NBG318S Series

Powerline Ethernet Series

User's Guide

Version 3.60
1/2008
Edition 3

DEFAULT LOGIN	
IP Address	http://192.168.1.1
Password	1234

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the NBG318S or NBG318S v2 using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.

It is recommended you use the web configurator to configure the NBG318S.

- Supporting Disk

  Refer to the included CD for support documents.
- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User’s Guide.

Warnings tell you about things that could harm you or your device.

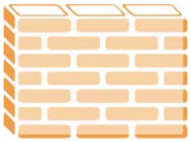
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The NBG318S and NBG318S v2 may be referred to as the “NBG318S”, the “device”, the “product” or the “system” in this User’s Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the “enter” or “return” key on your keyboard.
- “Enter” means for you to type one or more characters and then press the [ENTER] key. “Select” or “choose” means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance** > **Log** > **Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the “metric” value or the “scientific” value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The NBG318S icon is not an exact representation of your device.

NBG318S 	Computer 	Notebook computer
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router
Modem 		

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- 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.

This product is recyclable. Dispose of it properly.

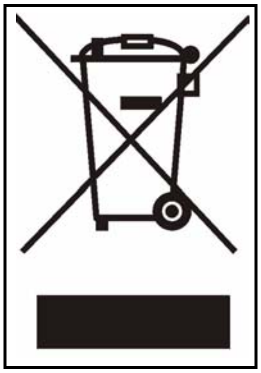


Table of Contents

Contents Overview

List of Figures

List of Tables

PART I
Introduction

1

Getting to Know Your NBG318S

This chapter introduces the main features and applications of the NBG318S.

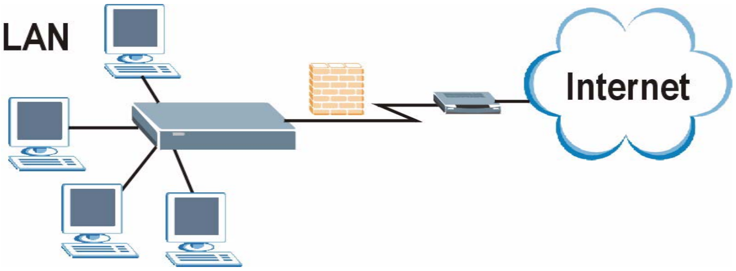
1.1 Overview

The NBG318S is the ideal secure HomePlug AV wireless firewall router for all data passing between the Internet and your local network.

1.1.1 Secure Broadband Internet Access

Connect a broadband modem to your NBG318S for shared Internet access protected by firewall and content filtering. You can also use media bandwidth management to efficiently manage traffic on your network. The Quality of Service (QoS) features allow you to prioritize time-sensitive or highly important applications such as Voice over Internet (VoIP).

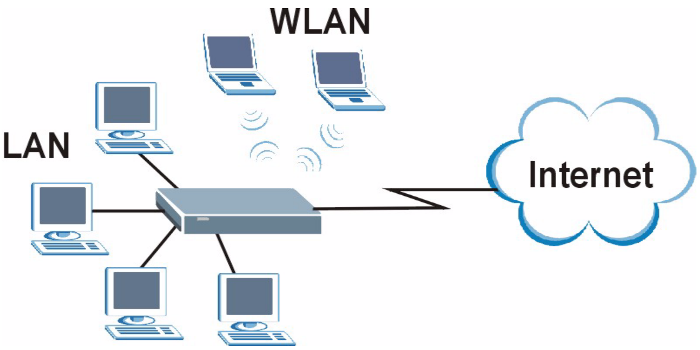
Figure 1 Secure Internet Access



1.1.2 Wireless LAN Application

The NBG318S Wireless LAN feature allows IEEE 802.11b or IEEE 802.11g compatible wireless clients to access the Internet or the local network as well as to communicate with each other. Wireless stations can move freely anywhere in the coverage area and use resources on the wired network. The Super G function allows compatible clients to connect to the NBG318S at up to 108 Mbps.

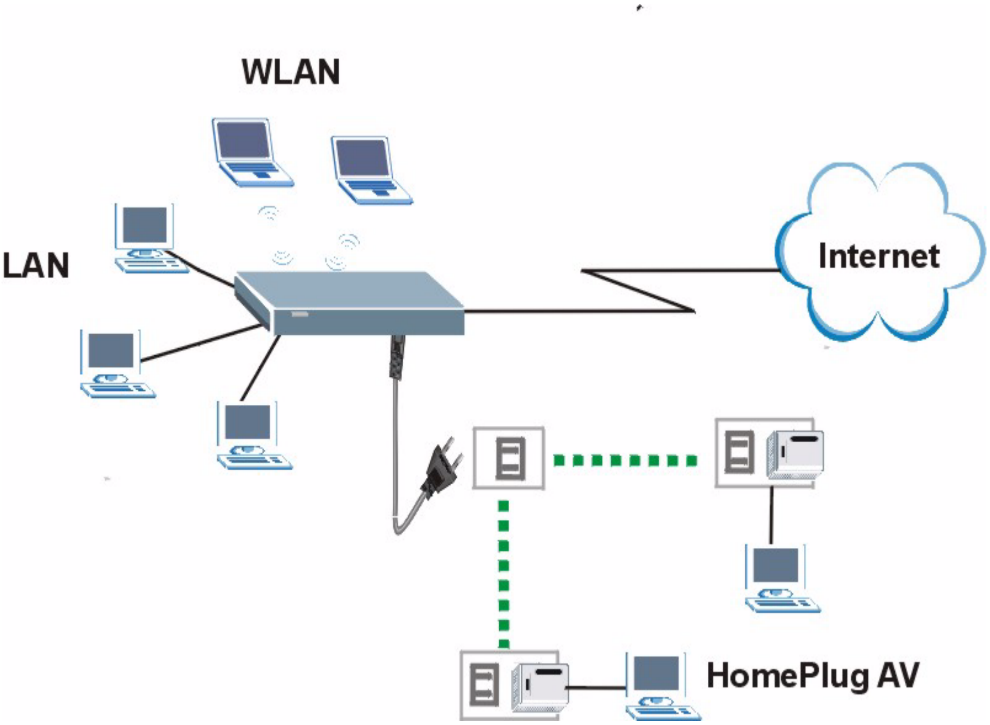
Figure 2 WLAN Application Example



1.1.3 HomePlug AV

Connect to other HomePlug AV compatible devices through your home electrical wiring. A HomePlug AV network is capable of up to 200Mbps data transfer without the need for network cables.

Figure 3 HomePlug AV Internet Connection Example



1.2 Ways to Manage the NBG318S

Use any of the following methods to manage the NBG318S.

- WPS (Wi-Fi Protected Setup): You can use the **WPS** button or the WPS section of the web configurator to set up a wireless network with your NBG318S.

- ENCRYPT: You can use the **ENCRYPT** button to set up a powerline network with your NBG318S.
- Web Configurator. This is recommended for everyday management of the NBG318S using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/restore.

Upgrade to the latest firmware to enable the ENCRYPT feature on your NBG318S.

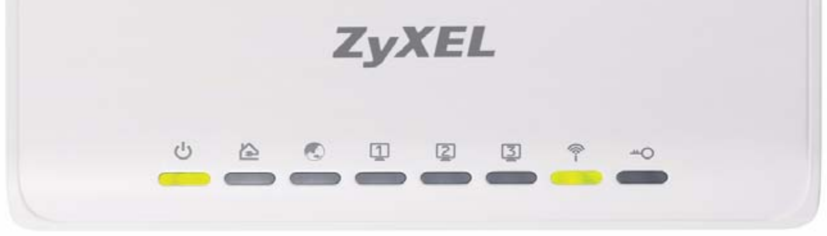
1.3 Good Habits for Managing the NBG318S

Do the following things regularly to make the NBG318S more secure and to manage the NBG318S 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 NBG318S to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG318S. You could simply restore your last configuration.

1.4 LEDs

Figure 4 Front Panel



The following table describes the NBG318S's LEDs.

Table 1 NBG318S Front Panel LEDs

LED	ICON	COLOR	STATUS	DESCRIPTION
Power	⏻	Green	On	The NBG318S is receiving power and functioning properly.
			Off	The NBG318S is not receiving power.

Table 1 NBG318S Front Panel LEDs (continued)

LED	ICON	COLOR	STATUS	DESCRIPTION
HomePlug	🏠	Green	On	The NBG318S has a successful HomePlug AV connection.
			Blinking	The NBG318S is sending/receiving data.
			Off	The HomePlug AV connection is not ready, or failed.
WAN	🌐	Green	On	The NBG318S has a successful WAN connection.
			Blinking	The NBG318S is sending/receiving data.
		None	Off	The WAN connection is not ready, or has failed.
LAN 1-3	1 2 3	Green	On	The NBG318S has a successful Ethernet connection.
			Blinking	The NBG318S is sending/receiving data.
			Off	The LAN is not connected.
WLAN	📶	Green	On	The NBG318S is ready, but is not sending/receiving data through the wireless LAN.
			Blinking	The NBG318S is sending/receiving data through the wireless LAN.
		None	Off	The wireless LAN is not ready or has failed.
WPS	🔑	Green	On	WPS (WiFi Protected Setup) is configured on your device. Note: Upgrade your firmware to install the WPS feature on your device.
			Blinking	The NBG318S is attempting to connect with another wireless devices using WPS.
			Off	WPS is disabled on your device.

The following table describes the NBG318S v2's LEDs.

Table 2 NBG318S v2 Front Panel LEDs

LED	ICON	COLOR	STATUS	DESCRIPTION
Power	⏻	Green	On	The NBG318S v2 is receiving power and functioning properly.
			Off	The NBG318S v2 is not receiving power.

Table 2 NBG318S v2 Front Panel LEDs (continued)

LED	ICON	COLOR	STATUS	DESCRIPTION
HomePlug	🏠	Green	On	The NBG318S v2 has a successful HomePlug AV connection at 40 Mbps.
			Blinking	The NBG318S v2 is sending/receiving data at over 40 Mbps.
		Amber	On	The NBG318S v2 has a successful HomePlug AV connection at 10~40 Mbps.
			Blinking	The NBG318S v2 is sending/receiving data at 10~40 Mbps.
		Red	On	The NBG318S v2 has a successful HomePlug AV connection at 0~10 Mbps.
			Blinking	The NBG318S v2 is sending/receiving data at 0~10 Mbps.
			Off	The HomePlug AV connection is not ready, or failed.
WAN	🌐	Green	On	The NBG318S v2 has a successful WAN connection.
			Blinking	The NBG318S v2 is sending/receiving data.
		None	Off	The WAN connection is not ready, or has failed.
LAN 1-3	1 2 3	Green	On	The NBG318S v2 has a successful Ethernet connection.
			Blinking	The NBG318S v2 is sending/receiving data.
			Off	The LAN is not connected.
WLAN	📶	Green	On	The NBG318S v2 is ready, but is not sending/receiving data through the wireless LAN.
			Blinking	The NBG318S v2 is sending/receiving data through the wireless LAN.
		None	Off	The wireless LAN is not ready or has failed.
WPS	🔑	Amber	On	WPS (WiFi Protected Setup) is configured on your device.
			Blinking	The NBG318S v2 is attempting to connect with another wireless devices using WPS.
			Off	WPS is disabled on your device.

2

The WPS Button

2.1 Overview

Your NBG318S 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.

2.2 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the NBG318S, see Section 7.4 on page 85).
3. Press the button on one of the devices (it doesn't matter which).
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

For information on using the WPS PIN method, see Section 7.9 on page 101.

3

The ENCRYPT Button

Use the **ENCRYPT** button to automatically set up a secure powerline connection between your powerline devices.

3.1 ENCRYPT Button Overview

The **ENCRYPT** button allows you to set up a secure powerline connection with other HomePlug AV compliant powerline devices which also support the **ENCRYPT** feature. No other powerline setting changes are required to connect.

You can use the **ENCRYPT** button to:

- set up a new powerline network
- separate an existing powerline network into multiple networks

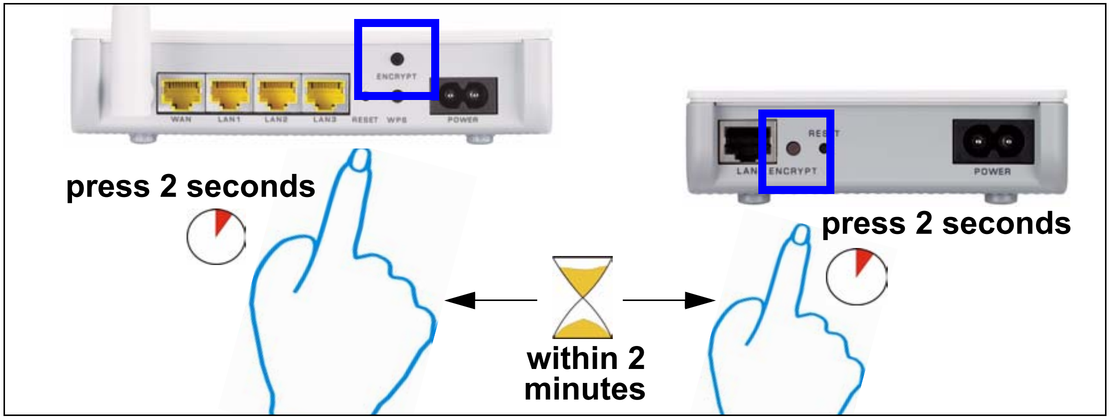
You need to have the latest firmware installed to enable the ENCRYPT feature.

3.2 Set Up a HomePlug AV Network with ENCRYPT

You can connect a number of devices on a powerline network, but you can use the **ENCRYPT** button on only two devices at a time. The NBG318S and PLA-400 v2 are shown below as examples.

1. Place a powerline device close to another powerline device so you have time to set up each one. After you set up the first powerline device, you have 120 seconds to set up the second powerline device.
2. You can disconnect them from your computer or modem (or other networking equipment) if you need to move them close to each other, but the powerline devices need to be plugged into power outlets.
3. Press the **ENCRYPT** button at the rear of your powerline device for more than 10 seconds until the HomePlug (⌂) light is off. This resets the network name to a random value and removes your device from any network it may belong to.
4. Press the **ENCRYPT** button at the rear of your powerline device for 1~2 seconds.

Figure 5 ENCRYPT Connection Procedure



5 Repeat step 4 in this section for the other powerline device you wish to connect. This must be done within 120 seconds of pressing the **ENCRYPT** button on the NBG318S.

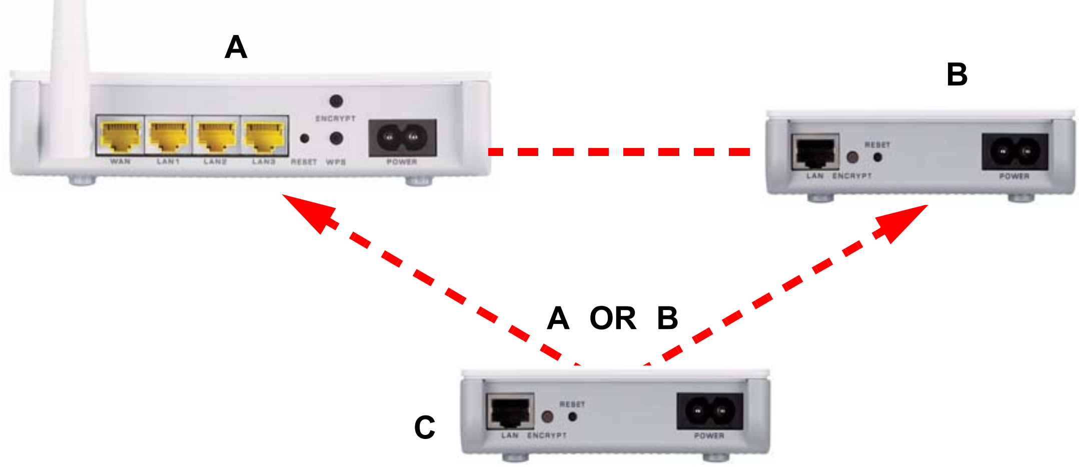
6 Check the lights on the two powerline devices. Wait for about one minute while your powerline devices connect. The HomePlug (⌂) lights on both devices turn on when the connection is made.

If the HomePlug (⌂) lights on both powerline devices do not light up, the powerline devices are not connected. Repeat steps 3, 4 and 5 in this section. If that doesn't work, see the Troubleshooting in Section 26.7 on page 235 for suggestions.

7 To add more powerline devices to your network, press the **ENCRYPT** button on device **C** (shown below) for more than 10 seconds until the HomePlug (⌂) light flashes.

8 Then repeat steps 4 and 5 in this section using any powerline device (**A** or **B**) you have connected using **ENCRYPT** and the powerline device you want to connect (**C**). You must use the **ENCRYPT** button on both devices.

Figure 6 Adding More Powerline Adapters to Your Network



9 If you disconnected your computer or modem (or any other networking product connected to your powerline device) in step 1 of this section, you can now reconnect them.

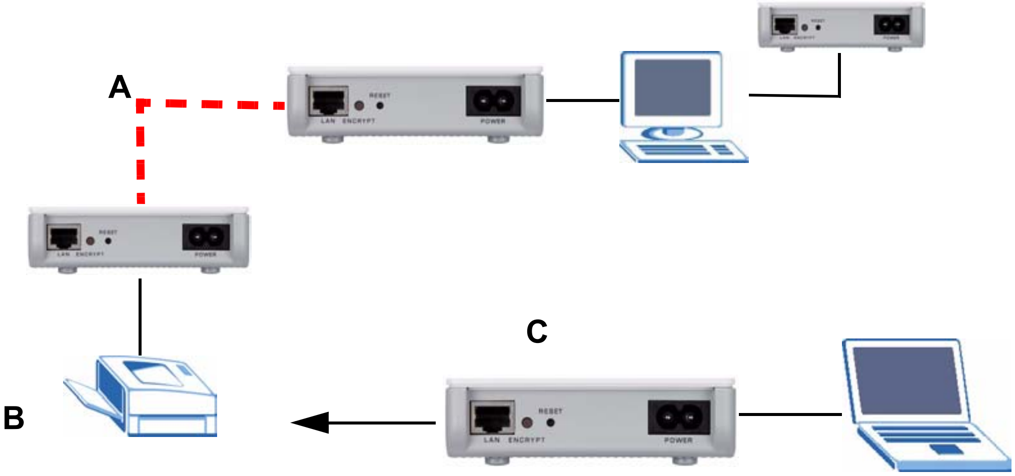
This sets up your powerline network between your powerline devices.

3.3 Setting Up Multiple Networks

You can use the **ENCRYPT** button to set up multiple powerline networks using your existing powerline network.

For example, you have already set up a powerline network in your home (**A**) which accesses a printer (**B**). Now you want a separate powerline network connection from your laptop to your printer (**C**).

Figure 7 One Existing Powerline Network



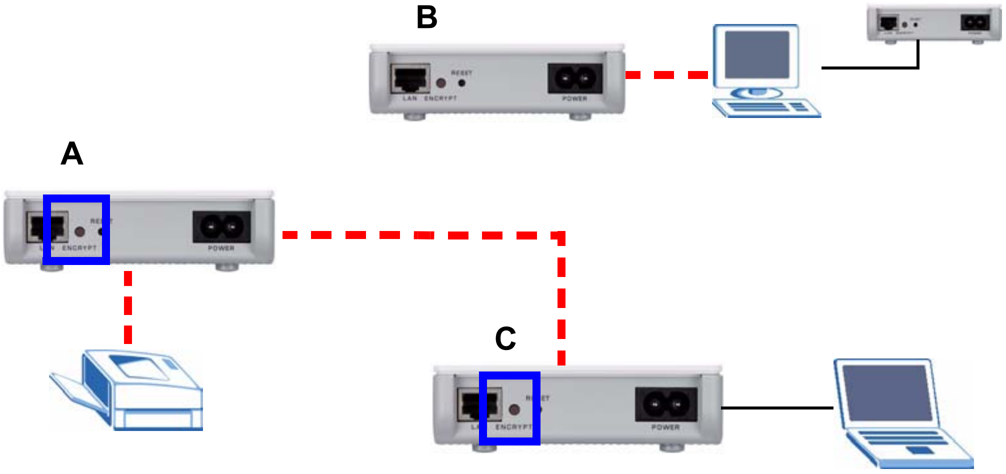
1 Click the **ENCRYPT** button on (**A**) for more than 10 seconds until the HomePlug (⌂) light is off. This disconnects (**A**) from (**B**).

2 Click the **ENCRYPT** button on (**A**) and (**C**) for 1~2 seconds and within two minutes of each other.

3 Wait for about one minute while (**A**) and (**C**) connect.

4 Check the lights on both (**A**) and (**C**). When the HomePlug (⌂) lights shine steadily, the devices are connected.

Figure 8 Two Separate Powerline Networks



Congratulations. You now have two separate powerline networks as shown above.

If the HomePlug (⌂) lights on both powerline devices do not light up, the powerline devices are not connected. Repeat the connection process, making certain you press the **ENCRYPT** buttons for the correct time and within two minutes of each other. If that does not work see Section 26.7 on page 235 for suggestions.

3.4 ENCRYPT Button Behavior

The following table summarizes the actions that occur when the **ENCRYPT** button is pressed for specific lengths of time.

Table 3 Time **ENCRYPT** Button is Pressed and Action

	ACTION	HOMEPLUG LIGHT BEHAVIOR
less than 3 seconds	The device joins a network. It shares the same network name as other devices on the network.	The HomePlug (⌂) light turns on if your device is connected to another powerline device or a powerline network.
more than 10 seconds	The device leaves any network it is associated with and its network name assumes a random value.	The HomePlug (⌂) light turns off when it disconnects from the powerline network.

See Troubleshooting in Chapter 26 on page 235 for suggestions on problems with the **ENCRYPT** button and the lights.

4

Introducing the Web Configurator

This chapter describes how to access the NBG318S web configurator and provides an overview of its screens.

4.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy setup and management of the NBG318S via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

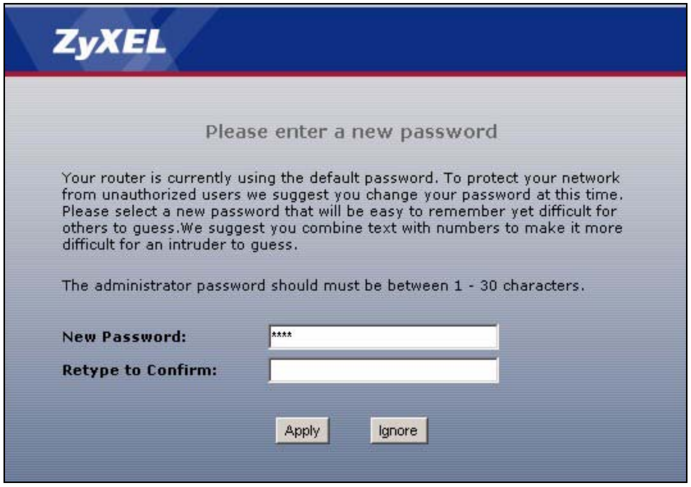
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter to see how to make sure these functions are allowed in Internet Explorer.

4.2 Accessing the Web Configurator

1. Make sure your NBG318S hardware is properly connected and prepare your computer or computer network to connect to the NBG318S (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "http://192.168.1.1" as the URL.
4. Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
5. You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 9 Change Password Screen



Please enter a new password

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

The administrator password should must be between 1 - 30 characters.

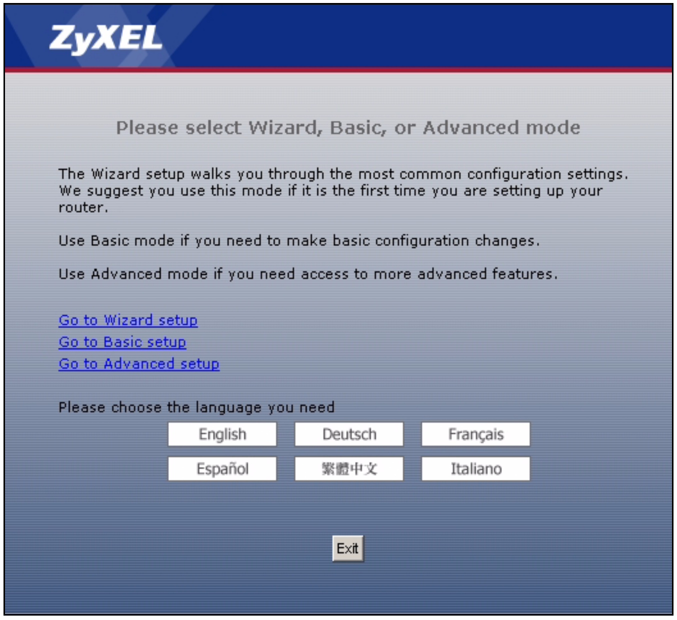
New Password: ****

Retype to Confirm:

The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the NBG318S if this happens.

6 Select the setup mode you want to use.

- Click **Go to Wizard Setup** to use the Configuration Wizard for basic Internet and Wireless setup.
- Click **Go to Basic Setup** if you want to view and configure basic settings that are not part of the wizard setup. Not all Web Configurator screens are available in this mode.
- **Click Go to Advanced Setup** to view and configure all the NBG318S's settings.



Please select Wizard, Basic, or Advanced mode

The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router.

Use Basic mode if you need to make basic configuration changes.

Use Advanced mode if you need access to more advanced features.

Please choose the language you need

4.3 Resetting the NBG318S

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the NBG318S to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, and the password will be reset to “1234”.

4.3.1 Procedure to Use the Reset Button

1. Make sure the **POWER** LED is on.
2. Press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the NBG318S restarts.

4.4 Navigating the Web Configurator

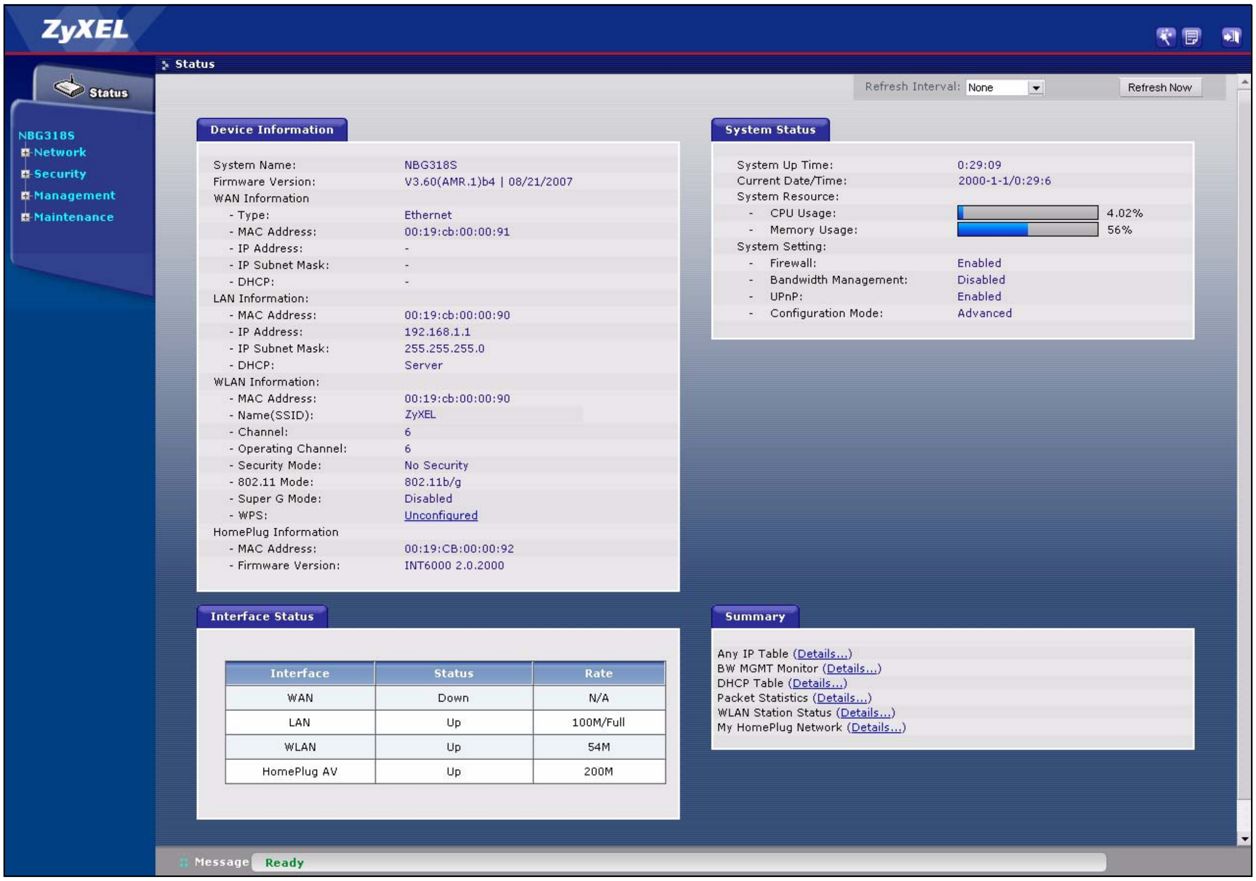
The following summarizes how to navigate the web configurator from the **Status** screen.

4.4.1 The Status Screen

The following screen displays when you log into the NBG318S.

Not all fields are available when you select **Basic** mode (see Section 4.2 on page 43). See the **Configuration Mode** field in the **System Status** box to check whether you are in **Basic** or **Advanced** mode. Use the **Config Mode > General** screen to change between modes.

Figure 10 Web Configurator Status Screen



Refresh Interval: None

Device Information

System Name:	NBG318S
Firmware Version:	V3.60(AMR.1)b4 | 08/21/2007
WAN Information	
- Type:	Ethernet
- MAC Address:	00:19:cb:00:00:91
- IP Address:	-
- IP Subnet Mask:	-
- DHCP:	-
LAN Information:	
- MAC Address:	00:19:cb:00:00:90
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information:	
- MAC Address:	00:19:cb:00:00:90
- Name(SSID):	ZyXEL
- Channel:	6
- Operating Channel:	6
- Security Mode:	No Security
- 802.11 Mode:	802.11b/g
- Super G Mode:	Disabled
- WPS:	Unconfigured
HomePlug Information	
- MAC Address:	00:19:CB:00:00:92
- Firmware Version:	INT6000 2.0.2000

System Status

System Up Time:	0:29:09
Current Date/Time:	2000-1-1/0:29:6
System Resource:	
- CPU Usage:	4.02%
- Memory Usage:	56%
System Setting:	
- Firewall:	Enabled
- Bandwidth Management:	Disabled
- UPnP:	Enabled
- Configuration Mode:	Advanced

Interface Status

Interface	Status	Rate
WAN	Down	N/A
LAN	Up	100M/Full
WLAN	Up	54M
HomePlug AV	Up	200M

Summary

Any IP Table (Details...)
BW MGMT Monitor (Details...)
DHCP Table (Details...)
Packet Statistics (Details...)
WLAN Station Status (Details...)
My HomePlug Network (Details...)

Message Ready

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

Table 4 Status Screen Icon Key

	DESCRIPTION
🪄	Click this icon to open the setup wizard.
📄	Click this icon to view copyright and a link for related product information.
⇥	Click this icon at any time to exit the web configurator.
Refresh Interval: 20 seconds ▾	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.
Refresh Now	Click this button to refresh the status screen statistics.

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

Table 5 Web Configurator Status Screen

LABEL	DESCRIPTION
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance** > **System** > **General** screen. It is for identification purposes.

Table 5 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
Firmware Version	This is the ZyNOS firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
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.
- DHCP	This shows the WAN port's DHCP role - **Client** or **None**.
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 Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Name (SSID)	This shows a descriptive name used to identify the NBG318S in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the NBG318S is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG318S is using.
- 802.11 Mode	This shows the wireless standard.
- Super G Mode	This shows whether SuperG is enabled or not.
- WPS	This shows whether WiFi Protected Setup is configured or not. Click this to go to the Network > Wireless LAN > WPS screen (see Section 7.9 on page 101).
HomePlug Information	
- MAC Address	This shows the MAC Address of your device.
- Firmware Version	This shows the HomePlug firmware version number.
System Status	
System Uptime	This is the total time the NBG318S has been on.
Current Date/Time	This field displays your NBG318S's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG318S's processing ability is currently used. When this percentage is close to 100%, the NBG318S 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 NBG318S is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT and the firewall.
System Setting	
- Firewall	This shows whether the firewall is active or not.
- Bandwidth Management	This shows whether the bandwidth management is active or not.
- UPnP	This shows whether UPnP is active or not.

Table 5 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
- Configuration Mode	This shows whether the advanced screens of each feature are turned on (**Advanced**) or not (**Basic**).
Interface Status	
Interface	This displays the NBG318S port types. The port types are: **WAN**, **LAN, WLAN** and **HomePlug AV**.
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. For the HomePlug AV port it displays **Up** when the power cord is connected.
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. For the HomePlug AV port it displays the maximum transmission rate when the HomePlug AV is enabled.
Summary	
Any IP Table	Use this screen to view details of IP addresses assigned to devices not in the same subnet as the NBG318S.
BW MGMT Monitor	Use this screen to view the NBG318S's bandwidth usage and allotments.
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 Station Status	Use this screen to view the wireless stations that are currently associated to the NBG318S.
My HomePlug Network	Use this screen to view information on the stations connected to your Home Plug network.

4.4.2 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure NBG318S features.

The following table describes the sub-menus.

Table 6 Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the NBG318S's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		

Table 6 Screens Summary

LINK	TAB	FUNCTION
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG318S to block access to devices or block the devices from accessing the NBG318S.
	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 set up Wi-Fi Protected Setup on your NBG318S. This allows you to connect other WPS enabled devices at the touch of a button.
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 partition your LAN interface into subnets.
	Advanced	Use this screen to enable other advanced properties.
HomePlug	Network Settings	Use this screen to configure HomePlug AV devices and set up a power line network.
DHCP Server	General	Use this screen to enable the NBG318S's DHCP server.
	Advanced	Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
	Client List	Use this screen to view current DHCP client information and to always assign an IP address to a MAC address (and host name).
NAT	General	Use this screen to enable NAT.
	Application	Use this screen to configure servers behind the NBG318S.
	Advanced	Use this screen to change your NBG318S's port triggering settings.
DDNS	General	Use this screen to set up dynamic DNS.
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	Filter	Use this screen to block certain web features and sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for the NBG318S to perform content filtering.
Management		
Static Route	IP Static Route	Use this screen to configure IP static routes.
Bandwidth MGMT	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 NBG318S's bandwidth usage and allotments.

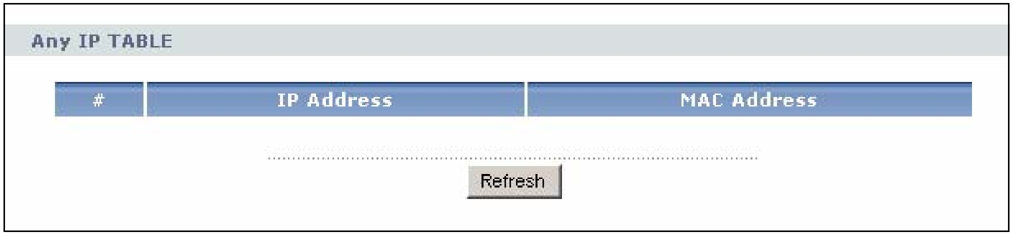
Table 6 Screens Summary

LINK	TAB	FUNCTION
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the NBG318S.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the NBG318S.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the NBG318S.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the NBG318S.
UPnP	General	Use this screen to enable UPnP on the NBG318S.
Maintenance		
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Time Setting	Use this screen to change your NBG318S's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your NBG318S's log settings.
Tools	Firmware	Use this screen to upload firmware to your NBG318S.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG318S.
	Restart	This screen allows you to reboot the NBG318S without turning the power off.
Config Mode	General	This screen allows you to display or hide the advanced screens or features.
Sys OP Mode	General	This screen allows you to select whether the NBG318S operates as a router or an access point. The router option allows you to select whether you have an Ethernet or a powerline WAN connection to the Internet.
Language	Language	This allows you to change the web configurator's language settings.

4.4.3 Summary: Any IP Table

This screen displays the IP address of each computer that is using the NBG318S via the any IP feature. Any IP allows computers to access the Internet through the NBG318S without changing their network settings when NAT is enabled. To access this screen, open the **Status** screen (see Section 4.4.1 on page 45), and click **(Details...)** next to **Any IP Table**.

Figure 11 Any IP Table



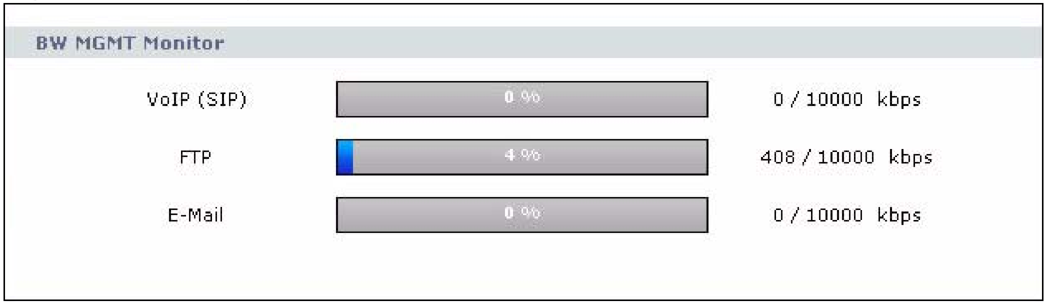
Any IP TABLE

#	IP Address	MAC Address

4.4.4 Summary: Bandwidth Management Monitor

Select the **BW MGMT Monitor (Details...)** hyperlink in **Status** screen. View the bandwidth usage of the WAN configured bandwidth rules. This is also shown as bandwidth usage over the bandwidth budget for each rule. The gray section of the bar represents the percentage of unused bandwidth and the blue color represents the percentage of bandwidth in use.

Figure 12 Summary: BW MGMT Monitor



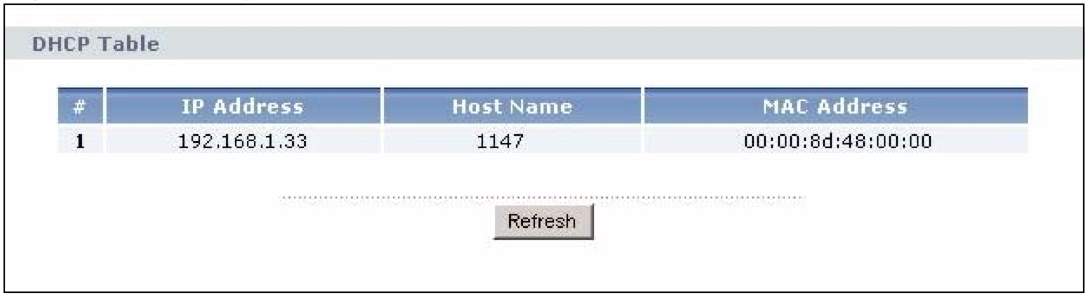
VoIP (SIP)	0 %	0 / 10000 kbps
FTP	4 %	408 / 10000 kbps
E-Mail	0 %	0 / 10000 kbps

4.4.5 Summary: DHCP Table

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the NBG318S as a DHCP server or disable it. When configured as a server, the NBG318S 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.

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 NBG318S's DHCP server.

Figure 13 Summary: DHCP Table



#	IP Address	Host Name	MAC Address
1	192.168.1.33	1147	00:00:8d:48:00:00

The following table describes the labels in this screen.

Table 7 Summary: DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.

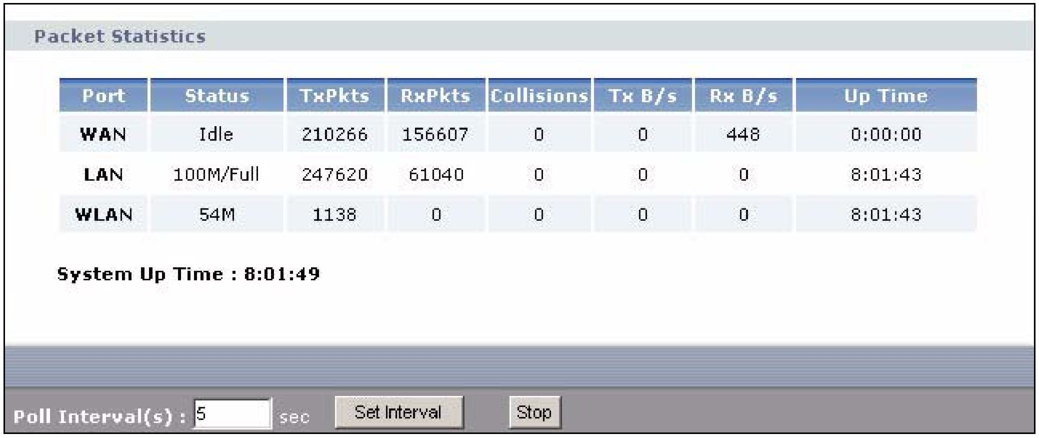
Table 7 Summary: DHCP Table (continued)

LABEL	DESCRIPTION
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. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click **Refresh** to renew the screen.

4.4.6 Summary: Packet Statistics

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

Figure 14 Summary: Packet Statistics



Packet Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Idle	210266	156607	0	0	448	0:00:00
LAN	100M/Full	247620	61040	0	0	0	8:01:43
WLAN	54M	1138	0	0	0	0	8:01:43

System Up Time : 8:01:49

Poll Interval(s) : 5 sec

The following table describes the labels in this screen.

Table 8 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the NBG318S'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 the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **Down** when the WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
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 amount of time the line has been up.
System Up Time	This is the total time the NBG318S has been on.

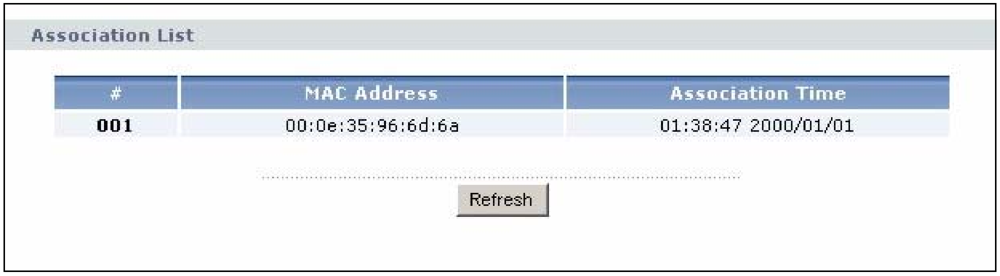
Table 8 Summary: Packet Statistics

LABEL	DESCRIPTION
Poll Interval(s)	Enter the time interval 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, click **Stop**.

4.4.7 Summary: Wireless Station Status

Click the **WLAN Station Status (Details...)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the NBG318S in the **Association List** screen.

Figure 15 Summary: Wireless Association List



Association List

#	MAC Address	Association Time
001	00:0e:35:96:6d:6a	01:38:47 2000/01/01

The following table describes the labels in this screen.

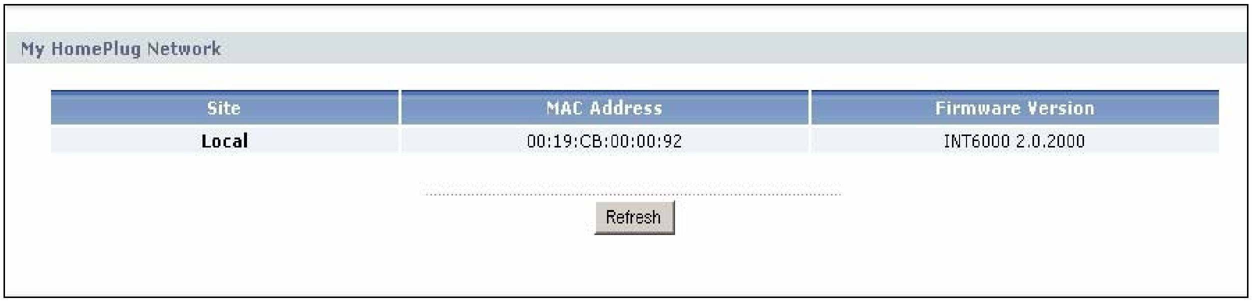
Table 9 Summary: Wireless Association List

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 NBG318S.
Refresh	Click **Refresh** to reload the list.

4.4.8 Summary: My HomePlug Network Status

Click the **My HomePlug Network (Details...)** hyperlink in the **Status** screen. View the powerline stations that are currently associated to the NBG318S in the **My Homeplug Network** screen.

Figure 16 Summary: My Homeplug Network.



My HomePlug Network

Site	MAC Address	Firmware Version
Local	00:19:CB:00:00:92	INT6000 2.0.2000

The following table describes the labels in this screen.

Table 10 Summary: My Homeplug Network

LABEL	DESCRIPTION
Site	Your NBG318S is the **Local** device. All other devices on your network will be **Remote.**
MAC Address	This field displays the MAC address of a HomePlug AV device detected by your NBG318S.
Firmware Version	This shows the firmware version used by the HomePlug chipset.
Refresh	Click **Refresh** to reload the list.

