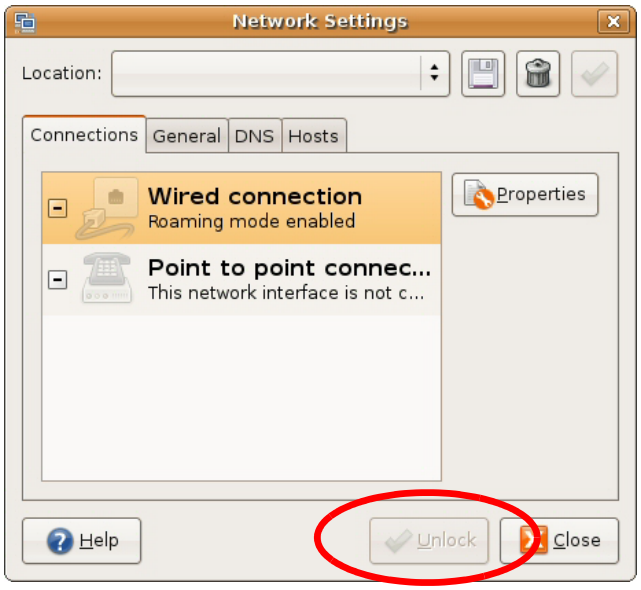
Note: Make sure you are logged in as the root administrator.

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

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



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



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

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

5 The **Properties** dialog box opens.

- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

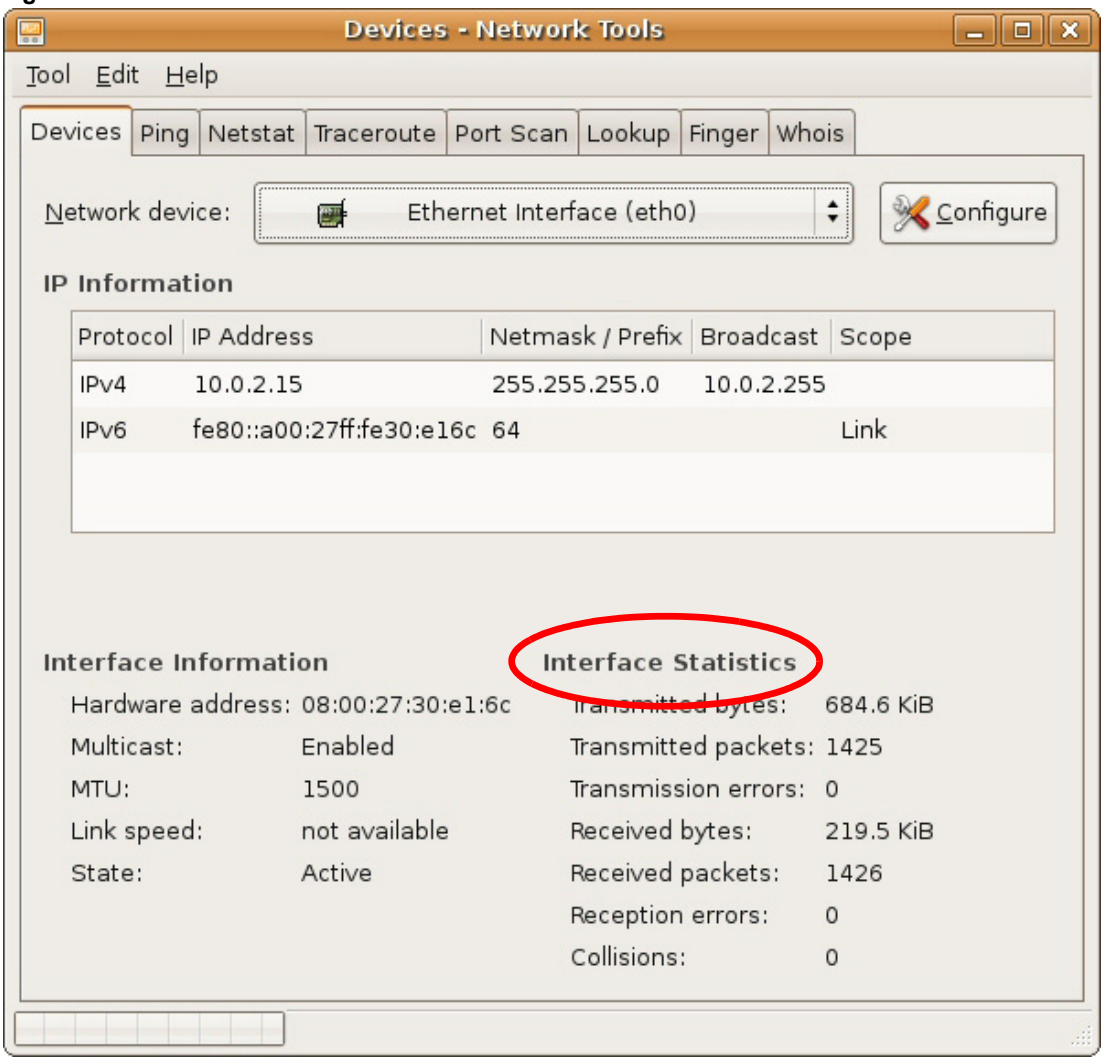
7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