5

Connection Wizard

This chapter provides information on the wizard setup screens in the web configurator.

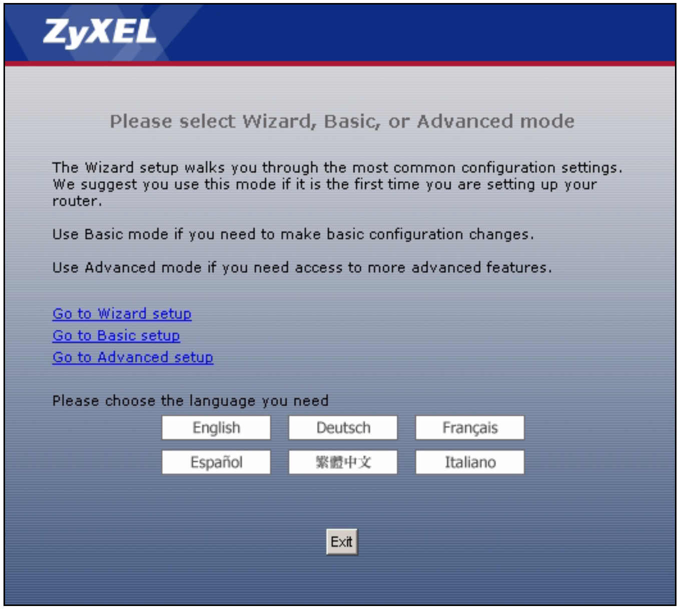
5.1 Wizard Setup

The web configurator's wizard setup helps you configure your device to access the Internet. Leave a field blank if you don't have that information. You can access the Wizard by clicking the Wizard icon in the web configurator or when you first log in as follows.

1 After you first log into the NBG318S web configurator, click the **Go to Wizard setup** hyperlink.

You can click the **Go to Basic setup** or **Go to Advanced setup** hyperlink to skip this wizard setup and configure basic or advanced features accordingly.

Figure 17 Select Wizard or Advanced Mode



Please select Wizard, Basic, or Advanced mode

The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router.

Use Basic mode if you need to make basic configuration changes.

Use Advanced mode if you need access to more advanced features.

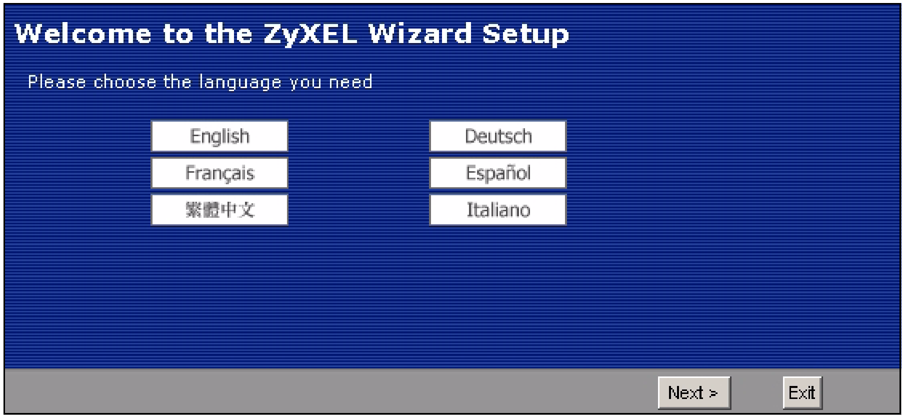
Go to Wizard setup
Go to Basic setup
Go to Advanced setup

Please choose the language you need

2 Choose your language if necessary.

3 Click the **Next** button to proceed to the next screen.

Figure 18 Select a Language

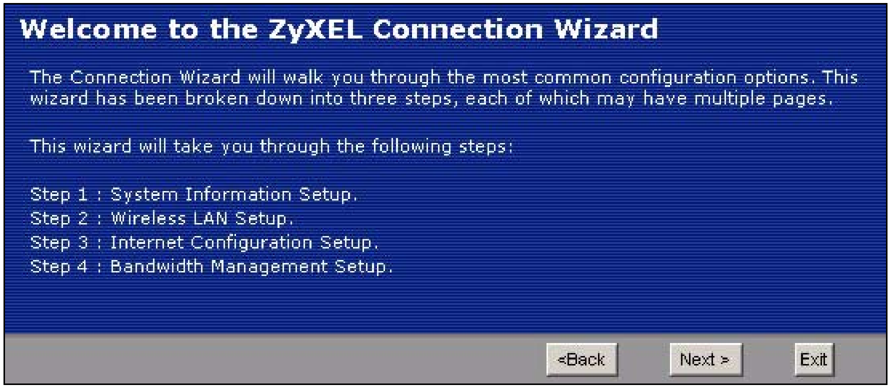


Welcome to the ZyXEL Wizard Setup

Please choose the language you need

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

Figure 19 Welcome to the Connection Wizard



Welcome to the ZyXEL Connection Wizard

The Connection Wizard will walk you through the most common configuration options. This wizard has been broken down into three steps, each of which may have multiple pages.

This wizard will take you through the following steps:

Step 1 : System Information Setup.
Step 2 : Wireless LAN Setup.
Step 3 : Internet Configuration Setup.
Step 4 : Bandwidth Management Setup.

5.2 Connection Wizard: STEP 1: System Information

System Information contains administrative and system-related information.

5.2.1 System Name

System Name is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

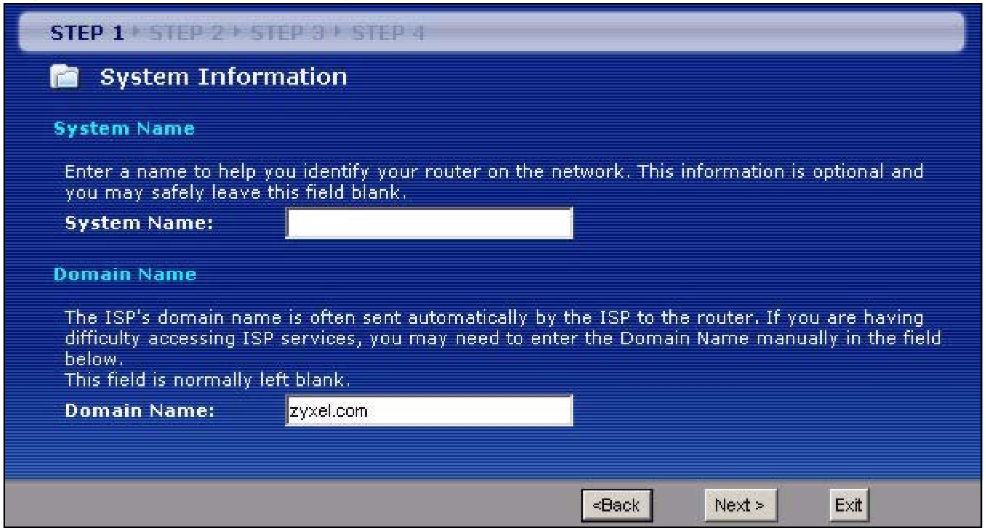
- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the NBG318S **System Name**.

5.2.2 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the NBG318S via DHCP.

Click **Next** to configure the NBG318S for Internet access.

Figure 20 Wizard Step 1: System Information



System Information

System Name

Enter a name to help you identify your router on the network. This information is optional and you may safely leave this field blank.

System Name:

Domain Name

The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.
This field is normally left blank.

Domain Name: zyxel.com

The following table describes the labels in this screen.

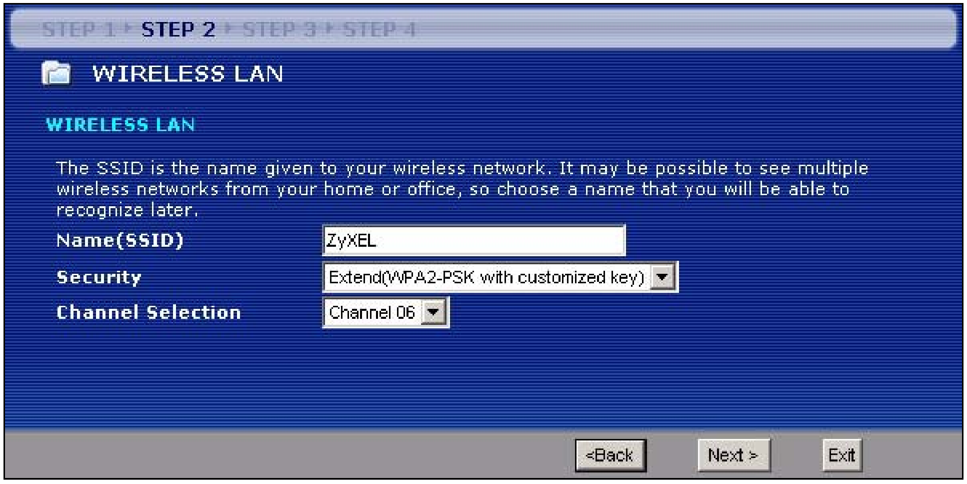
Table 11 Wizard Step 1: System Information

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the NBG318S in an Ethernet network. Enter a descriptive name. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Type the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

5.3 Connection Wizard: STEP 2: Wireless LAN

Set up your wireless LAN using the following screen.

Figure 21 Wizard Step 2: Wireless LAN



WIRELESS LAN

WIRELESS LAN

The SSID is the name given to your wireless network. It may be possible to see multiple wireless networks from your home or office, so choose a name that you will be able to recognize later.

Name(SSID): ZyXEL

Security: Extend(WPA2-PSK with customized key)

Channel Selection: Channel 06

The following table describes the labels in this screen.

Table 12 Wizard Step 2: Wireless LAN

LABEL	DESCRIPTION
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 NBG318S, make sure all wireless stations use the same SSID in order to access the network.
Security	Select a **Security** level from the drop-down list box. Choose **Auto** to have the NBG318S generate a pre-shared key automatically. A screen pops up displaying the generated pre-shared key after you click **Next**. Write down the key for use later when connecting other wireless devices to your network. Click **OK** to continue. Choose **None** to have no wireless LAN security configured. If you do not enable any wireless security on your NBG318S, your network is accessible to any wireless networking device that is within range. If you choose this option, skip directly to Section 5.4 on page 61. Choose **Basic (WEP)** security if you want to configure WEP Encryption parameters. If you choose this option, go directly to Section 5.3.2 on page 59. Choose **Extend** (**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. If you choose this option, skip directly to Section 5.3.3 on page 61.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Select a channel if interference from other wireless devices may be a problem.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

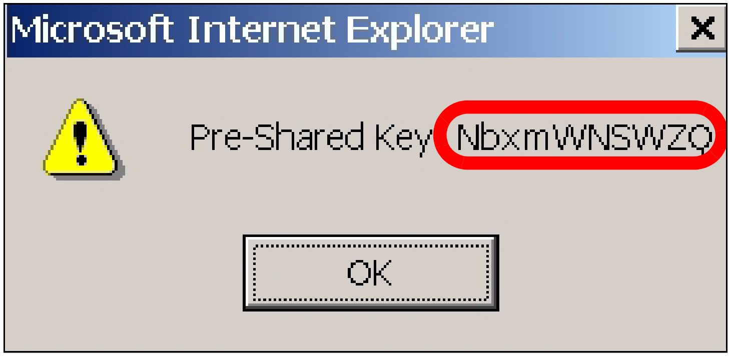
The NBG318S and other wireless devices must use the same SSID, channel ID and WEP encryption key (if WEP is enabled), WPA-PSK (if WPA-PSK is enabled) or WPA2-PSK (if WPA2-PSK is enabled) for wireless communication.

5.3.1 Auto Security

Choose **Auto** to automatically generate a WPA-PSK pre-shared key. A window appears displaying the key.

Make sure you write down the key! You will need it later to connect other wireless devices to your network.

Figure 22 Popup Pre-Shared Key



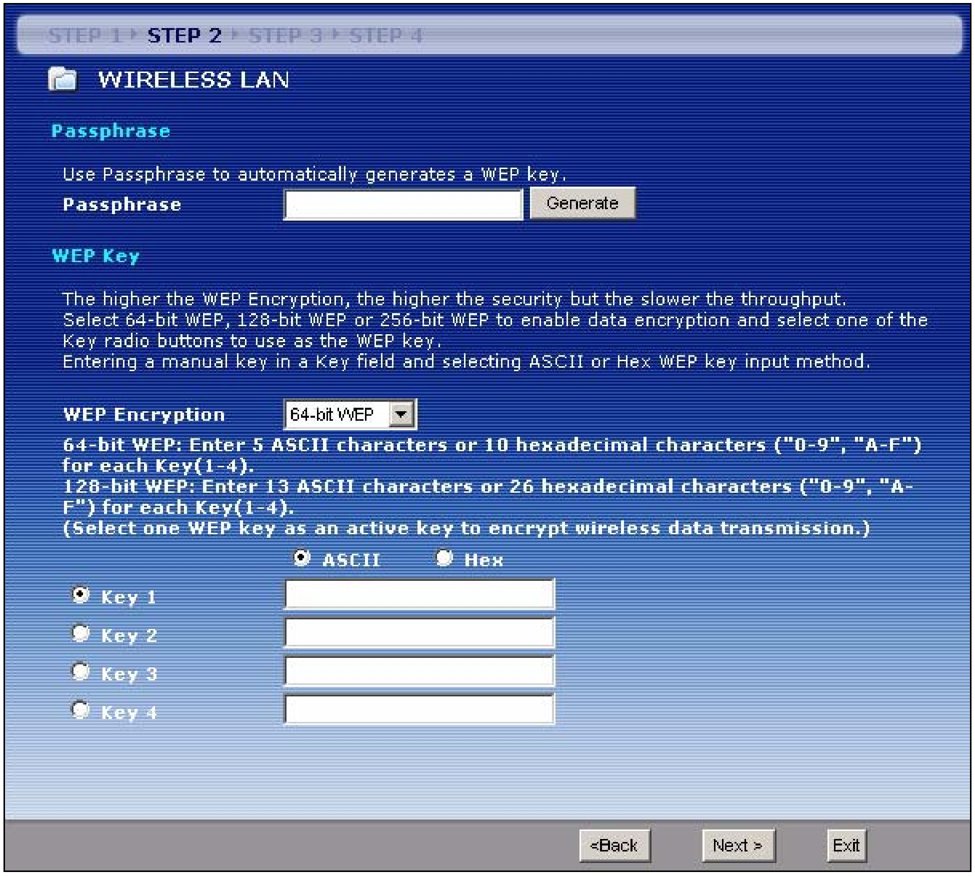
Microsoft Internet Explorer

Pre-Shared Key NbxmWNSWZQ

5.3.2 Basic (WEP) Security

Choose **Basic (WEP)** to set up WEP Encryption parameters.

Figure 23 Wizard Step 2: Basic (WEP) Security



Passphrase

Use Passphrase to automatically generates a WEP key.

Passphrase

WEP Key

The higher the WEP Encryption, the higher the security but the slower the throughput.
Select 64-bit WEP, 128-bit WEP or 256-bit WEP to enable data encryption and select one of the Key radio buttons to use as the WEP key.
Entering a manual key in a Key field and selecting ASCII or Hex WEP key input method.

WEP Encryption: 64-bit WEP

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

The following table describes the labels in this screen.

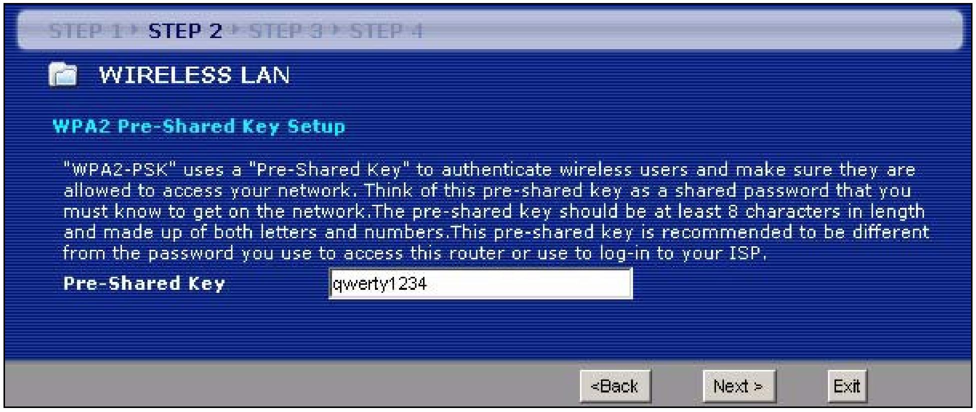
Table 13 Wizard Step 2: Basic (WEP) Security

LABEL	DESCRIPTION
Passphrase	Type a **Passphrase** (up to 32 printable characters) and click **Generate**. The NBG318S automatically generates a WEP key.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to allow data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys. ASCII characters include the characters available on a standard English language keyboard.
HEX	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the NBG318S and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

5.3.3 Extend (WPA-PSK or WPA2-PSK) Security

Choose **Extend (WPA-PSK)** or **Extend (WPA2-PSK)** security in the Wireless LAN setup screen to set up a **Pre-Shared Key**.

Figure 24 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security



WPA2 Pre-Shared Key Setup

"WPA2-PSK" uses a "Pre-Shared Key" to authenticate wireless users and make sure they are allowed to access your network. Think of this pre-shared key as a shared password that you must know to get on the network.The pre-shared key should be at least 8 characters in length and made up of both letters and numbers.This pre-shared key is recommended to be different from the password you use to access this router or use to log-in to your ISP.

Pre-Shared Key: qwerty1234

The following table describes the labels in this screen.

Table 14 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security

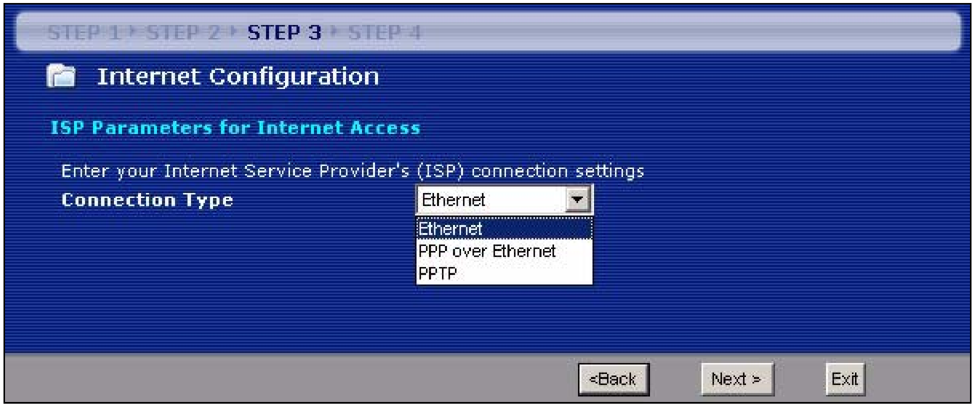
LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens. You need to configure an authentication server to do this.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

5.4 Connection Wizard: STEP 3: Internet Configuration

The NBG318S offers three Internet connection types. They are **Ethernet**, **PPP over Ethernet** or **PPTP**. The wizard attempts to detect which WAN connection type you are using. 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.

This wizard screen varies according to the connection type that you select.

Figure 25 Wizard Step 3: ISP Parameters.



Internet Configuration

ISP Parameters for Internet Access

Enter your Internet Service Provider's (ISP) connection settings

Connection Type: Ethernet

The following table describes the labels in this screen,

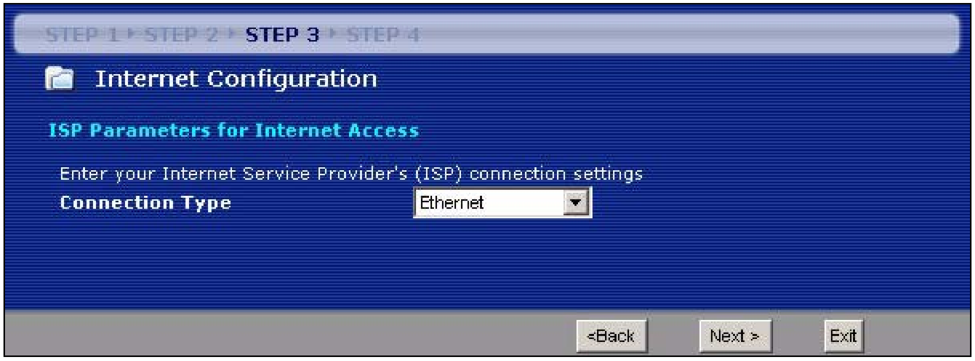
Table 15 Wizard Step 3: ISP Parameters

CONNECTION TYPE	DESCRIPTION
Ethernet	Select the **Ethernet** option when the WAN port is used as a regular Ethernet.
PPPoE	Select the **PPP over Ethernet** option for a dial-up connection. If your ISP gave you a an IP address and/or subnet mask, then select **PPTP**.
PPTP	Select the **PPTP** option for a dial-up connection.

5.4.1 Ethernet Connection

Choose **Ethernet** when the WAN port is used for a regular Ethernet connection.

Figure 26 Wizard Step 3: Ethernet Connection



Internet Configuration

ISP Parameters for Internet Access

Enter your Internet Service Provider's (ISP) connection settings

Connection Type: Ethernet

5.4.2 PPPoE Connection

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

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

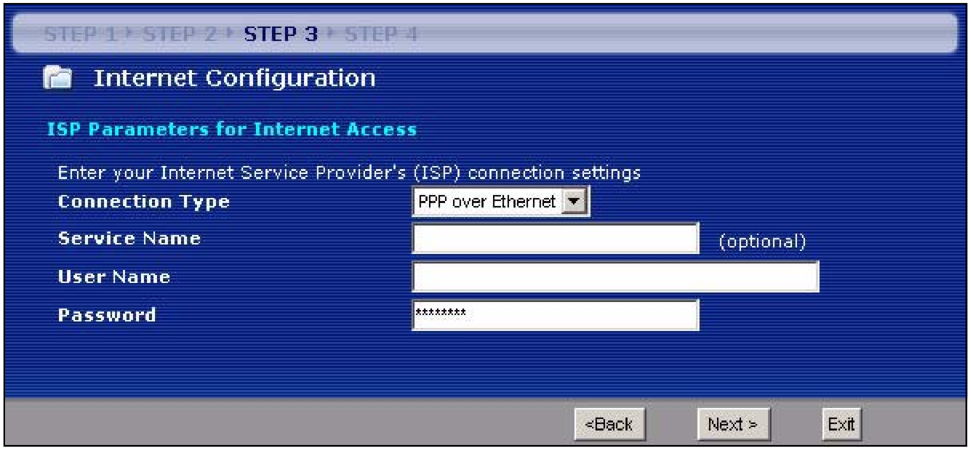
One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

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

By implementing PPPoE directly on the NBG318S (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG318S does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Refer to the appendix for more information on PPPoE.

Figure 27 Wizard Step 3: PPPoE Connection


STEP 1 ▸ STEP 2 ▸ STEP 3 ▸ STEP 4
Internet Configuration
ISP Parameters for Internet Access
<Back
Next >
Exit

Enter your Internet Service Provider's (ISP) connection settings

Connection Type: PPP over Ethernet

Service Name: (optional)

User Name:

Password: ********

The following table describes the labels in this screen.

Table 16 Wizard Step 3: PPPoE Connection

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Connection Type	Select the **PPP over Ethernet** option for a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

5.4.3 PPTP Connection

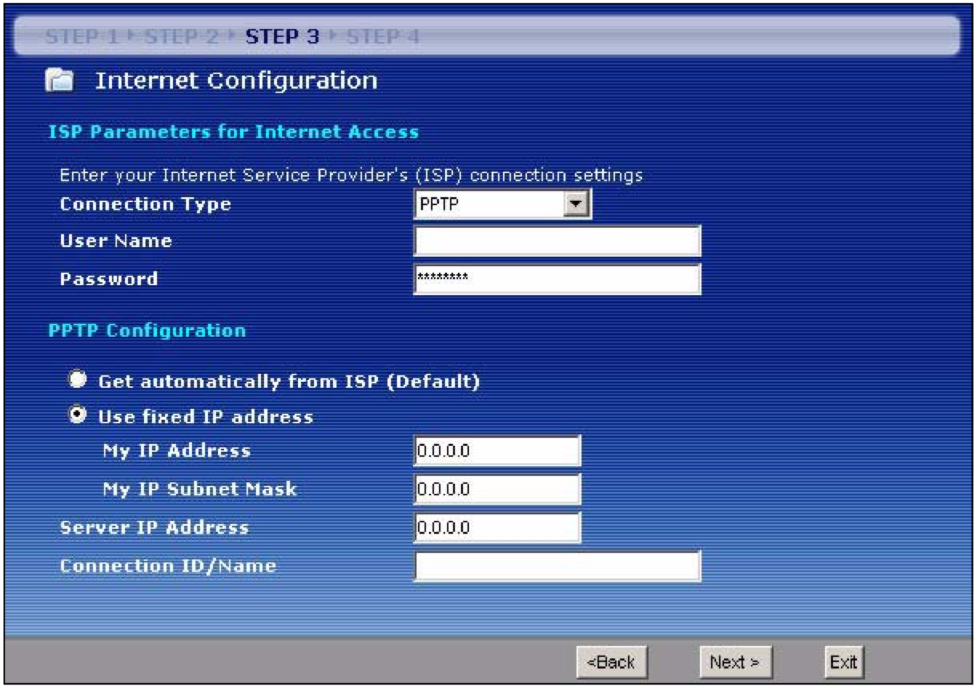
Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

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 NBG318S supports one PPTP server connection at any given time.

Figure 28 Wizard Step 3: PPTP Connection



Internet Configuration

ISP Parameters for Internet Access

Enter your Internet Service Provider's (ISP) connection settings

Connection Type: PPTP

User Name:

Password: ********

PPTP Configuration

○ Get automatically from ISP (Default)

● Use fixed IP address

My IP Address: 0.0.0.0

My IP Subnet Mask: 0.0.0.0

Server IP Address: 0.0.0.0

Connection ID/Name:

The following table describes the fields in this screen

Table 17 Wizard Step 3: PPTP Connection

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
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.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
PPTP Configuration	
Get automatically from ISP	Select this radio button if your ISP did not assign you a fixed IP address.
Use fixed IP address	Select this radio button, provided by your ISP to give the NBG318S a fixed, unique IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.
Back	Click **Back** to return to the previous screen.

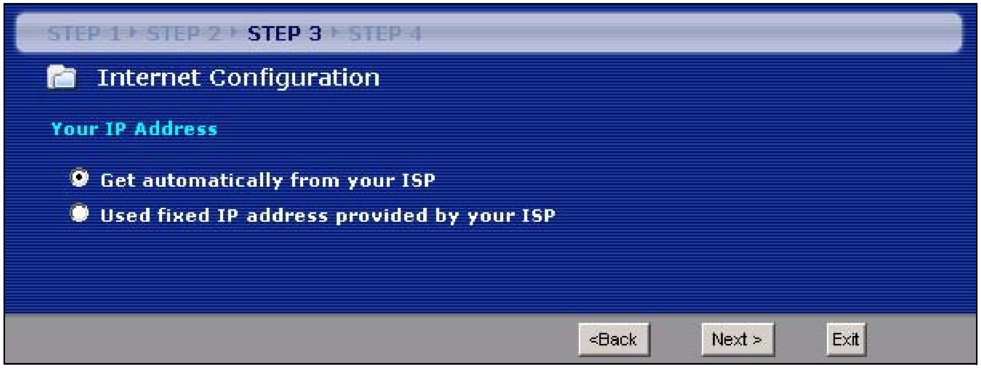
Table 17 Wizard Step 3: PPTP Connection

LABEL	DESCRIPTION
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

5.4.4 Your IP Address

The following wizard screen allows you to assign a fixed IP address or give the NBG318S an automatically assigned IP address depending on your ISP.

Figure 29 Wizard Step 3: Your IP Address



Internet Configuration

Your IP Address

● Get automatically from your ISP

○ Used fixed IP address provided by your ISP

The following table describes the labels in this screen

Table 18 Wizard Step 3: Your IP Address

LABEL	DESCRIPTION
Get automatically from your ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection. If you choose this option, skip directly to section 5.4.9.
Use fixed IP address provided by your ISP	Select this option if you were given IP address and/or DNS server settings by the ISP. The fixed IP address should be in the same subnet as your broadband modem or router.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

5.4.5 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, 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.

Table 19 Private IP Address Ranges

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 have it assigned by 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.

5.4.6 IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your NBG318S, 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 NBG318S 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 NBG318S unless you are instructed to do otherwise.

5.4.7 DNS Server Address Assignment

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

The NBG318S can get the DNS server addresses in the following ways.

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

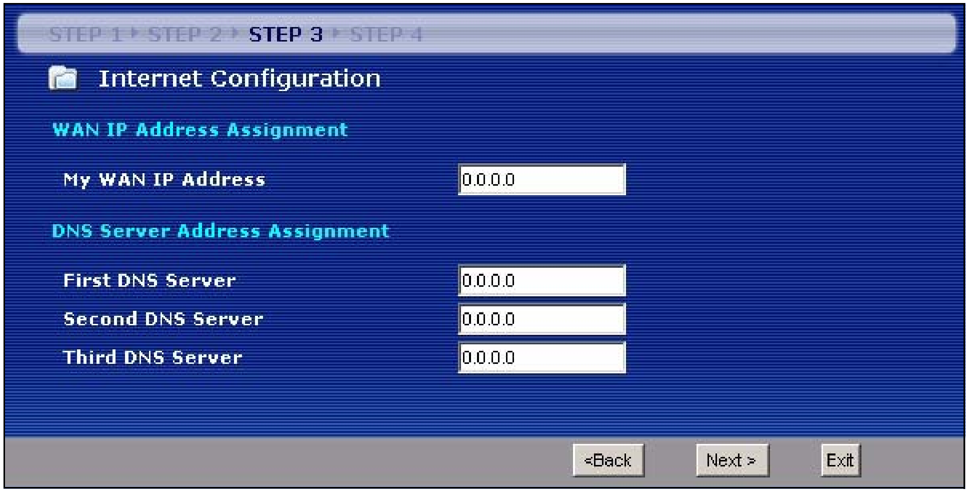
2 If the ISP did not give you DNS server information, leave the **DNS Server** fields set to **0.0.0.0** in the **Wizard** screen and/or set to **From ISP** in the **WAN > Internet Connection** screen for the ISP to dynamically assign the DNS server IP addresses.

5.4.8 WAN IP and DNS Server Address Assignment

The following wizard screens allows you to assign a fixed WAN IP address and DNS server addresses.

This screen appears if you selected PPP over Ethernet as your connection type in the Wizard.

Wizard Step 3: PPPoE: WAN IP and DNS Server Addresses



Internet Configuration

WAN IP Address Assignment

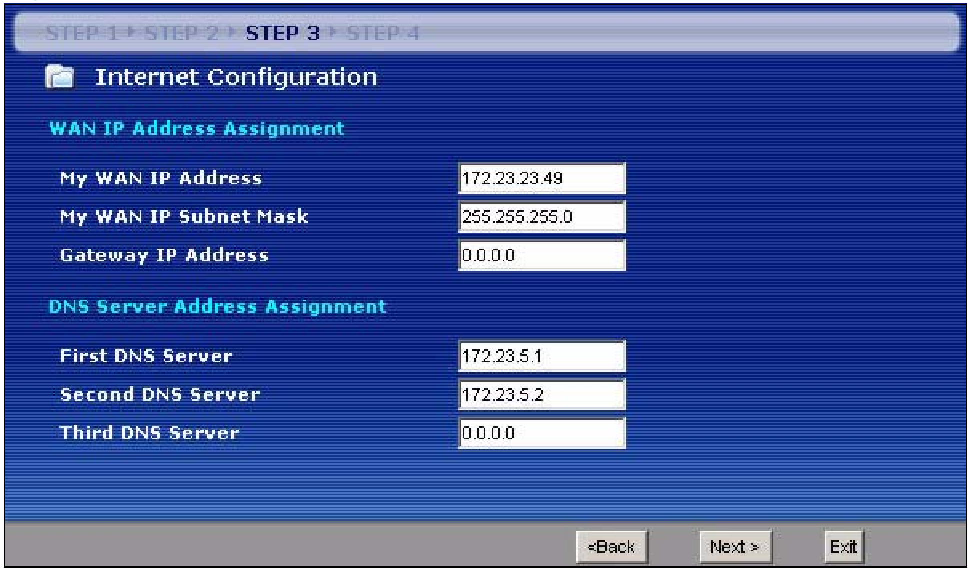
My WAN IP Address	0.0.0.0

DNS Server Address Assignment

First DNS Server	0.0.0.0
Second DNS Server	0.0.0.0
Third DNS Server	0.0.0.0

This screen appears if you selected Ethernet or PPTP as your connection type in the Wizard.

Figure 30 Wizard Step 3: WAN IP and DNS Server Addresses



Internet Configuration

WAN IP Address Assignment

My WAN IP Address	172.23.23.49
My WAN IP Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0

DNS Server Address Assignment

First DNS Server	172.23.5.1
Second DNS Server	172.23.5.2
Third DNS Server	0.0.0.0

The following table describes the labels in this screen

Table 20 Wizard Step 3: WAN IP and DNS Server Addresses

LABEL	DESCRIPTION
WAN IP Address Assignment	
My WAN IP Address	Enter your WAN IP address in this field. The WAN IP address should be in the same subnet as your DSL/Cable modem or router.
My WAN IP Subnet Mask	Enter the IP subnet mask in this field. (Not available if you selected PPP over Ethernet as your Connection type.)
Gateway IP Address	Enter the gateway IP address in this field. (Not available if you selected PPP over Ethernet as your Connection type.)
System DNS Server Address Assignment (if applicable) 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 NBG318S uses a system DNS server (in the order you specify here) to resolve domain names for DDNS and the time server.	
First DNS Server Second DNS Server Third DNS Server	Enter the DNS server's IP address in the fields provided. If you do not configure a system DNS server, you must use IP addresses when configuring DDNS and the time server.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

5.4.9 WAN MAC Address

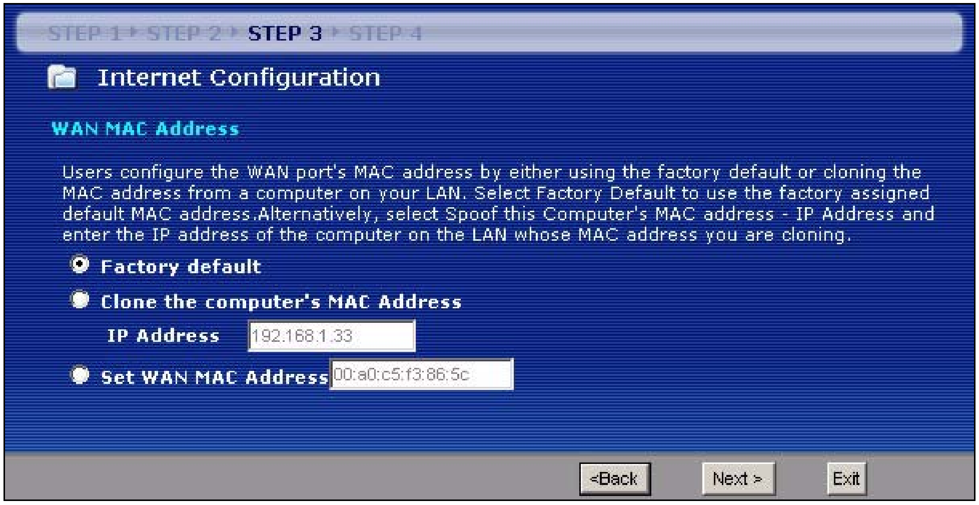
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Table 21 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(NBG318S LAN IP)

This screen allows users to configure the WAN port's MAC address by either using the NBG318S's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.

Figure 31 Wizard Step 3: WAN MAC Address



Internet Configuration

WAN MAC Address

Users configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Select Factory Default to use the factory assigned default MAC address.Alternatively, select Spoof this Computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC address you are cloning.

● Factory default

○ Clone the computer's MAC Address

IP Address 192.168.1.33

○ Set WAN MAC Address 00:a0:c5:f3:86:5c

The following table describes the fields in this screen.

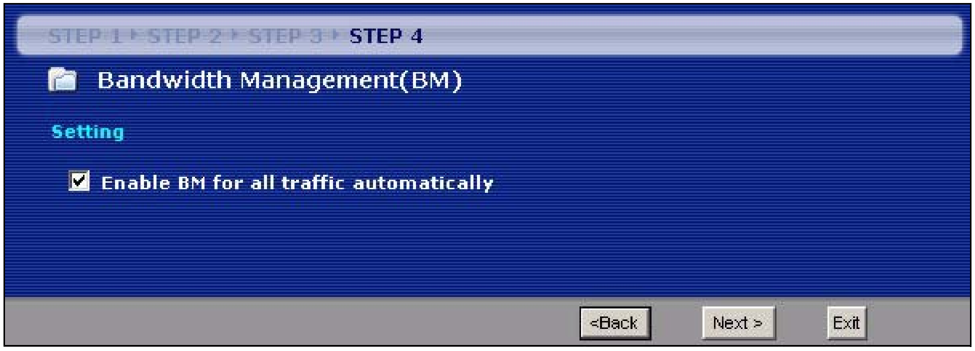
Table 22 Wizard Step 3: WAN MAC Address

LABEL	DESCRIPTION
Factory Default	Select **Factory Default** to use the factory assigned default MAC address.
Clone the computer's MAC address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

5.5 Connection Wizard: STEP 4: Bandwidth management

Bandwidth management allows you to control the amount of bandwidth going out through the NBG318S's WAN, LAN or WLAN port and prioritize the distribution of the bandwidth according to the traffic type. This helps keep one service from using all of the available bandwidth and shutting out other users.

Figure 32 Wizard Step 4: Bandwidth Management



Bandwidth Management(BM)

Setting

☑ Enable BM for all traffic automatically

The following fields describe the label in this screen.

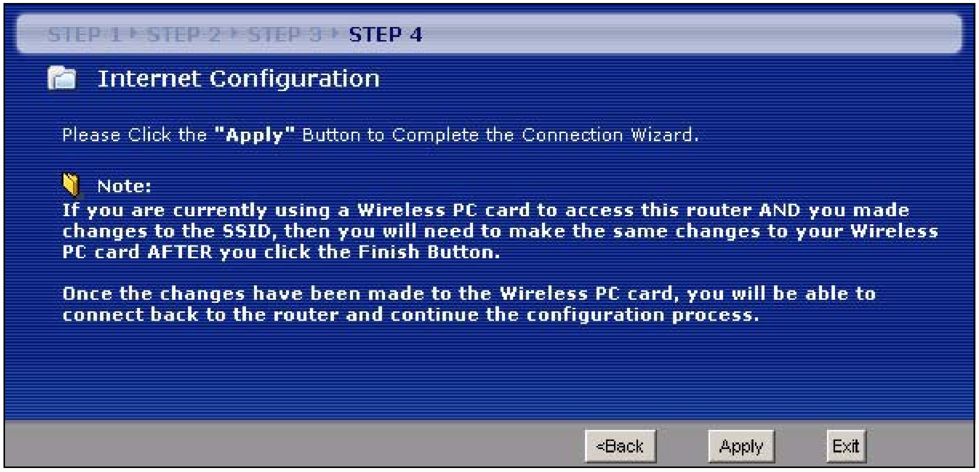
Table 23 Wizard Step 4: Bandwidth Management

LABEL	DESCRIPTION
Enable BM for all traffic automatically	Select the check box to have the NBG318S apply bandwidth management to traffic going out through the NBG318S's WAN, LAN, HomePlug AV or WLAN port. Bandwidth is allocated according to the traffic type automatically. Real-time packets, such as VoIP traffic always get higher priority.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

5.6 Connection Wizard Complete

Click **Apply** to save your configuration.

Figure 33 Connection Wizard Save



Internet Configuration

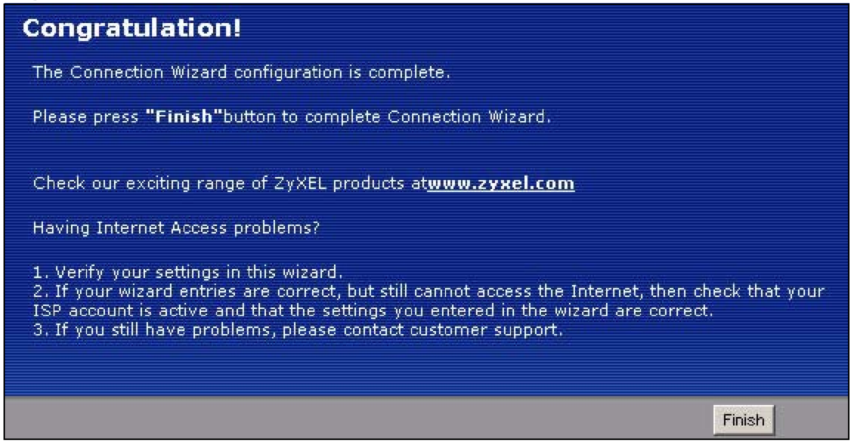
Please Click the **"Apply"** Button to Complete the Connection Wizard.

Note:
If you are currently using a Wireless PC card to access this router AND you made changes to the SSID, then you will need to make the same changes to your Wireless PC card AFTER you click the Finish Button.

Once the changes have been made to the Wireless PC card, you will be able to connect back to the router and continue the configuration process.

Follow the on-screen instructions and click **Finish** to complete the wizard setup.

Figure 34 Connection Wizard Complete



Congratulation!

The Connection Wizard configuration is complete.

Please press **"Finish"**button to complete Connection Wizard.

Check our exciting range of ZyXEL products at**www.zyxel.com**

Having Internet Access problems?

1. Verify your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.

Well done! You have successfully set up your NBG318S to operate on your network and access the Internet.

6

Tutorial

This chapter gives you examples of how to set up a wireless access point and a wireless client for wireless communication using some example settings.

6.1 Example Parameters

SSID	SSID_Example3
Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)
802.11 mode	IEEE 802.11b/g

An access point (AP) or wireless router is referred to as an "AP" and a computer with a wireless network card or USB/PCI adapter is referred to as a "wireless client" here.

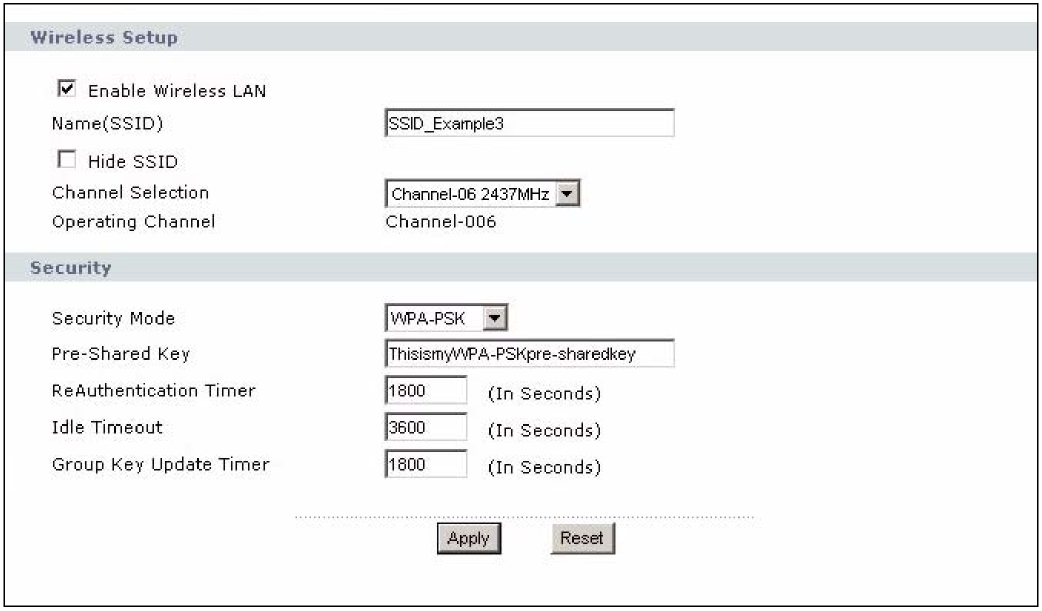
We use the M-302 utility screens as an example for the wireless client. The screens may vary for different models.

6.2 Configuring the AP

Flow the steps below to configure the wireless settings on your AP.

3 Open the **Wireless LAN** > **General** screen in the AP's web configurator.

Figure 35 Network > Wireless LAN > General



Wireless Setup

☑ Enable Wireless LAN

Name(SSID): SSID_Example3

☐ Hide SSID

Channel Selection: Channel-06 2437MHz

Operating Channel: Channel-006

Security

Security Mode: WPA-PSK

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Group Key Update Timer: 1800 (In Seconds)

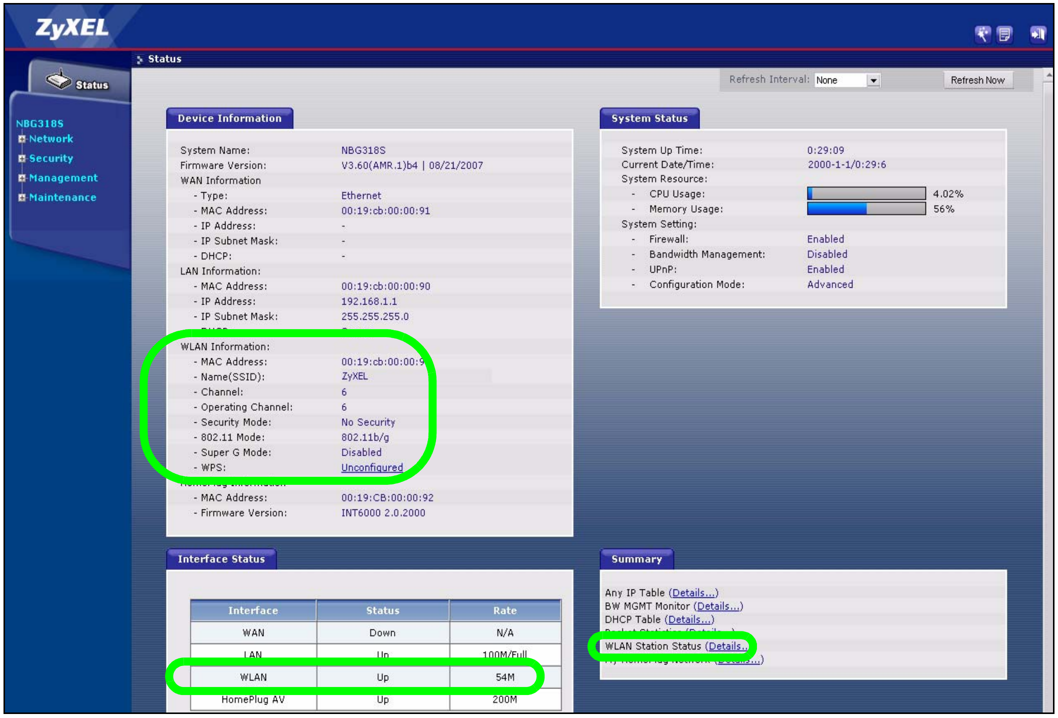
4 Make sure the **Enable Wireless LAN** check box is selected.

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

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

7 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 36 Network > Wireless LAN > General



Refresh Interval: None

Device Information

System Name: NBG318S
Firmware Version: V3.60(AMR.1)b4 | 08/21/2007
WAN Information
- Type: Ethernet
- MAC Address: 00:19:cb:00:00:91
- IP Address: -
- IP Subnet Mask: -
- DHCP: -

LAN Information:
- MAC Address: 00:19:cb:00:00:90
- IP Address: 192.168.1.1
- IP Subnet Mask: 255.255.255.0

WLAN Information:
- MAC Address: 00:19:cb:00:00:9
- Name(SSID): ZyXEL
- Channel: 6
- Operating Channel: 6
- Security Mode: No Security
- 802.11 Mode: 802.11b/g
- Super G Mode: Disabled
- WPS: Unconfigured

- MAC Address: 00:19:CB:00:00:92
- Firmware Version: INT6000 2.0.2000

System Status

System Up Time: 0:29:09
Current Date/Time: 2000-1-1/0:29:6
System Resource:
- CPU Usage: 4.02%
- Memory Usage: 56%

System Setting:
- Firewall: Enabled
- Bandwidth Management: Disabled
- UPnP: Enabled
- Configuration Mode: Advanced

Interface Status

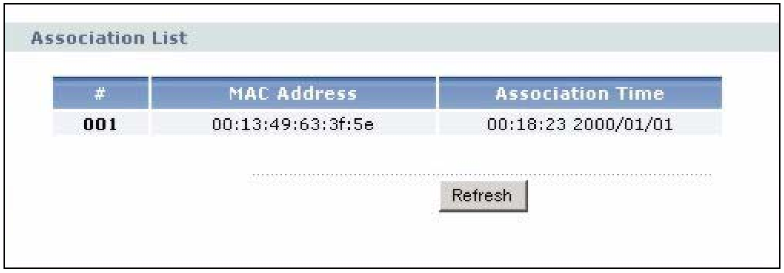
Interface	Status	Rate
WAN	Down	N/A
LAN	Up	100M/Full
WLAN	Up	54M
HomePlug AV	Up	200M

Summary

Any IP Table (Details...)
BW MGMT Monitor (Details...)
DHCP Table (Details...)
WLAN Station Status (Details...)

8 Click the **WLAN Station Status** hyperlink in the AP’s **Status** screen. You can see if any wireless client has connected to the AP.

Figure 37 AP: Status: WLAN Station Status



Association List

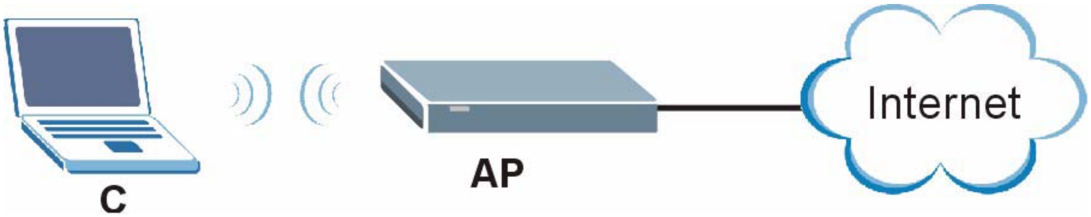
#	MAC Address	Association Time
001	00:13:49:63:3f:5e	00:18:23 2000/01/01

6.3 Configuring the Wireless Client

This section describes how to connect the wireless client to a network.

6.3.1 Connecting to a Wireless LAN

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labelled **C** and the access point is labelled **AP**.



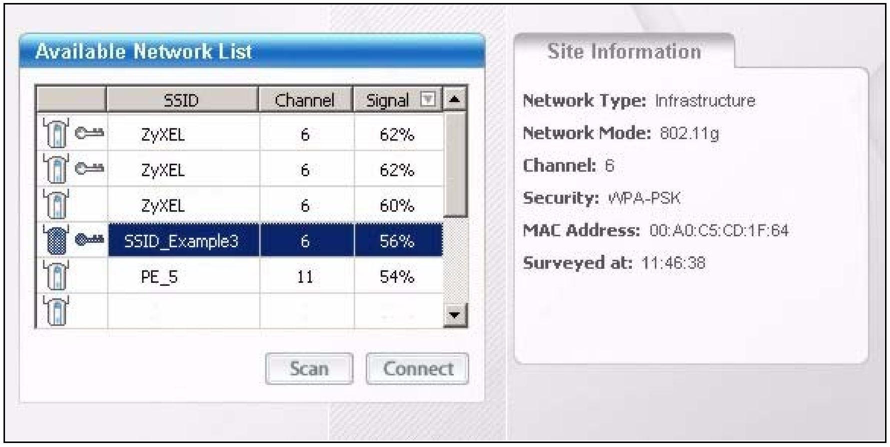
There are three ways to connect the client to an access point.

- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is “SSID_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey”.

After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.



Available Network List

	SSID	Channel	Signal
	ZyXEL	6	62%
	ZyXEL	6	62%
	ZyXEL	6	60%
	SSID_Example3	6	56%
	PE_5	11	54%

Site Information

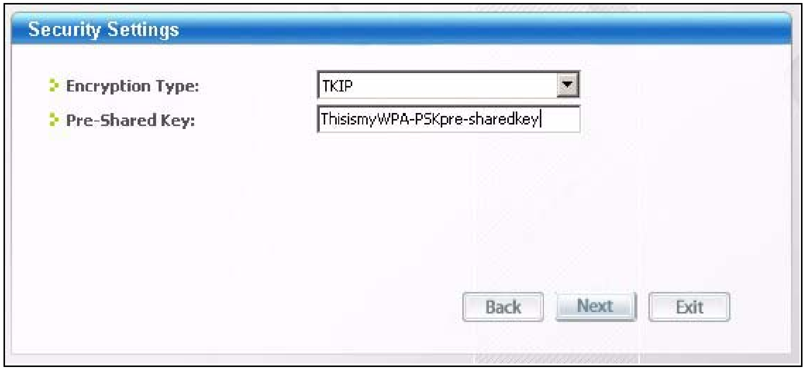
Network Type: Infrastructure
Network Mode: 802.11g
Channel: 6
Security: WPA-PSK
MAC Address: 00:A0:C5:CD:1F:64
Surveyed at: 11:46:38

2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the wireless client closer to the AP or peer computer.

3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

Figure 38 ZyXEL Utility: Security Settings

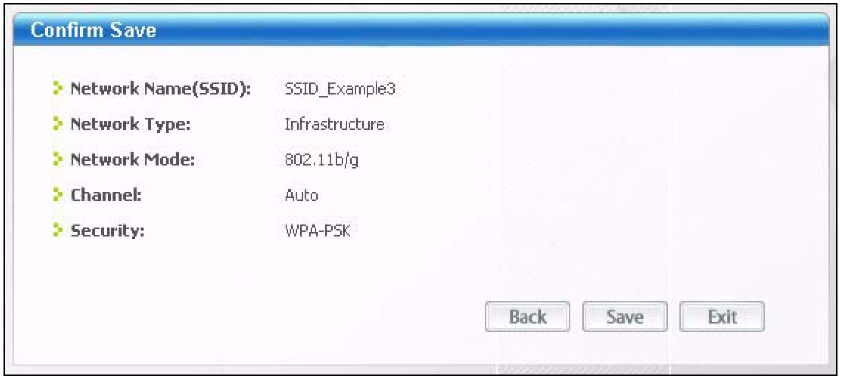


Security Settings

Encryption Type: TKIP
Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

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

Figure 39 ZyXEL Utility: Confirm Save

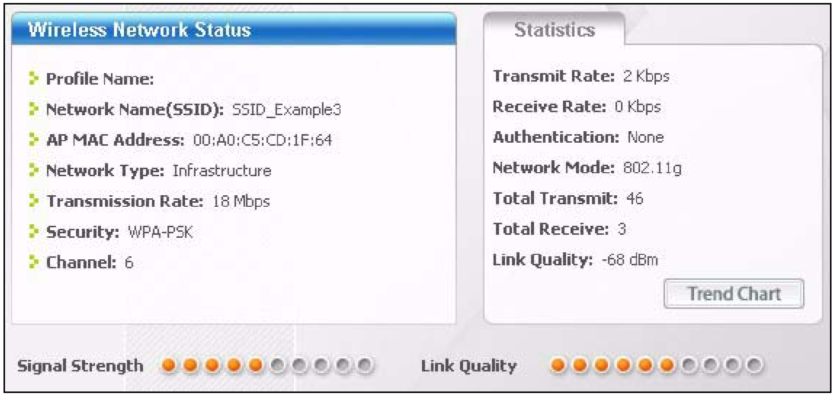


Confirm Save

- Network Name(SSID): SSID_Example3
- Network Type: Infrastructure
- Network Mode: 802.11b/g
- Channel: Auto
- Security: WPA-PSK

5 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.

Figure 40 ZyXEL Utility: Link Info



Wireless Network Status

- Profile Name:
- Network Name(SSID): SSID_Example3
- AP MAC Address: 00:A0:C5:CD:1F:64
- Network Type: Infrastructure
- Transmission Rate: 18 Mbps
- Security: WPA-PSK
- Channel: 6

Statistics

Transmit Rate: 2 Kbps
Receive Rate: 0 Kbps
Authentication: None
Network Mode: 802.11g
Total Transmit: 46
Total Receive: 3
Link Quality: -68 dBm

6 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.

If you cannot access the web site, try changing the encryption type in the **Security Settings** screen, check the Troubleshooting section of this User's Guide or contact your network administrator.

PART II
Network

7

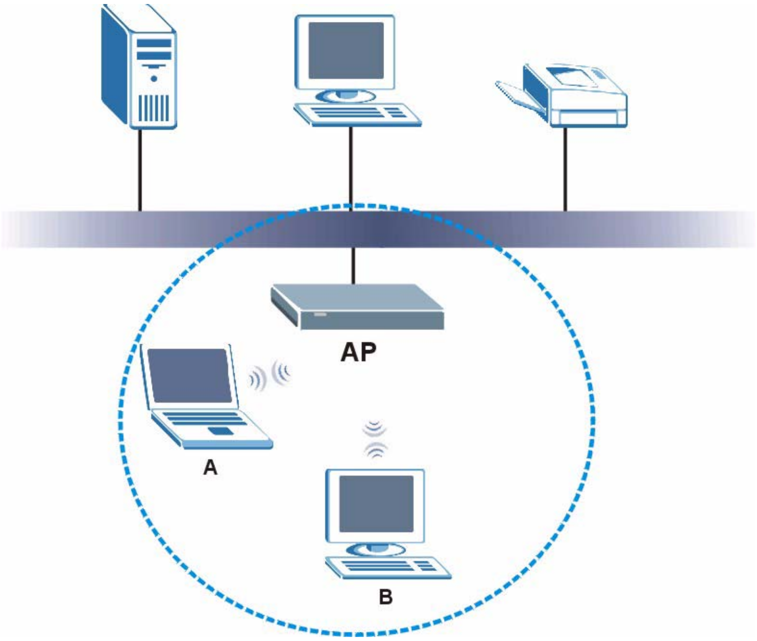
Wireless LAN

This chapter discusses how to configure the wireless network settings in your NBG318S. See the appendices for more detailed information about wireless networks.

7.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 41 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your NBG318S is the AP.

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.

7.2 Wireless Security Overview

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

7.2.1 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.

7.2.2 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 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.

7.2.3 User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

[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.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

Local user databases also have an additional limitation that is explained in the next section.

7.2.4 Encryption

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

The types of encryption you can choose depend on the type of user authentication. (See Section 7.2.3 on page 82 for information about this.)

Table 24 Types of Encryption for Each Type of Authentication

		RADIUS SERVER
Weakest	No Security	WPA
↕	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

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

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

It is recommended that wireless networks use **WPA-PSK**, **WPA**, 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.

It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

When you select **WPA2** or **WPA2-PSK** in your NBG318S, 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** or **WPA2** (depending on the type of wireless network login) and select the **WPA Compatible** option in the NBG318S.

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.

7.3 Quality of Service

This section discusses the Quality of Service (QoS) features available on the NBG318S.

7.3.1 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) ensures quality of service in wireless networks. It controls WLAN transmission priority on packets to be transmitted over the wireless network.

WMM QoS prioritizes wireless traffic according to delivery requirements. WMM QoS is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.

On APs without WMM QoS, all traffic streams are given the same access priority to the wireless network. If the introduction of another traffic stream creates a data transmission demand that exceeds the current network capacity, then the new traffic stream reduces the throughput of the other traffic streams.

The NBG318S uses WMM QoS to prioritize traffic streams according to the IEEE 802.1q tag or DSCP information in each packet's header. The NBG318S automatically determines the priority to use for an individual traffic stream. This prevents reductions in data transmission for applications that are sensitive to latency (delay) and jitter (variations in delay).

7.3.1.1 WMM QoS Priorities

The following table describes the WMM QoS priority levels that the NBG318S uses.

Table 25 WMM QoS Priorities

PRIORITY LEVEL	DESCRIPTION
voice (WMM_VOICE)	Typically used for traffic that is especially sensitive to jitter. Use this priority to reduce latency for improved voice quality.
video (WMM_VIDEO)	Typically used for traffic which has some tolerance for jitter but needs to be prioritized over other data traffic.
best effort (WMM_BEST_EFFORT)	Typically used for traffic from applications or devices that lack QoS capabilities. Use best effort priority for traffic that is less sensitive to latency, but is affected by long delays, such as Internet surfing.
background (WMM_BACKGROUND)	This is typically used for non-critical traffic such as bulk transfers and print jobs that are allowed but that should not affect other applications and users. Use background priority for applications that do not have strict latency and throughput requirements.

7.4 WPS Overview

WPS allows you to quickly set up a secure network with other WPS enabled devices, much more easily than manually configuring wireless connections and security through a web configurator.

Your NBG318S uses WPS to set up a secure connection with other WPS enabled wireless devices in two ways. The first method uses a push-button, either physically located on the housing of the wireless devices, or provided as a feature in the device's software. See Section on page 37 for more information on using the **WPS** button on the NBG318S. The second method relies on the exchanging of PINs (Personal Identification Numbers) between wireless devices. Both methods use the WPA(2) security standard, which uses a pre-shared key to encrypt network traffic.

7.4.1 WPS Setup Using a PIN

Each WPS-enabled device has its own PIN (Personal Identification Number). The PIN is located either on the outside of the device - the NBG318S's WPS default PIN is on a label on the bottom panel, or on the device's configuration interface similar to the NBG318S's web configurator.

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you may need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between the NBG318S and another WPS-enabled device (called a wireless client) using the PIN method.

1. Find the NBG318S's WPS PIN. The default PIN is on a label on the NBG318S's bottom panel. You can use this if the PIN is still at its default setting. You can find the most up-to-date PIN in Section 7.4 on page 85.
2. Look for the WPS PIN on the wireless client; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN).
3. Enter the NBG318S's PIN in the configuration interface of the wireless client. For the NBG318S, see Section 7.9 on page 101. You can also enter the PIN of the client in the NBG318S (see Section 7.10 on page 103) - it does not matter which method you use.
4. Start WPS on both devices within two minutes (for example, by clicking Start or Apply).

Use the configuration utility to activate WPS, not the push-button on the device itself. Also, you cannot press the WPS button on one device and use the PIN on another device to connect the two devices.

5 On a computer connected to the wireless client, try logging into the NBG318S's web configurator. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

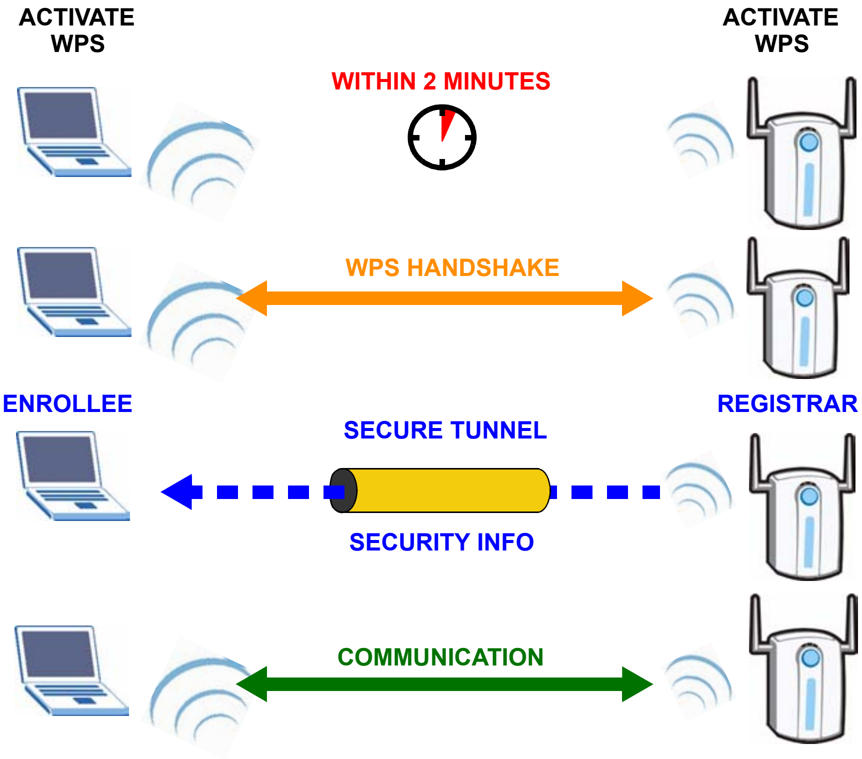
If you cannot connect using WPS, check both devices' configuration interfaces to ensure WPS is enabled on both devices. If that doesn't work, check you are using the correct PIN. After you have generated a new PIN (see Section 7.9 on page 101) the default PIN on the attached label is no longer valid.

7.4.2 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 42 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

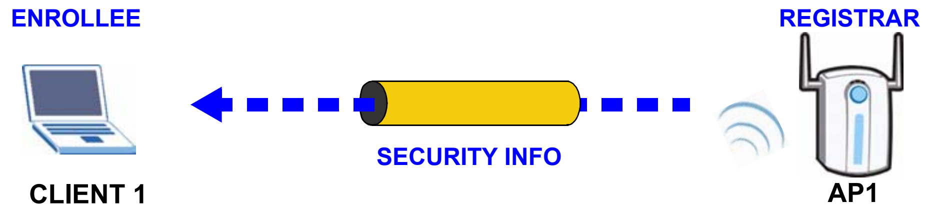
By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

7.4.2.1 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

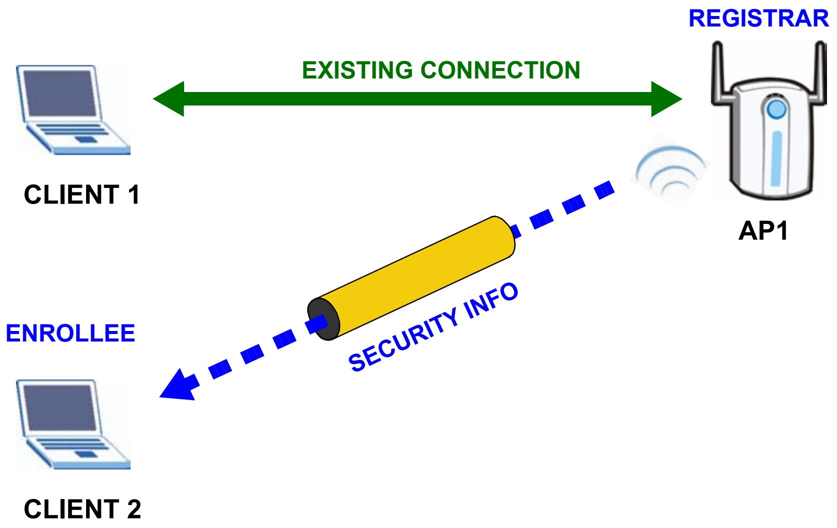
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 43 WPS: Example Network Step 1



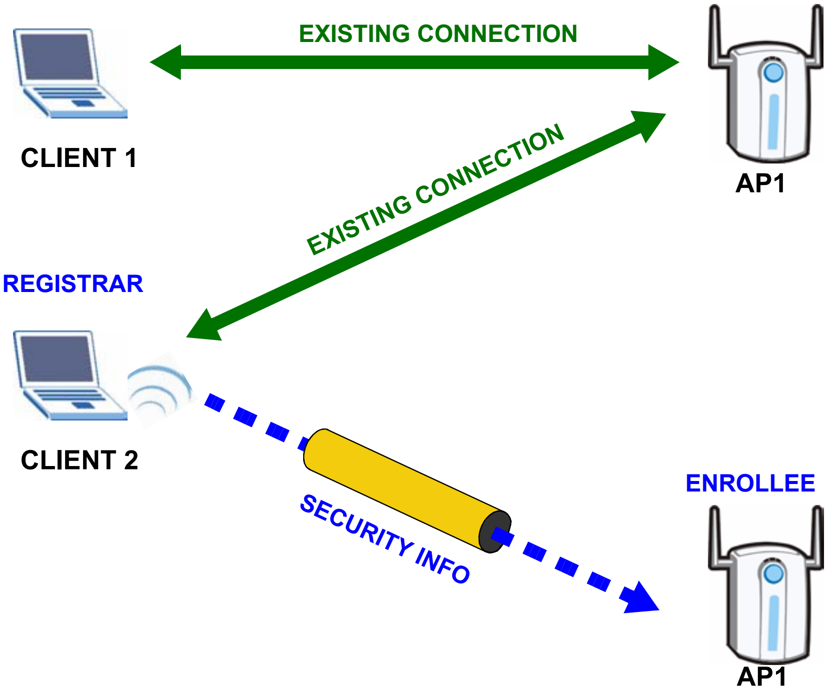
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 44 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 45 WPS: Example Network Step 3



7.4.3 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

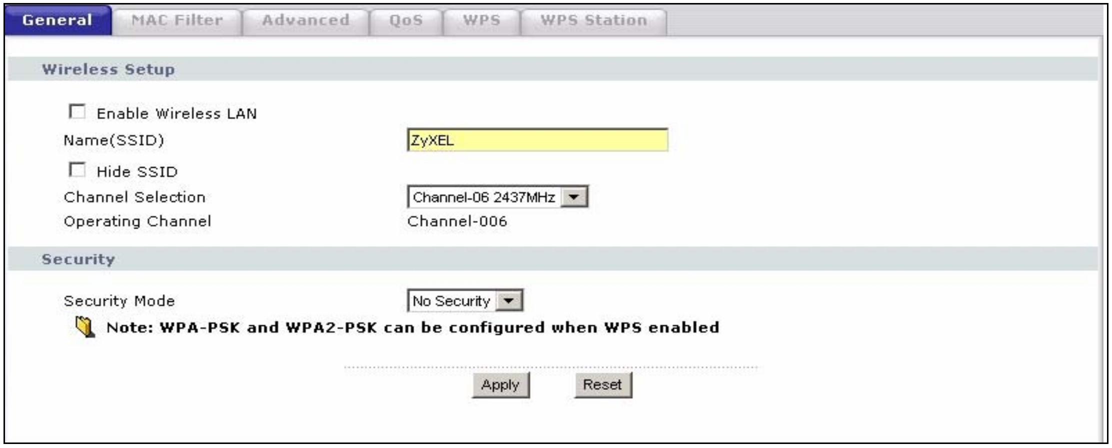
  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices (see Section 7.5.3 on page 93 for information on pre-shared keys). Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).
- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

7.5 General Wireless LAN Screen

If you are configuring the NBG318S from a computer connected to the wireless LAN and you change the NBG318S'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 NBG318S's new settings.

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

Figure 46 Network > Wireless LAN > General



Wireless Setup

□ Enable Wireless LAN

Name(SSID): ZyXEL

□ Hide SSID

Channel Selection: Channel-06 2437MHz

Operating Channel: Channel-006

Security

Security Mode: No Security

Note: WPA-PSK and WPA2-PSK can be configured when WPS enabled

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

Table 26 Network > Wireless LAN > General

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate wireless LAN.
Name(SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
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.
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 whether you are using A or B/G frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels.
Operating Channel	This displays the channel the NBG318S is currently using.
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to reload the previous configuration for this screen.

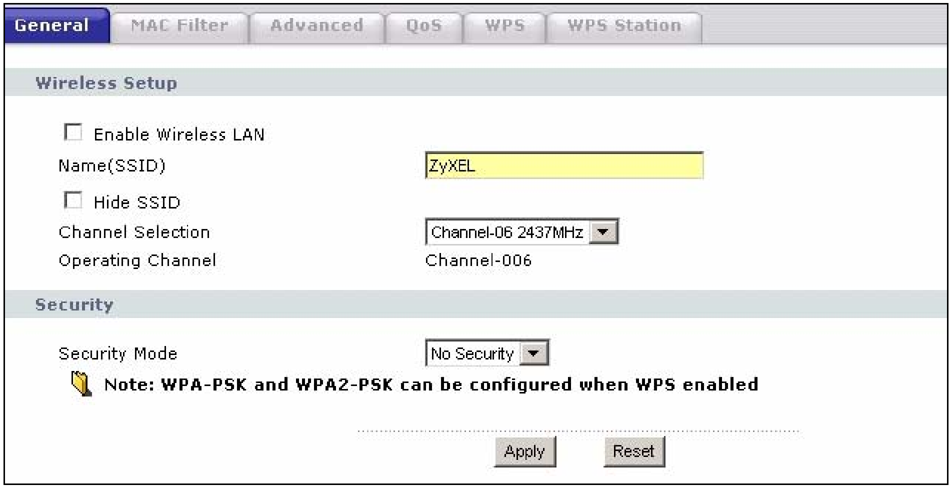
See the rest of this chapter for information on the other labels in this screen.

7.5.1 No Security

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

If you do not enable any wireless security on your NBG318S, your network is accessible to any wireless networking device that is within range.

Figure 47 Network > Wireless LAN > General: No Security



□ Enable Wireless LAN

Name(SSID): ZyXEL

□ Hide SSID

Channel Selection: Channel-06 2437MHz

Operating Channel: Channel-006

Security Mode: No Security

Note: WPA-PSK and WPA2-PSK can be configured when WPS enabled

The following table describes the labels in this screen.

Table 27 Wireless 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 NBG318S.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5.2 WEP Encryption

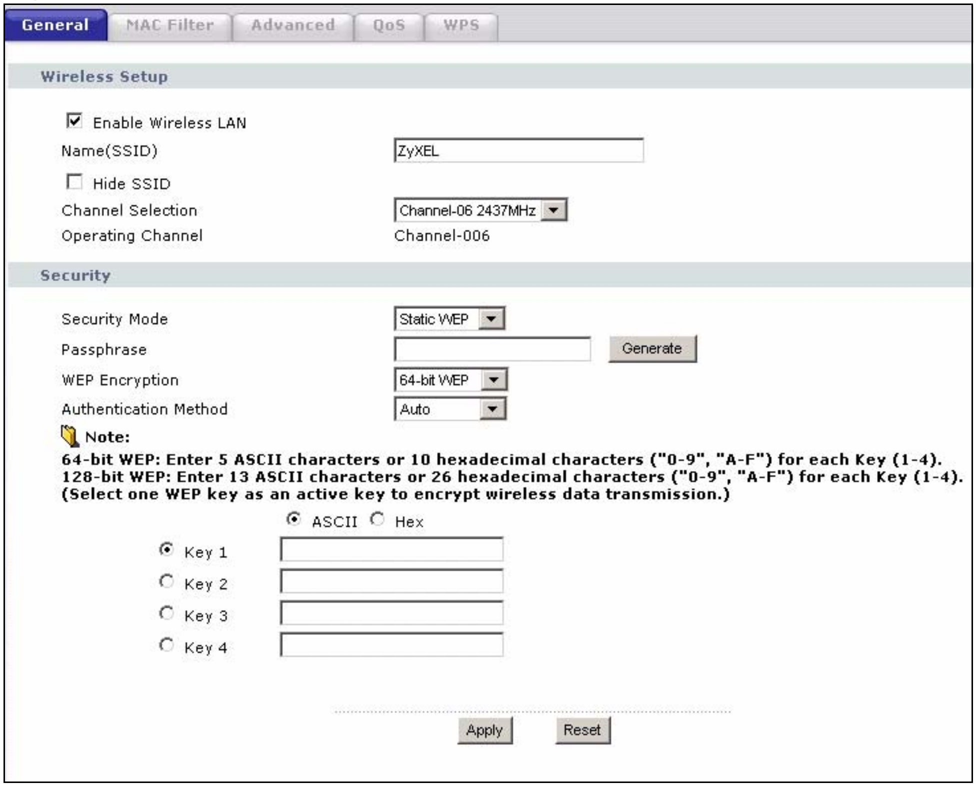
WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your NBG318S allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

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

If the WPS is enabled, WEP encryption is not available from the drop-down menu. Disable WPS for the WEP screen to appear.

Figure 48 Network > Wireless LAN > General: Static WEP



Wireless Setup

☑ Enable Wireless LAN

Name(SSID) ZyXEL

□ Hide SSID

Channel Selection Channel-06 2437MHz

Operating Channel Channel-006

Security

Security Mode Static WEP

Passphrase

WEP Encryption 64-bit WEP

Authentication Method Auto

Note:
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1

○ Key 2

○ Key 3

○ Key 4

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

Table 28 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Passphrase	Enter a passphrase (password phrase) of up to 32 printable characters and click **Generate**. The NBG318S automatically generates four different WEP keys and displays them in the **Key** fields below.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Authentication Method	This field is activated when you select **64-bit WEP** or **128-bit WEP** in the **WEP Encryption** field. Select **Auto**, **Open System** or **Shared Key** from the drop-down list box.
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.

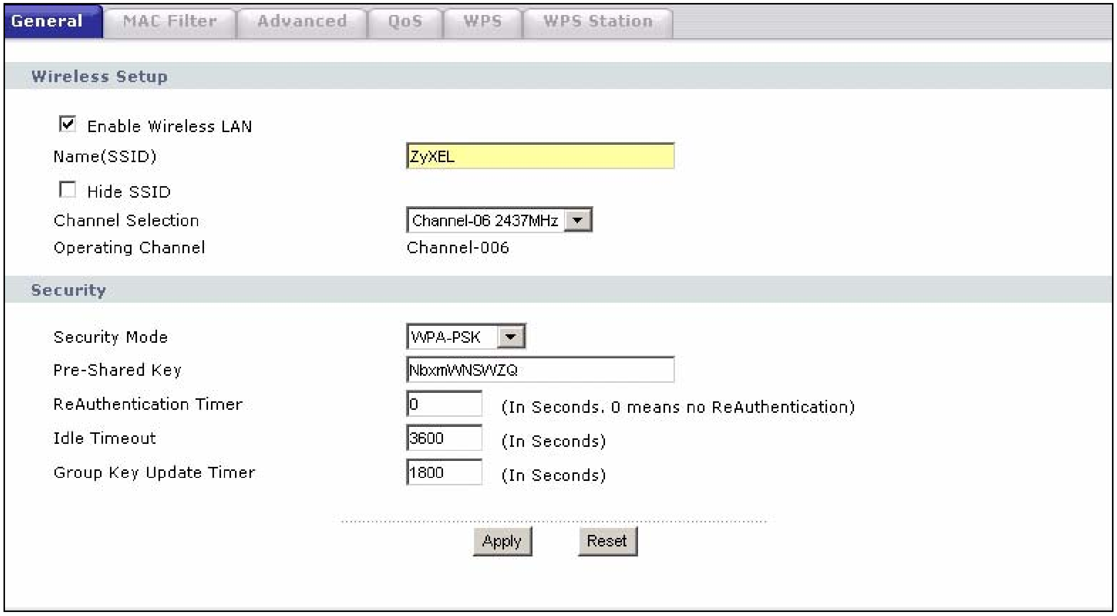
Table 28 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the NBG318S and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5.3 WPA-PSK/WPA2-PSK

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

Figure 49 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK



Wireless Setup

☑ Enable Wireless LAN

Name(SSID) ZyXEL

□ Hide SSID

Channel Selection Channel-06 2437MHz

Operating Channel Channel-006

Security

Security Mode WPA-PSK

Pre-Shared Key NbxmWNSWZQ

ReAuthentication Timer 0 (In Seconds, 0 means no ReAuthentication)

Idle Timeout 3600 (In Seconds)

Group Key Update Timer 1800 (In Seconds)

The following table describes the labels in this screen.

Table 29 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the NBG318S even when the NBG318S is using WPA2-PSK or WPA2.
Pre-Shared Key	The encryption mechanisms used for **WPA/WPA2** and **WPA-PSK/WPA2-PSK** are the same. The only difference between the two is that **WPA-PSK/WPA2-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).

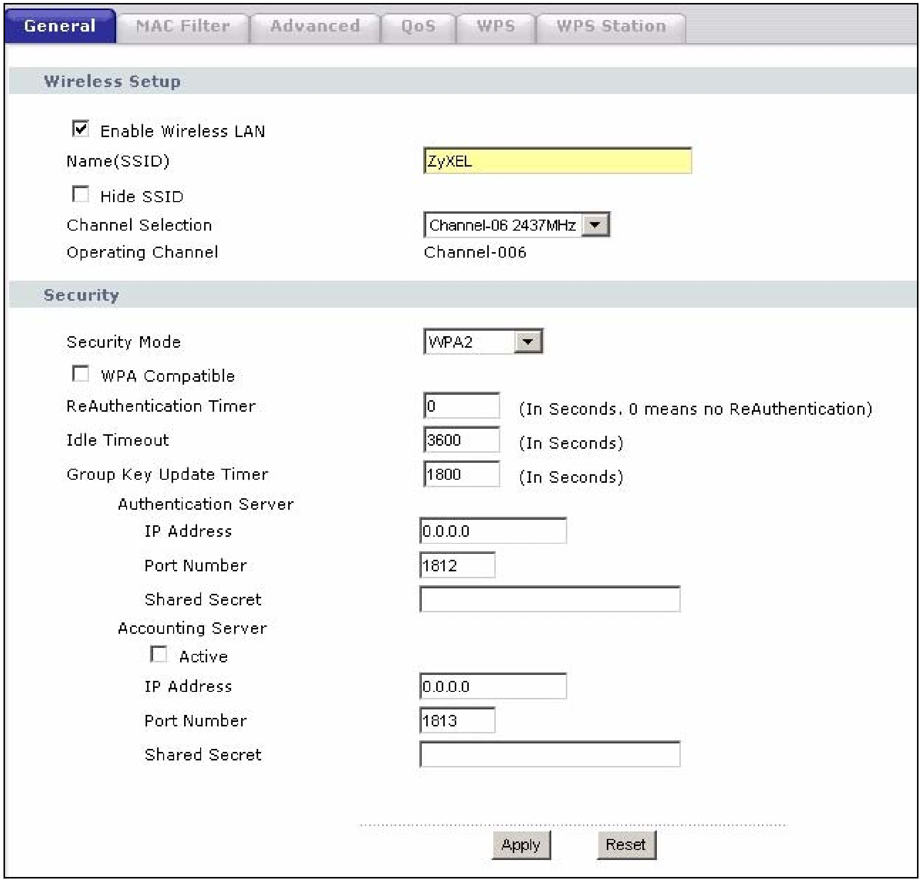
Table 29 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The NBG318S automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK/ WPA2-PSK** key management) or RADIUS server (if using **WPA/WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA-PSK/WPA2-PSK** mode. The default is **1800** seconds (30 minutes).
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5.4 WPA/WPA2

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

Figure 50 Network > Wireless LAN > General: WPA/WPA2



Wireless Setup

☑ Enable Wireless LAN

Name(SSID): ZyXEL

□ Hide SSID

Channel Selection: Channel-06 2437MHz

Operating Channel: Channel-006

Security

Security Mode: WPA2

□ WPA Compatible

ReAuthentication Timer: 0 (In Seconds, 0 means no ReAuthentication)

Idle Timeout: 3600 (In Seconds)

Group Key Update Timer: 1800 (In Seconds)

Authentication Server

IP Address: 0.0.0.0

Port Number: 1812

Shared Secret:

Accounting Server

□ Active

IP Address: 0.0.0.0

Port Number: 1813

Shared Secret:

The following table describes the labels in this screen.

Table 30 Network > Wireless LAN > General: WPA/WPA2

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the NBG318S even when the NBG318S is using WPA2-PSK or WPA2.
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The NBG318S automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).

Table 30 Network > Wireless LAN > General: WPA/WPA2

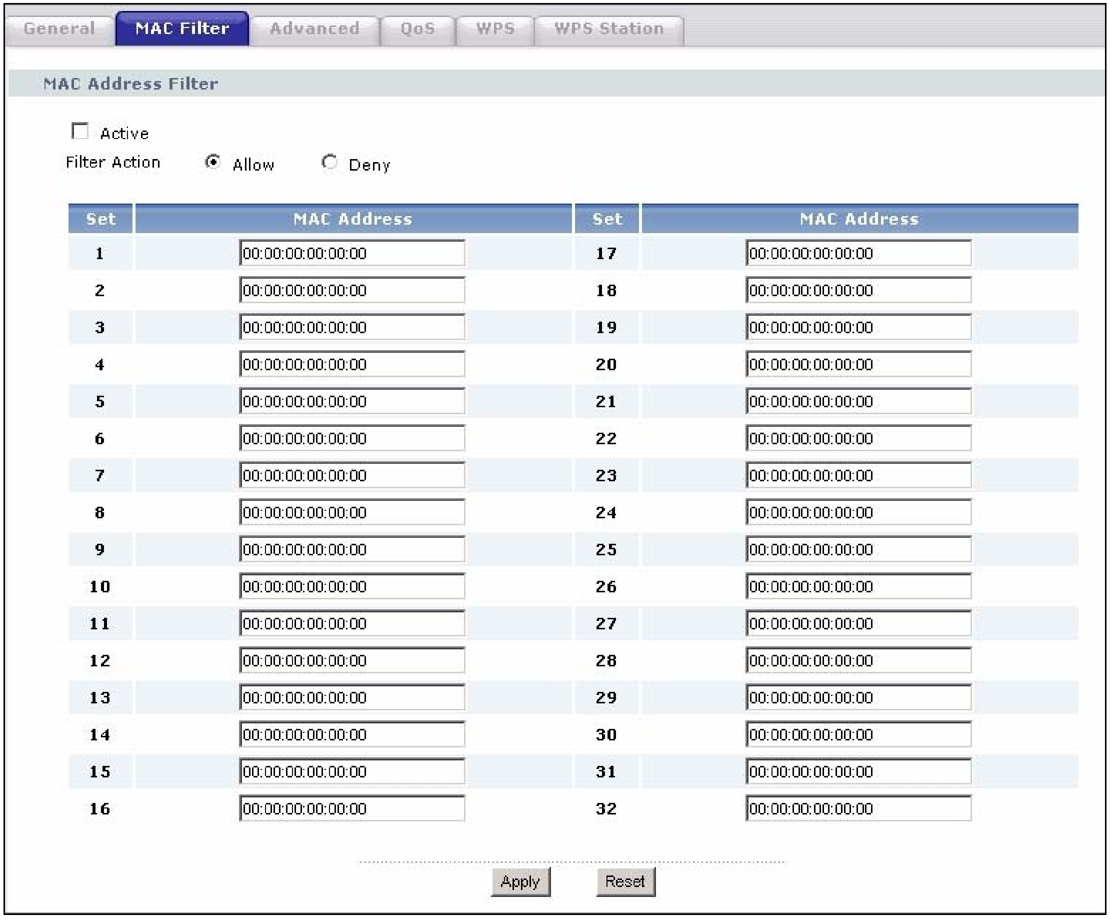
LABEL	DESCRIPTION
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK/WPA2-PSK** key management) or RADIUS server (if using **WPA/WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA-PSK/WPA2-PSK** mode. The NBG318S default is **1800** seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the NBG318S. The key must be the same on the external authentication server and your NBG318S. The key is not sent over the network.
Accounting Server	
Active	Select **Yes** from the drop down list box to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the NBG318S. The key must be the same on the external accounting server and your NBG318S. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.6 MAC Filter

The MAC filter screen allows you to configure the NBG318S to give exclusive access to up to 32 devices (Allow) or exclude up to 32 devices from accessing the NBG318S (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 NBG318S's MAC filter settings, click **Network** > **Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 51 Network > Wireless LAN > MAC Filter



MAC Address Filter

□ Active

Filter Action ● Allow ○ Deny

Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
6	00:00:00:00:00:00	22	00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

The following table describes the labels in this menu.

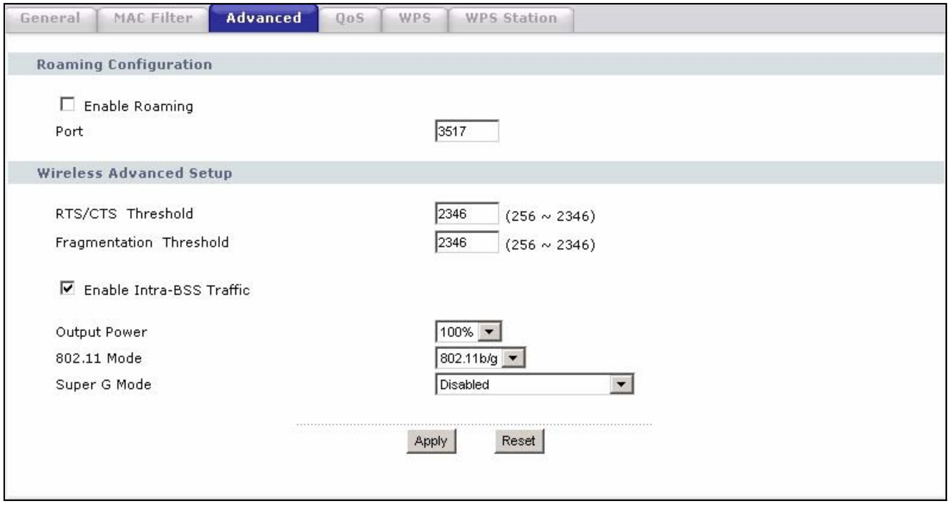
Table 31 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Active	Select **Yes** from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny** to block access to the NBG318S, MAC addresses not listed will be allowed to access the NBG318S Select **Allow** to permit access to the NBG318S, MAC addresses not listed will be denied access to the NBG318S.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the NBG318S 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.
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.7 Wireless LAN Advanced Screen

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

Figure 52 Network > Wireless LAN > Advanced



Roaming Configuration

□ Enable Roaming

Port 3517

Wireless Advanced Setup

RTS/CTS Threshold 2346 (256 ~ 2346)

Fragmentation Threshold 2346 (256 ~ 2346)

☑ Enable Intra-BSS Traffic

Output Power 100%

802.11 Mode 802.11b/g

Super G Mode Disabled

The following table describes the labels in this screen.