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

Verifying Settings

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

Figure 129 Ubuntu 8: Network Tools



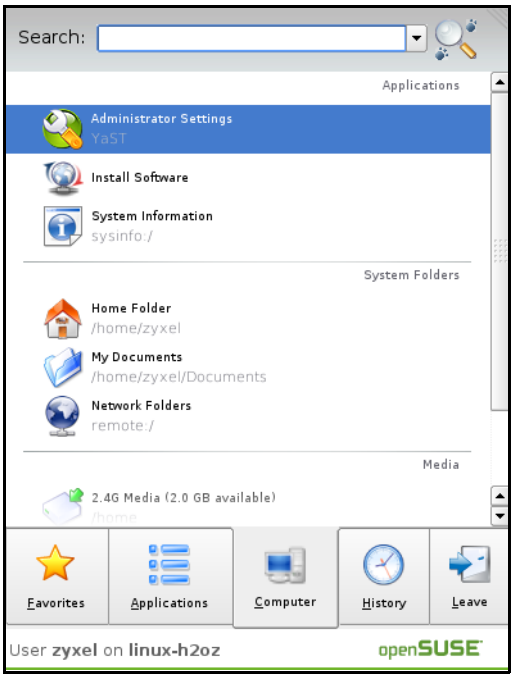
Linux: openSUSE 10.3 (KDE)

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

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

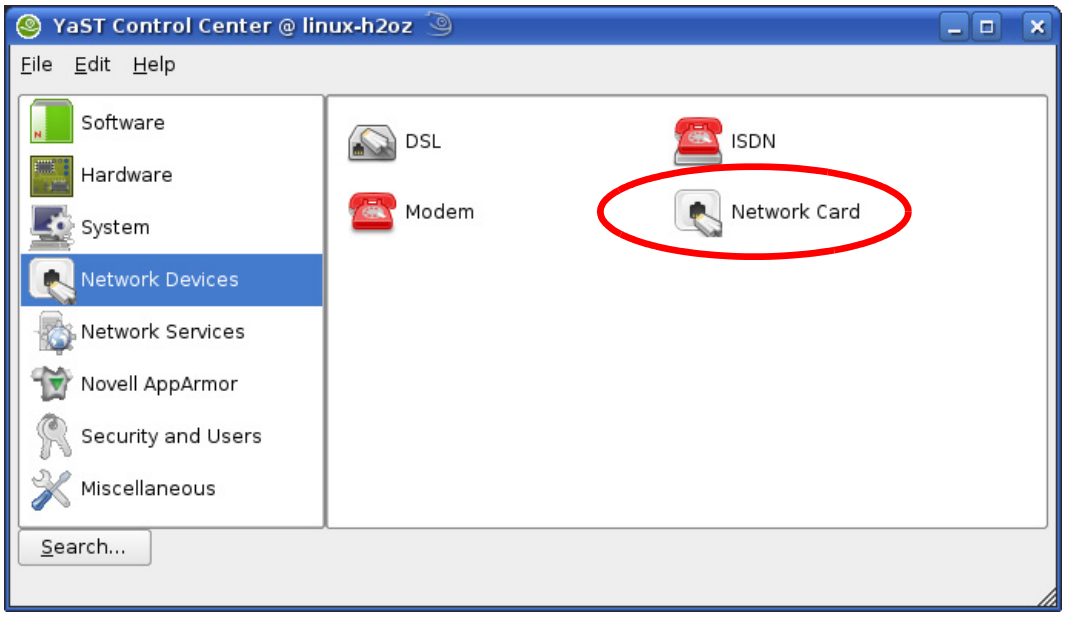
Follow the steps below to configure your computer IP address in the KDE:

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

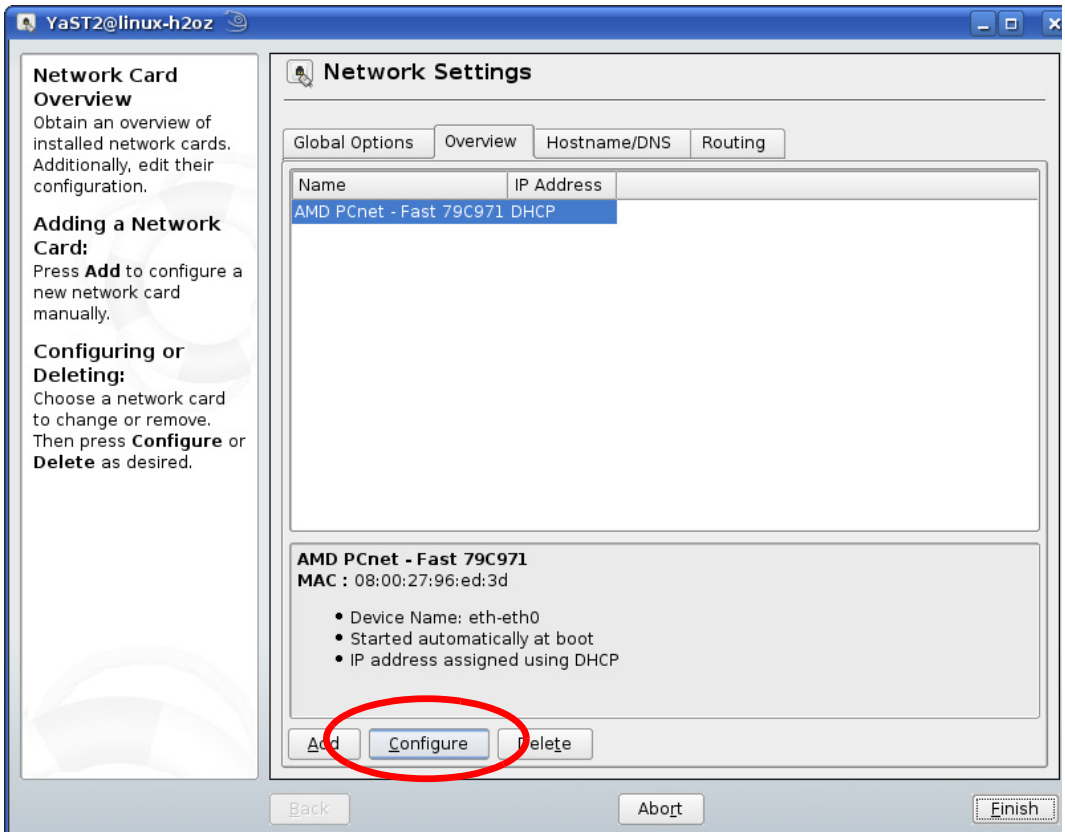


2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

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

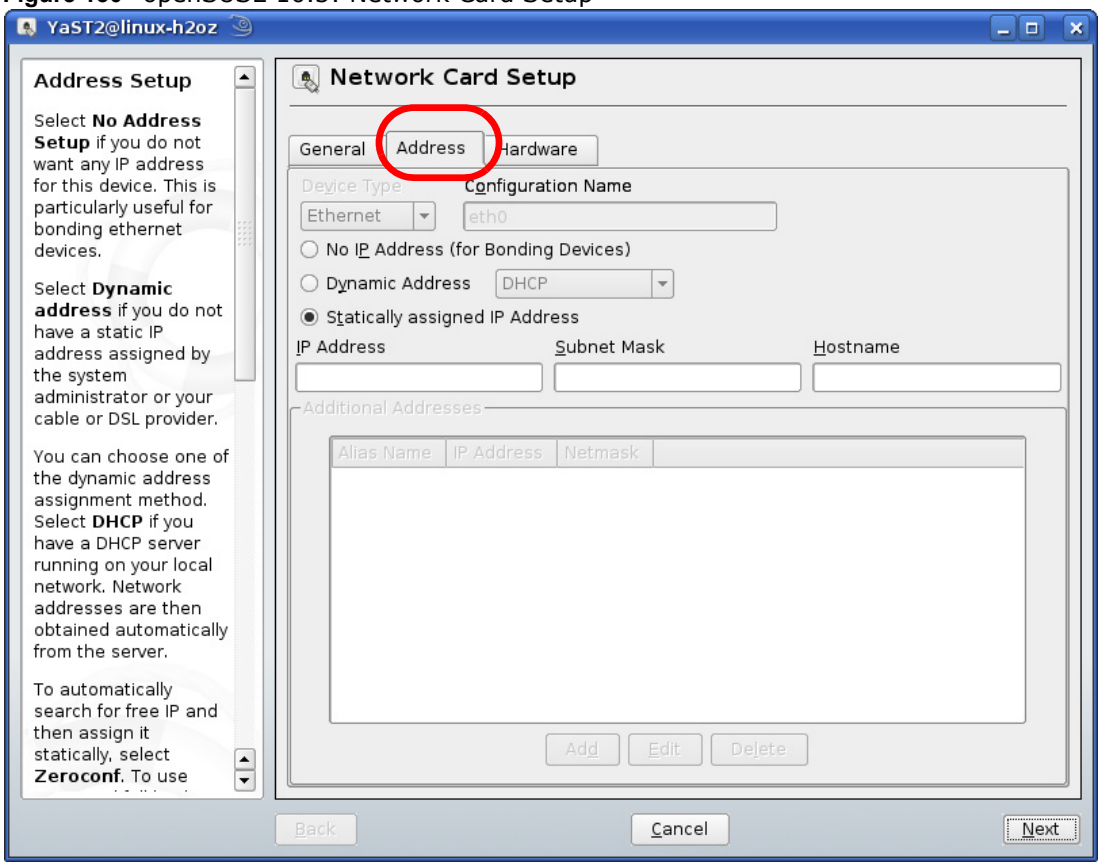