Table 32 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Roaming Configuration	
Enable Roaming	Select this option if your network environment has multiple APs and you want your wireless device to be able to access the network as you move between wireless networks.
Wireless Advanced Setup	
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. If the RTS/CTS value is greater than the **Fragmentation Threshold** value, then the RTS/CTS handshake will never occur as data frames will be fragmented before they reach RTS/CTS size. Enter a value between 0 and 2432.
Fragmentation Threshold	It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
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 NBG318S in this field. If there is a high density of APs within an area, decrease the output power of the NBG318S to reduce interference with other APs.
802.11 Mode	Select **802.11b** to allow only IEEE 802.11b compliant WLAN devices to associate with the NBG318S. Select **802.11g** to allow only IEEE 802.11g compliant WLAN devices to associate with the NBG318S. Select **802.11b/g** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the NBG318S. The transmission rate of your NBG318S might be reduced.

Table 32 Network > Wireless LAN > Advanced

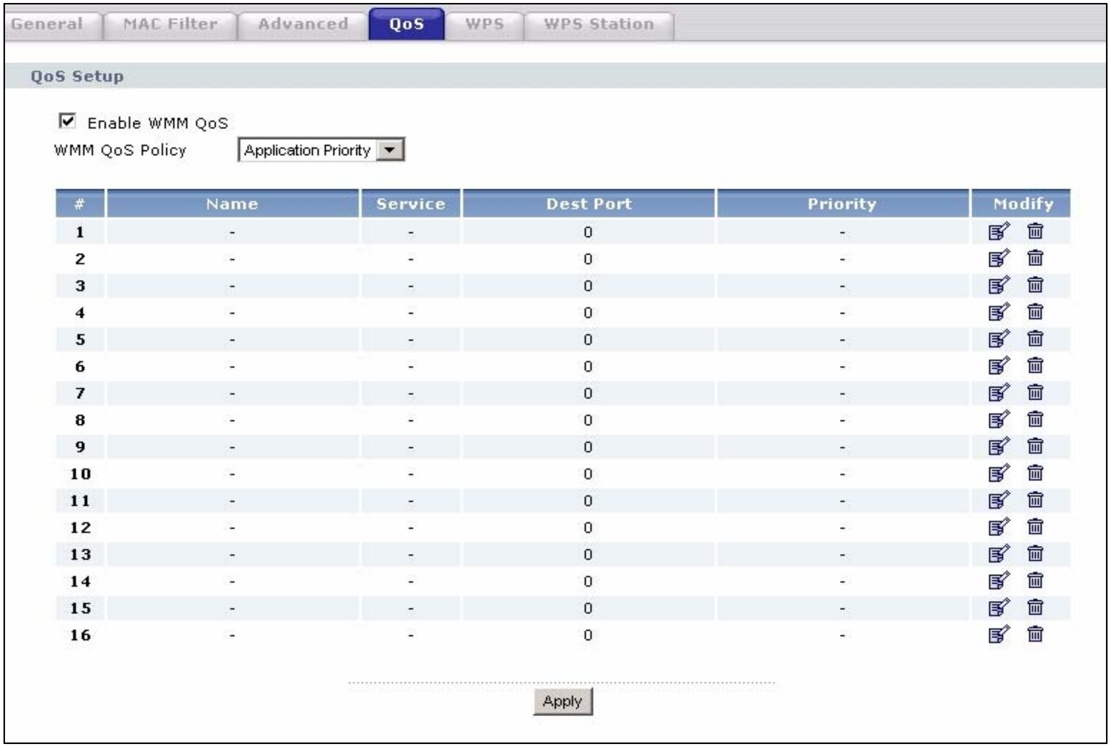
LABEL	DESCRIPTION
Super G Mode	Use this field to enable or disable the Super G function. Super G mode is available only if you select **802.11g** or **802.11b/g** in the **802.11 Mode** field. Super G provides higher data transmission rates than 802.11g. Select **Disabled** if your wireless clients do not support Super G. Select **Super G with Dynamic Turbo** if some or all of your wireless clients support Super G with Dynamic Turbo. Dynamic Turbo uses two channels bonded together to achieve higher transmission rates than 802.11g or Super G without Dynamic Turbo. Dynamic turbo is on only when all wireless devices on the network support it. The wireless channel is automatically fixed at 6 if you select this mode. Select **Super G without Turbo** if the wireless clients on your network support Super G but do not support dynamic turbo.
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.8 Quality of Service (QoS) Screen

The QoS screen allows you to automatically give a service (such as e-mail, VoIP or FTP) a priority level.

Click **Network** > **Wireless LAN** > **QoS**. The following screen appears.

Figure 53 Network > Wireless LAN > QoS



QoS Setup

☑ Enable WMM QoS

WMM QoS Policy: Application Priority

#	Name	Service	Dest Port	Priority	Modify
1	-	-	0	-	✎ 🗑
2	-	-	0	-	✎ 🗑
3	-	-	0	-	✎ 🗑
4	-	-	0	-	✎ 🗑
5	-	-	0	-	✎ 🗑
6	-	-	0	-	✎ 🗑
7	-	-	0	-	✎ 🗑
8	-	-	0	-	✎ 🗑
9	-	-	0	-	✎ 🗑
10	-	-	0	-	✎ 🗑
11	-	-	0	-	✎ 🗑
12	-	-	0	-	✎ 🗑
13	-	-	0	-	✎ 🗑
14	-	-	0	-	✎ 🗑
15	-	-	0	-	✎ 🗑
16	-	-	0	-	✎ 🗑

The following table describes the labels in this screen.

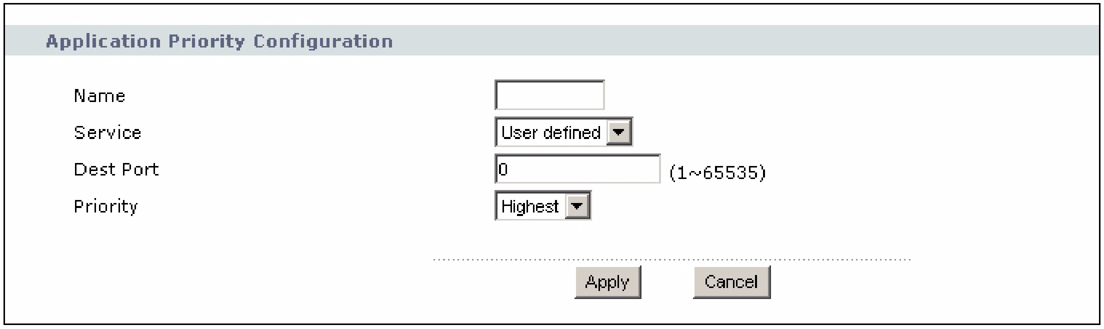
Table 33 Network > Wireless LAN > QoS

	DESCRIPTION
Enable WMM QoS	Select this to turn on WMM QoS (Wireless MultiMedia Quality of Service). The NBG318S assigns priority to packets based on the 802.1q or DSCP information in their headers. If a packet has no WMM information in its header, it is assigned the default priority.
WMM QoS Policy	Select **Default** to have the NBG318S 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. Select **Application Priority** from the drop-down list box to display a table of application names, services, ports and priorities to which you want to apply WMM QoS.
	The table appears only if you select **Application Priority** in **WMM QoS Policy**.
#	This is the number of an individual application entry.
Name	This field displays a description given to an application entry.
Service	This field displays either **FTP**, **WWW**, **E-mail** or a **User Defined** service to which you want to apply WMM QoS.
Dest Port	This field displays the destination port number to which the application sends traffic.
Priority	This field displays the priority of the application. **Highest** - Typically used for voice or video that should be high-quality. **High** - Typically used for voice or video that can be medium-quality. **Mid** - Typically used for applications that do not fit into another priority. For example, Internet surfing. **Low** - Typically used for non-critical “background” applications, such as large file transfers and print jobs that should not affect other applications.
Modify	Click the **Edit** icon to open the **Application Priority Configuration** screen. Modify an existing application entry or create a application entry in the **Application Priority Configuration** screen. Click the **Remove** icon to delete an application entry.
Apply	Click **Apply** to save your changes to the NBG318S.

7.8.1 Application Priority Configuration

Use this screen to edit a WMM QoS application entry. Click the edit icon under **Modify**. The following screen displays.

Figure 54 Network > Wireless LAN > QoS: Application Priority Configuration



Application Priority Configuration

Name	
Service	User defined
Dest Port	0 (1~65535)
Priority	Highest

See Appendix F on page 287 for a list of commonly-used services and destination ports. The following table describes the fields in this screen.

Table 34 Network > Wireless LAN > QoS: Application Priority Configuration

	DESCRIPTION
Application Priority Configuration	
Name	Type a description of the application priority.
Service	The following is a description of the applications you can prioritize with WMM QoS. Select a service from the drop-down list box. • **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: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80 • **FTP** File Transfer Protocol enables fast transfer of files, including large files that it may not be possible to send via e-mail. FTP uses port number 21. • **WWW** The World Wide Web 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. • **User-Defined** User-defined services are user specific services configured using known ports and applications.
Dest Port	This displays the port the selected service uses. Type a port number in the field provided if you want to use a different port to the default port.
Priority	Select a priority from the drop-down list box.
Apply	Click **Apply** to save your changes back to the NBG318S.
Cancel	Click **Cancel** to return to the previous screen.

7.9 WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your NBG318S.

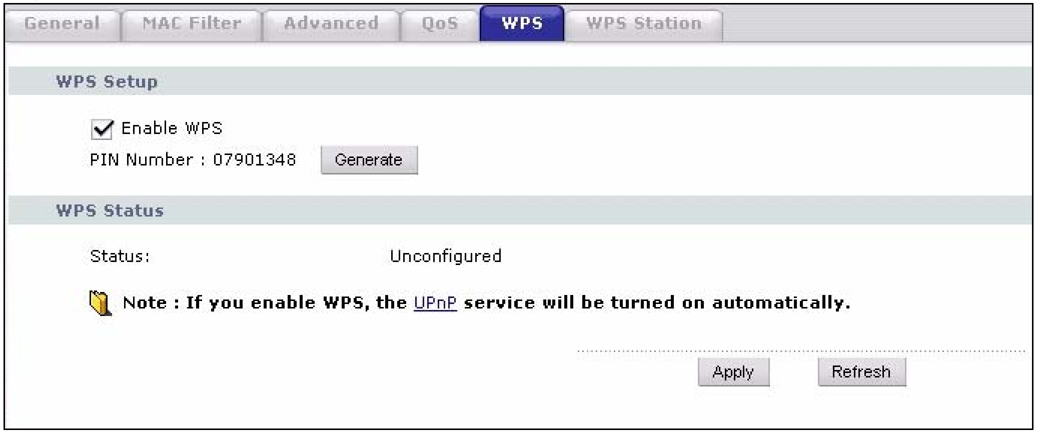
WPS allows you to quickly set up a secure network with other WPS enabled devices, much more easily than manually configuring wireless connections and security through a web configurator.

Your NBG318S uses WPS to set up a secure connection with other WPS enabled wireless devices in two ways. The first method uses a push-button, either physically located on the housing of the wireless devices, or provided as a feature in the device's software. See Section on page 37 for more information on using the **WPS** button on the NBG318S. The second method relies on the exchanging of PINs (Personal Identification Numbers) between wireless devices. Both methods use the WPA(2) security standard, which uses a pre-shared key to encrypt network traffic.

See Section 7.4.1 on page 85 for instruction son how to set up connect two wireless devices with WPS by using the PIN method.

Click **Network** > **Wireless** >**WPS**. The following screen displays.

Figure 55 Network > Wireless > WPS



WPS Setup

☑ Enable WPS

PIN Number : 07901348

WPS Status

Status: Unconfigured

Note : If you enable WPS, the UPnP service will be turned on automatically.

The following table describes the labels in this screen.

Table 35 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Use this to turn WiFi Protected Setup on or off.
PIN Number	This is the PIN (Personal Identification Number) the NBG318S uses to authenticate other WPS-enabled wireless devices. The PIN is not necessary when using WPS's push-button method. Enter this PIN in the configuration utility of the device you want to connect to using WPS. You may need to write this down.
Generate	Click this to have the NBG318S use a different WPS PIN. The new PIN is automatically generated. The NBG318S uses the new PIN once you click **Apply**. To connect additional devices to your NBG318S using WPS you can use the same PIN again or generate a new one for each setup procedure.
WPS Status	
Status	This displays the current WPS configuration status. If no wireless settings (such as security settings) are configured **Unconfigured** displays. Once the WPS process is complete, **Configured** displays in this field.

Table 35 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
Apply	Click this to save your changes to the NBG318S.
Refresh	Click this to reload the information in this screen.

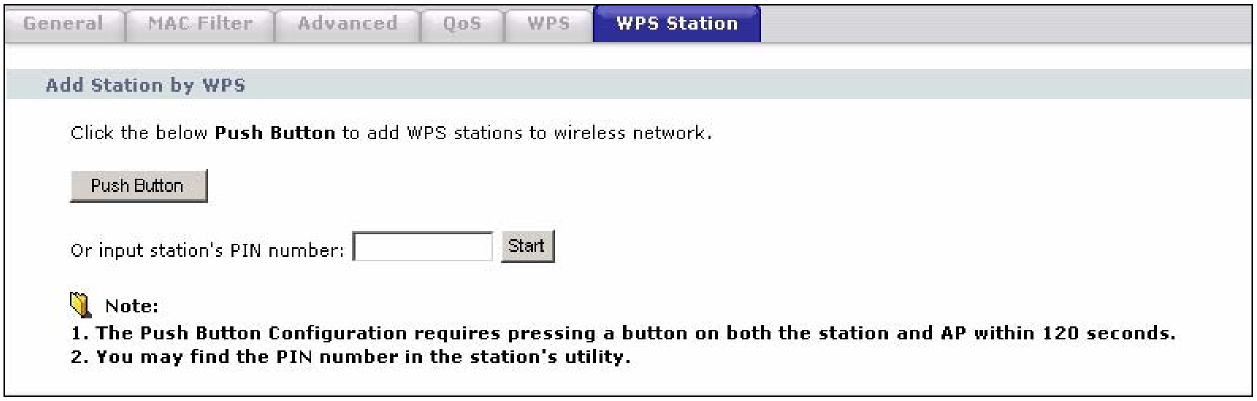
7.10 WPS Station Screen

Use this screen to set up a WPS connection using the Push Button Configuration (PBC) method. You can use the push-button in the screen below or the external push-button on the side of your device, if it has one. See Section 2.2 on page 37 for instructions on using WPS using the external **WPS** button.

You can also use this screen to set up a WPS connection using the PIN of another WPS-enabled device. See Section 7.4.1 on page 85 for instructions on using WPS with a PIN.

Click **Network** > **Wireless LAN** > **WPS Station** for the following screen to display.

Figure 56 Network > Wireless LAN > WPS Station



Add Station by WPS

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

Push Button

Or input station's PIN number: Start

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

The following table describes the labels in this screen.

Table 36 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
Push Button	Click this button to begin the WPS process. You have two minutes to press the button on the device you wish to connect with. This button may either be a physical button on the outside of device, or a menu button similar to the **Push Button** button on this screen.
Or input station's PIN number	Type the PIN of the device that you are setting up a WPS connection with. You can find the PIN either on the outside of the device, or by checking the device's settings. Click **Start** to begin the WPS procedure.

8

WAN

This chapter describes how to configure WAN settings.

8.1 WAN Overview

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

8.2 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 the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

8.3 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.

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. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The NBG318S supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the NBG318S queries all directly connected networks to gather group membership. After that, the NBG318S periodically updates this information. IP multicasting can be enabled/disabled on the NBG318S LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

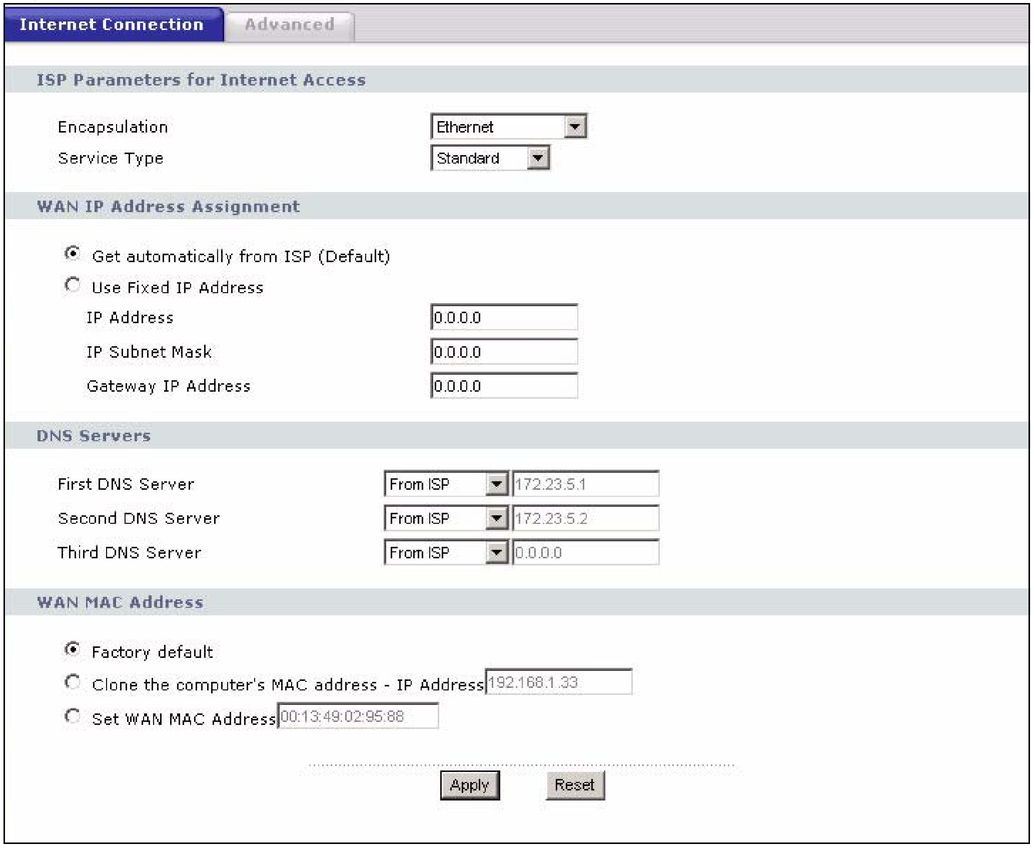
8.4 Internet Connection

Use this screen to change your NBG318S's Internet access settings. Click **Network** > **WAN**. The screen differs according to the encapsulation you choose.

8.4.1 Ethernet Encapsulation

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

Figure 57 Network > WAN > Internet Connection: Ethernet Encapsulation



ISP Parameters for Internet Access

Encapsulation	Ethernet
Service Type	Standard

WAN IP Address Assignment

● Get automatically from ISP (Default)

○ Use Fixed IP Address

IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0

DNS Servers

First DNS Server	From ISP	172.23.5.1
Second DNS Server	From ISP	172.23.5.2
Third DNS Server	From ISP	0.0.0.0

WAN MAC Address

● Factory default

○ Clone the computer's MAC address - IP Address 192.168.1.33

○ Set WAN MAC Address 00:13:49:02:95:88

The following table describes the labels in this screen.

Table 37 Network > WAN > Internet Connection: Ethernet Encapsulation

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from **Standard**, **RR-Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Toshiba** (Roadrunner Toshiba authentication method) or **Telia Login**. The following fields do not appear with the **Standard** service type.
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.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one. This field is not available for **Telia Login**.
Login Server (Telia Login only)	Type the domain name of the Telia login server, for example login1.telia.com.
Relogin Every(min) (Telia Login only)	The Telia server logs the NBG318S out if the NBG318S does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the NBG318S to wait between logins.
WAN IP Address Assignment	
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	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.
DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG318S'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 NBG318S'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	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. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.

Table 37 Network > WAN > Internet Connection: Ethernet Encapsulation

LABEL	DESCRIPTION
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 NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4.2 PPPoE Encapsulation

The NBG318S 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).

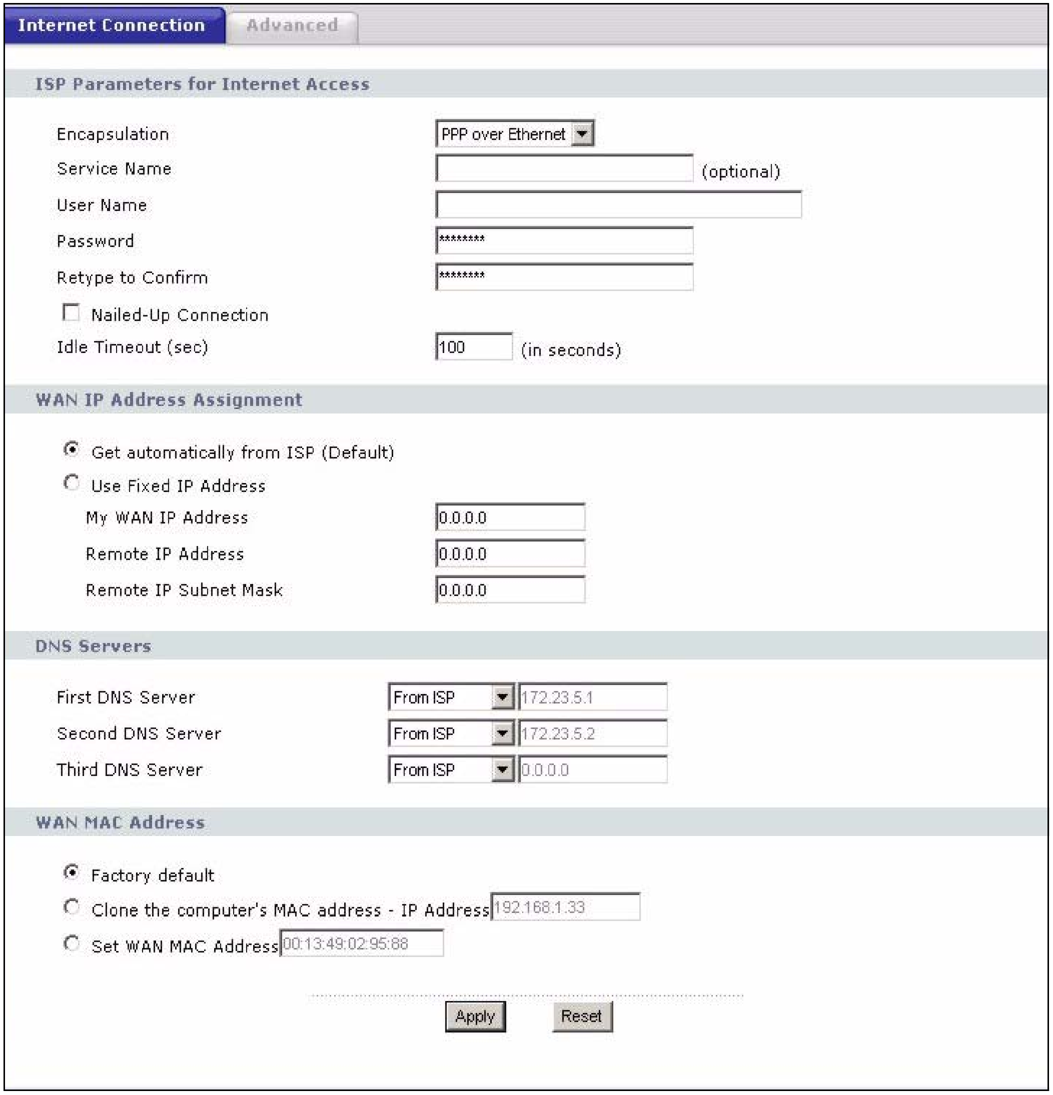
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

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 NBG318S (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG318S 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 58 Network > WAN > Internet Connection: PPPoE Encapsulation



ISP Parameters for Internet Access

Encapsulation: PPP over Ethernet

Service Name: (optional)

User Name:

Password: ********

Retype to Confirm: ********

□ Nailed-Up Connection

Idle Timeout (sec): 100 (in seconds)

WAN IP Address Assignment

● Get automatically from ISP (Default)

○ Use Fixed IP Address

My WAN IP Address: 0.0.0.0

Remote IP Address: 0.0.0.0

Remote IP Subnet Mask: 0.0.0.0

DNS Servers

First DNS Server: From ISP 172.23.5.1

Second DNS Server: From ISP 172.23.5.2

Third DNS Server: From ISP 0.0.0.0

WAN MAC Address

● Factory default

○ Clone the computer's MAC address - IP Address 192.168.1.33

○ Set WAN MAC Address 00:13:49:02:95:88

The following table describes the labels in this screen.

Table 38 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The **PPP over Ethernet** choice is for a dial-up connection using PPPoE. The NBG318S supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/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. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.

Table 38 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
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.
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 seconds that elapses before the router automatically disconnects from the PPPoE server.
WAN IP Address Assignment	
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**.
Remote IP Address	Enter the remote IP address (if your ISP gave you one) in this field.
Remote IP Subnet Mask	Enter the remote IP subnet mask in this field.
DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG318S'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 NBG318S'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	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. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

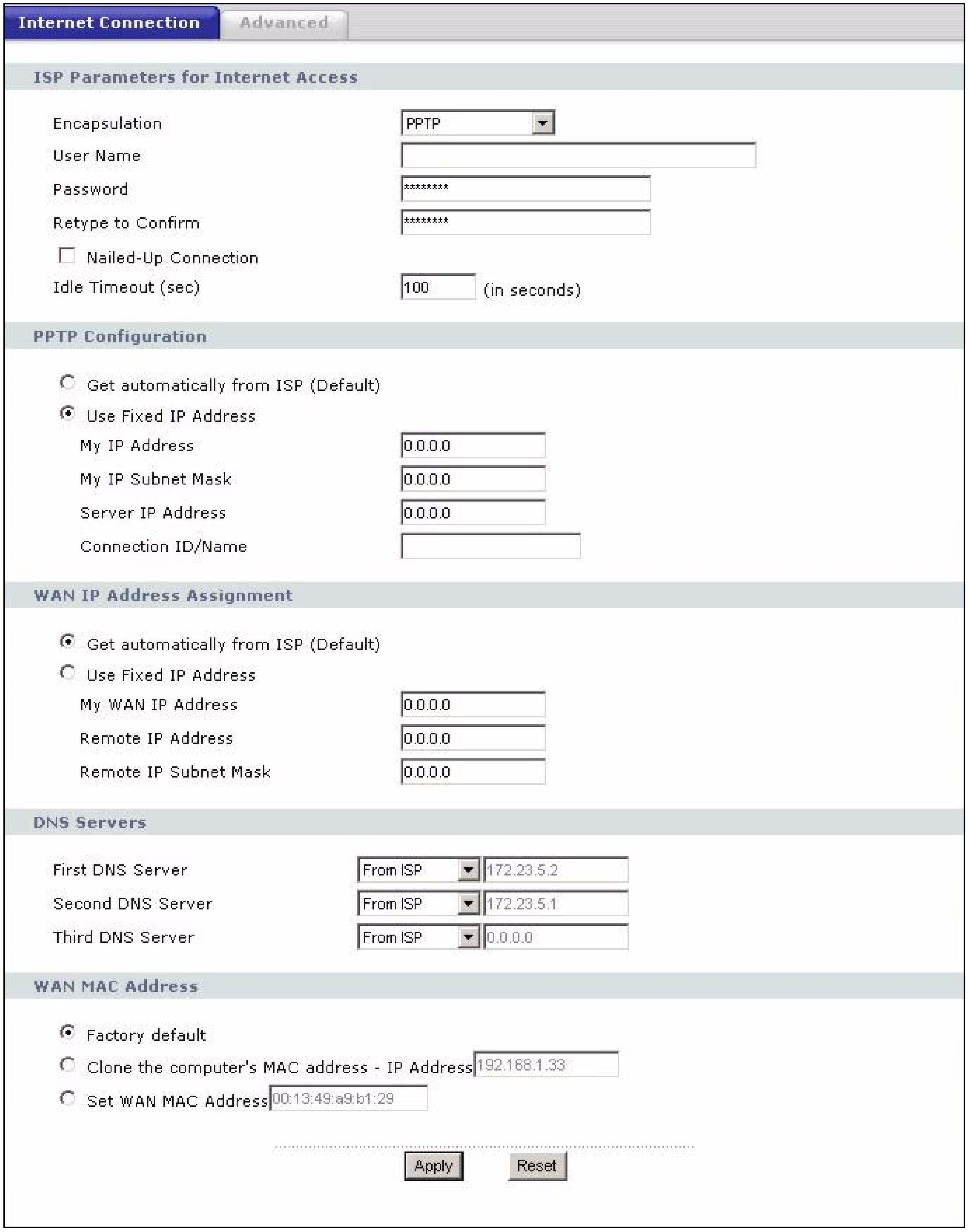
8.4.3 PPTP Encapsulation

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 59 Network > WAN > Internet Connection: PPTP Encapsulation



ISP Parameters for Internet Access

Encapsulation	PPTP
User Name	
Password	********
Retype to Confirm	********
□ Nailed-Up Connection	
Idle Timeout (sec)	100 (in seconds)

PPTP Configuration

○ Get automatically from ISP (Default)
● Use Fixed IP Address

My IP Address	0.0.0.0
My IP Subnet Mask	0.0.0.0
Server IP Address	0.0.0.0
Connection ID/Name	

WAN IP Address Assignment

● Get automatically from ISP (Default)
○ Use Fixed IP Address

My WAN IP Address	0.0.0.0
Remote IP Address	0.0.0.0
Remote IP Subnet Mask	0.0.0.0

DNS Servers

First DNS Server	From ISP	172.23.5.2
Second DNS Server	From ISP	172.23.5.1
Third DNS Server	From ISP	0.0.0.0

WAN MAC Address

● Factory default
○ Clone the computer's MAC address - IP Address 192.168.1.33
○ Set WAN MAC Address 00:13:49:a9:b1:29

The following table describes the labels in this screen.

Table 39 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
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. The NBG318S supports only one PPTP server connection at any given time. 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.
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 seconds that elapses before the NBG318S automatically disconnects from the PPTP server.
PPTP Configuration	
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 IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your NBG318S 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 NBG318S.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Type your identification name for the PPTP server.
WAN IP Address Assignment	
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**.
Remote IP Address	Enter the remote IP address (if your ISP gave you one) in this field.
Remote IP Subnet Mask	Enter the remote IP subnet mask in this field.
DNS Servers	

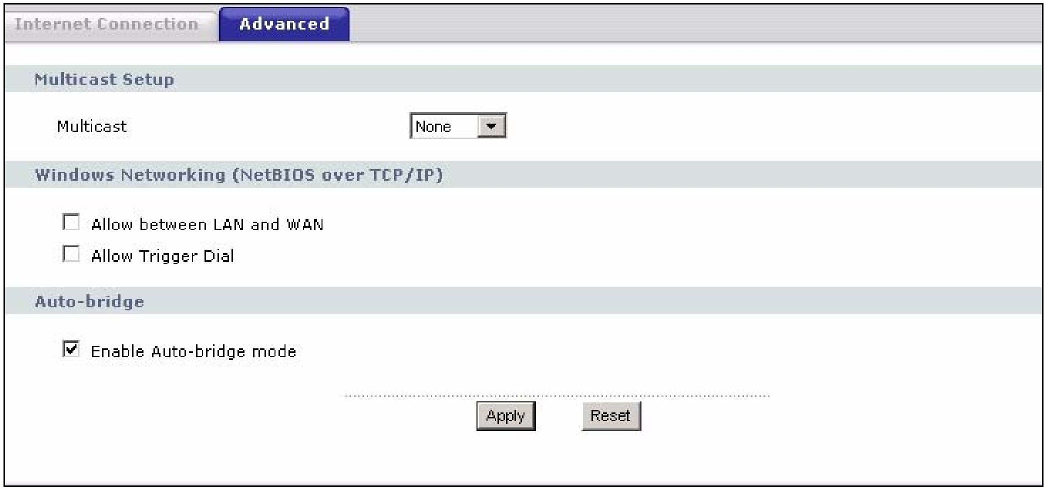
Table 39 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG318S'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 NBG318S'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	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. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

8.5 Advanced WAN Screen

To change your NBG318S's advanced WAN settings, click **Network** > **WAN** > **Advanced**. The screen appears as shown.

Figure 60 Network > WAN > Advanced



Multicast Setup

Multicast: None

Windows Networking (NetBIOS over TCP/IP)

□ Allow between LAN and WAN

□ Allow Trigger Dial

Auto-bridge

☑ Enable Auto-bridge mode

The following table describes the labels in this screen.

Table 40 WAN > Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast	Select **IGMP V-1**, **IGMP V-2** or **None**. 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. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Auto-bridge	
Enable Auto-bridge mode	Select **Enable Auto-bridge mode** to allow the NBG318S to automatically configure itself as a bridge between two networks when it receives an IP address in the range 192.168.0.0 ~ 192.168.9.9. In wireless networks it sets itself as an AP, in wired networks it acts as a switch. NAT, the DHCP server and IP routing are disabled in this mode.
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

9

LAN

This chapter describes how to configure LAN settings.

9.1 LAN Overview

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.

9.1.1 IP Pool Setup

The NBG318S 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 NBG318S 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.

9.1.2 System DNS Servers

Refer to the IP address and subnet mask section in the **Connection Wizard** chapter.

9.2 LAN TCP/IP

The NBG318S has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

9.2.1 Factory LAN Defaults

The LAN parameters of the NBG318S 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.

9.2.2 IP Address and Subnet Mask

Refer to the IP address and subnet mask section in the **Connection Wizard** chapter for this information.

9.2.3 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.

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. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The NBG318S supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the NBG318S queries all directly connected networks to gather group membership. After that, the NBG318S periodically updates this information. IP multicasting can be enabled/disabled on the NBG318S LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

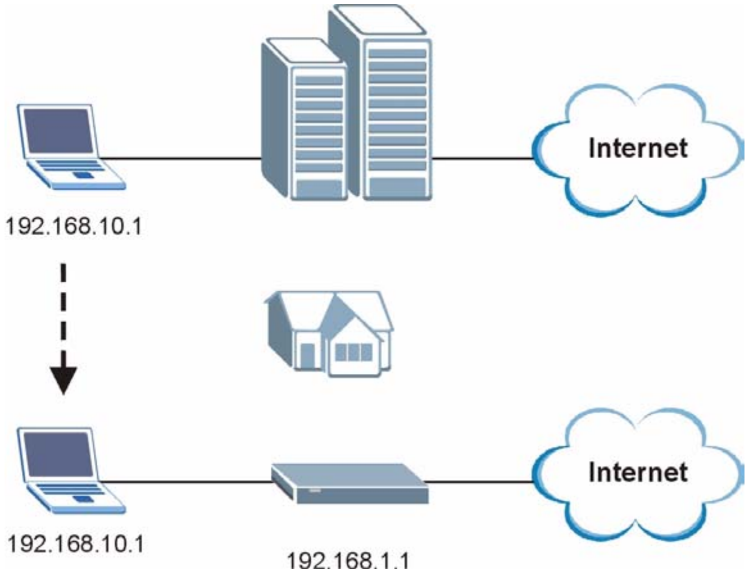
9.2.4 Any IP

Traditionally, you must set the IP addresses and the subnet masks of a computer and the NBG318S to be in the same subnet to allow the computer to access the Internet (through the NBG318S). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the NBG318S.

With the Any IP feature and NAT enabled, the NBG318S allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the NBG318S are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the NBG318S and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a NBG318S is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the NBG318S are not in the same subnet.

Figure 61 Any IP Example



The Any IP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the NBG318S's IP address.

You *must* enable NAT to use the Any IP feature on the NBG318S.

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the NBG318S) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the NBG318S.

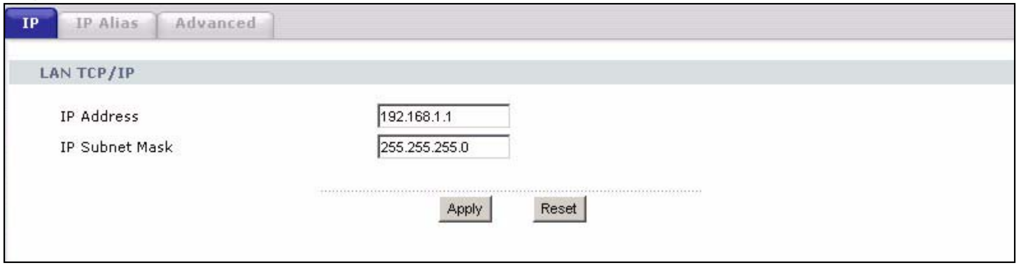
1. When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the NBG318S) by looking at the MAC address in its ARP table.
2. When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.
3. The NBG318S receives the ARP request and replies to the computer with its own MAC address.
4. The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the NBG318S.
5. When the NBG318S receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

After all the routing information is updated, the computer can access the NBG318S and the Internet as if it is in the same subnet as the NBG318S.

9.3 LAN IP Screen

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

Figure 62 Network > LAN > IP



LAN TCP/IP

IP Address 192.168.1.1

IP Subnet Mask 255.255.255.0

The following table describes the labels in this screen.

Table 41 Network > LAN > IP

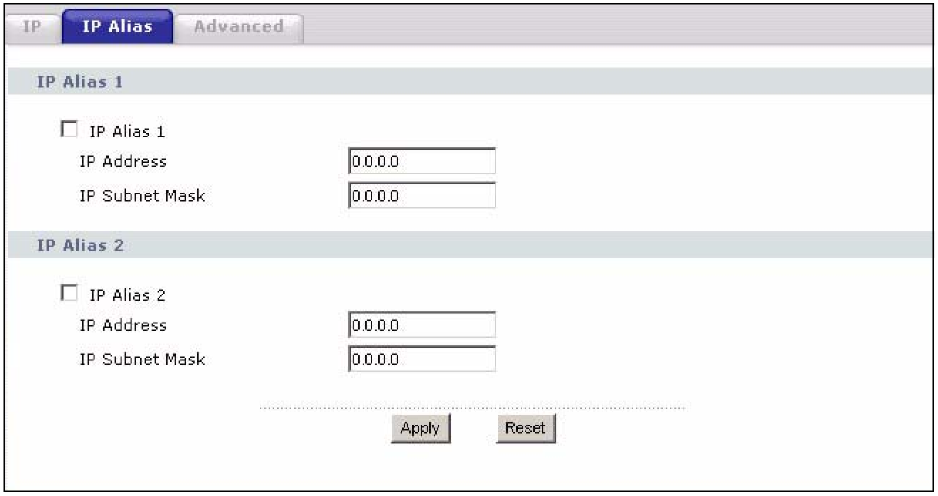
LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Type the IP address of your NBG318S in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG318S will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG318S.
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

9.4 LAN IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The NBG318S supports three logical LAN interfaces via its single physical Ethernet interface with the NBG318S itself as the gateway for each LAN network.

To change your NBG318S's IP alias settings, click **Network** > **LAN** > **IP Alias**. The screen appears as shown.

Figure 63 Network > LAN > IP Alias



IP Alias 1

□ IP Alias 1

IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

IP Alias 2

□ IP Alias 2

IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

The following table describes the labels in this screen.

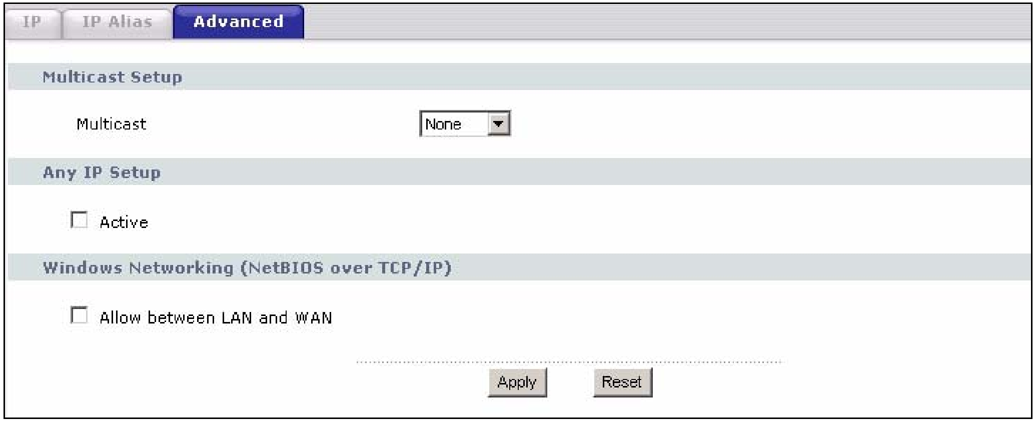
Table 42 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias 1,2	Select the check box to configure another LAN network for the NBG318S.
IP Address	Enter the IP address of your NBG318S in dotted decimal notation.
IP Subnet Mask	Your NBG318S 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 NBG318S.
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

9.5 Advanced LAN Screen

To change your NBG318S's advanced IP settings, click **Network** > **LAN** > **Advanced**. The screen appears as shown.

Figure 64 Network > LAN > Advanced



Multicast Setup

Multicast: None

Any IP Setup

□ Active

Windows Networking (NetBIOS over TCP/IP)

□ Allow between LAN and WAN

The following table describes the labels in this screen.

Table 43 Network > LAN > Advanced

LABEL	DESCRIPTION
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. 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. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Any IP Setup	
Active	Select this if you want to let computers on different subnets use the NBG318S.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

10

HomePlug AV

This chapter introduces the main applications and management of the powerline feature.

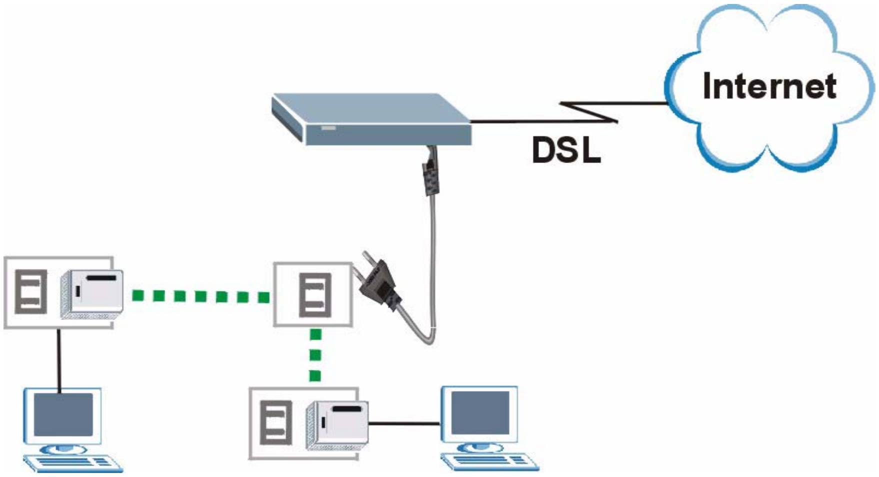
10.1 Overview

The NBG318S is a HomePlug AV compliant powerline Ethernet adapter. The NBG318S and other HomePlug AV powerline adapters in your network communicate with each other by sending and receiving information over your home's electrical wiring.

The NBG318S plugs into an ordinary outlet to create a new network which can extend to any other electrical outlet in any room of a house.

The following section shows you a typical application.

Figure 65 Expand Your Network



To set up your powerline network do the following.

1. Connect your NBG318S to the Internet.
2. Then plug your NBG318S into a power outlet.

The NBG318S is ready for connection on a powerline network.

3. Connect another HomePlug AV compatible adapter to a computer and then plug it in on the same home or office wiring.

After configuring the settings on all adapters (see Section 10.3 on page 124) your computer can now connect to the powerline network and to the Internet. Your powerline network can be further expanded by plugging additional powerline adapters into other outlets in your home and connecting other computers or network devices (for example, a printer) to them.

In this User’s Guide the electrical wiring network may be referred to as the “powerline network”.

✍ Your NBG318S is only compatible with ZyXEL HomePlug AV products with the latest firmware. You can upgrade your other ZyXEL HomePlug AV products by downloading the latest firmware from the ZyXEL website (www.zyxel.com).

10.2 Privacy and Powerline Adapters

When the NBG318S communicates with each other HomePlug AV compliant powerline adapters, they use encryption to scramble the information that is sent in the powerline network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message. The HomePlug AV standard uses 128-bit AES (Advanced Encryption Standard) to safely transmit data between powerline adapters.

For the NBG318S and powerline adapters to communicate with each other they all need to use the same Network Membership Key (NMK). Otherwise, they cannot unscramble the encrypted data sent in the powerline network.

The NMK is derived from the network password you assign to the NBG318S and powerline adapters. By default all HomePlug powerline adapters are configured with the network password **HomePlugAV**. This allows all HomePlug powerline adapters and the NBG318S to communicate with each other without any software configuration. This also means that if you don’t change the network password, any HomePlug AV powerline adapter connected to your powerline circuit can see your network data.