4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



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

Figure 130 openSUSE 10.3: Network Card Setup

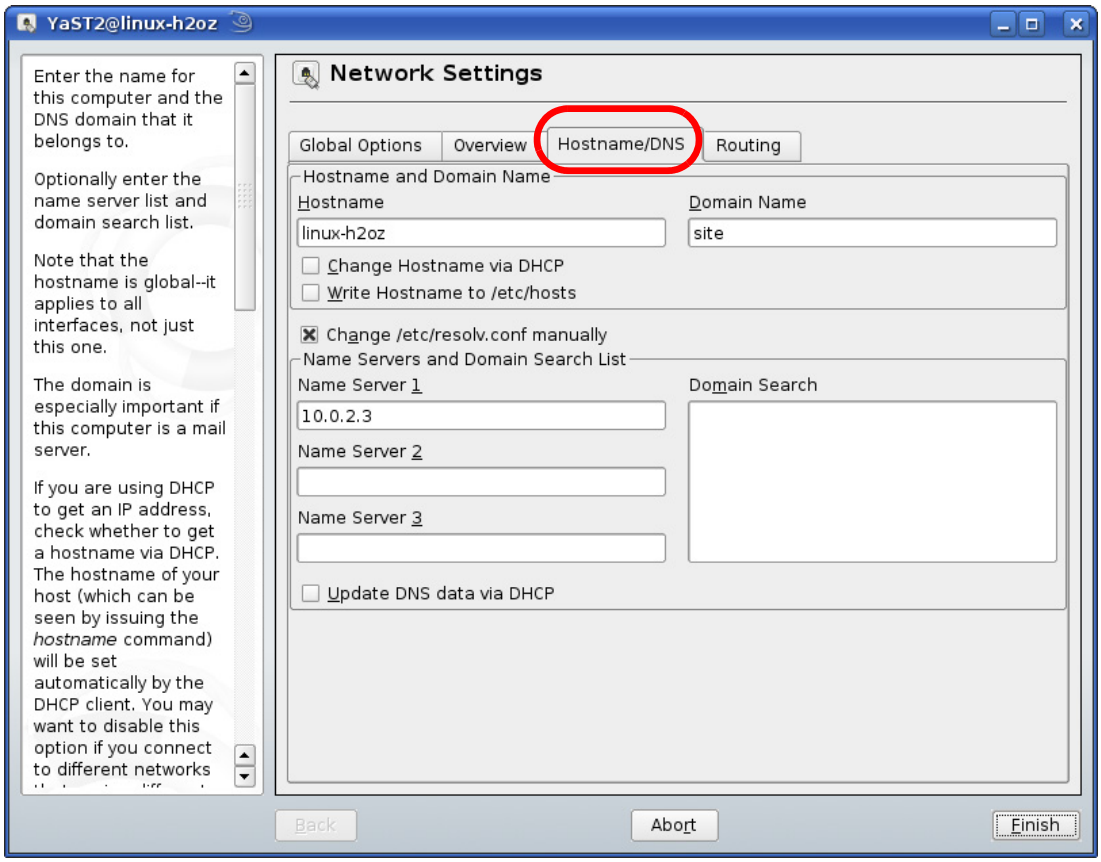


6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

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

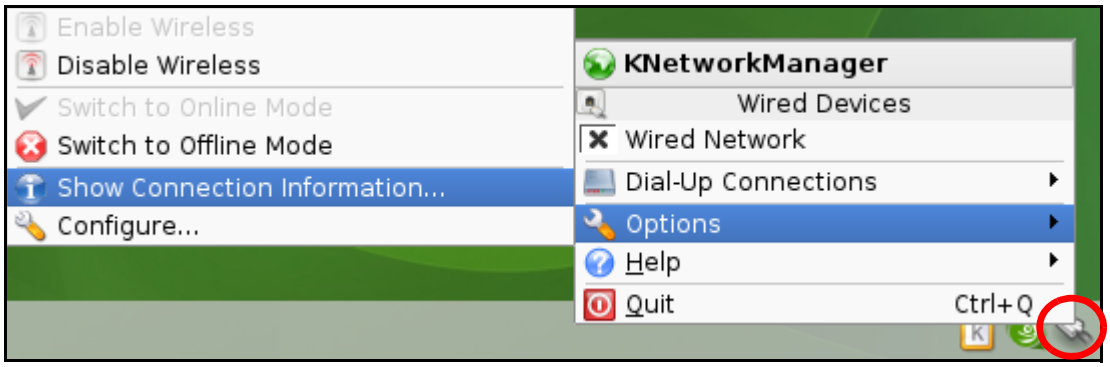


9 Click **Finish** to save your settings and close the window.

Verifying Settings

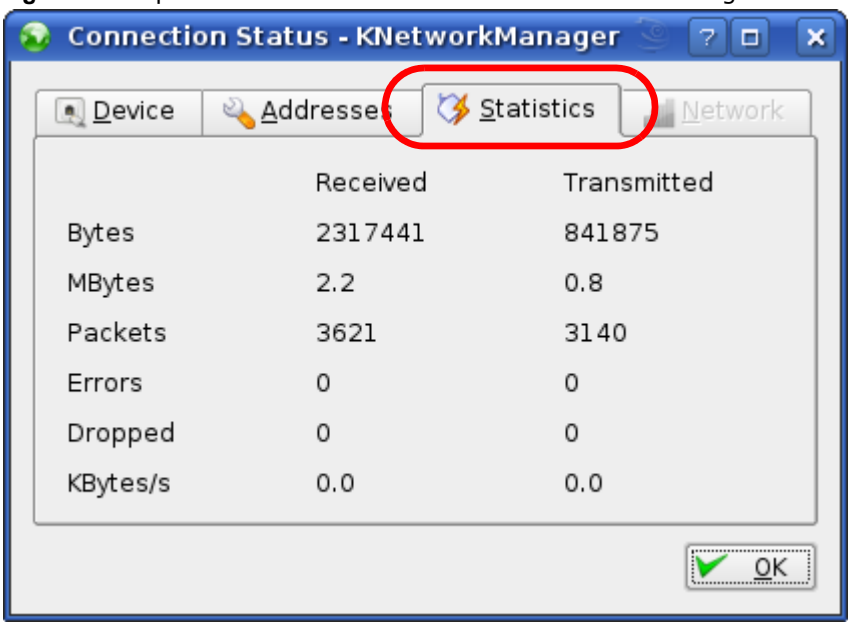
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 131 openSUSE 10.3: KNetwork Manager