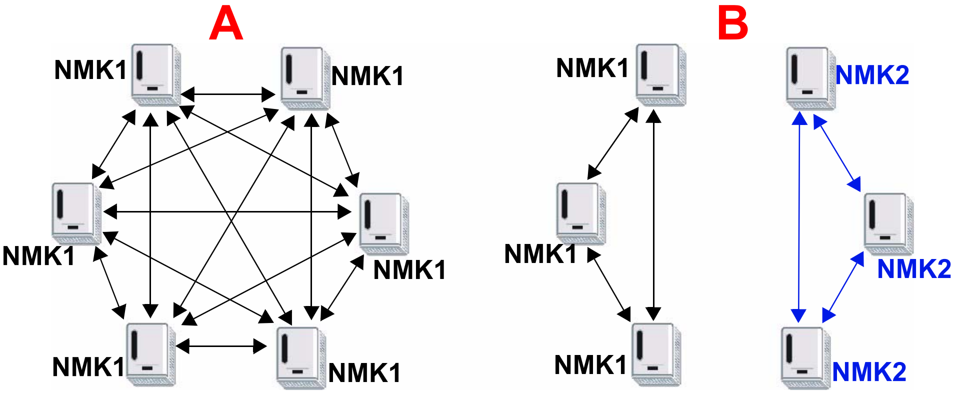
✍ **Change the network password on your powerline adapters to ensure secure data transmission on your powerline network.**

10.2.1 Setting Up a Private Powerline Network

To prevent others compromising your network security, you can create a private network. Create a private network by changing the network password only on the powerline adapters you want to communicate in your network. The NBG318S and powerline adapters convert the network password to a Network Membership Key (NMK). Only the powerline adapters with the same NMK can communicate in your network.

The following figure shows a scenario **A** - where all the powerline adapters have the same NMK (**NMK1**) and scenario **B** - where some adapters use **NMK1** and some use **NMK2**.

Figure 66 Powerline Network Scenario



In both cases the powerline adapters reside on the same electrical circuit. In scenario **A** all the powerline adapters can communicate with each other. In scenario **B** only the adapters with the same NMK can receive and unscramble communication between each other.

10.2.2 Setting Up Multiple Powerline Networks.

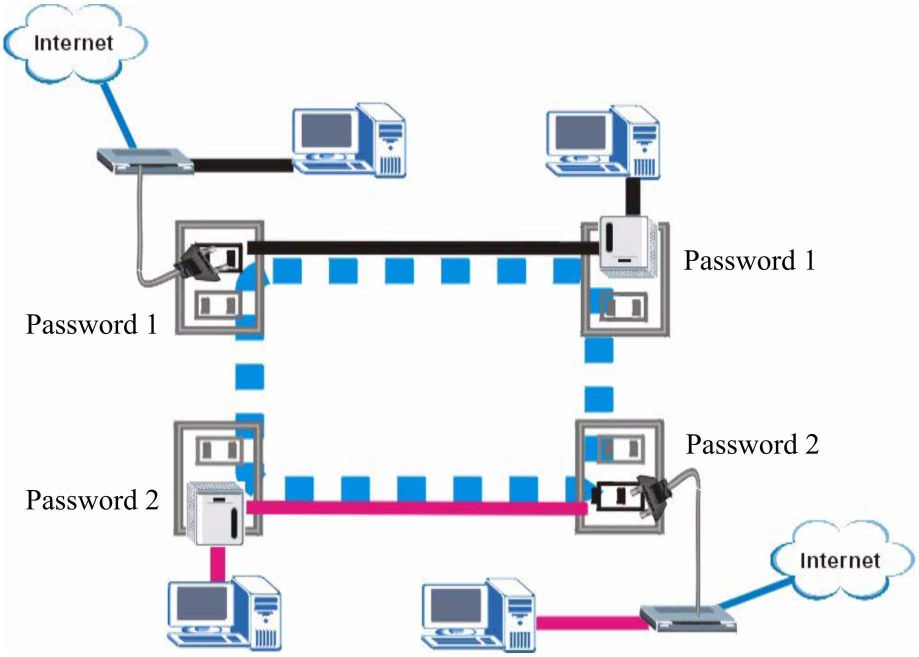
Multiple powerline networks can coexist on a single powerline circuit. You might want to implement multiple powerline networks in a small office environment where you have two separate Ethernet networks.

Connect one powerline adapter to a router or switch on the first Ethernet network and assign a network password (for example, “Password1”) to this powerline adapter. Add additional powerline adapters to your network by plugging them into your powerline outlets and assigning them the same network password, “Password1”. This completes the configuration of your first powerline network.

Connect another powerline adapter to a router or switch on the second Ethernet network and assign a different network password (for example “Password2”) to this powerline adapter. Again, add additional powerline adapters and assign them the same second network password, “Password2”.

You now have two private networks on your powerline circuit. Information is not shared between the two networks as only powerline adapters with the same password can communicate with each other. The following figure shows two private powerline networks on the same electrical circuit.

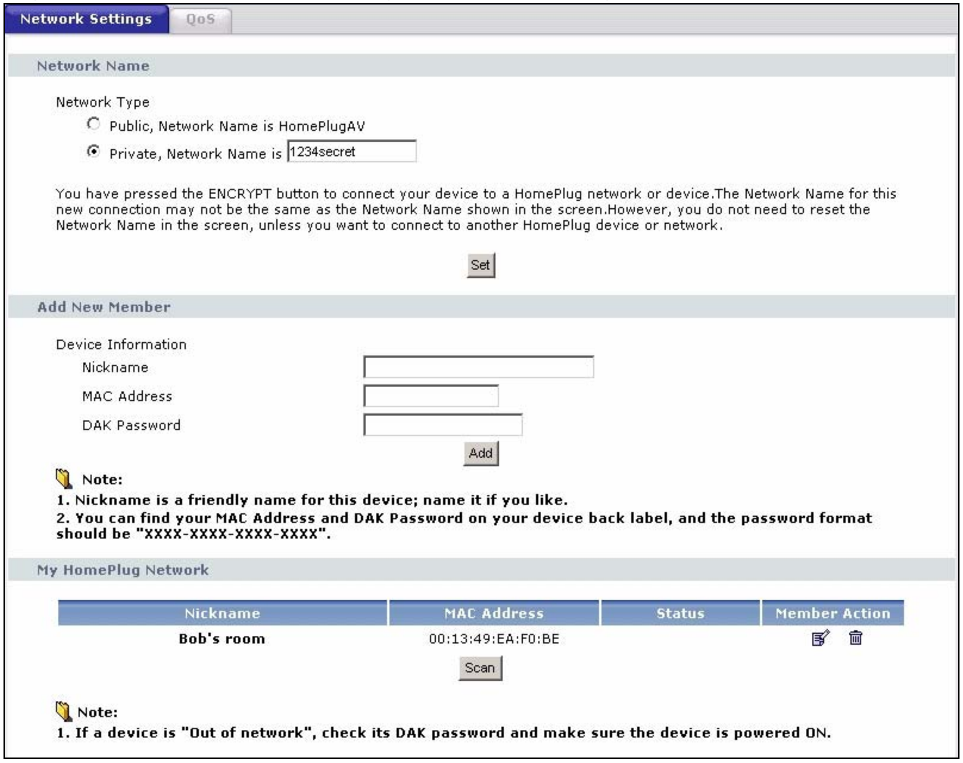
Figure 67 Two Private Powerline Networks on One Circuit



10.3 Configuring Your HomePlug AV Devices

Click on **Network > HomePlug** to see the screen below. Use this screen to set up a HomePlug AV network and to check the status of HomePlug AV devices on your electrical circuit.

Figure 68 Network > HomePlug > Network Settings



Network Name

Network Type

○ Public, Network Name is HomePlugAV

● Private, Network Name is 1234secret

You have pressed the ENCRYPT button to connect your device to a HomePlug network or device.The Network Name for this new connection may not be the same as the Network Name shown in the screen.However, you do not need to reset the Network Name in the screen, unless you want to connect to another HomePlug device or network.

Add New Member

Device Information

Nickname	
MAC Address	
DAK Password	

Note:

1. Nickname is a friendly name for this device; name it if you like.

2. You can find your MAC Address and DAK Password on your device back label, and the password format should be "XXXX-XXXX-XXXX-XXXX".

My HomePlug Network

Nickname	MAC Address	Status	Member Action
Bob's room	00:13:49:EA:F0:BE		

Note:

1. If a device is "Out of network", check its DAK password and make sure the device is powered ON.

The following table describes the labels in the screen.

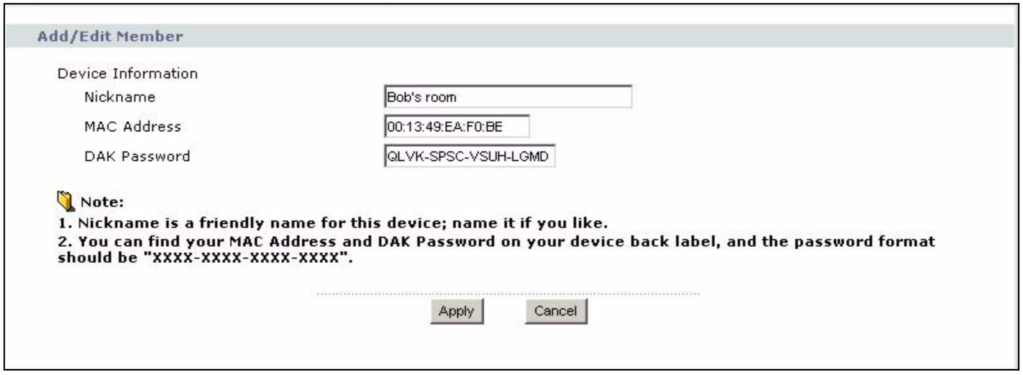
Table 44 Network > HomePlug > Network Settings

LABEL	DESCRIPTION
Network Name	This section lets you set the name of your network and to make it either public or private. The **Network Name** performs the same function as a network password. All devices on your HomePlug network have the same **Network Name.** A device with a different **Network Name** cannot be on your network. You can add other HomePlugAV devices to your network by giving them the same **Network Name**.
Network Type	The network may be either public or private.
Public, Network Name is HomePlug AV	Select this option if you want to make your powerline network public with the default **Network Name** of “HomePlug AV”. Since this is a well known **Network Name** it is less secure than a private **Network Name**. (The **Network Name** is often referred to as the NMK (Network Membership Key))
Private, Network Name is	Select this option if you wish to make your powerline network more secure with a private **Network Name**. Type the name of your private powerline network in the field. You may enter up to 64 alphanumeric characters for the **Network Name**.
Set	Click **Set** to change the **Network Name** of all the devices currently in your network.
Add New Member	This section lets you add new Home Plug AV enabled devices to your powerline network. When you add the device it is given the current **Network Name**.
Device Information	In this section type information to identify the new powerline device you are adding on your network.
Nickname	Type a name you wish to use to identify a specific powerline adapter, for example, “Mary’s room”.
MAC Address	Type the MAC address of the adapter you wish to add. The MAC address of your powerline adapter can be found by looking at the label on your device. It consists of six pairs of hexadecimal characters (hexadecimal characters are “0-9” and “a-f”). In the case of the NBG318S, this label is on the bottom of the device.
DAK Password	The **DAK Password** (DAK stands for Device Access Key), is used to verify that you are authorized to perform changes on a device. You can find the **DAK** printed on a sticker on the bottom of a HomePlug enabled device.
My Homeplug Network	This section provides information on the HomePlug AV devices in your network (or that were previously connected on it but are currently disconnected).
Nickname	This is the nickname you gave to the HomePlug AV device.
MAC Address	This is the MAC address of the HomePlug AV device.
Status	This field shows the status of the device. If the field shows **Active**, then the device is connected to your network. If the field shows **Out of Network,** the device has been added to the network but it is not ready. Check whether it is turned on and connected. If the field shows **Not Member**, it is not on the network. The NBG318S is aware of it, but cannot manage the device. If you click **Set**, the device’s **Network Name** will not change. You can add it to the network by clicking on **Edit** or entering its details in the **Add New member section**.

LABEL	DESCRIPTION
Member Action	This field shows the **Edit** icon and the **Delete** icon. Click on **Edit** to add a device to the network or to edit details such as the device's **Nickname**. Click on **Delete** to remove the device from the network. If you want to set up a second network, remove the devices from **My HomePlug Network** that you want to keep in your first network before you set the new **Network Name** for the second network.
Scan	Click **Scan** to detect devices on the same electrical circuit as the NBG318S.

Click on **Network > HomePlug > Edit** to see the screen below. Use this screen to add a new HomePlug AV device to the network. You can also edit a device's details.

Figure 69 Network > HomePlug > Edit



Add/Edit Member

Device Information

Nickname: Bob's room

MAC Address: 00:13:49:EA:F0:BE

DAK Password: QLVK-SPSC-VSUH-LGMD

Note:
1. Nickname is a friendly name for this device; name it if you like.
2. You can find your MAC Address and DAK Password on your device back label, and the password format should be "XXXX-XXXX-XXXX-XXXX".

The following table describes the labels in the screen.

Table 45 Network > HomePlug > Edit

	DESCRIPTION
Device Information	
Nickname	Type a name you wish to use to identify a specific powerline adapter, for example, "Bob's room".
MAC Address	This is the MAC address of the HomePlug AV device. The MAC Address will appear in this field if the device's status is either **Active** or **Not Member**. If the device's status is **Out of Network** or your NBG318S can not detect it, type the MAC Address here.
DAK Password	The **DAK Password** (DAK stands for Device Access Key), is used to verify that you are authorized to perform changes on a device. You can find the **DAK** printed on a sticker on the bottom of a HomePlug enabled device.
Apply	Click this button to apply add the device to the network or to apply your changes.
Cancel	Click this button to return to the previous screen.

10.4 HomePlug AV QoS

Your NBG318S can send different kinds of traffic through your powerline network at different speeds depending on the priority you give it. This feature is called Quality of Service (QoS).

- You can configure your NBG318S to give priority to powerline network traffic depending on its destination (**MAC Address or IP Port Number Priority**).
- You can also map the priority settings (VLAN or ToS priority settings) of traffic from outside your powerline network to priority settings for your powerline network (**Priority Mapping**).
- Priority can also be assigned according to traffic type such as IGMP (**Default Priority**).

Powerline traffic priority can be set at **Highest**, **High**, **Mid** and **Low**. The following priority settings are guidelines. The requirements of your powerline network may differ.

Table 46 Priority Settings

PRIORITY LEVEL	APPLICATION
Highest	Voice Application
High	Video and Audio Applications
Mid	Data Applications
Low	Data Applications

10.4.1 QoS Based on IP or MAC Address

You can prioritize traffic passing through your NBG318S based on the device it is intended for. Do this by setting the MAC address or IP address of a device(s) on your network and the level of priority of network traffic going to that device.

For example, if you have a digital media adapter such as the DMA-1100P on your network set up to play movie files on your T.V., you can set this device to **High**. This is because if video or music traffic is delivered too slowly, quality problems may occur.

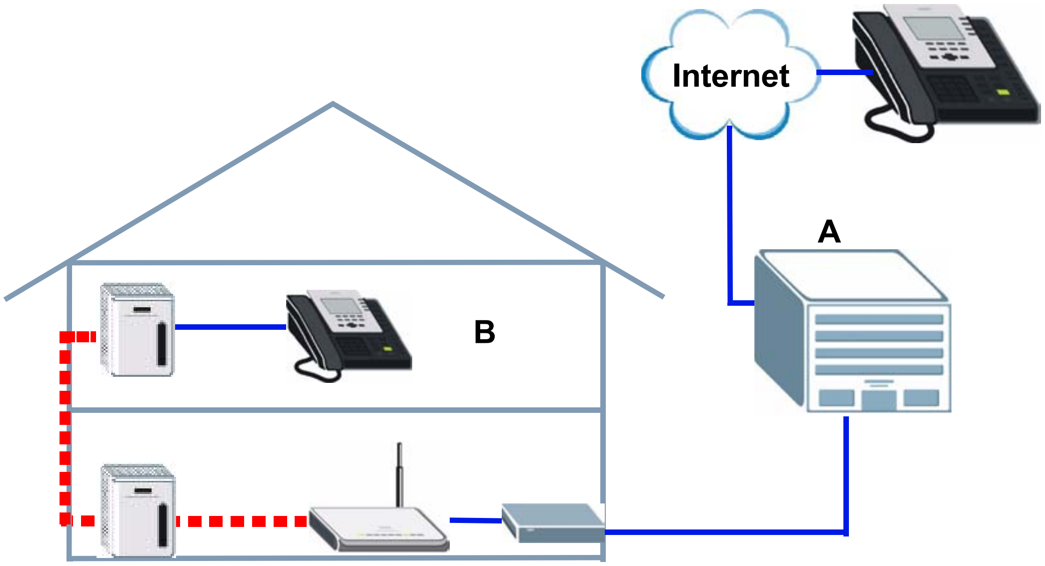
10.4.2 Mapping other QoS Priority Settings to HomePlug AV QoS

Wired networks use QoS priority settings such as VLAN priority settings or ToS (Type of Service) settings to help network traffic flow more smoothly. However, powerline devices cannot use these priority settings unless they are mapped over to HomePlug AV QoS priority settings.

(VLAN priority settings are not to be confused with VLAN ID. The VLAN tag contains both priority settings (0~7) and ID information (1~4095).)

For example, your ISP (**A**) may use VLAN priority settings to identify and prioritize VoIP (Voice over IP) traffic or you may have a VoIP device (**B**) attached to your NBG318S which adds ToS (Type of Service) priorities to data it sends. By giving high priority to VoIP traffic in your powerline network, VoIP traffic flows more smoothly.

Figure 70 Prioritized Traffic Between Your Home Powerline Network and the Internet



The following mappings are suggestions only. VLAN and ToS priority settings may not map exactly to Homeplug AV priority settings. Priority settings for VLAN Tags and ToS bits range from 0 to 7 with 7 as the highest.

Table 47 Suggested Mappings

VLAN/TOS PRIORITY SETTINGS	HOMEPLUG AV PRIORITY SETTINGS
5~7	Highest
4	High
2~3	Mid
0~1	Low

10.4.3 QoS Based on Traffic Type

You can prioritize traffic on your powerline network based on four kinds of traffic types. These are **IGMP, IGMP managed Multicast Stream, Unicast** and **Multicast/Broadcast.** However, it is recommended that you do not change the default settings.

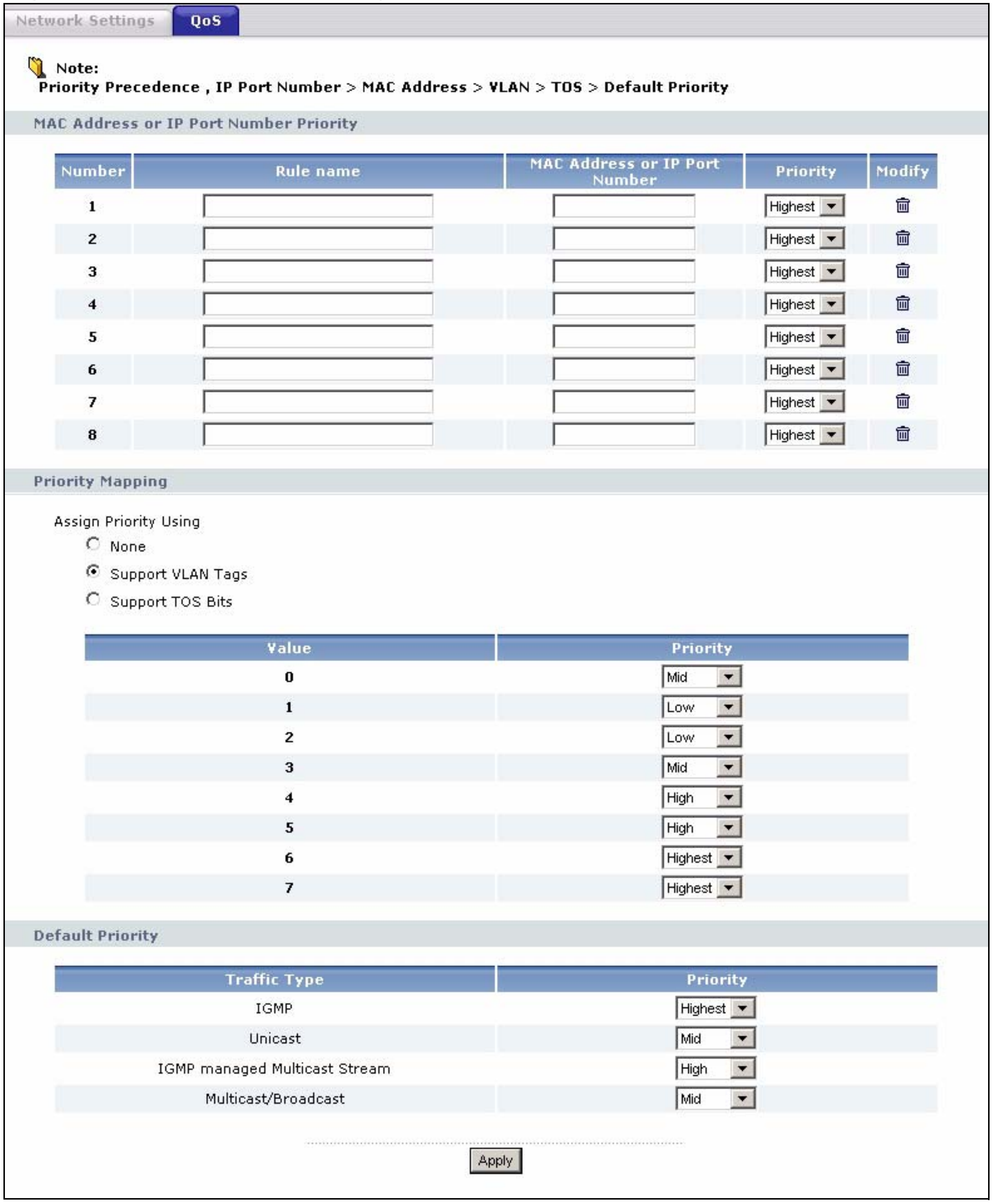
Unicast and **Multicast/Broadcast** refer to how IP packets are transmitted. Unicast transmission is from one sender to one recipient. Broadcast transmission is from one sender to all devices on a network. Multicast transmission is from one sender to some of the devices on the network.

IGMP (Internet Group Membership Protocol) is a network protocol which lets devices on a network join or leave a multicast group. An **IGMP managed Multicast Stream** refers to streaming media (such as video or audio) to a group of devices on a network using IGMP to manage the multicast.

IGMP is assigned highest priority as it controls multicast services such as **IGMP managed Multicast Stream** which allows streamed traffic such as video or VoIP. **Unicast**, **Multicast/ Broadcast** require less priority than the traffic that manages them.

Select **Network** > **HomePlug** > **QoS** to set levels of service for different kinds of traffic on your powerline connection. The following screen displays

Figure 71 Network > HomePlug > QoS.



Note:
Priority Precedence , IP Port Number > MAC Address > VLAN > TOS > Default Priority

MAC Address or IP Port Number Priority

Number	Rule name	MAC Address or IP Port Number	Priority	Modify
1			Highest	🗑
2			Highest	🗑
3			Highest	🗑
4			Highest	🗑
5			Highest	🗑
6			Highest	🗑
7			Highest	🗑
8			Highest	🗑

Priority Mapping

Assign Priority Using
○ None
● Support VLAN Tags
○ Support TOS Bits

Value	Priority
0	Mid
1	Low
2	Low
3	Mid
4	High
5	High
6	Highest
7	Highest

Default Priority

Traffic Type	Priority
IGMP	Highest
Unicast	Mid
IGMP managed Multicast Stream	High
Multicast/Broadcast	Mid

The following table describes the labels in the screen.

Table 48 Network > HomePlug > Edit

LABEL	DESCRIPTION
MAC Address or IP Port Number Priority	
Number	This is the index number for a priority rule.

Table 48 Network > HomePlug > Edit

LABEL	DESCRIPTION
Rule Name	Type a descriptive name for a priority rule. You can enter up to 31 characters containing “0”~”9”, “a”~”z”, “A”~”Z”, “_” or -. Spaces are allowed.
MAC Address or IP Port Number	Type the MAC (Media Access Control) address or IP address of a device on your network. Network traffic to this device is prioritized according to the priority level of this rule. Enter the MAC address using six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. Enter the IP address in dotted decimal notation, for example, 192.168.1.1.
Priority	Select the priority level for this rule. The options are **Highest**, **High**, **Mid** and **Low**.
Modify	Click the modify icon to remove the rule.
Priority Mapping	
Assign Priority Using	Use this section to enable or disable priority rules based on VLAN priority settings or ToS bits. Select **None** if you are not prioritizing traffic based on VLAN priority settings or ToS bits. Select **Support VLAN Tags** to map VLAN priority settings to powerline priority settings. For example, ISPs often assign VLAN tags to traffic based on customer contracts or traffic type. Selecting this option supports ISP assigned priority settings. • VLAN priority settings are not to be confused with VLAN ID. The VLAN tag contains both priority settings (0~7) and ID information (1~4095). Select **Support TOS Bits** to map ToS settings to powerline priority settings. Do this if you receive network traffic which has been assigned ToS (Type of Service) bits by the device or application that generated it, or by an intermediate device. For example, a VoIP device on your network may assign priority to the traffic it has generated. Selecting this option supports the priority settings such a device may have assigned.
Value	VLAN priority settings and ToS bits priority settings range from 0 to 7 with 7 as the highest priority.
Priority	Assign a priority setting to packets passing through your NBG318S based on their VLAN tag or ToS bit priority setting. The options are **Highest**, **High**, **Mid** and **Low**. Use Figure 47 on page 128 as a guide if you are unsure of what mappings to assign.
Default Priority	
Traffic Type	This option applies priority settings to traffic based on its traffic type. You can prioritize **IGMP**, **Unicast**, **IGMP managed Multicast Stream** or **Multicast/ Broadcast network traffic**. However, it is recommended that you do not change the default settings.
Apply	Click **Apply** to save your settings.

11

DHCP

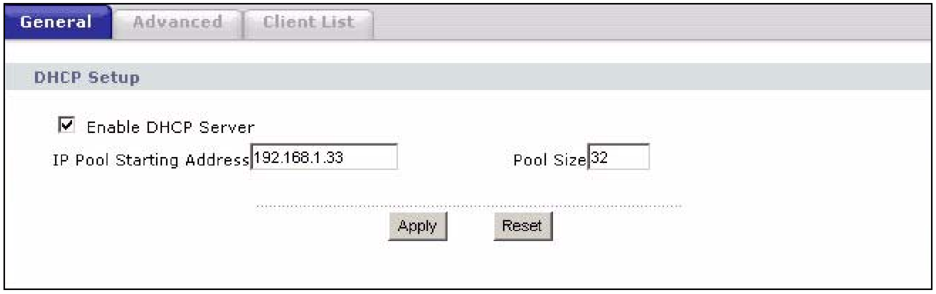
11.1 DHCP

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 NBG318S as a DHCP server or disable it. When configured as a server, the NBG318S 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.

11.2 DHCP Server General Screen

Click **Network** > **DHCP Server**. The following screen displays.

Figure 72 Network > DHCP Server > General



☑ Enable DHCP Server

IP Pool Starting Address 192.168.1.33

Pool Size 32

The following table describes the labels in this screen.

Table 49 Network > DHCP Server > General

LABEL	DESCRIPTION
Enable DHCP Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Leave the **Enable DHCP Server** check box selected unless your ISP instructs you to do otherwise. Clear it to disable the NBG318S acting as a DHCP server. When configured as a server, the NBG318S provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

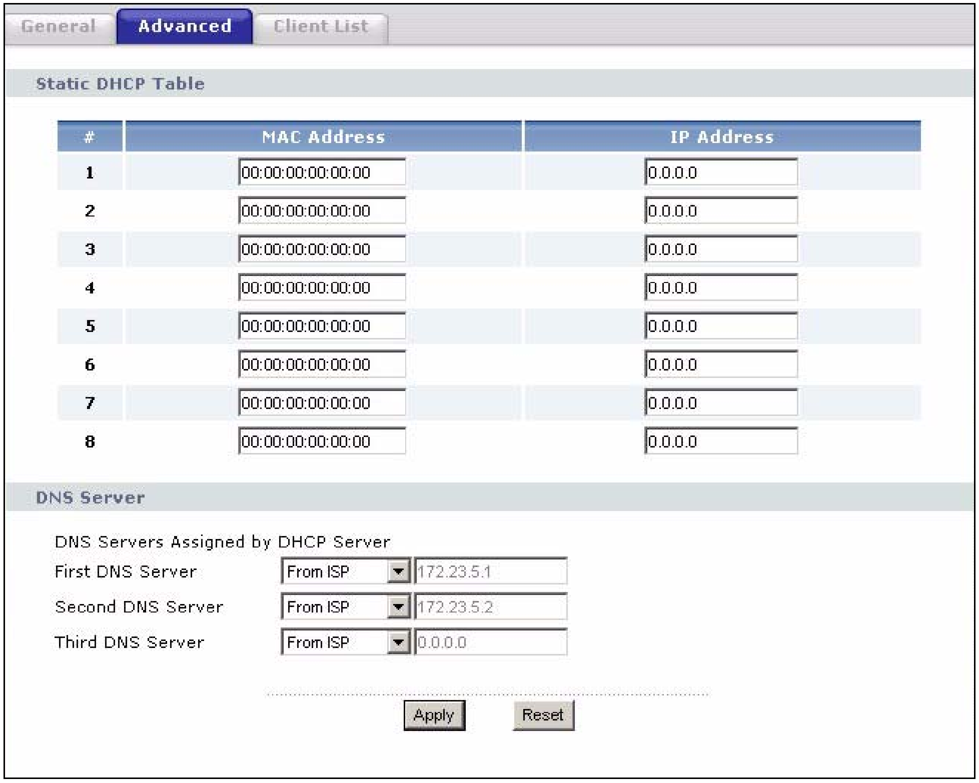
11.3 DHCP Server Advanced Screen

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 NBG318S sends to the DHCP clients.

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.

To change your NBG318S's static DHCP settings, click **Network** > **DHCP Server** > **Advanced**. The following screen displays.

Figure 73 Network > DHCP Server > Advanced



Static DHCP Table

#	MAC Address	IP Address
1	00:00:00:00:00:00	0.0.0.0
2	00:00:00:00:00:00	0.0.0.0
3	00:00:00:00:00:00	0.0.0.0
4	00:00:00:00:00:00	0.0.0.0
5	00:00:00:00:00:00	0.0.0.0
6	00:00:00:00:00:00	0.0.0.0
7	00:00:00:00:00:00	0.0.0.0
8	00:00:00:00:00:00	0.0.0.0

DNS Server

DNS Servers Assigned by DHCP Server

First DNS Server	From ISP	172.23.5.1
Second DNS Server	From ISP	172.23.5.2
Third DNS Server	From ISP	0.0.0.0

The following table describes the labels in this screen.

Table 50 Network > DHCP Server > Advanced

LABEL	DESCRIPTION
#	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.
IP Address	Type the LAN IP address of a computer on your LAN.
DNS Servers Assigned by DHCP Server The NBG318S passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The NBG318S 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.	

Table 50 Network > DHCP Server > Advanced

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG318S'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 NBG318S act as a DNS proxy. The NBG318S's LAN IP address displays in the field to the right (read-only). The NBG318S tells the DHCP clients on the LAN that the NBG318S itself is the DNS server. When a computer on the LAN sends a DNS query to the NBG318S, the NBG318S forwards the query to the NBG318S'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 NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

11.4 Client List Screen

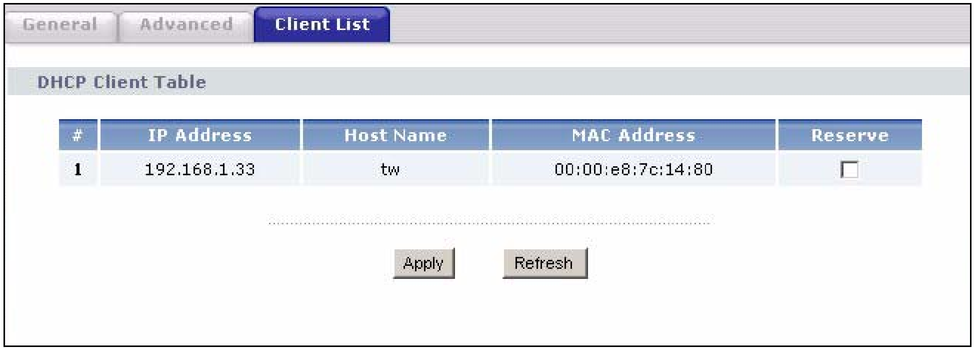
The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the NBG318S's DHCP server.

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

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

The following screen displays.

Figure 74 Network > DHCP Server > Client List



DHCP Client Table

#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.33	tw	00:00:e8:7c:14:80	□

The following table describes the labels in this screen.

Table 51 Network > DHCP Server > Client List

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select this check box to have the NBG318S always assign this IP address to this MAC address (and host name). After you click **Apply**, the MAC address and IP address also display in the **Advanced** screen (where you can edit them).
Refresh	Click **Refresh** to reload the DHCP table.

12

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the NBG318S.

12.1 NAT 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.

12.2 Using NAT

You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the NBG318S.

12.2.1 Port Forwarding: Services and Port Numbers

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

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

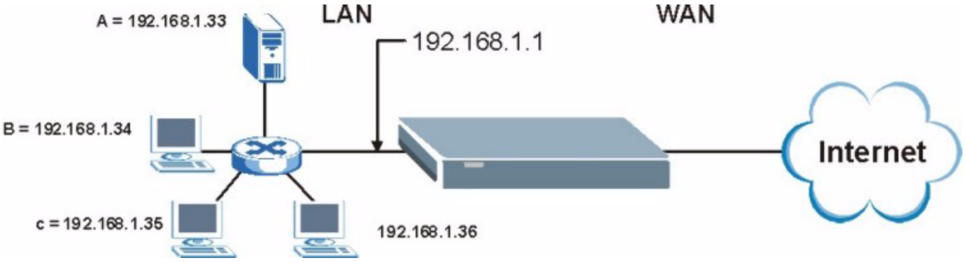
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

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.

12.2.2 Configuring Servers Behind Port Forwarding Example

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

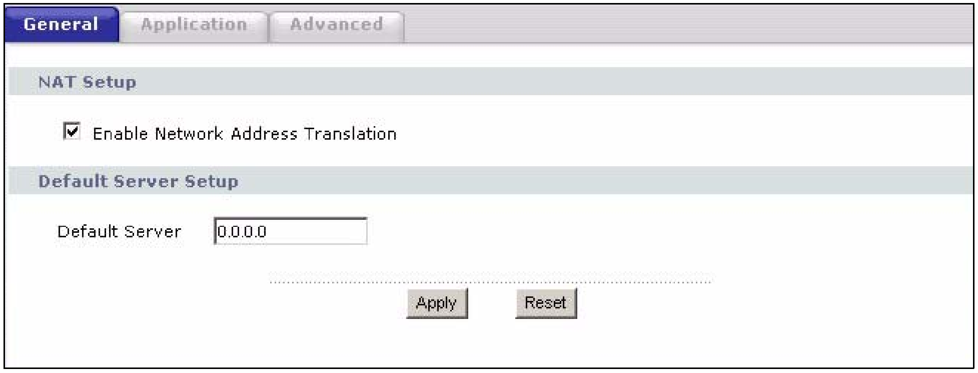
Figure 75 Multiple Servers Behind NAT Example



12.3 General NAT Screen

Click **Network** > **NAT** to open the **General** screen.

Figure 76 Network > NAT > General



NAT Setup

☑ Enable Network Address Translation

Default Server Setup

Default Server 0.0.0.0

The following table describes the labels in this screen.

Table 52 Network > NAT > General

LABEL	DESCRIPTION
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	
	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 NBG318S 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 NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

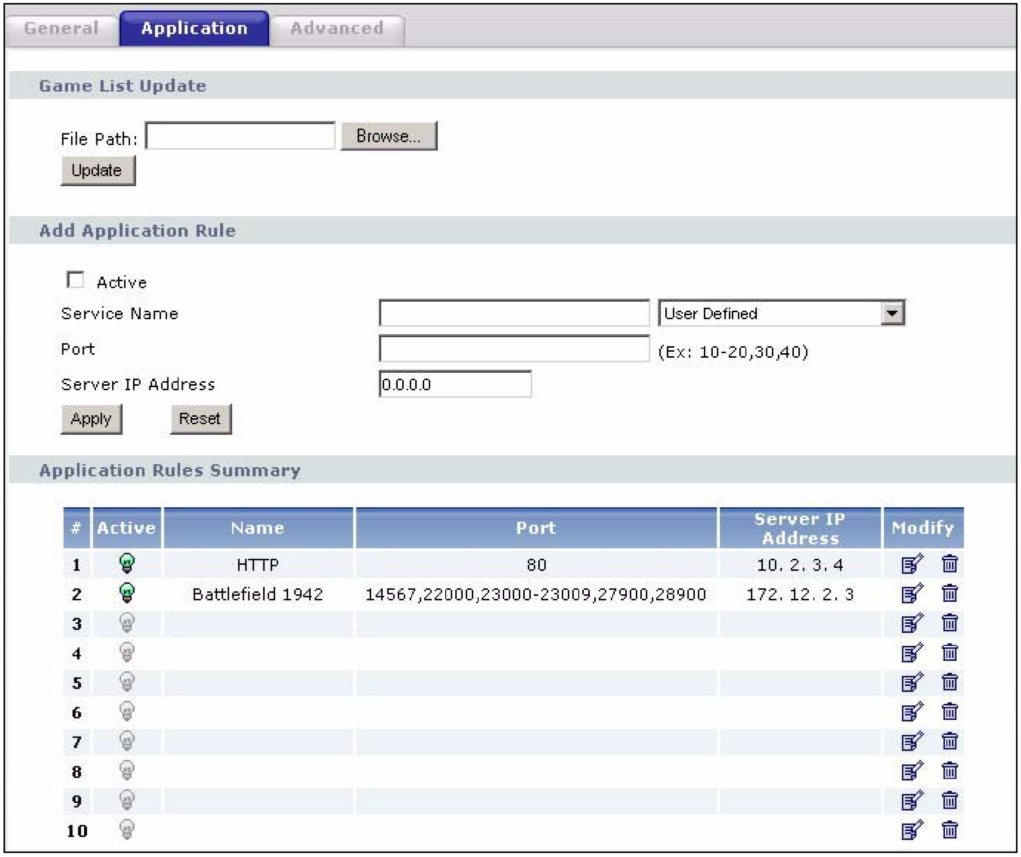
12.4 NAT Application Screen

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your NBG318S's port forwarding settings, click **Network > NAT** > **Application**. The screen appears as shown.

If you do not assign a **Default Server** IP address in the **NAT > General** screen, the NBG318S discards all packets received for ports that are not specified in this screen or remote management.

Refer to Appendix F on page 287 for port numbers commonly used for particular services.

Figure 77 Network > NAT > Application



Game List Update

File Path:
Browse...
Update

Add Application Rule

□ Active

Service Name: User Defined

Port: (Ex: 10-20,30,40)

Server IP Address: 0.0.0.0

Apply
Reset

Application Rules Summary

#	Active	Name	Port	Server IP Address	Modify
1	●	HTTP	80	10.2.3.4	
2	●	Battlefield 1942	14567,22000,23000-23009,27900,28900	172.12.2.3	
3	○				
4	○				
5	○				
6	○				
7	○				
8	○				
9	○				
10	○				

The following table describes the labels in this screen.

Table 53 NAT Application

LABEL	DESCRIPTION
Game List Update	A game list includes the pre-defined service name(s) and port number(s). You can edit and upload it to the NBG318S to replace the existing entries in the second field next to **Service Name**.
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.txt file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Update	Click **Update** to begin the upload process. This process may take up to two minutes.
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.

Table 53 NAT Application (continued)

LABEL	DESCRIPTION
Port	Type a port number(s) to be forwarded. To specify a range of ports, enter a hyphen (-) between the first port and the last port, such as 10-20. To specify two or more non-consecutive port numbers, separate them by a comma without spaces, such as 123,567.
Server IP Address	Type the inside IP address of the server that receives packets from the port(s) specified in the **Port** field.
Apply	Click **Apply** to save your changes to the **Application Rules Summary** table.
Reset	Click **Reset** to not save and return your new changes in the **Service Name** and **Port** fields to the previous one.
Application Rules Summary	
#	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.

12.4.1 Game List Example

Here is an example game list text file. The index number, service name and associated port(s) are specified by semi-colons (no spaces). Use the name=xxx (where xxx is the service name) to create a new service. Port range can be separated with a hyphen (-) (no spaces). Multiple (non-consecutive) ports can be separated by commas.

Figure 78 Game List Example

```
version=1
1;name=Battlefield 1942;port=14567,22000,23000-23009,27900,28900
2;name=Call of Duty;port=28960
3;name=Civilization IV;port=2056
4;name=Diablo I and II;port=6112-6119,4000
5;name=Doom 3;port=27666
6;name=F.E.A.R;port=27888
7;name=Final Fantasy XI;port=25,80,110,443,50000-65535
8;name=Guild Wars;port=6112,80
9;name=Half Life;port=6003,7002,27005,27010,27011,27015
10;name=Jedi Knight III: Jedi Academy;port=28060-28062,28070-28081
11;name=Need for Speed: Hot Pursuit 2;port=1230,8511-
8512,27900,28900,61200-61230
12;name=Neverwinter Nights;port=5120-5300,6500,27900,28900
13;name=Quake 2;port=27910
14;name=Quake 3;port=27660,27960
15;name=Rainbow Six 3: Raven Shield;port=7777-7787,8777-8787
16;name=Serious Sam II;port=25600-25605
17;name=Silent Hunter III;port=17997-18003
18;name=Soldier of Fortune II;port=20100-20112
19;name=Starcraft;port=6112-6119,4000
20;name=Star Trek: Elite Force II;port=29250,29256
21;name=SWAT 4;port=10480-10483
22;name=Warcraft II and III;port=6112-6119,4000
23;name=World of Warcraft;port=3724
```

12.5 Trigger Port Forwarding

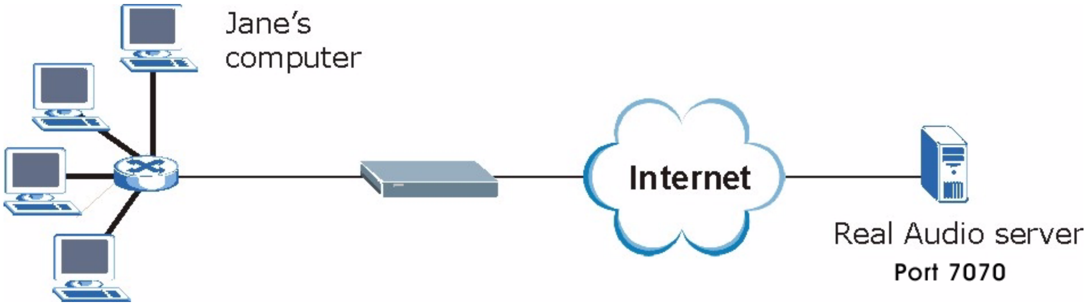
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem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

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The NBG318S 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 NBG318S's WAN port receives a response with a specific port number and protocol ("incoming" port), the NBG318S 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.

12.5.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 79 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 NBG318S to record Jane’s computer IP address. The NBG318S 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 NBG318S 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 NBG318S times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

12.5.2 Two Points To Remember About Trigger Ports

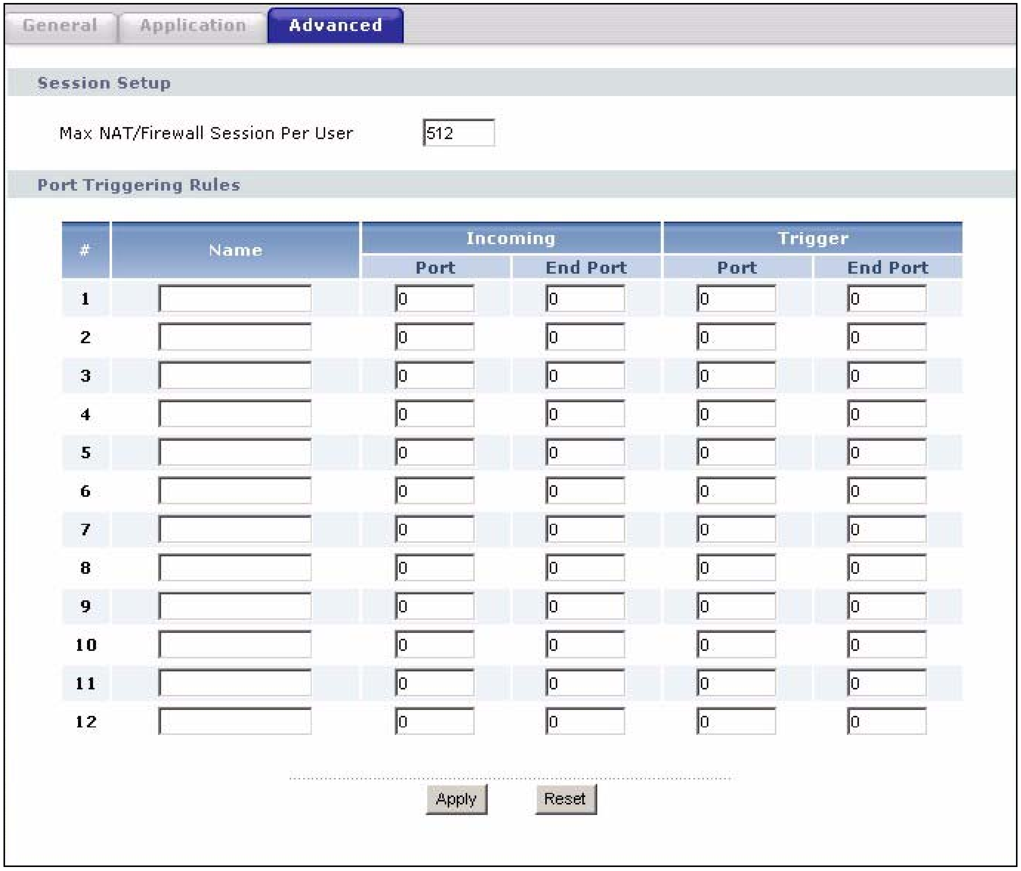
1. Trigger events only happen on data that is going coming from inside the NBG318S and going to the outside.
2. If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can’t trigger it.

12.6 NAT Advanced Screen

To change your NBG318S’s trigger port settings, click **Network > NAT** > **Advanced**. The screen appears as shown.

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

Figure 80 Network > NAT > Advanced



Session Setup

Max NAT/Firewall Session Per User: 512

Port Triggering Rules

#	Name	Incoming		Trigger	
		Port	End Port	Port	End Port
1		0	0	0	0
2		0	0	0	0
3		0	0	0	0
4		0	0	0	0
5		0	0	0	0
6		0	0	0	0
7		0	0	0	0
8		0	0	0	0
9		0	0	0	0
10		0	0	0	0
11		0	0	0	0
12		0	0	0	0

The following table describes the labels in this screen.

Table 54 Network > NAT > Advanced

LABEL	DESCRIPTION
Max NAT/Firewall Session Per User	Type a number ranging from 1 to 2048 to limit the number of NAT/firewall sessions that a host can create. When computers use peer to peer applications, such as file sharing applications, they may use a large number of NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet. Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the NBG318S. If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using all of the available NAT sessions.
Port Triggering Rules	
#	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.

Table 54 Network > NAT > Advanced

LABEL	DESCRIPTION
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 NBG318S 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 NBG318S 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 NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

13

Dynamic DNS

13.1 Dynamic DNS Introduction

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.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

13.1.1 DynDNS Wildcard

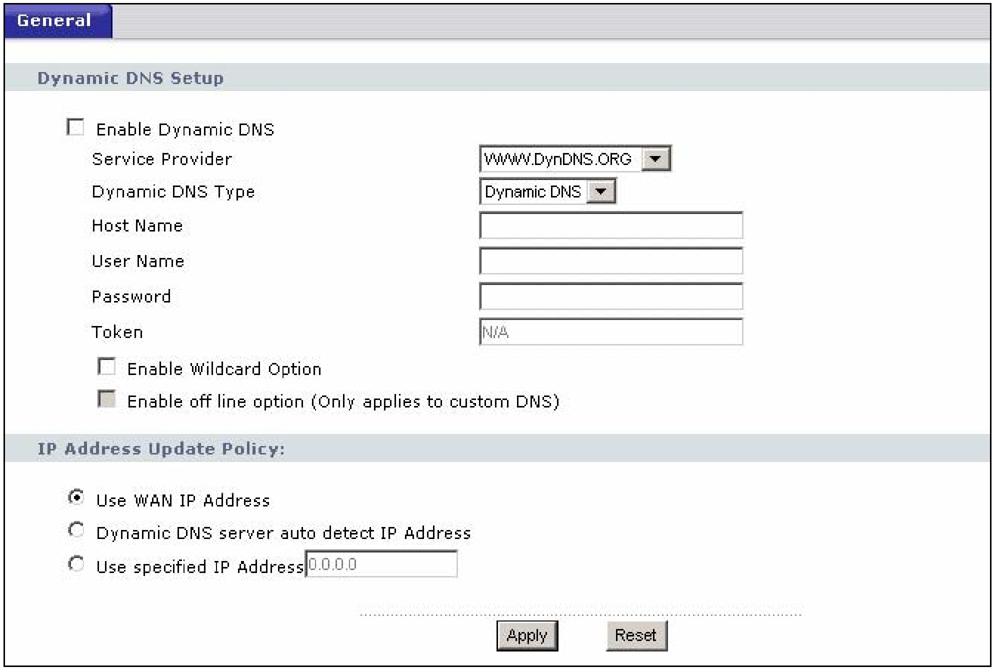
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

13.2 Dynamic DNS Screen

To change your NBG318S's DDNS, click **Network > DDNS**. The screen appears as shown.

Figure 81 Dynamic DNS



Dynamic DNS Setup

☐ Enable Dynamic DNS

Service Provider	WWW.DynDNS.ORG ▼
Dynamic DNS Type	Dynamic DNS ▼
Host Name	
User Name	
Password	
Token	N/A

☐ Enable Wildcard Option

☐ Enable off line option (Only applies to custom DNS)

IP Address Update Policy:

● Use WAN IP Address

○ Dynamic DNS server auto detect IP Address

○ Use specified IP Address 0.0.0.0

The following table describes the labels in this screen.

Table 55 Dynamic DNS

LABEL	DESCRIPTION
Enable Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	If you have selected **WWW.DynDNS.ORG** as your DNS Service Provider, you can select the type of service that you are registered for. The options are **dynamic**, **static** or **custom**.
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.
Token	If you have selected **WWW.REGFISH.COM** as your DNS Service Provider, you can use token instead of a user name and password (RegFish only). This token is provided automatically for a domain when activating DynDNS and can be replaced at any time with a new token.
Enable Wildcard Option	If you have selected **WWW.DynDNS.ORG** as your DNS Service Provider, you can select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when **CustomDNS** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.
Dynamic DNS server auto detect IP Address	If you have selected **WWW.DynDNS.ORG** as your DNS Service Provider, you can select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.

Table 55 Dynamic DNS

LABEL	DESCRIPTION
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

PART III
Security

14

Firewall

This chapter gives some background information on firewalls and explains how to get started with the NBG318S's firewall.

14.1 Introduction to ZyXEL's Firewall

14.1.1 What is a Firewall?

Originally, the term “firewall” referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from a network that is not trusted. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

14.1.2 Stateful Inspection Firewall

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

14.1.3 About the NBG318S Firewall

The NBG318S firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The NBG318S's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG318S 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 NBG318S 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 NBG318S 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.

14.1.4 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.
2. Think about access control before you connect to the network in any way, including attaching a modem to the port.
3. Limit who can access your router.
4. Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

14.2 Triangle Routes

If an alternate gateway on the LAN has an IP address in the same subnet as the NBG318S’s LAN IP address, return traffic may not go through the NBG318S. This is called an asymmetrical or “triangle” route. This causes the NBG318S to reset the connection, as the connection has not been acknowledged.

You can have the NBG318S permit the use of asymmetrical route topology on the network (not reset the connection).

Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the NBG318S. A better solution is to use IP alias to put the NBG318S and the backup gateway on separate subnets.

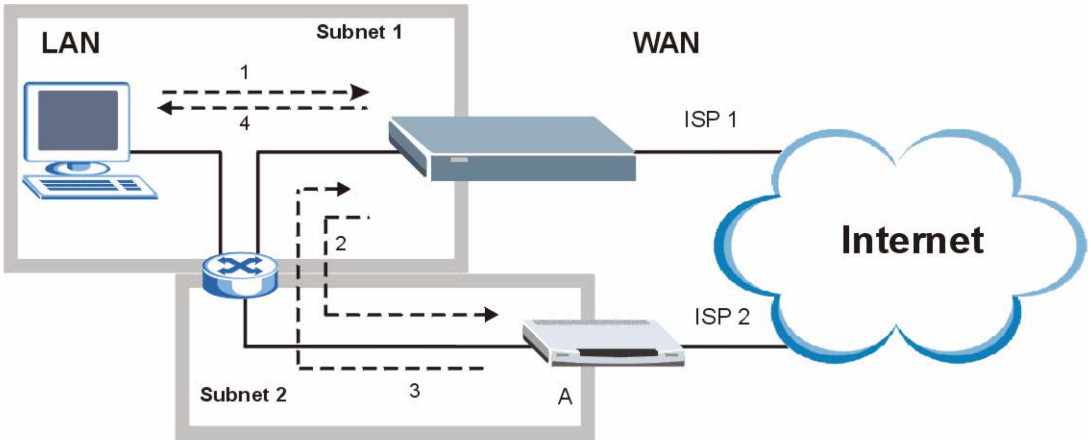
14.2.1 Triangle Routes and IP Alias

You can use IP alias instead of allowing triangle routes. IP Alias allow you to partition your network into logical sections over the same interface.

By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the NBG318S to your LAN. The following steps describe such a scenario.

1. A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The NBG318S reroutes the packet to Gateway **A**, which is in **Subnet 2**.
3. The reply from the WAN goes to the NBG318S.
4. The NBG318S then sends it to the computer on the LAN in **Subnet 1**.

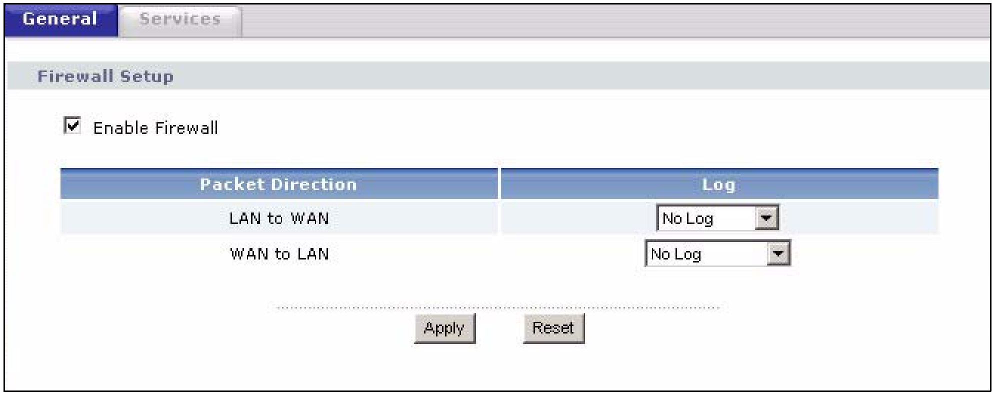
Figure 82 Using IP Alias to Solve the Triangle Route Problem



14.3 General Firewall Screen

Click **Security** > **Firewall** to open the **General** screen. Use this screen to enable or disable the NBG318S's firewall, and set up firewall logs.

Figure 83 Security > Firewall > General I



☑ Enable Firewall

Packet Direction	Log
LAN to WAN	No Log
WAN to LAN	No Log

The following table describes the labels in this screen.

Table 56 Security > Firewall > General

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The NBG318S performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Packet Direction	This is the direction of travel of packets. Firewall rules are grouped based on the direction of travel of packets to which they apply.

Table 56 Security > Firewall > General

LABEL	DESCRIPTION
Log	Select whether to create a log for packets that are traveling in the selected direction when the packets are blocked or forwarded. To log packets related to firewall rules, make sure that **Access Control** under **Log** is selected in the **Logs** > **Log Settings** screen.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

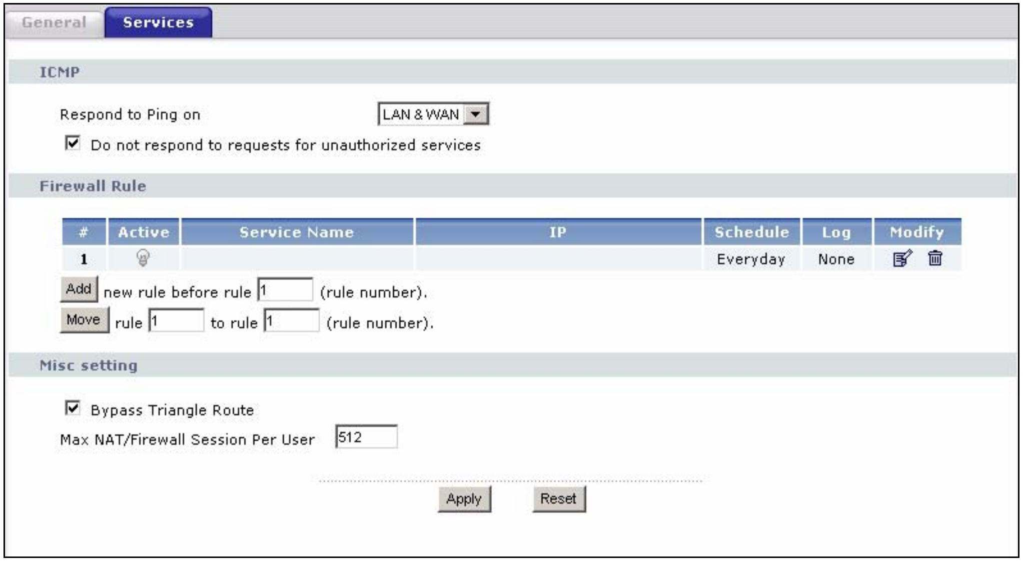
14.4 Services Screen

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

If an outside user attempts to probe an unsupported port on your NBG318S, an ICMP response packet is automatically returned. This allows the outside user to know the NBG318S exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your NBG318S 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.

Figure 84 Security > Firewall > Services



ICMP

Respond to Ping on: LAN & WAN

☑ Do not respond to requests for unauthorized services

Firewall Rule

#	Active	Service Name	IP	Schedule	Log	Modify
1				Everyday	None	

Add new rule before rule 1 (rule number).

Move rule 1 to rule 1 (rule number).

Misc setting

☑ Bypass Triangle Route

Max NAT/Firewall Session Per User: 512

The following table describes the labels in this screen.

Table 57 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 NBG318S 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 both incoming LAN and WAN Ping requests.

Table 57 Security > Firewall > Services

LABEL	DESCRIPTION
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the NBG318S by probing for unused ports. If you select this option, the NBG318S will not respond to port request(s) for unused ports, thus leaving the unused ports and the NBG318S unseen. By default this option is not selected and the NBG318S will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the NBG318S's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the NBG318S reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on|off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.
Service Setup	
Enable Services Blocking	Select this check box to enable this feature.
Available Services	This is a list of pre-defined services (ports) you may prohibit your LAN computers from using. Select the port you want to block using the drop-down list and click **Add** to add the port to the **Blocked Services** field.
Blocked Services	This is a list of services (ports) that will be inaccessible to computers on your LAN once you enable service blocking.
Custom Port	A custom port is a service that is not available in the pre-defined **Available Services** list and you must define using the next two fields.
Type	Choose the IP port (**TCP** or **UDP**) that defines your customized port from the drop down list box.
Port Number	Enter the port number range that defines the service. For example, if you want to define the Gnutella service, then select **TCP** type and enter a port range from 6345 to 6349.
Add	Select a service from the **Available Services** drop-down list and then click **Add** to add a service to the **Blocked Services**
Delete	Select a service from the **Blocked Services** list and then click **Delete** to remove this service from the list.
Clear All	Click **Clear All** to empty the **Blocked Services**.
Schedule to Block	
Day to Block:	Select a check box to configure which days of the week (or everyday) you want service blocking to be active.
Time of Day to Block (24-Hour Format)	Select the time of day you want service blocking to take effect. Configure blocking to take effect all day by selecting **All Day**. You can also configure specific times by selecting **From** and entering the start time in the **Start (hour)** and **Start (min)** fields and the end time in the **End (hour)** and **End (min)** fields. Enter times in 24-hour format, for example, "3:00pm" should be entered as "15:00".
Misc setting	
Bypass Triangle Route	Select this check box to have the NBG318S firewall ignore the use of triangle route topology on the network.
Max NAT/Firewall Session Per User	Type a number ranging from 1 to 2048 to limit the number of NAT/firewall sessions that a host can create.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

15

Content Filtering

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

15.1 Introduction to Content Filtering

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.

15.2 Restrict Web Features

The NBG318S can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

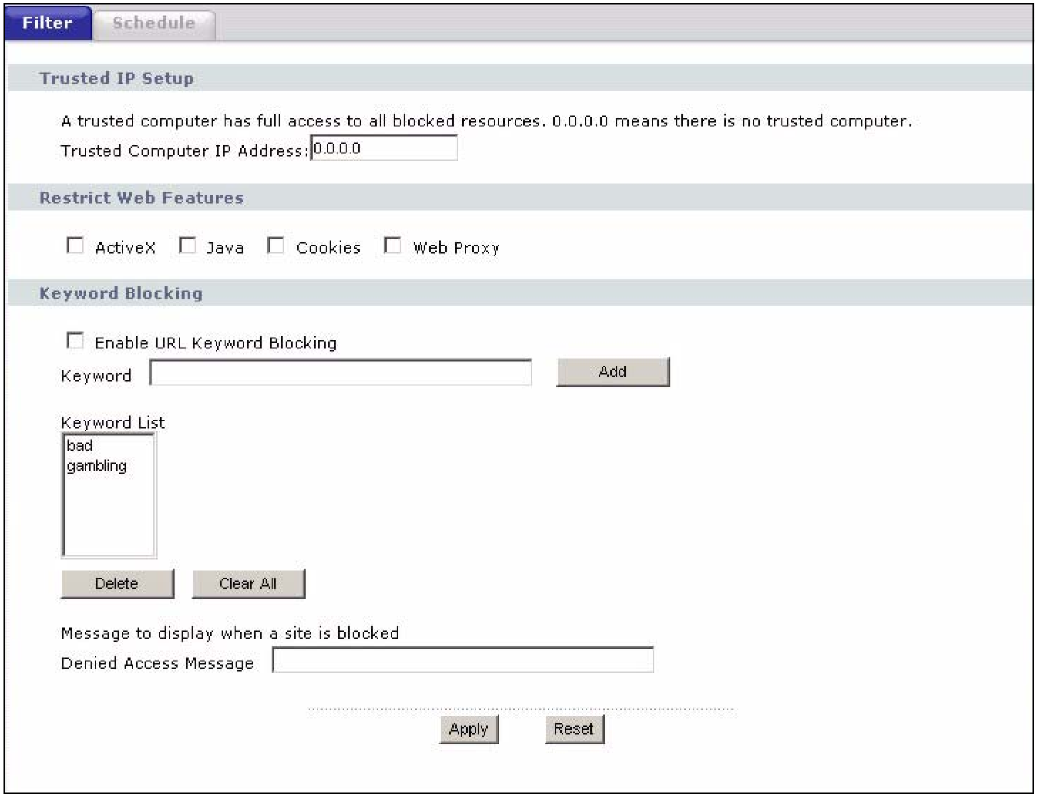
15.3 Days and Times

The NBG318S also allows you to define time periods and days during which the NBG318S performs content filtering.

15.4 Filter Screen

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

Figure 85 Security > Content Filter > Filter



Trusted IP Setup

A trusted computer has full access to all blocked resources. 0.0.0.0 means there is no trusted computer.

Trusted Computer IP Address: 0.0.0.0

Restrict Web Features

☐ ActiveX ☐ Java ☐ Cookies ☐ Web Proxy

Keyword Blocking

☐ Enable URL Keyword Blocking

Keyword

Keyword List

bad
gambling

Message to display when a site is blocked

Denied Access Message

The following table describes the labels in this screen.

Table 58 Security > Content Filter > Filter

LABEL	DESCRIPTION
Trusted Computer IP Address	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.
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.
Keyword Blocking	
Enable URL Keyword Blocking	The NBG318S 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.

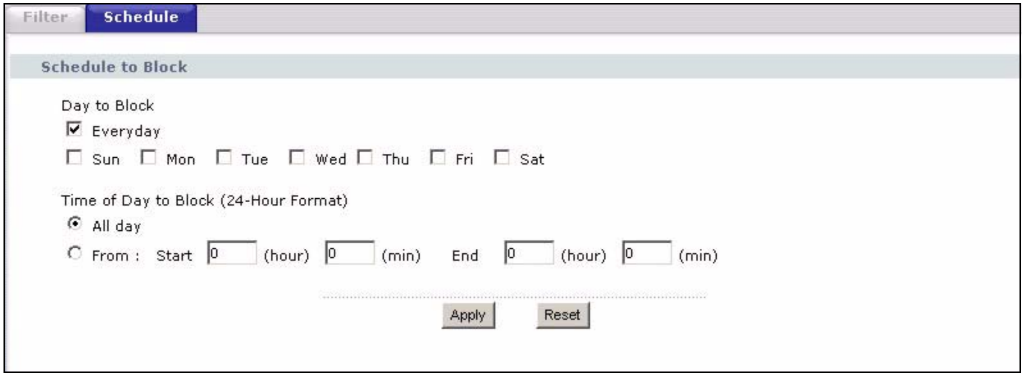
Table 58 Security > Content Filter > Filter

LABEL	DESCRIPTION
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.
Denied Access Message	Enter a message to be displayed when a user tries to access a restricted web site. The default message is “Please contact your network administrator!!”
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh

15.5 Schedule

Use this screen to set the day(s) and time you want the NBG318S to use content filtering. Click **Security** > **Content Filter** > **Schedule**. The following screen displays.

Figure 86 Security > Content Filter > Schedule



Schedule to Block

Day to Block

☑ Everyday

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Time of Day to Block (24-Hour Format)

● All day

○ From : Start 0 (hour) 0 (min) End 0 (hour) 0 (min)

The following table describes the labels in this screen.

Table 59 Security > Content Filter > Schedule

LABEL	DESCRIPTION
Day to Block	Select check boxes for the days that you want the NBG318S to perform content filtering. Select the **Everyday** check box to have content filtering turned on all days of the week.
Time of Day to Block (24-Hour Format)	**Time of Day to Block** allows the administrator to define during which time periods content filtering is enabled. **Time of Day to Block** restrictions only apply to the keywords (see above). Restrict web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected. Select **All Day** to have content filtering always active on the days selected in **Day to Block** with time of day limitations not enforced. Select **From** and enter the time period, in 24-hour format, during which content filtering will be enforced.

Table 59 Security > Content Filter > Schedule

LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh

15.6 Customizing Keyword Blocking URL Checking

You can use commands to set how much of a website's URL the content filter is to check for keyword blocking. See the appendices for information on how to access and use the command interpreter.

15.6.1 Domain Name or IP Address URL Checking

By default, the NBG318S checks the URL's domain name or IP address when performing keyword blocking.

This means that the NBG318S checks the characters that come before the first slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, content filtering only searches for keywords within www.zyxel.com.tw.

15.6.2 Full Path URL Checking

Full path URL checking has the NBG318S check the characters that come before the last slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, full path URL checking searches for keywords within www.zyxel.com.tw/news/.

Use the `ip urlfilter customize actionFlags 6 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's full path.

15.6.3 File Name URL Checking

Filename URL checking has the NBG318S check all of the characters in the URL.

For example, filename URL checking searches for keywords within the URL www.zyxel.com.tw/news/pressroom.php.

Use the `ip urlfilter customize actionFlags 8 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's complete filename.

PART IV
Management

16

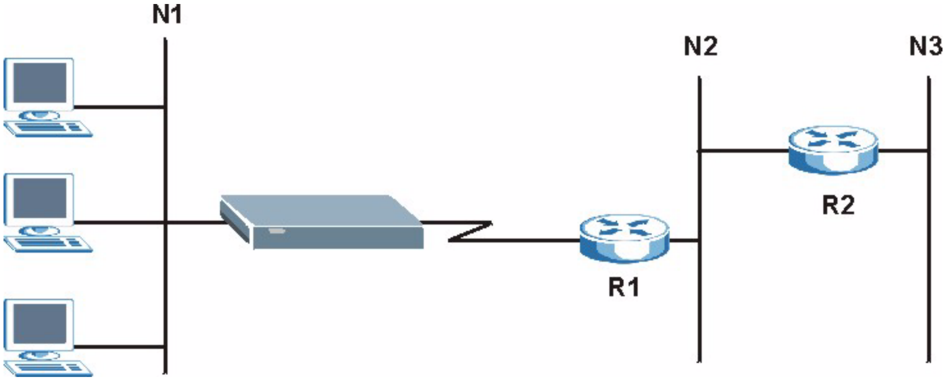
Static Route Screens

This chapter shows you how to configure static routes for your NBG318S.

16.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the NBG318S has no knowledge of the networks beyond. For instance, the NBG318S knows about network **N2** in the following figure through remote node router **R1**. However, the NBG318S 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 **R1** (via gateway router **R2**). The static routes are for you to tell the NBG318S about the networks beyond the remote nodes.

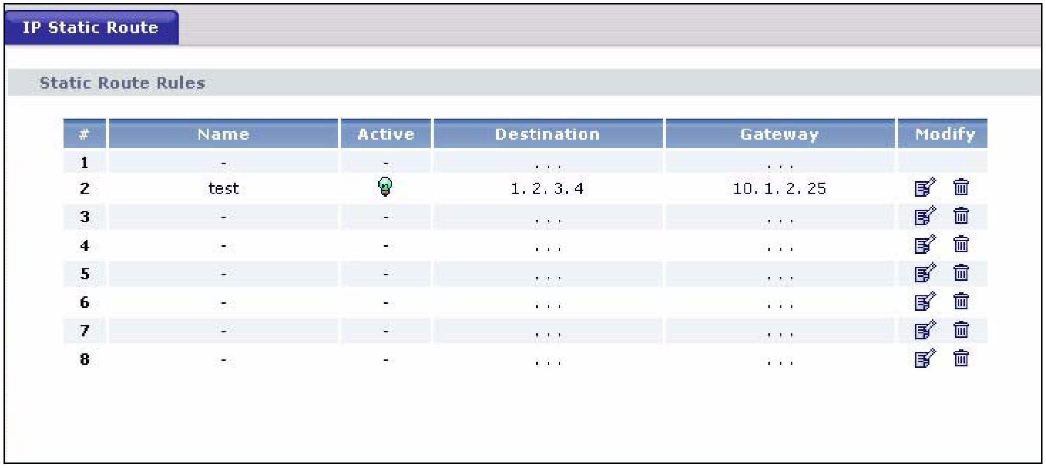
Figure 87 Example of Static Routing Topology



16.2 IP Static Route Screen

Click **Management** > **Static Route** to open the **IP Static Route** screen. The following screen displays.

Figure 88 Management > Static Route > IP Static Route



IP Static Route

Static Route Rules

#	Name	Active	Destination	Gateway	Modify
1	-	-	. . .	. . .	
2	test	●	1.2.3.4	10.1.2.25	✎ 🗑
3	-	-	. . .	. . .	✎ 🗑
4	-	-	. . .	. . .	✎ 🗑
5	-	-	. . .	. . .	✎ 🗑
6	-	-	. . .	. . .	✎ 🗑
7	-	-	. . .	. . .	✎ 🗑
8	-	-	. . .	. . .	✎ 🗑

The following table describes the labels in this screen.

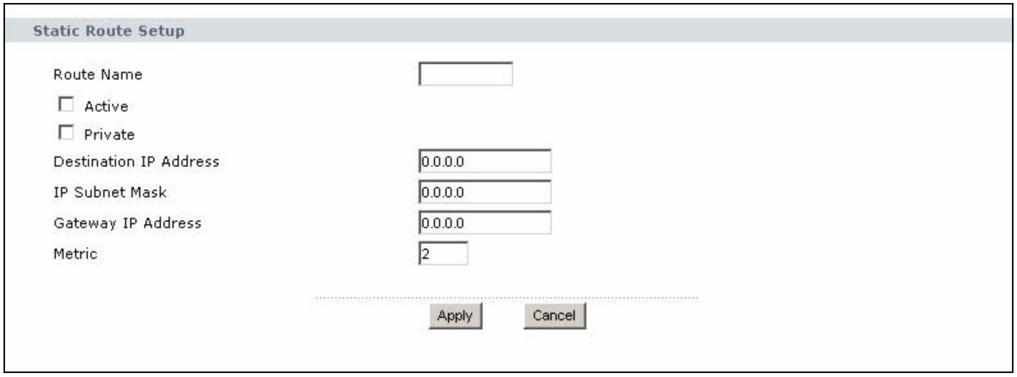
Table 60 Management > Static Route > IP Static Route

LABEL	DESCRIPTION
#	This is the index number of an individual static route. The first entry is for the default route and not editable.
Name	This is the name that describes or identifies this route.
Active	This icon is turned on when this static route is active. Click the **Edit** icon under **Modify** and select the **Active** checkbox in the **Static Route Setup** screen to enable the static route. Clear the checkbox to disable this static route without having to delete the entry.
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 an immediate neighbor of your NBG318S that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your NBG318S; over the WAN, the gateway must be the IP address of one of the remote nodes.
Modify	Click the **Edit** icon to open the static route setup screen. Modify a static route or create a new static route in the **Static Route Setup** screen. Click the **Remove** icon to delete a static route.

16.2.1 Static Route Setup Screen

To edit a static route, click the edit icon under **Modify**. The following screen displays. Fill in the required information for each static route.

Figure 89 Management > Static Route > IP Static Route: Static Route Setup



Static Route Setup

Route Name	
□ Active	
□ Private	
Destination IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Metric	2

The following table describes the labels in this screen.

Table 61 Management > Static Route > IP Static Route: Static Route Setup

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Private	This parameter determines if the NBG318S will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox to propagate this route to other hosts through RIP broadcasts.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your NBG318S that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your NBG318S; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Apply	Click **Apply** to save your changes back to the NBG318S.
Cancel	Click **Cancel** to return to the previous screen and not save your changes.

17

Bandwidth Management

This chapter contains information about configuring bandwidth management, editing rules and viewing the NBG318S's bandwidth management logs.

17.1 Bandwidth Management Overview

ZyXEL's Bandwidth Management allows you to specify bandwidth management rules based on an application and/or subnet. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth rules.

The NBG318S applies bandwidth management to traffic that it forwards out through an interface. The NBG318S does not control the bandwidth of traffic that comes into an interface.

Bandwidth management applies to all traffic flowing out of the router, regardless of the traffic's source.

Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the NBG318S and be managed by bandwidth management.

- The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN, WAN to WAN / NBG318S) must be less than or equal to the **Upstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen.
- The sum of the bandwidth allotments that apply to the LAN port (WAN to LAN, WLAN to LAN, LAN to LAN / NBG318S) must be less than or equal to 100,000 kbps (you cannot configure the bandwidth budget for the LAN port).
- The sum of the bandwidth allotments that apply to the WLAN port (LAN to WLAN, WAN to WLAN, WLAN to WLAN / NBG318S) must be less than or equal to 54,000 kbps (you cannot configure the bandwidth budget for the WLAN port).

17.2 Application-based Bandwidth Management

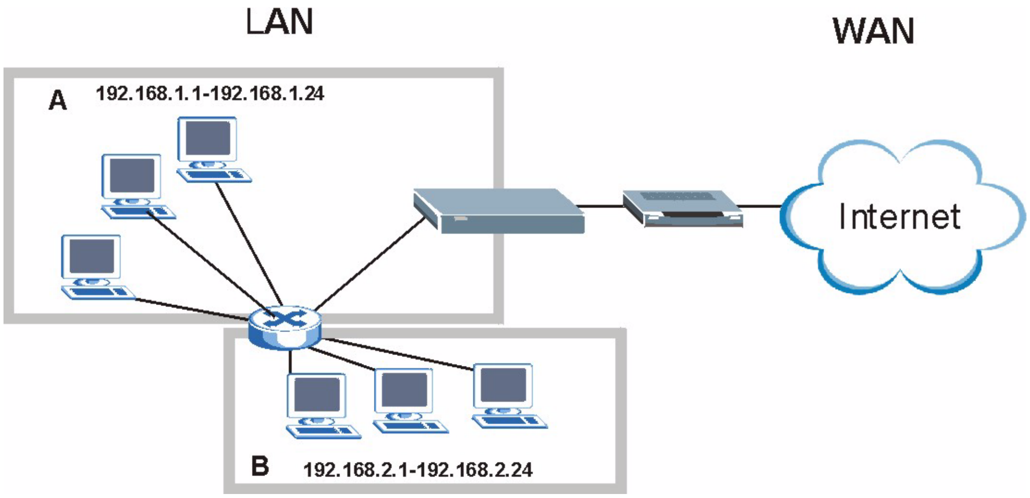
You can create bandwidth classes based on individual applications (like VoIP, Web, FTP, E-mail and Video for example).

17.3 Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets.

The following figure shows LAN subnets. You could configure one bandwidth class for subnet **A** and another for subnet **B**.

Figure 90 Subnet-based Bandwidth Management Example



17.4 Application and Subnet-based Bandwidth Management

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

Table 62 Application and Subnet-based Bandwidth Management Example

	FROM SUBNET A	FROM SUBNET B
VoIP	64 Kbps	64 Kbps
Web	64 Kbps	64 Kbps
FTP	64 Kbps	64 Kbps
E-mail	64 Kbps	64 Kbps
Video	64 Kbps	64 Kbps

17.5 Bandwidth Management Priorities

The following table describes the priorities that you can apply to traffic that the NBG318S forwards out through an interface.

Table 63 Bandwidth Management Priorities

PRIORITY LEVELS: TRAFFIC WITH A HIGHER PRIORITY GETS THROUGH FASTER WHILE TRAFFIC WITH A LOWER PRIORITY IS DROPPED IF THE NETWORK IS CONGESTED.	
High	Typically used for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay).

Table 63 Bandwidth Management Priorities

PRIORITY LEVELS: TRAFFIC WITH A HIGHER PRIORITY GETS THROUGH FASTER WHILE TRAFFIC WITH A LOWER PRIORITY IS DROPPED IF THE NETWORK IS CONGESTED.	
Mid	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Low	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.

17.6 Predefined Bandwidth Management Services

The following is a description of the services that you can select and to which you can apply media bandwidth management using the wizard screens.

Table 64 Media Bandwidth Management Setup: Services

	DESCRIPTION
Xbox Live	This is Microsoft’s online gaming service that lets you play multiplayer Xbox games on the Internet via broadband technology. Xbox Live uses port 3074.
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, using the default port number 5060.
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses port number 21.
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: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80
eMule	EMule is a free P2P file sharing tool which allows you to download and share files. Similar to other P2P applications, users download a section of a file and then share it with peers. EMule does not rely on any specific port as it selects ports at random on startup.
BitTorrent	BitTorrent is a free P2P (peer-to-peer) sharing tool allowing you to distribute large software and media files using ports 6881 to 6889. BitTorrent requires you to search for a file with a searching engine yourself. It distributes files by co-orporation 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.
MSN Webcam	MSN messenger allows you to chat online and send instant messages. If you use MSN messenger and also have a webcam, you can send your image/photo in real-time along with messages
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.

17.6.1 Services and Port Numbers

The commonly used services and port numbers are shown in Appendix F on page 287.

17.6.2 Default Bandwidth Management Classes and Priorities

If you enable bandwidth management but do not configure a rule for critical traffic like VoIP, the voice traffic may then get delayed due to insufficient bandwidth. With the automatic traffic classifier feature activated, the NBG318S automatically assigns a default bandwidth management class and priority to traffic that does not match any of the user-defined rules. The traffic is classified based on the traffic type. Real-time traffic always gets higher priority over other traffic.

The following table shows you the priorities between the three default classes (**AutoClass_H**, **AutoClass_M** and **Default Class**) and user-defined rules. 6 is the highest priority.

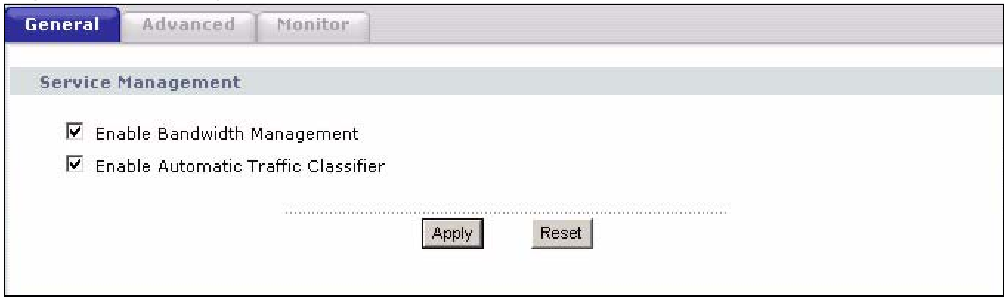
Table 65 Bandwidth Management Priority with Default Classes

CLASS TYPE	PRIORITY
User-defined with high priority	6
AutoClass_H	5
User-defined with medium priority	4
AutoClass_M	3
User-defined with low priority	2
Default Class	1

17.7 Bandwidth Management General Configuration

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

Figure 91 Management > Bandwidth MGMT > General



Service Management

☑ Enable Bandwidth Management

☑ Enable Automatic Traffic Classifier

The following table describes the labels in this screen.

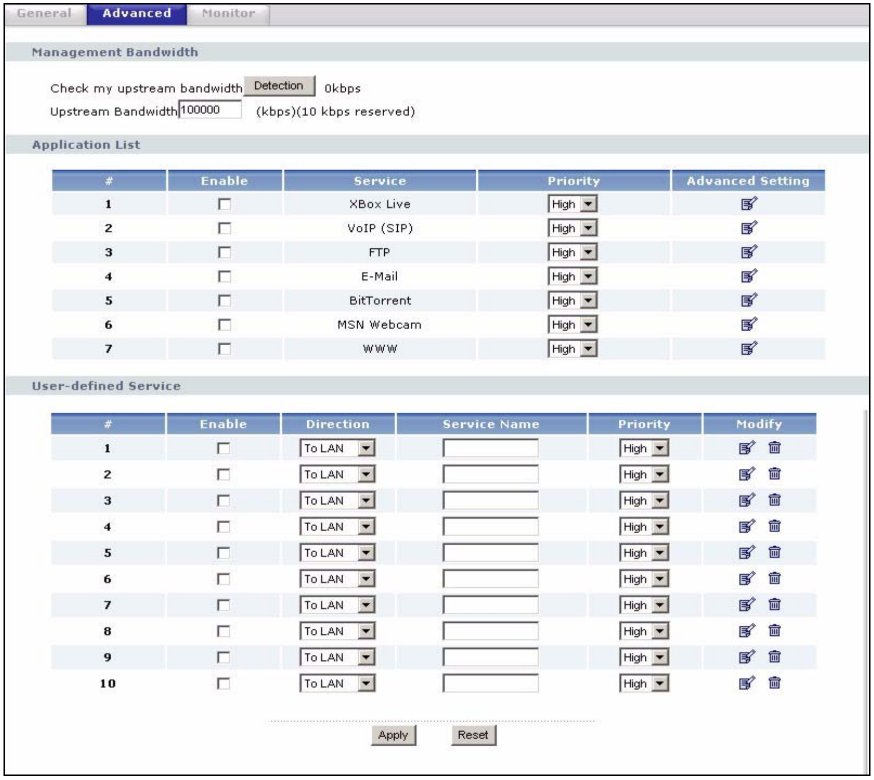
Table 66 Management > Bandwidth MGMT > General

LABEL	DESCRIPTION
Enable Bandwidth Management	Select this check box to have the NBG318S 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.
Enable Automatic Traffic Classifier	This field is only applicable when you select the **Enable Bandwidth Management** check box. Select this check box to have the NBG318S base on the default bandwidth classes to apply bandwidth management. Real-time packets, such as VoIP traffic always get higher priority.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

17.8 Bandwidth Management Advanced Configuration

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

Figure 92 Management > Bandwidth MGMT > Advanced



Management Bandwidth

Check my upstream bandwidth [Detection] 0kbps

Upstream Bandwidth 100000 (kbps)(10 kbps reserved)

Application List

#	Enable	Service	Priority	Advanced Setting
1	□	XBox Live	High	✎
2	□	VoIP (SIP)	High	✎
3	□	FTP	High	✎
4	□	E-Mail	High	✎
5	□	BitTorrent	High	✎
6	□	MSN Webcam	High	✎
7	□	WWW	High	✎

User-defined Service

#	Enable	Direction	Service Name	Priority	Modify
1	□	To LAN		High	✎ 🗑
2	□	To LAN		High	✎ 🗑
3	□	To LAN		High	✎ 🗑
4	□	To LAN		High	✎ 🗑
5	□	To LAN		High	✎ 🗑
6	□	To LAN		High	✎ 🗑
7	□	To LAN		High	✎ 🗑
8	□	To LAN		High	✎ 🗑
9	□	To LAN		High	✎ 🗑
10	□	To LAN		High	✎ 🗑

The following table describes the labels in this screen.

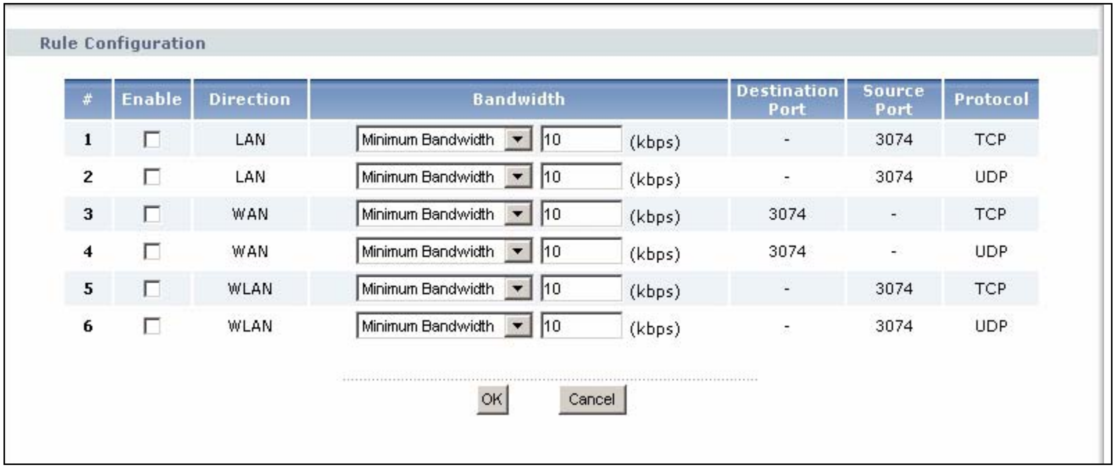
Table 67 Management > Bandwidth MGMT > Advanced

	DESCRIPTION
Check my upstream bandwidth	Click the **Detection** button to check the size of your upstream bandwidth.
Upstream Bandwidth (kbps)	Enter the amount of bandwidth in kbps (2 to 100,000) that you want to allocate for traffic. 20 kbps to 20,000 kbps is recommended. The recommendation is to set this speed to be equal to or less than the speed of the broadband device connected to the WAN port. For example, set the speed to 1000 Kbps (or less) if the broadband device connected to the WAN port has an upstream speed of 1000 Kbps.
Application List	Use this table to allocate specific amounts of bandwidth based on the pre-defined service.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the NBG318S apply this bandwidth management rule.
Service	This is the name of the service.
Priority	Select a priority from the drop down list box. Choose **High**, **Mid** or **Low**.
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 and/or subnets.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the NBG318S apply this bandwidth management rule.
Direction	Select **To LAN** to apply bandwidth management to traffic that the NBG318S forwards to the LAN. Select **To WAN** to apply bandwidth management to traffic that the NBG318S forwards to the WAN. Select **To WLAN** to apply bandwidth management to traffic that the NBG318S forwards to the WLAN.
Service Name	Enter a descriptive name of up to 19 alphanumeric characters, including spaces.
Priority	Select a priority from the drop down list box. Choose **High**, **Mid** or **Low**.
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 17.8.2 on page 173 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.

17.8.1 Rule Configuration with the Pre-defined Service

To edit a bandwidth management rule for the pre-defined service in the NBG318S, click the **Edit** icon in the **Application List** table of the **Advanced** screen. **Enable Bandwidth Management** needs to be selected in the General screen. The following screen displays.

Figure 93 Management > Bandwidth MGMT > Advanced: Rule Configuration



Rule Configuration

#	Enable	Direction	Bandwidth	Destination Port	Source Port	Protocol
1	□	LAN	Minimum Bandwidth ▼ 10 (kbps)	-	3074	TCP
2	□	LAN	Minimum Bandwidth ▼ 10 (kbps)	-	3074	UDP
3	□	WAN	Minimum Bandwidth ▼ 10 (kbps)	3074	-	TCP
4	□	WAN	Minimum Bandwidth ▼ 10 (kbps)	3074	-	UDP
5	□	WLAN	Minimum Bandwidth ▼ 10 (kbps)	-	3074	TCP
6	□	WLAN	Minimum Bandwidth ▼ 10 (kbps)	-	3074	UDP

The following table describes the labels in this screen.