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

Figure 132 openSUSE: Connection Status - KNetwork Manager



C

Wireless LANs

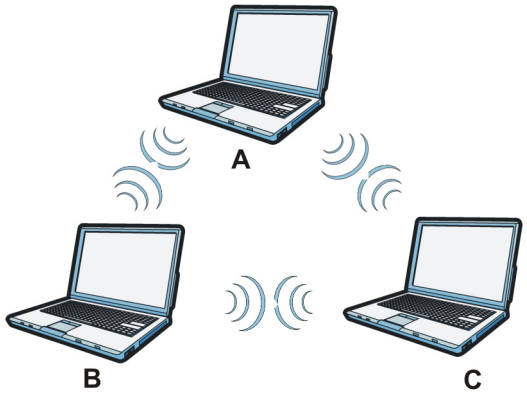
Wireless LAN Topologies

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

Ad-hoc Wireless LAN Configuration

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

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



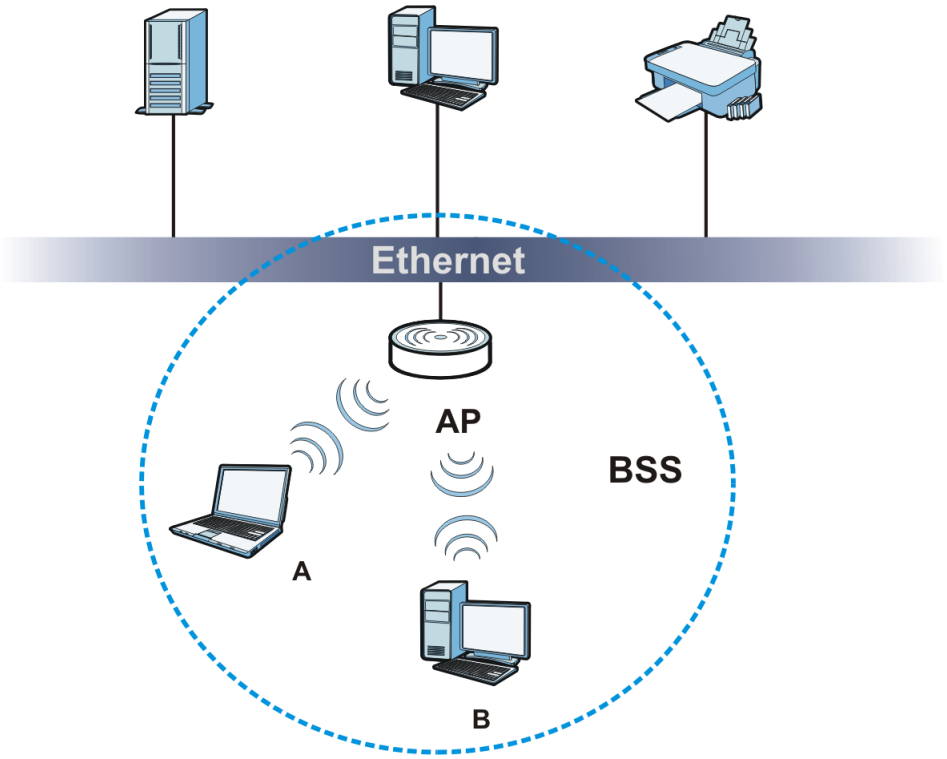
BSS

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

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

disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 134 Basic Service Set



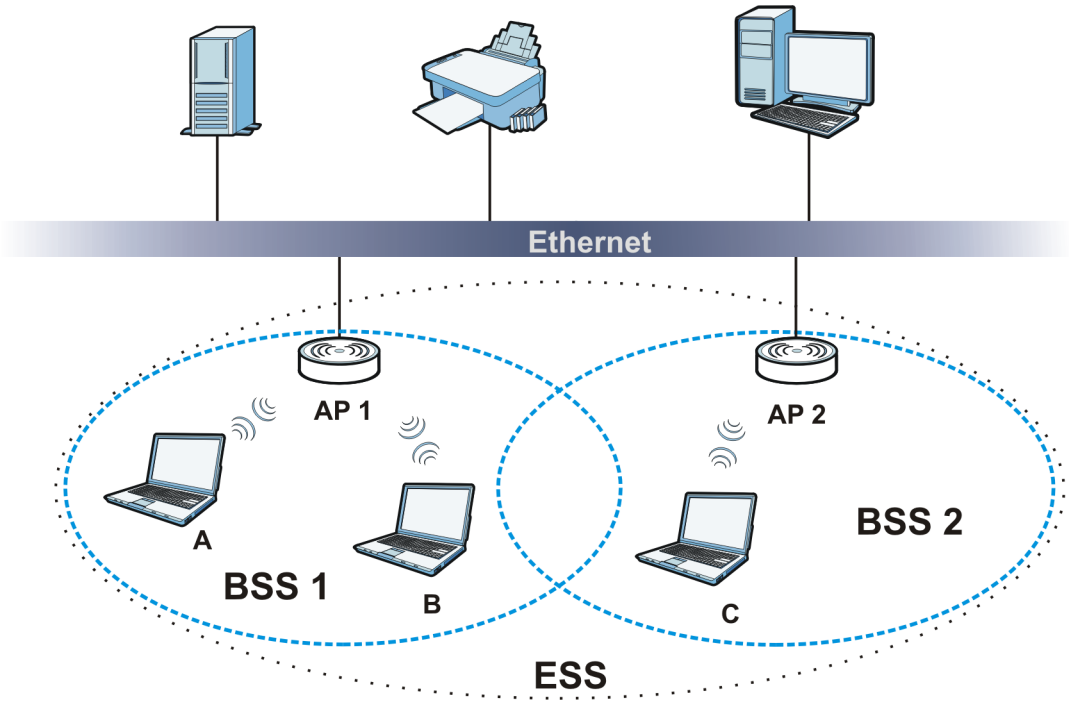
ESS

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

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

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

Figure 135 Infrastructure WLAN