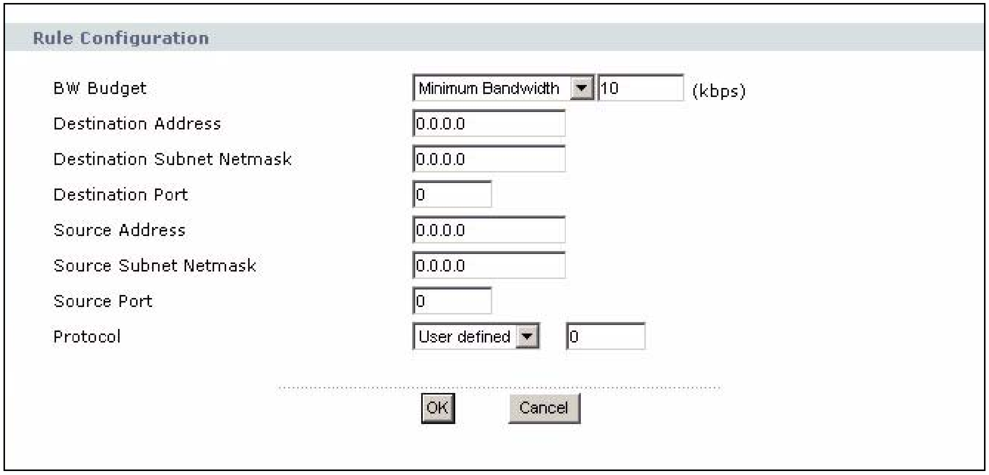
Table 68 Management > Bandwidth MGMT > Advanced: Application Rule Configuration

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 NBG318S 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. See Appendix F on page 287 for some common services and port numbers.
Source Port	This is the port number of the source. See Appendix F on page 287 for some common services and port numbers.
Protocol	This is the protocol (**TCP** or **UDP**) used for the service.
OK	Click **OK** to save your customized settings.
Cancel	Click **Cancel** to exit this screen without saving.

17.8.2 Rule Configuration with the User-defined Service

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

Figure 94 Management > Bandwidth MGMT > Advanced: User-defined Service Rule Configuration



Rule Configuration

BW Budget	Minimum Bandwidth ▼ 10 (kbps)
Destination Address	0.0.0.0
Destination Subnet Netmask	0.0.0.0
Destination Port	0
Source Address	0.0.0.0
Source Subnet Netmask	0.0.0.0
Source Port	0
Protocol	User defined ▼ 0

The following table describes the labels in this screen

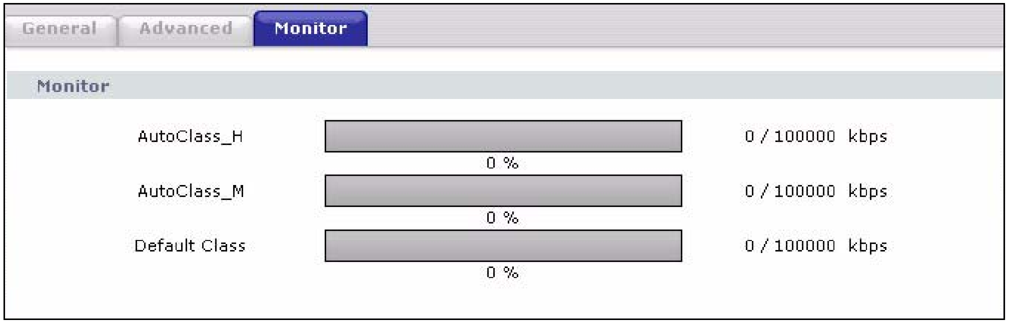
Table 69 Management > Bandwidth MGMT > Advanced: User-defined Service Rule Configuration

	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 destination IP address in dotted decimal notation.
Destination Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a **Destination Address**. Refer to the appendices for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See Appendix F on page 287 for some common services and port numbers.
Source Address	Enter the source IP address in dotted decimal notation.
Source Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a **Source Address**. Refer to the appendices for more information on IP subnetting.
Source Port	Enter the port number of the source. See Appendix F on page 287 for some common services and port numbers.
Protocol	Select the protocol (**TCP** or **UDP**) or select **User defined** and enter the protocol (service type) number.
OK	Click **OK** to save your customized settings.
Cancel	Click **Cancel** to exit this screen without saving.

17.9 Bandwidth Management Monitor

Click **Management** > **Bandwidth MGMT** > **Monitor** to open the bandwidth management **Monitor** screen. View the bandwidth usage of the WAN configured bandwidth rules. This is also shown as bandwidth usage over the bandwidth budget for each rule. The gray section of the bar represents the percentage of unused bandwidth and the blue color represents the percentage of bandwidth in use.

Figure 95 Management > Bandwidth MGMT > Monitor



Monitor

AutoClass_H 0 % 0 / 100000 kbps

AutoClass_M 0 % 0 / 100000 kbps

Default Class 0 % 0 / 100000 kbps

18

Remote Management

This chapter provides information on the Remote Management screens.

18.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which NBG318S interface (if any) from which computers.

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

You may manage your NBG318S from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN and WAN)
- Neither (Disable).

When you choose **WAN** or **LAN & WAN**, you still need to configure a firewall rule to allow access.

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

You may only have one remote management session running at a time. The NBG318S automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Telnet
2. HTTP

18.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. You have disabled that service in one of the remote management screens.
2. The IP address in the **Secured Client IP Address** field does not match the client IP address. If it does not match, the NBG318S will disconnect the session immediately.
3. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
4. There is a firewall rule that blocks it.

18.1.2 Remote Management and NAT

When NAT is enabled:

- Use the NBG318S's WAN IP address when configuring from the WAN.
- Use the NBG318S's LAN IP address when configuring from the LAN.

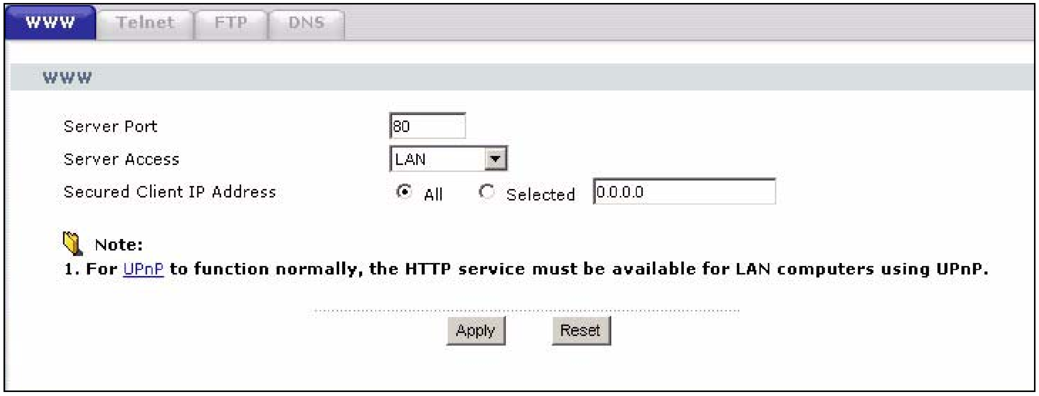
18.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The NBG318S 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

18.2 WWW Screen

To change your NBG318S's World Wide Web settings, click **Management** > **Remote MGMT** to display the **WWW** screen.

Figure 96 Management > Remote MGMT > WWW



WWW

Server Port: 80

Server Access: LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Note:
1. For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

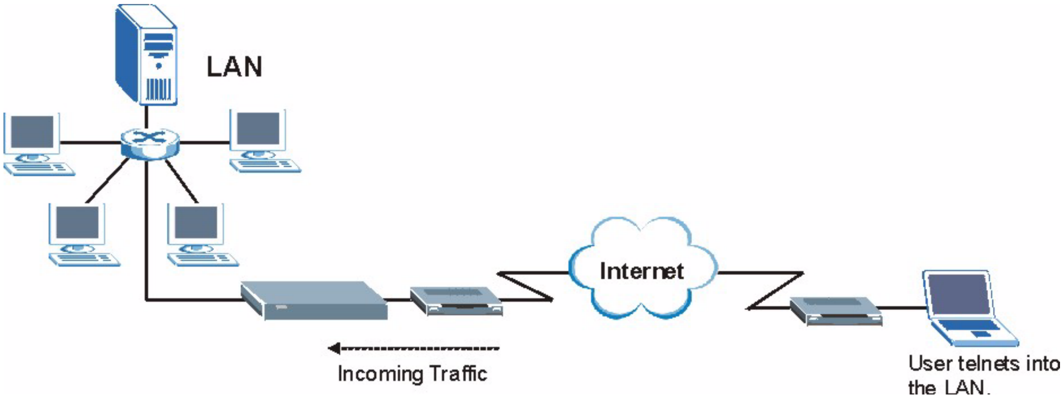
The following table describes the labels in this screen

Table 70 Management > Remote MGMT > WWW

18.3 Telnet

You can configure your NBG318S for remote Telnet access as shown next. The administrator uses Telnet from a computer on a remote network to access the NBG318S.

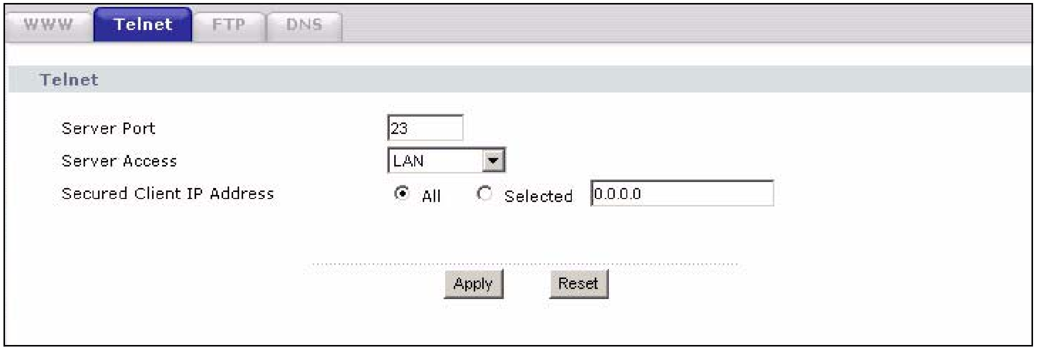
Figure 97 Telnet Configuration on a TCP/IP Network



18.4 Telnet Screen

To change your NBG318S's Telnet settings, click **Management** > **Remote MGMT** > **Telnet**. The following screen displays.

Figure 98 Management > Remote MGMT > Telnet



Telnet

Server Port: 23

Server Access: LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

Table 71 Management > Remote MGMT > Telnet

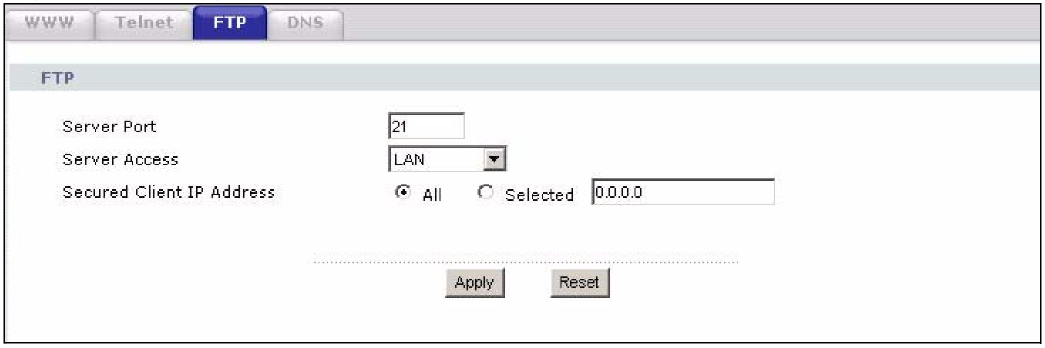
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NBG318S using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the NBG318S using this service. Select **All** to allow any computer to access the NBG318S using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the NBG318S using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

18.5 FTP Screen

You can upload and download the NBG318S's firmware and configuration files using FTP, please see the chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your NBG318S's FTP settings, click **Management** > **Remote MGMT** > **FTP**. The screen appears as shown.

Figure 99 Management > Remote MGMT > FTP



Server Port: 21

Server Access: LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

Table 72 Management > Remote MGMT > FTP

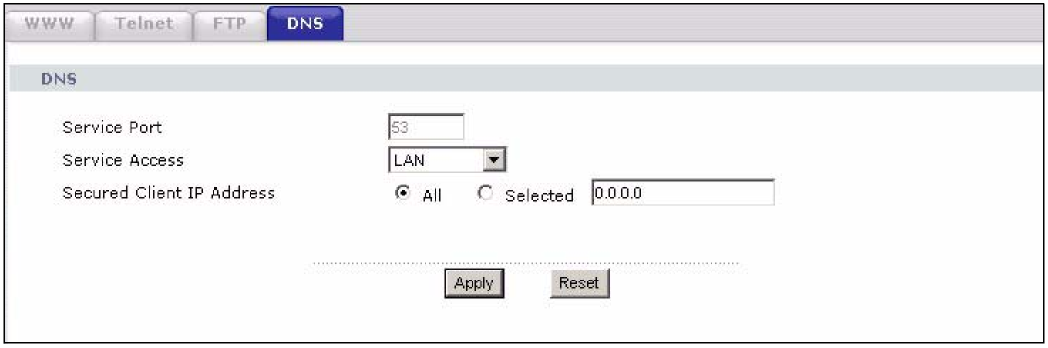
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NBG318S using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the NBG318S using this service. Select **All** to allow any computer to access the NBG318S using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the NBG318S using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

18.6 DNS Screen

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to the chapter on Wizard Setup for background information.

To change your NBG318S's DNS settings, click **Management** > **Remote MGMT** > **DNS**. The screen appears as shown.

Figure 100 Management > Remote MGMT > DNS



DNS

Service Port 53

Service Access LAN

Secured Client IP Address ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

Table 73 Management > Remote MGMT > DNS

LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interface(s) through which a computer may send DNS queries to the NBG318S.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to send DNS queries to the NBG318S. Select **All** to allow any computer to send DNS queries to the NBG318S. Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the NBG318S.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

19

Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

19.1 Introducing Universal Plug and Play

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.

See Section 19.3 on page 184 for configuration instructions.

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

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

19.1.2 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.

19.1.3 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 NBG318S 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.

19.2 UPnP and ZyXEL

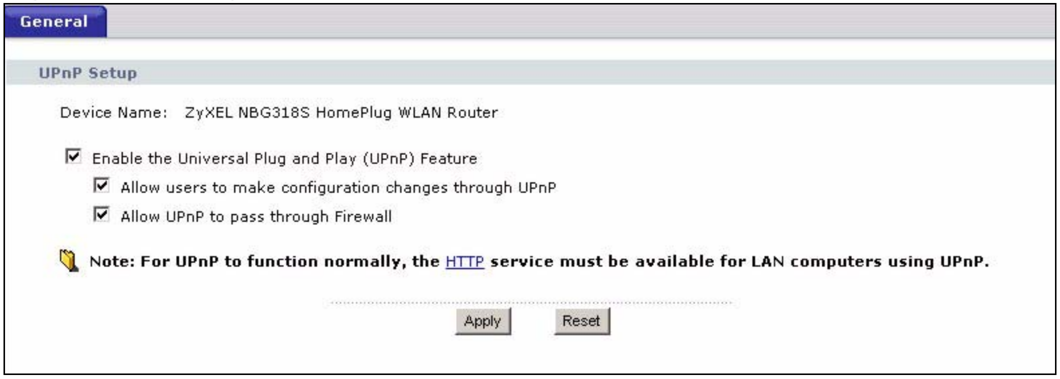
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See the following sections for examples of installing and using UPnP.

19.3 UPnP Screen

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

Figure 101 Management > UPnP > General



Device Name: ZyXEL NBG318S HomePlug WLAN Router

☑ Enable the Universal Plug and Play (UPnP) Feature

☑ Allow users to make configuration changes through UPnP

☑ Allow UPnP to pass through Firewall

Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

The following table describes the labels in this screen.

Table 74 Management > UPnP > General

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the NBG318S's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the NBG318S so that they can communicate through the NBG318S, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through Firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).

Table 74 Management > UPnP > General

LABEL	DESCRIPTION
Apply	Click **Apply** to save the setting to the NBG318S.
Cancel	Click **Cancel** to return to the previously saved settings.

19.4 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

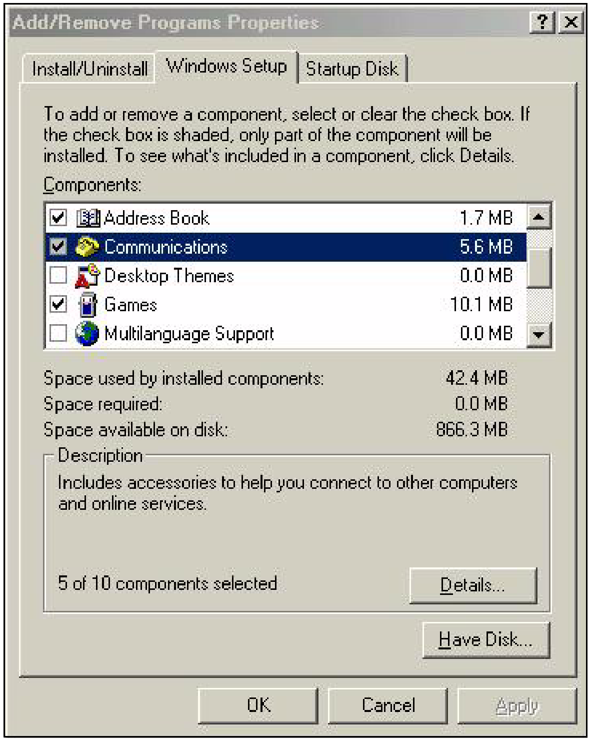
19.4.0.1 Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 102 Add/Remove Programs: Windows Setup: Communication



Add/Remove Programs Properties

To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Address Book	1.7 MB
☑	Communications	5.6 MB
□	Desktop Themes	0.0 MB
☑	Games	10.1 MB
□	Multilanguage Support	0.0 MB

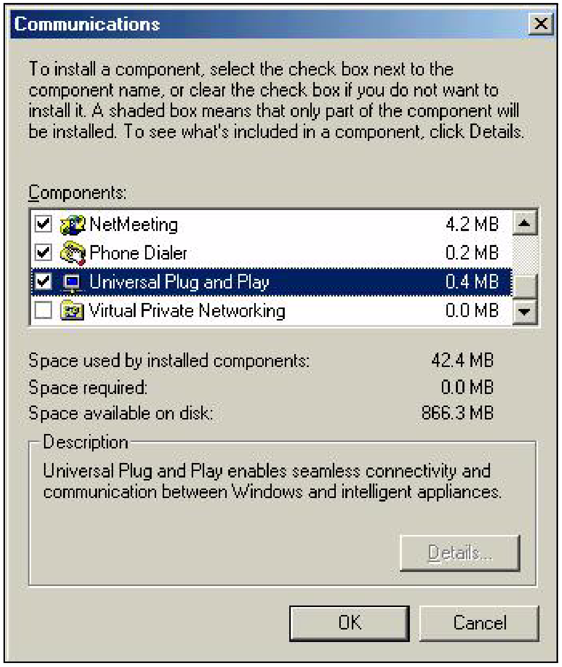
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

Description
Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 103 Add/Remove Programs: Windows Setup: Communication: Components



Communications

To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	NetMeeting	4.2 MB
☑	Phone Dialer	0.2 MB
☑	Universal Plug and Play	0.4 MB
☐	Virtual Private Networking	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

Description

Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Installing UPnP in Windows XP

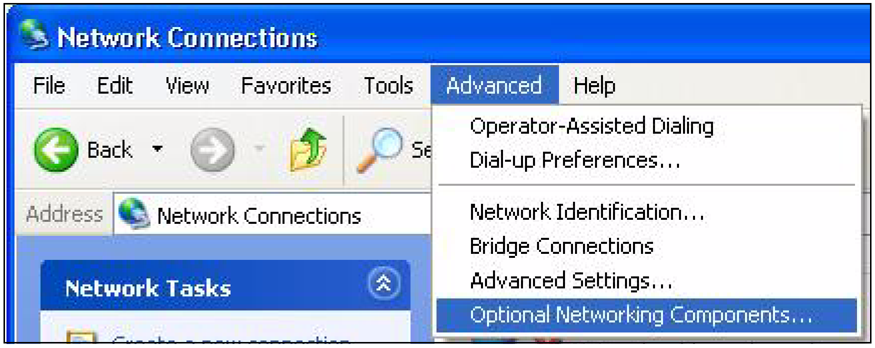
Follow the steps below to install the UPnP in Windows XP.

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

2 Double-click **Network Connections**.

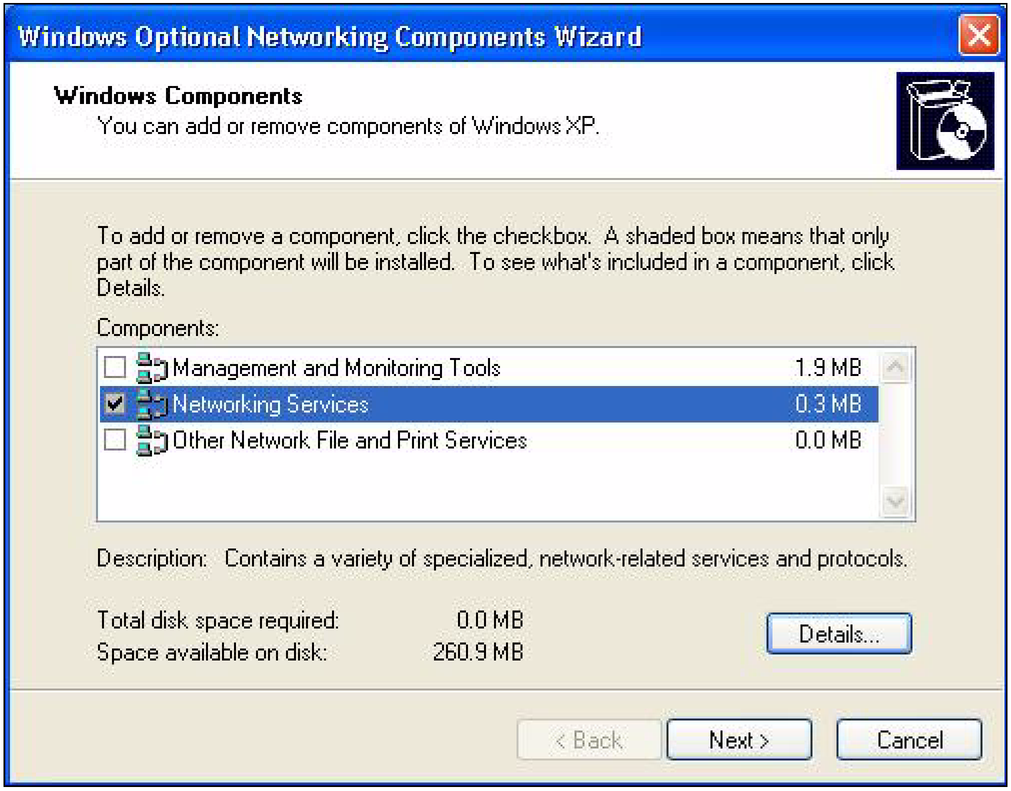
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**

Figure 104 Network Connections



4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 105 Windows Optional Networking Components Wizard



Windows Optional Networking Components Wizard

Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

□	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB

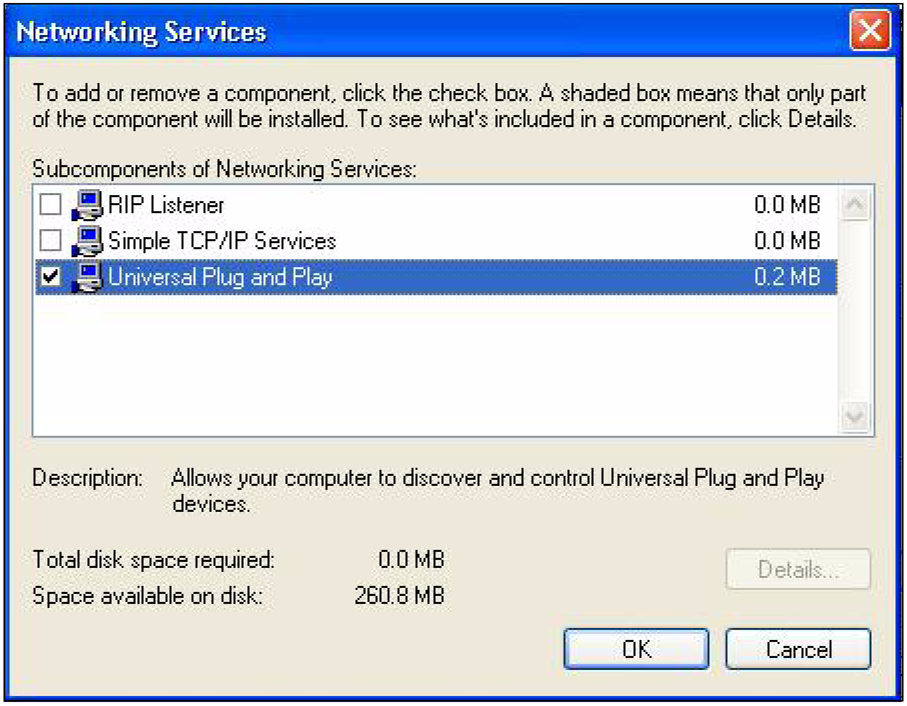
Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 260.9 MB

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 106 Networking Services



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

□	RIP Listener	0.0 MB
□	Simple TCP/IP Services	0.0 MB
☑	Universal Plug and Play	0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB

Space available on disk: 260.8 MB

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

19.4.0.2 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 NBG318S.

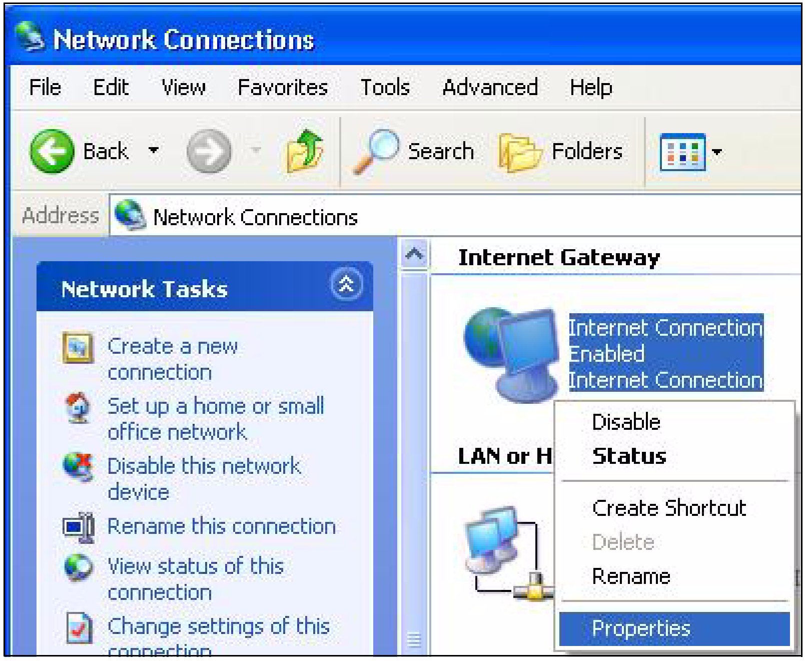
Make sure the computer is connected to a LAN port of the NBG318S. Turn on your computer and the NBG318S.

Auto-discover Your UPnP-enabled Network Device

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

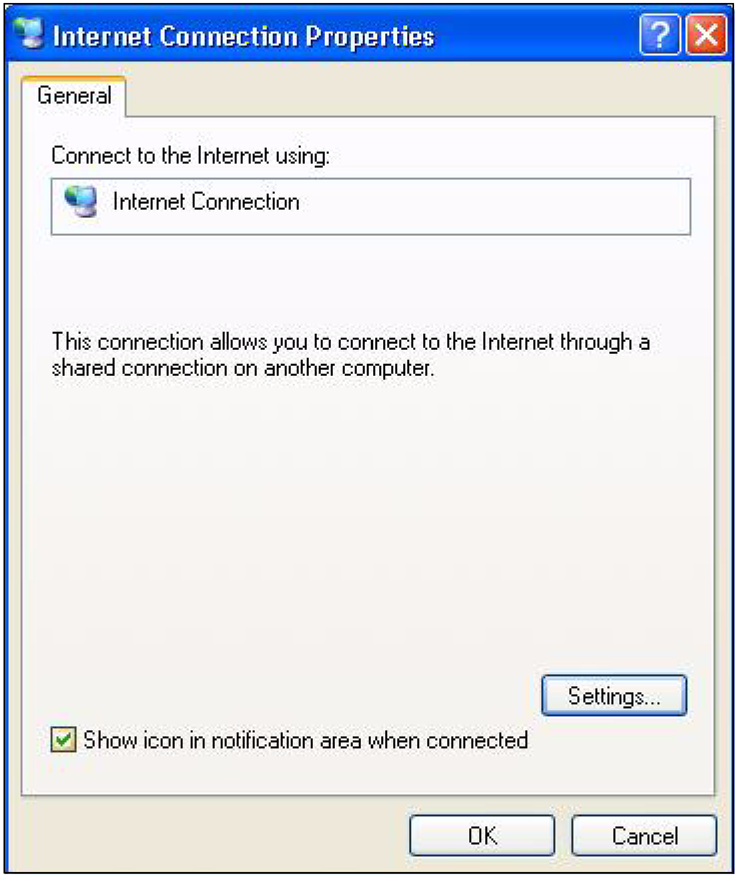
2 Right-click the icon and select **Properties**.

Figure 107 Network Connections



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

Figure 108 Internet Connection Properties



Connect to the Internet using:

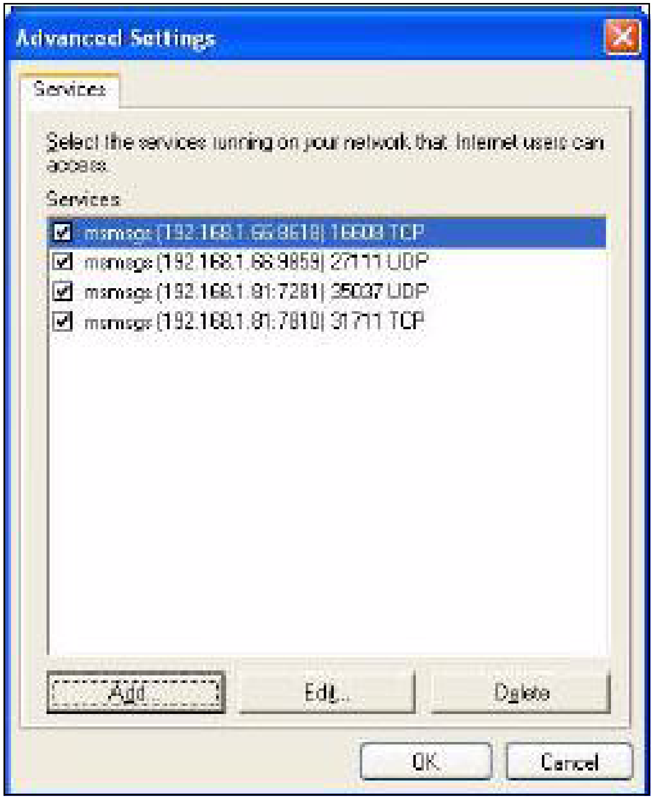
Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

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

Figure 109 Internet Connection Properties: Advanced Settings

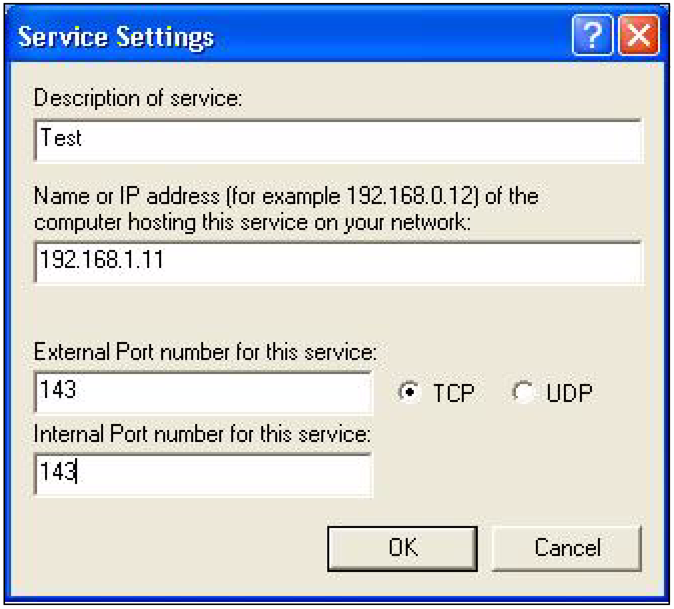


Select the services running on your network that Internet users can access.

Services

- ☑ msmsgs (192.168.1.66:8618) 16609 TCP
- ☑ msmsgs (192.168.1.66:9859) 27111 UDP
- ☑ msmsgs (192.168.1.81:7281) 35037 UDP
- ☑ msmsgs (192.168.1.81:7810) 31711 TCP

Figure 110 Internet Connection Properties: Advanced Settings: Add



Description of service:
Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
192.168.1.11

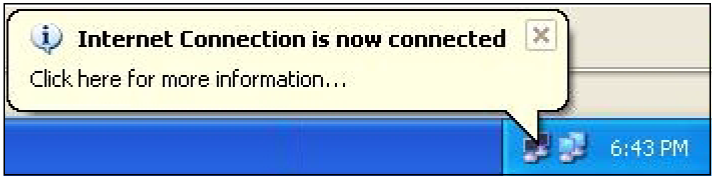
External Port number for this service:
143 ● TCP ○ UDP

Internal Port number for this service:
143

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

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

Figure 111 System Tray Icon

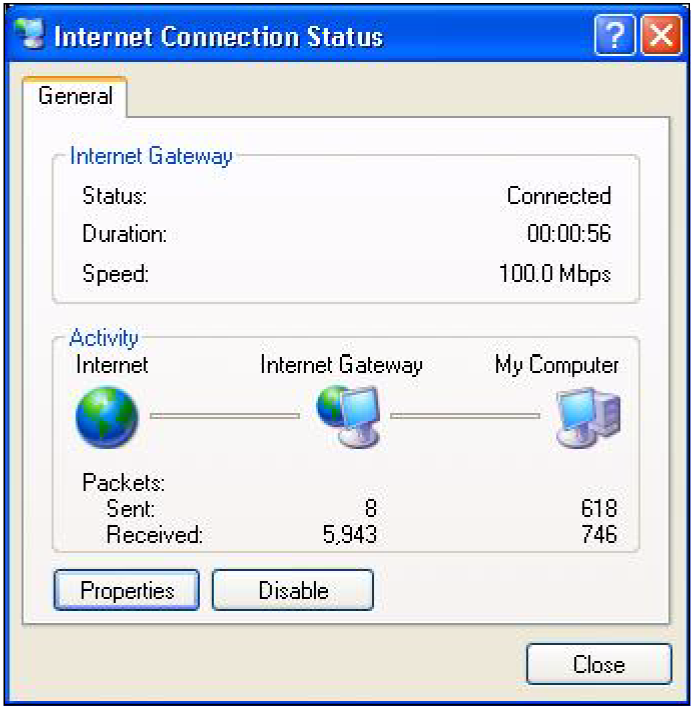


Internet Connection is now connected

Click here for more information...

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

Figure 112 Internet Connection Status



Internet Connection Status

Internet Gateway

Status: Connected

Duration: 00:00:56

Speed: 100.0 Mbps

Activity

Internet	Internet Gateway	My Computer
Packets:		
Sent:	8	618
Received:	5,943	746

Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the NBG318S without finding out the IP address of the NBG318S first. This comes helpful if you do not know the IP address of the NBG318S.

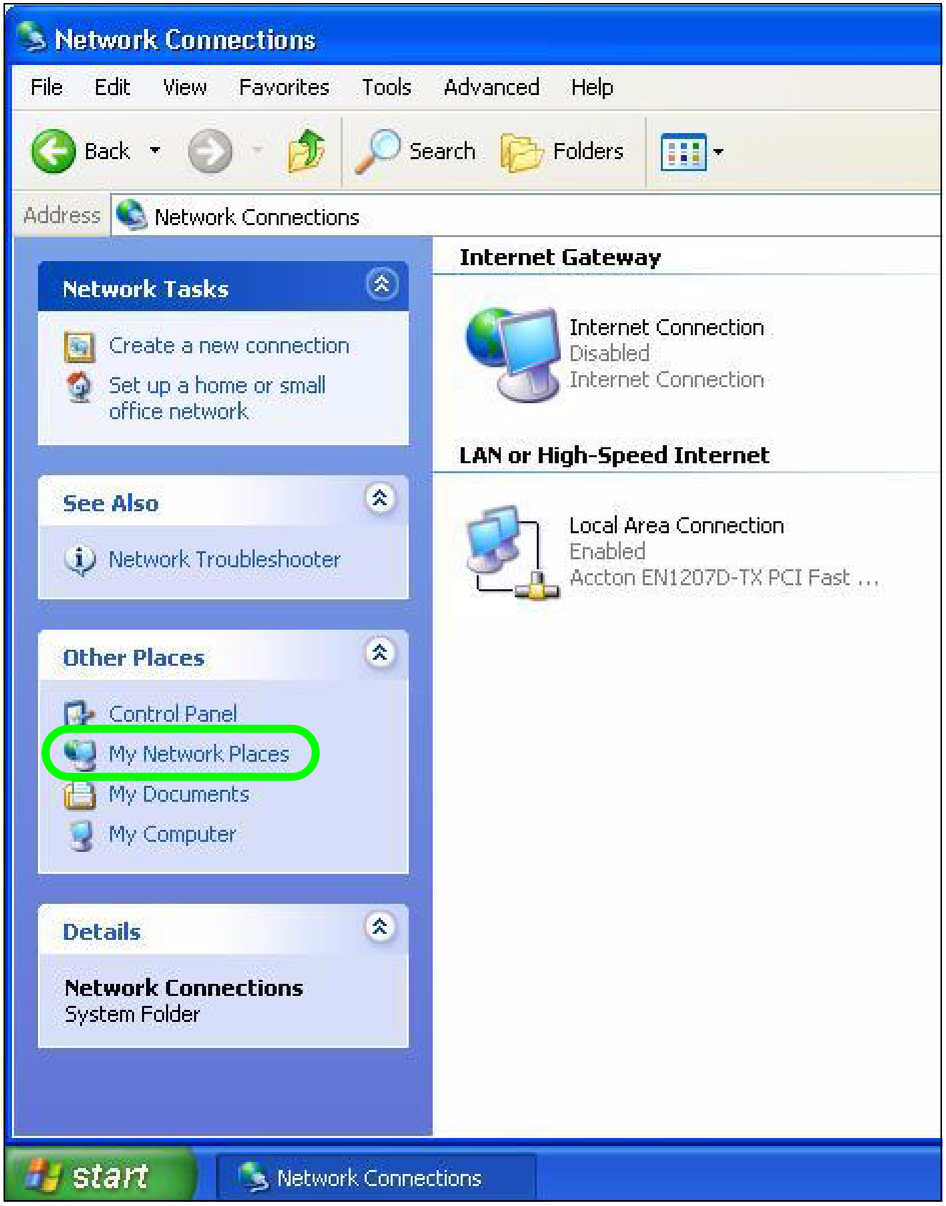
Follow the steps below to access the web configurator.

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

2 Double-click **Network Connections**.

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

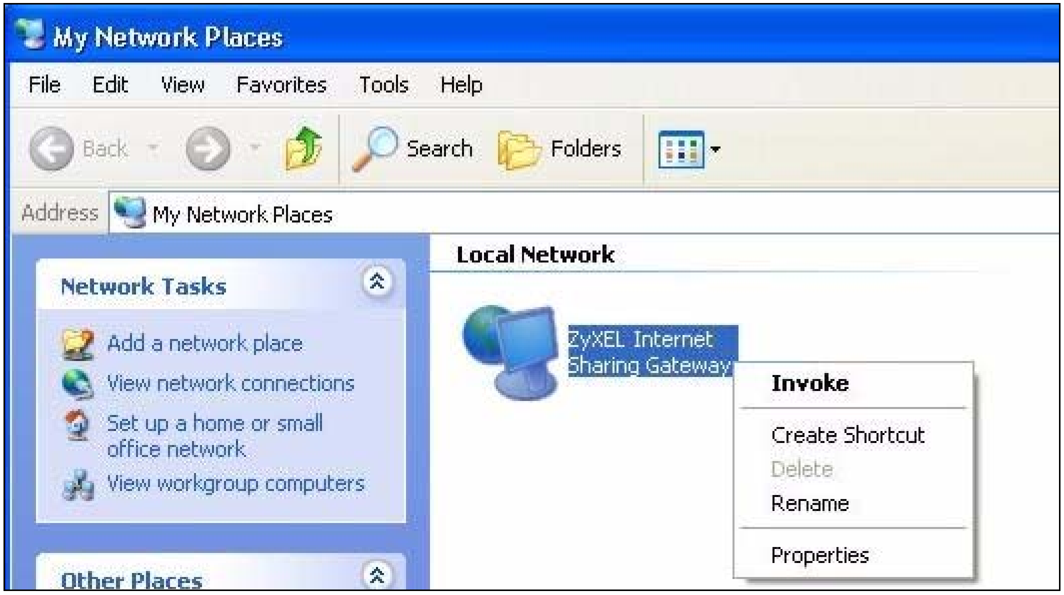
Figure 113 Network Connections



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

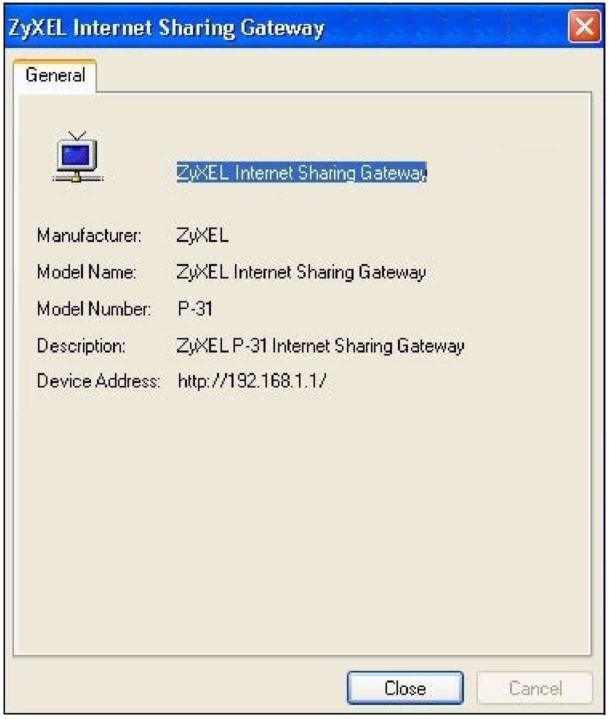
5 Right-click on the icon for your NBG318S and select **Invoke**. The web configurator login screen displays.

Figure 114 Network Connections: My Network Places



6 Right-click on the icon for your NBG318S and select **Properties**. A properties window displays with basic information about the NBG318S.

Figure 115 Network Connections: My Network Places: Properties: Example



ZyXEL Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number: P-31

Description: ZyXEL P-31 Internet Sharing Gateway

Device Address: http://192.168.1.1/

PART V
Maintenance and Troubleshooting

20

System

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

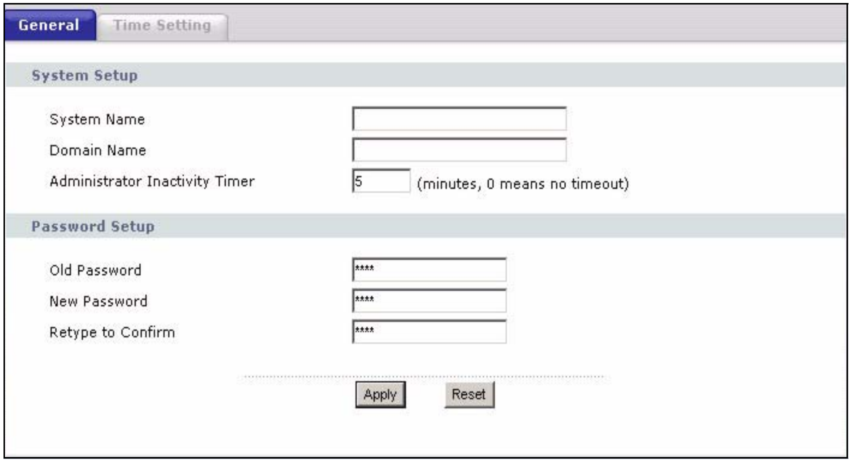
20.1 System Overview

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

20.2 System General Screen

Click **Maintenance** > **System**. The following screen displays.

Figure 116 Maintenance > System > General



System Name

Domain Name

Administrator Inactivity Timer: 5 (minutes, 0 means no timeout)

Old Password: ****

New Password: ****

Retype to Confirm: ****

The following table describes the labels in this screen.

Table 75 Maintenance > System > General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the NBG318S in an Ethernet network. It is recommended you enter your computer's "Computer name" in this field (see the chapter about wizard setup for how to find your computer's name). This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.