Channel

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

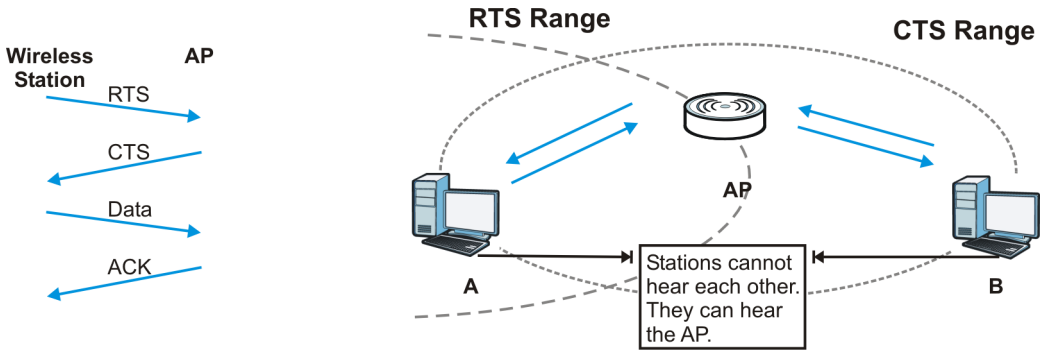
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel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

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they

cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 136 RTS/CTS



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

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

When a data frame exceeds the **RTS/CTS** value you set, 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 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 Router uses long preamble.

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

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 Router are data encryption, wireless client authentication, restricting access by device MAC address and hiding the Router identity.

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

Table 82 Wireless Security Levels

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

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

IEEE 802.1x

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

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

RADIUS

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

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

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

Types of RADIUS Messages

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

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

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

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

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

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

Types of EAP Authentication

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

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

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

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

EAP-MD5 (Message-Digest Algorithm 5)

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

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

EAP-TLS (Transport Layer Security)

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

EAP-TTLS (Tunneled Transport Layer Service)

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

PEAP (Protected EAP)

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

LEAP

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

Dynamic WEP Key Exchange

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

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

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

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

Table 83 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.

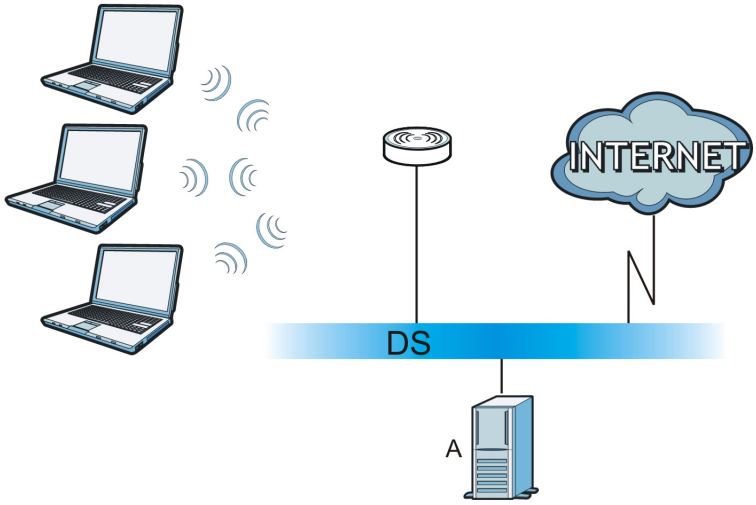
WPA(2) with RADIUS Application Example

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 137 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

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

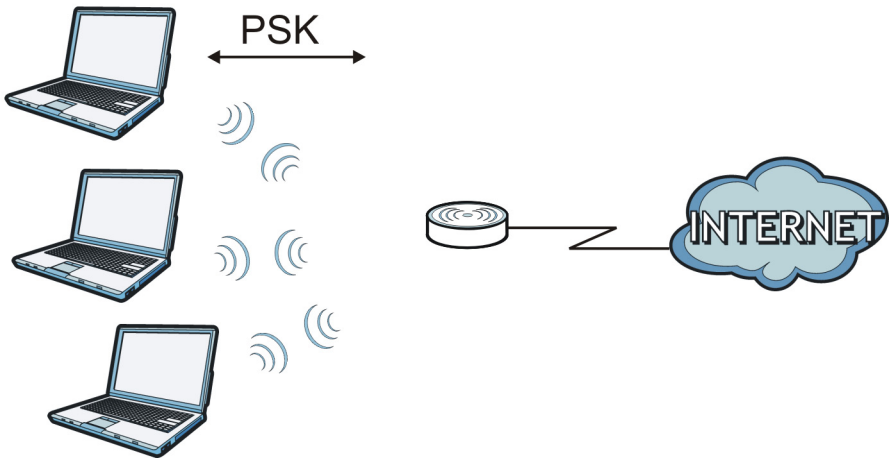
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

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

Figure 138 WPA(2)-PSK Authentication



Security Parameters Summary

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

Table 84 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.

D

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 85 Commonly Used Services

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

Table 85 Commonly Used Services (continued)

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

Table 85 Commonly Used Services (continued)

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

E

Legal Information

Copyright

Disclaimer

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

Certifications

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

1 Reorient or relocate the receiving antenna.

2 Increase the separation between the equipment and the receiver.

3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4 Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

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

注意 ！

依據　低功率電波輻射性電機管理辦法

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

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

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

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

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

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

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

Industry Canada Statement

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

1 this device may not cause interference and

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

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

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

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

IC Radiation Exposure Statement:

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

Viewing Certifications

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

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in 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.

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.

Regulatory Information

European Union

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

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

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

[Czech]	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[German]	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕC.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.

[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/ЕС.
[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.

CE !

National Restrictions

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

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

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

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

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

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

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

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

Belgium

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

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

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

Denmark

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

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

France

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

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

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

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the

boundaries of the owner's property, its use requires a “general authorization.” Please check http://www.sviluppoeconomico.gov.it/ for more details.

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

Latvia

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

2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

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

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.

- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

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

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X