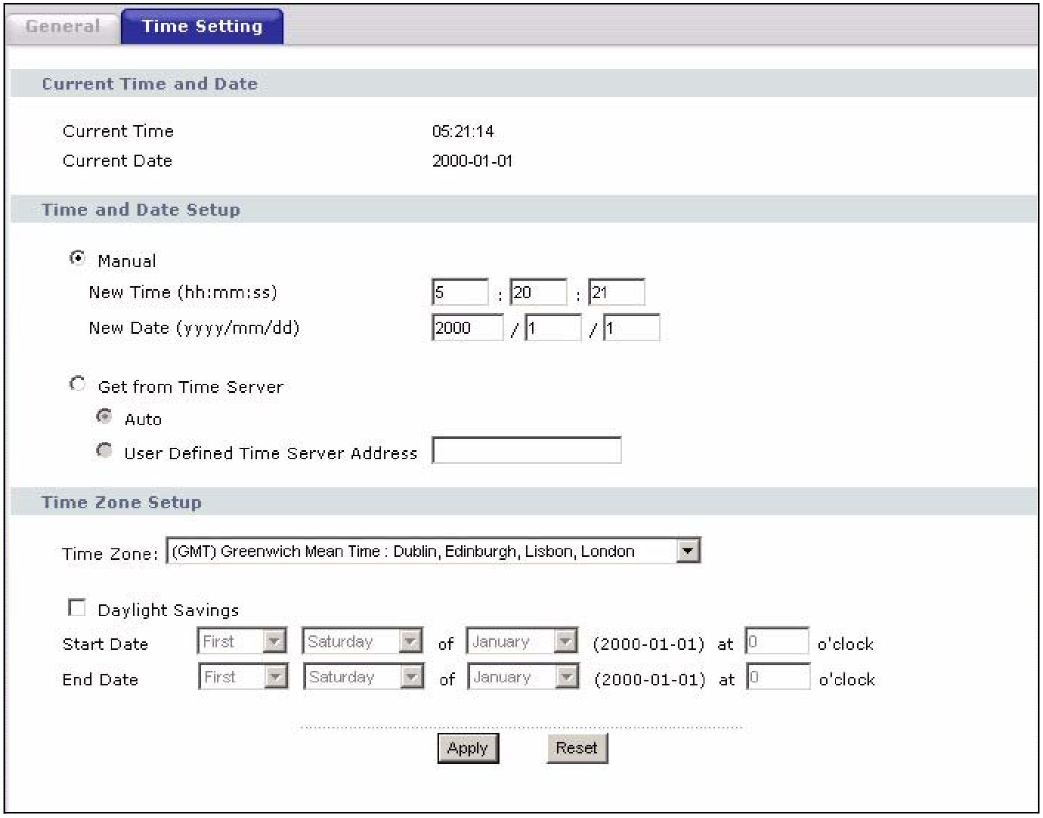
Table 75 Maintenance > System > General

LABEL	DESCRIPTION
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password Setup	Change your NBG318S'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 NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

20.3 Time Setting Screen

To change your NBG318S's time and date, click **Maintenance** > **System** > **Time Setting**. The screen appears as shown. Use this screen to configure the NBG318S's time based on your local time zone.

Figure 117 Maintenance > System > Time Setting



Current Time and Date

Current Time 05:21:14

Current Date 2000-01-01

Time and Date Setup

● Manual

New Time (hh:mm:ss) 5 : 20 : 21

New Date (yyyy/mm/dd) 2000 / 1 / 1

○ Get from Time Server

● Auto

○ User Defined Time Server Address

Time Zone Setup

Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

□ Daylight Savings

Start Date First Saturday of January (2000-01-01) at 0 o'clock

End Date First Saturday of January (2000-01-01) at 0 o'clock

The following table describes the labels in this screen.

Table 76 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NBG318S. Each time you reload this page, the NBG318S synchronizes the time with the time server.
Current Date	This field displays the date of your NBG318S. Each time you reload this page, the NBG318S synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the NBG318S get the time and date from the time server you specified below.
Auto	Select **Auto** to have the NBG318S 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 type 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 type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 76 Maintenance > System > Time Setting

LABEL	DESCRIPTION
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 type 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 type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the NBG318S.
Reset	Click **Reset** to begin configuring this screen afresh.

21

Logs

This chapter contains information about configuring general log settings and viewing the NBG318S's logs. Refer to the appendices for example log message explanations.

21.1 View Log

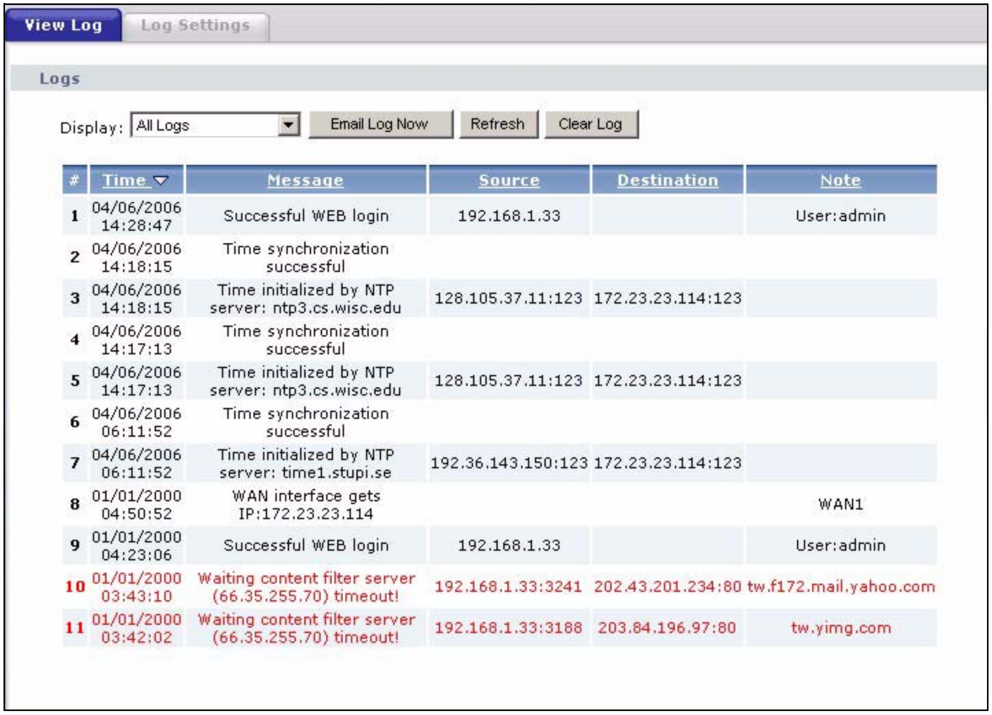
The web configurator allows you to look at all of the NBG318S's logs in one location.

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

Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 21.2 on page 202). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, Java and cookies), attacks (such as DoS) and IPSec.

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

Figure 118 Maintenance > Logs > View Log



#	Time	Message	Source	Destination	Note
1	04/06/2006 14:28:47	Successful WEB login	192.168.1.33		User:admin
2	04/06/2006 14:18:15	Time synchronization successful			
3	04/06/2006 14:18:15	Time initialized by NTP server: ntp3.cs.wisc.edu	128.105.37.11:123	172.23.23.114:123	
4	04/06/2006 14:17:13	Time synchronization successful			
5	04/06/2006 14:17:13	Time initialized by NTP server: ntp3.cs.wisc.edu	128.105.37.11:123	172.23.23.114:123	
6	04/06/2006 06:11:52	Time synchronization successful			
7	04/06/2006 06:11:52	Time initialized by NTP server: time1.stupi.se	192.36.143.150:123	172.23.23.114:123	
8	01/01/2000 04:50:52	WAN interface gets IP:172.23.23.114			WAN1
9	01/01/2000 04:23:06	Successful WEB login	192.168.1.33		User:admin
10	01/01/2000 03:43:10	Waiting content filter server (66.35.255.70) timeout!	192.168.1.33:3241	202.43.201.234:80	tw.f172.mail.yahoo.com
11	01/01/2000 03:42:02	Waiting content filter server (66.35.255.70) timeout!	192.168.1.33:3188	203.84.196.97:80	tw.yimg.com

The following table describes the labels in this screen.

Table 77 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** page (see Section 21.2 on page 202) display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **Address Info** fields in **Log Settings**).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the NBG318S's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.

21.2 Log Settings

You can configure the NBG318S's general log settings in one location.

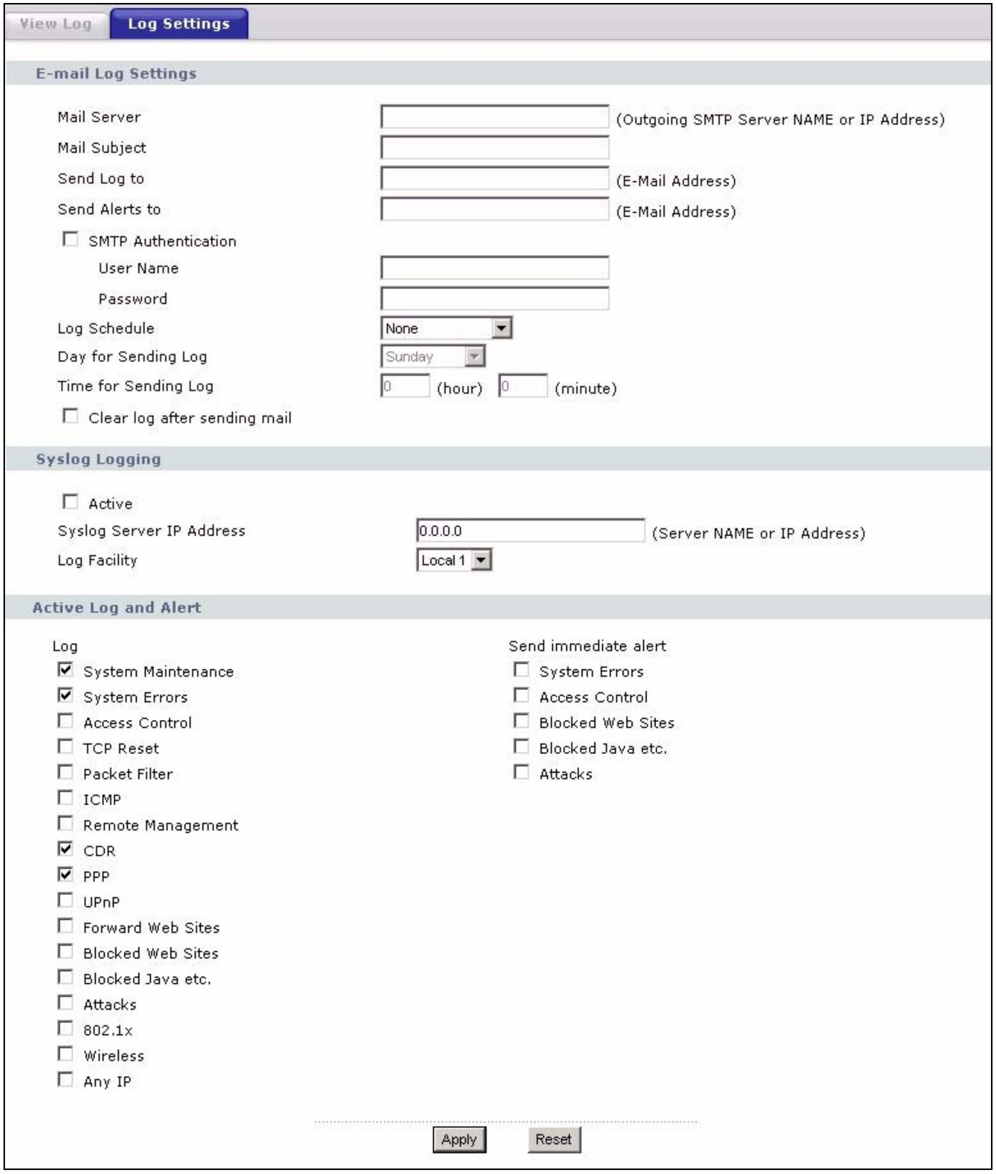
Click **Maintenance** > **Logs** > **Log Settings** to open the **Log Settings** screen.

Use the **Log Settings** screen to configure to where the NBG318S is to send logs; the schedule for when the NBG318S is to send the logs and which logs and/or immediate alerts the NBG318S to send.

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

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

Figure 119 Maintenance > Logs > Log Settings



E-mail Log Settings

Mail Server ______ (Outgoing SMTP Server NAME or IP Address)

Mail Subject ______

Send Log to ______ (E-Mail Address)

Send Alerts to ______ (E-Mail Address)

□ SMTP Authentication

User Name ______

Password ______

Log Schedule: None

Day for Sending Log: Sunday

Time for Sending Log: 0 (hour) 0 (minute)

□ Clear log after sending mail

Syslog Logging

□ Active

Syslog Server IP Address: 0.0.0.0 (Server NAME or IP Address)

Log Facility: Local 1

Active Log and Alert

Log	Send immediate alert
☑ System Maintenance	□ System Errors
☑ System Errors	□ Access Control
□ Access Control	□ Blocked Web Sites
□ TCP Reset	□ Blocked Java etc.
□ Packet Filter	□ Attacks
□ ICMP	
□ Remote Management	
☑ CDR	
☑ PPP	
□ UPnP	
□ Forward Web Sites	
□ Blocked Web Sites	
□ Blocked Java etc.	
□ Attacks	
□ 802.1x	
□ Wireless	
□ Any IP	

The following table describes the labels in this screen.

Table 78 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the NBG318S sends. Not all NBG318S models have this field.
Send Log To	The NBG318S sends logs to the e-mail address specified in this field. If this field is left blank, the NBG318S does not send logs via e-mail.

Table 78 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Send Alerts To	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
SMTP Authentication	SMTP (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. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • Daily • Weekly • Hourly • When Log is Full • None. If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the checkbox to delete all the logs after the NBG318S sends an E-mail of the logs.
Syslog Logging	The NBG318S sends a log to an external syslog server.
Active	Click **Active** to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the NBG318S to send E-mail alerts immediately.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

21.3 Log Descriptions

This section provides descriptions of example log messages.

Table 79 System Maintenance Logs

	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`WAN interface gets IP:%s`	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns%s`	The DHCP server assigned an IP address to a client.
`Successful WEB login`	Someone has logged on to the router's web configurator interface.
`WEB login failed`	Someone has failed to log on to the router's web configurator interface.
`Successful TELNET login`	Someone has logged on to the router via telnet.
`TELNET login failed`	Someone has failed to log on to the router via telnet.
`Successful FTP login`	Someone has logged on to the router via ftp.
`FTP login failed`	Someone has failed to log on to the router via ftp.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.
`Starting Connectivity Monitor`	Starting Connectivity Monitor.
`Time initialized by Daytime Server`	The router got the time and date from the Daytime server.
`Time initialized by Time server`	The router got the time and date from the time server.
`Time initialized by NTP server`	The router got the time and date from the NTP server.
`Connect to Daytime server fail`	The router was not able to connect to the Daytime server.
`Connect to Time server fail`	The router was not able to connect to the Time server.
`Connect to NTP server fail`	The router was not able to connect to the NTP server.
`Too large ICMP packet has been dropped`	The router dropped an ICMP packet that was too large.
`Configuration Change: PC = 0x%x, Task ID = 0x%x`	The router is saving configuration changes.
`Successful SSH login`	Someone has logged on to the router’s SSH server.
`SSH login failed`	Someone has failed to log on to the router’s SSH server.
`Successful HTTPS login`	Someone has logged on to the router's web configurator interface using HTTPS protocol.
`HTTPS login failed`	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.

Table 80 System Error Logs

	DESCRIPTION
`%s exceeds the max. number of session per host!`	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
`setNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`readNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`WAN connection is down.`	A WAN connection is down. You cannot access the network through this interface.

Table 81 Access Control Logs

	DESCRIPTION
`Firewall default policy: [TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>`	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
`Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <rule:%d>`	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
`Triangle route packet forwarded: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Router sent blocked web site message: TCP`	The router sent a message to notify a user that the router blocked access to a web site that the user requested.

Table 82 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
`Under SYN flood attack, sent TCP RST`	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
`Exceed TCP MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen.
`Peer TCP state out of order, sent TCP RST`	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.

Table 82 TCP Reset Logs (continued)

LOG MESSAGE	DESCRIPTION
`Firewall session time out, sent TCP RST`	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds
`Exceed MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.) Note: When the number of incomplete connections (TCP + UDP) > “Maximum Incomplete High”, the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < “Maximum Incomplete Low”.
`Access block, sent TCP RST`	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: "sys firewall tcprst").

Table 83 Packet Filter Logs

	DESCRIPTION
`[TCP | UDP | ICMP | IGMP | Generic] packet filter matched (set:%d, rule:%d)`	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

Table 84 ICMP Logs

	DESCRIPTION
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	ICMP access matched the default policy and was blocked or forwarded according to the user's setting. For type and code details, see Table 93 on page 212.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	ICMP access matched (or didn’t match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule. For type and code details, see Table 93 on page 212.
`Triangle route packet forwarded: ICMP`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: ICMP`	The router blocked a packet that didn’t have a corresponding NAT table entry.
`Unsupported/out-of-order ICMP: ICMP`	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
`Router reply ICMP packet: ICMP`	The router sent an ICMP reply packet to the sender.

Table 85 CDR Logs

	DESCRIPTION
`board%d line%d channel%d, call%d,%s C01 Outgoing Call dev=%x ch=%x%s`	The router received the setup requirements for a call. “call” is the reference (count) number of the call. “dev” is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or “ch” is the call channel ID.For example,"board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.
`board%d line%d channel%d, call%d,%s C02 OutCall Connected%d%s`	The PPPoE, PPTP or dial-up call is connected.
`board%d line%d channel%d, call%d,%s C02 Call Terminated`	The PPPoE, PPTP or dial-up call was disconnected.

Table 86 PPP Logs

	DESCRIPTION
`ppp:LCP Starting`	The PPP connection’s Link Control Protocol stage has started.
`ppp:LCP Opening`	The PPP connection’s Link Control Protocol stage is opening.
`ppp:CHAP Opening`	The PPP connection’s Challenge Handshake Authentication Protocol stage is opening.
`ppp:IPCP Starting`	The PPP connection’s Internet Protocol Control Protocol stage is starting.
`ppp:IPCP Opening`	The PPP connection’s Internet Protocol Control Protocol stage is opening.
`ppp:LCP Closing`	The PPP connection’s Link Control Protocol stage is closing.
`ppp:IPCP Closing`	The PPP connection’s Internet Protocol Control Protocol stage is closing.

Table 87 UPnP Logs

	DESCRIPTION
`UPnP pass through Firewall`	UPnP packets can pass through the firewall.

Table 88 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
`%s: Keyword blocking`	The content of a requested web page matched a user defined keyword.
`%s: Not in trusted web list`	The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites.
`%s: Forbidden Web site`	The web site is in the forbidden web site list.
`%s: Contains ActiveX`	The web site contains ActiveX.
`%s: Contains Java applet`	The web site contains a Java applet.
`%s: Contains cookie`	The web site contains a cookie.

Table 88 Content Filtering Logs (continued)

LOG MESSAGE	DESCRIPTION
%s: Proxy mode detected	The router detected proxy mode in the packet.
%s	The content filter server responded that the web site is in the blocked category list, but it did not return the category type.
%s:%s	The content filter server responded that the web site is in the blocked category list, and returned the category type.
%s(cache hit)	The system detected that the web site is in the blocked list from the local cache, but does not know the category type.
%s:%s(cache hit)	The system detected that the web site is in blocked list from the local cache, and knows the category type.
%s: Trusted Web site	The web site is in a trusted domain.
%s	When the content filter is not on according to the time schedule or you didn't select the "Block Matched Web Site" check box, the system forwards the web content.
Waiting content filter server timeout	The external content filtering server did not respond within the timeout period.
DNS resolving failed	The NBG318S cannot get the IP address of the external content filtering via DNS query.
Creating socket failed	The NBG318S cannot issue a query because TCP/IP socket creation failed, port:port number.
Connecting to content filter server fail	The connection to the external content filtering server failed.
License key is invalid	The external content filtering license key is invalid.

Table 89 Attack Logs

LOG MESSAGE	DESCRIPTION
attack [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack. For type and code details, see Table 93 on page 212.
land [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack. For type and code details, see Table 93 on page 212.
ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port. For type and code details, see Table 93 on page 212.
icmp echo: ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack. For type and code details, see Table 93 on page 212.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.

Table 89 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
`teardrop UDP`	The firewall detected an UDP teardrop attack.
`teardrop ICMP (type:%d, code:%d)`	The firewall detected an ICMP teardrop attack. For type and code details, see Table 93 on page 212.
`illegal command TCP`	The firewall detected a TCP illegal command attack.
`NetBIOS TCP`	The firewall detected a TCP NetBIOS attack.
`ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall classified a packet with no source routing entry as an IP spoofing attack.
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
`vulnerability ICMP (type:%d, code:%d)`	The firewall detected an ICMP vulnerability attack. For type and code details, see Table 93 on page 212.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack. For type and code details, see Table 93 on page 212.

Table 90 PKI Logs

LOG MESSAGE	DESCRIPTION
`Enrollment successful`	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
`Enrollment failed`	The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
`Failed to resolve <SCEP CA server url>`	The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved.
`Enrollment successful`	The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port.
`Enrollment failed`	The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
`Failed to resolve <CMP CA server url>`	The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved.
`Rcvd ca cert: <subject name>`	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd user cert: <subject name>`	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd CRL <size>: <issuer name>`	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd ARL <size>: <issuer name>`	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.

Table 90 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`Failed to decode the received ca cert`	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received user cert`	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received CRL`	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ARL`	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Rcvd data <size> too large! Max size allowed: <max size>`	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
`Cert trusted: <subject name>`	The router has verified the path of the certificate with the listed subject name.
`Due to <reason codes>, cert not trusted: <subject name>`	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 93 on page 212 for the corresponding descriptions of the codes.

Table 91 802.1X Logs

LOG MESSAGE	DESCRIPTION
`Local User Database accepts user.`	A user was authenticated by the local user database.
`Local User Database reports user credential error.`	A user was not authenticated by the local user database because of an incorrect user password.
``Local User Database does not find user`s credential.``	A user was not authenticated by the local user database because the user is not listed in the local user database.
`RADIUS accepts user.`	A user was authenticated by the RADIUS Server.
`RADIUS rejects user. Pls check RADIUS Server.`	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
`Local User Database does not support authentication method.`	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
`User logout because of session timeout expired.`	The router logged out a user whose session expired.
`User logout because of user deassociation.`	The router logged out a user who ended the session.
`User logout because of no authentication response from user.`	The router logged out a user from which there was no authentication response.
`User logout because of idle timeout expired.`	The router logged out a user whose idle timeout period expired.
`User logout because of user request.`	A user logged out.

Table 91 802.1X Logs (continued)

LOG MESSAGE	DESCRIPTION
`Local User Database does not support authentication method.`	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
`No response from RADIUS. Pls check RADIUS Server.`	There is no response message from the RADIUS server, please check the RADIUS server.
`Use Local User Database to authenticate user.`	The local user database is operating as the authentication server.
`Use RADIUS to authenticate user.`	The RADIUS server is operating as the authentication server.
`No Server to authenticate user.`	There is no authentication server to authenticate a user.
`Local User Database does not find user`s credential.`	A user was not authenticated by the local user database because the user is not listed in the local user database.

Table 92 ACL Setting Notes

	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(L to L/P)	LAN to LAN/ NBG318S	ACL set for packets traveling from the LAN to the LAN or the NBG318S.
(W to W/P)	WAN to WAN/ NBG318S	ACL set for packets traveling from the WAN to the WAN or the NBG318S.

Table 93 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host

Table 93 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 94 Syslog Logs

	DESCRIPTION
`<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>`	"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU->LOGS->Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 95 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash

Table 95 RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
`SIG`	Signature
`NONCE`	Nonce
`NOTFY`	Notification
`DEL`	Delete
`VID`	Vendor ID

22

Tools

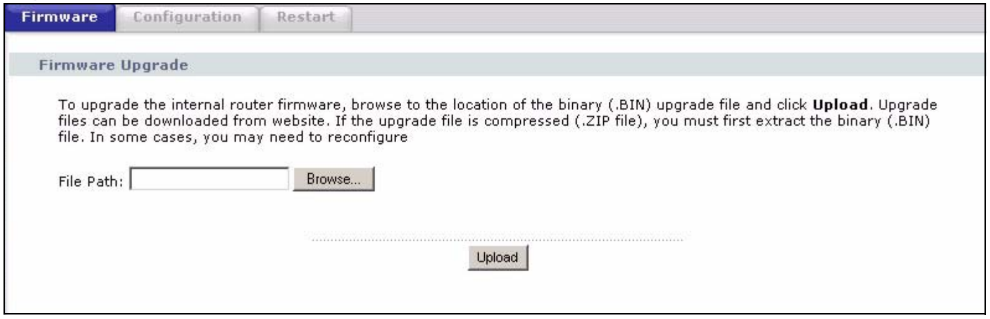
This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the NBG318S.

22.1 Firmware Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a “*.bin” extension, e.g., “NBG318S.bin”. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the Firmware and Configuration File Maintenance chapter for upgrading firmware using FTP/TFTP commands.

Click **Maintenance** > **Tools**. Follow the instructions in this screen to upload firmware to your NBG318S.

Figure 120 Maintenance > Tools > Firmware



To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click **Upload**. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure

File Path:

The following table describes the labels in this screen.

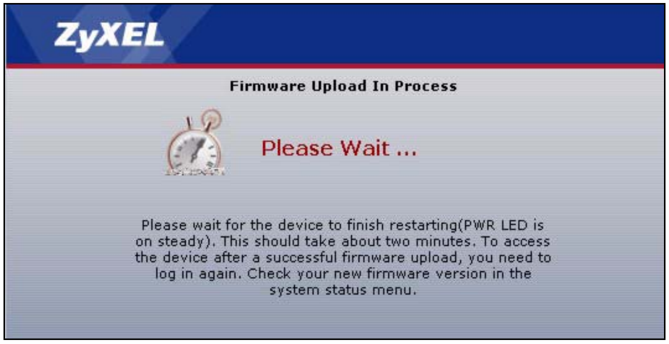
Table 96 Maintenance > Tools > Firmware

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.

Do not turn off the NBG318S while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the NBG318S again.

Figure 121 Upload Warning



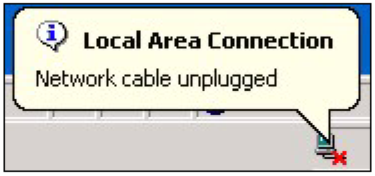
Firmware Upload In Process

Please Wait ...

Please wait for the device to finish restarting(PWR LED is on steady). This should take about two minutes. To access the device after a successful firmware upload, you need to log in again. Check your new firmware version in the system status menu.

The NBG318S automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 122 Network Temporarily Disconnected



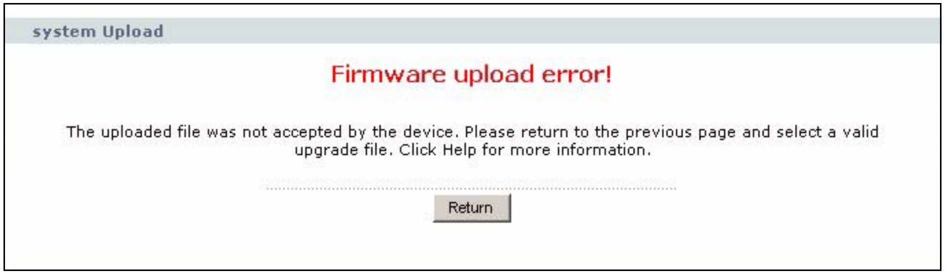
Local Area Connection

Network cable unplugged

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

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

Figure 123 Upload Error Message



system Upload

Firmware upload error!

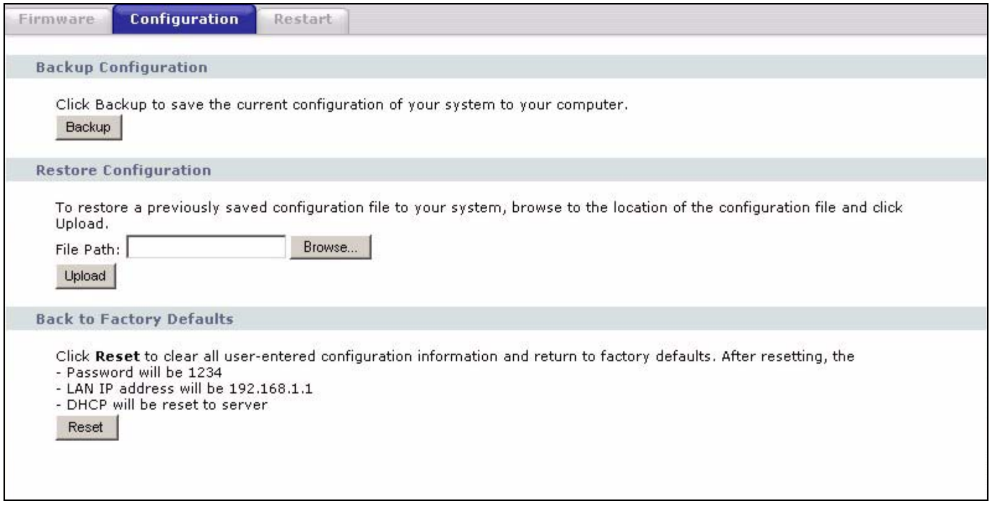
The uploaded file was not accepted by the device. Please return to the previous page and select a valid upgrade file. Click Help for more information.

22.2 Configuration Screen

See the Firmware and Configuration File Maintenance chapter for transferring configuration files using FTP/TFTP commands.

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

Figure 124 Maintenance > Tools > Configuration



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

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path:

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

22.2.1 Backup Configuration

Backup configuration allows you to back up (save) the NBG318S's current configuration to a file on your computer. Once your NBG318S is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the NBG318S's current configuration to your computer.

22.2.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG318S.

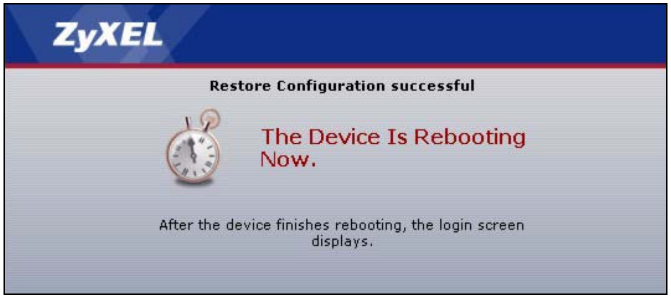
Table 97 Maintenance Restore Configuration

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 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.

Do not turn off the NBG318S 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 NBG318S again.

Figure 125 Configuration Restore Successful



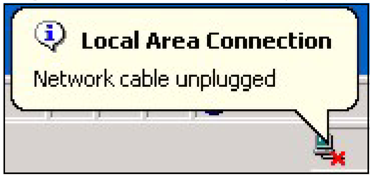
Restore Configuration successful

The Device Is Rebooting Now.

After the device finishes rebooting, the login screen displays.

The NBG318S automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 126 Temporarily Disconnected



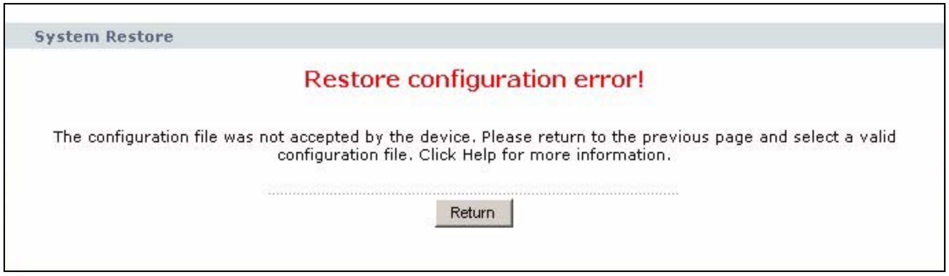
Local Area Connection

Network cable unplugged

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 NBG318S IP address (192.168.1.1). See your Quick Start Guide for details on how to set up your computer's IP address.

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

Figure 127 Configuration Restore Error



System Restore

Restore configuration error!

The configuration file was not accepted by the device. Please return to the previous page and select a valid configuration file. Click Help for more information.

22.2.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the NBG318S to its factory defaults.

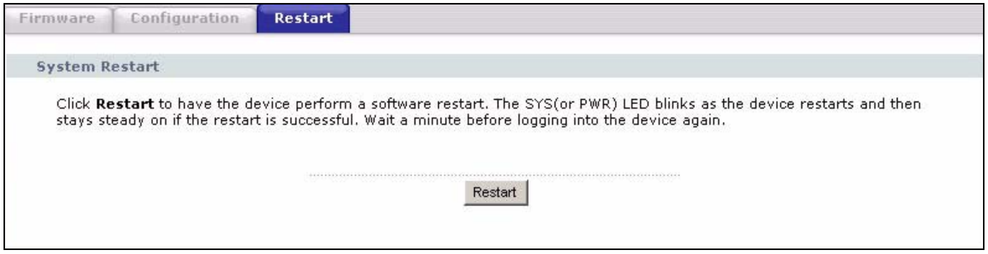
You can also press the **RESET** button on the rear panel to reset the factory defaults of your NBG318S. Refer to the chapter about introducing the web configurator for more information on the **RESET** button.

22.3 Restart Screen

System restart allows you to reboot the NBG318S without turning the power off.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the NBG318S reboot. This does not affect the NBG318S's configuration.

Figure 128 Maintenance > Tools > Restart



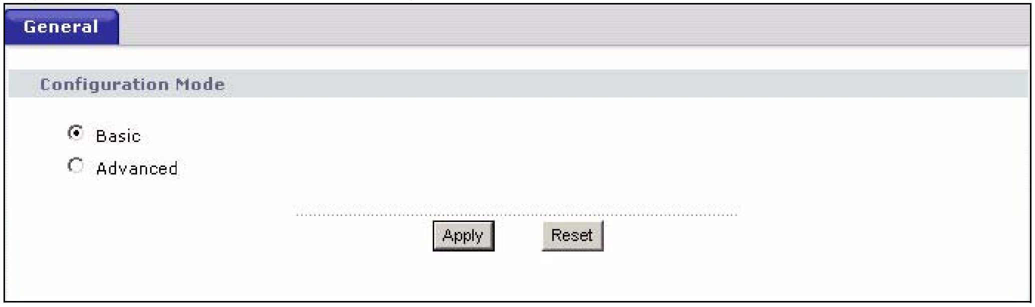
Click **Restart** to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.

23

Configuration Mode

Click **Maintenance** > **Config Mode** to open the following screen. This screen allows you to hide or display the advanced screens of some features or the advanced features, such as MAC filter or static route. **Basic** is selected by default and you cannot see the advanced screens or features. If you want to view and configure all screens including the advanced ones, select **Advanced** and click **Apply**.

Figure 129 Maintenance > Config Mode > General



Configuration Mode

● Basic
○ Advanced

The following table describes the labels in the screen.

Table 98 Maintenance > Config Mode > General

	DESCRIPTION
Configuration Mode	
Basic	Select **Basic** mode to enable or disable features and to monitor the status of your device.
Advanced	Select **Advanced** mode to set advanced settings.
Apply	Click on this to set the mode.
Reset	Click on this to reset your selection to the default (**Advanced**).

The following table includes the screens that you can view and configure only when you select **Advanced**.

Table 99 Advanced Configuration Options

	LINK	TAB
Network	Wireless LAN	MAC Filter
		Advanced
		QoS
	WAN	Advanced
	LAN	IP Alias
		Advanced
	DHCP Server	Advanced
	NAT	Advanced
Security	Firewall	Services
	Content Filter	Schedule
Management	Static Route	IP Static Route
	Bandwidth MGMT	Advanced
		Monitor
	Remote MGMT	Telnet
		FTP
		DNS
Maintenance	Logs	Log Settings

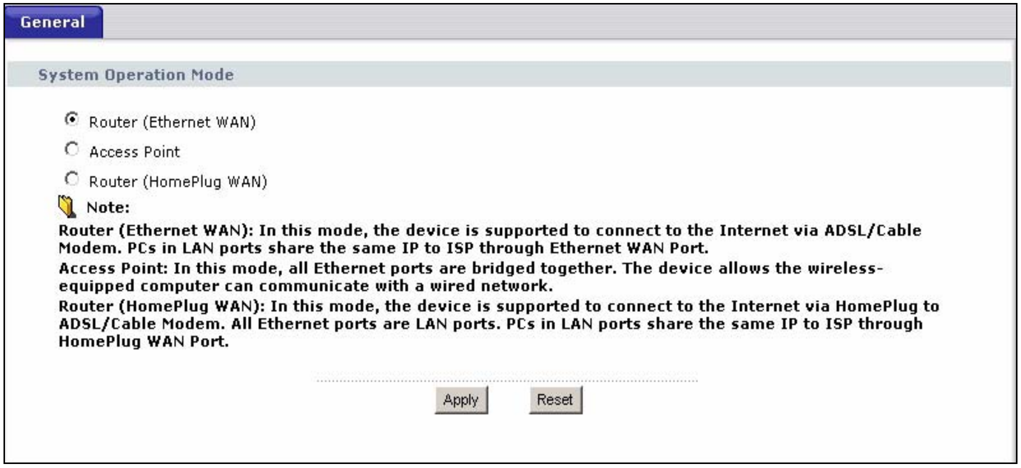
24

Sys Op Mode

24.1 Selecting System Operation Mode

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

Figure 130 Maintenance > Sys OP Mode > General



System Operation Mode

● Router (Ethernet WAN)

○ Access Point

○ Router (HomePlug WAN)

Note:

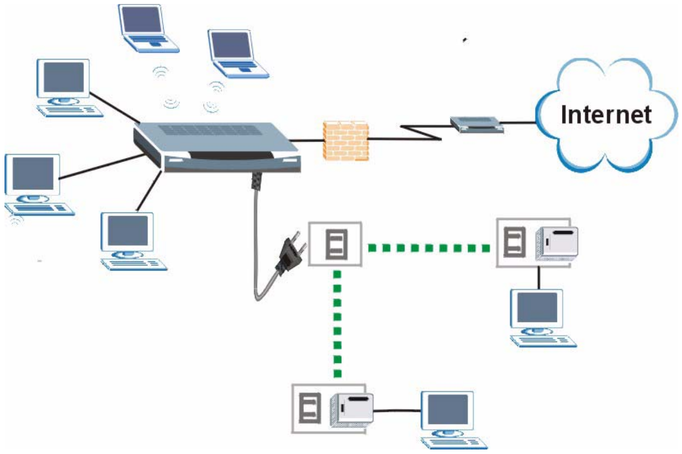
Router (Ethernet WAN): In this mode, the device is supported to connect to the Internet via ADSL/Cable Modem. PCs in LAN ports share the same IP to ISP through Ethernet WAN Port.

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

Router (HomePlug WAN): In this mode, the device is supported to connect to the Internet via HomePlug to ADSL/Cable Modem. All Ethernet ports are LAN ports. PCs in LAN ports share the same IP to ISP through HomePlug WAN Port.

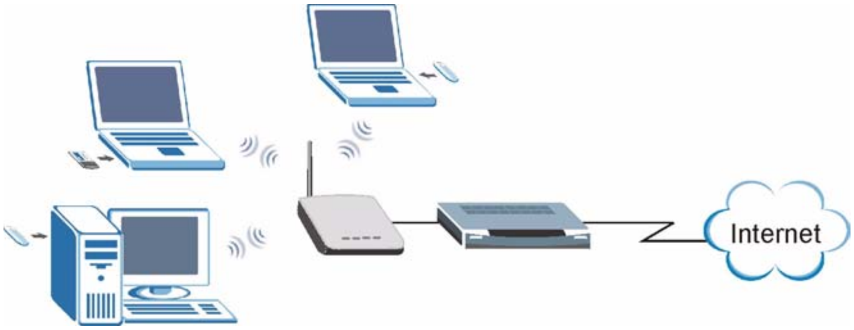
The figure below shows devices connecting to the Internet through a DSL connection. Select **Router(Ethernet WAN)** in the screen if you connect to the Internet as shown in diagram.

Figure 131 System Operation Mode: Ethernet WAN



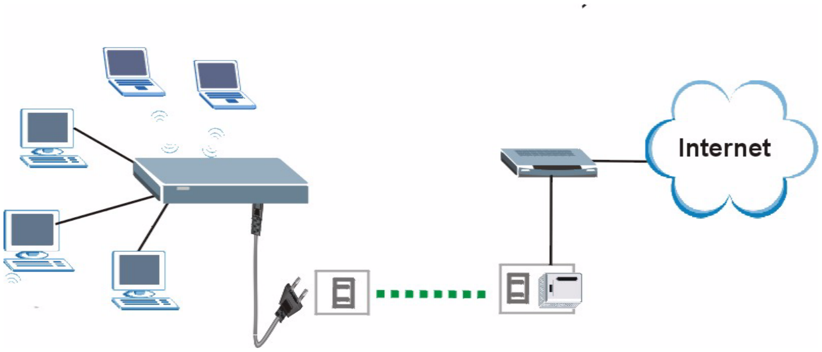
The figure below shows the NBG318S connecting to the Internet as an access point. Select **Access Point** in the screen if you connect to the Internet as shown in the diagram.

Figure 132 System Operation Mode: Access Point



The figure below shows a network connecting to the Internet through a HomePlug connection. Select **Router(HomePlug WAN)** in the screen if you connect to the Internet as shown in the diagram.

Figure 133 System Operation Mode: HomePlug WAN



The following table describes the labels in the screen.

Table 100 Maintenance > Sys OP Mode > General

	DESCRIPTION
System Operation Mode	
Router (Ethernet WAN)	Select this option if you connect to the Internet through a DSL or cable connection. In this mode three of the four ports are LAN ports, the other is a WAN port.
Access Point	Select this option if you connect to the Internet through a device such as a router which allocates IP addresses. In this mode all four of your ports operate as LAN ports.
Router (HomePlug WAN)	Select this option if you connect to the Internet through a DSL or cable modem connected to your HomePlug AV network. In this mode all four of your ports operate as LAN ports.
Apply	Click this button to apply your settings.
Reset	Click this button to reset your settings to the default (**Ethernet WAN**)

If you select the incorrect System Operation Mode you cannot connect to the Internet.

25

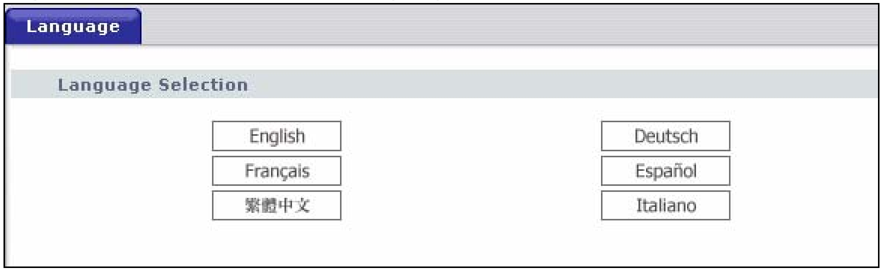
Language

Use this screen to select the language in which the web configurator displays.

25.1 Selecting Language

Click **Maintenance** > **Language**. The following screen displays.

Figure 134 Maintenance > Language



Click the button for language you want to use. The web configurator reloads and displays in the selected language.

26 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
- NBG318S Access and Login
- Internet Access
- Resetting the NBG318S to Its Factory Defaults
- Wireless Router/AP Troubleshooting
- HomePlug AV Troubleshooting
- Advanced Features

26.1 Power, Hardware Connections, and LEDs

? The NBG318S does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the NBG318S.
2. Make sure the power adaptor or cord is connected to the NBG318S 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 NBG318S.
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 1.4 on page 33.
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 NBG318S.
5. If the problem continues, contact the vendor.

26.2 NBG318S Access and Login

I forgot the IP address for the NBG318S.

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 NBG318S 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 NBG318S (it depends on the network), so enter this IP address in your Internet browser.
3. If this does not work, you have to reset the device to its factory defaults. See Section 26.4 on page 233.

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 26.4 on page 233.

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 9.3 on page 118), use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the NBG318S.
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 JavaScripts and Java enabled. See Appendix B on page 245.
4. Make sure your computer is in the same subnet as the NBG318S. (If you know that there are routers between your computer and the NBG318S, skip this step.)
   - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 9.3 on page 118. Your NBG318S is a DHCP server by default.
   - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG318S. See Section 9.3 on page 118.
5. Reset the device to its factory defaults, and try to access the NBG318S with the default IP address. See Section 9.3 on page 118.

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

Advanced Suggestions

- Try to access the NBG318S using another service, such as Telnet. If you can access the NBG318S, check the remote management settings and firewall rules to find out why the NBG318S does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN/ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the NBG318S.

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 You cannot log in to the web configurator while someone is using Telnet to access the NBG318S. Log out of the NBG318S in the other session, or ask the person who is logged in to log out.

3 Disconnect and re-connect the power adaptor or cord to the NBG318S.

4 If this does not work, you have to reset the device to its factory defaults. See Section 26.4 on page 233.

I cannot Telnet to the NBG318S.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

26.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
5 Go to Maintenance > Sys OP Mode > General. Check your System Operation Mode setting.
   - Select Router (Ethernet WAN) if your network is configured to access the Internet through an Ethernet connection to a DSL or cable modem.
   - Select Access Point if your network is configured to access the Internet through a device such as a router which allocates IP addresses.
   - Select Router (HomePlug WAN) if your network is configured to access the Internet through a HomePlug connection.
6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NBG318S), 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 1.4 on page 33.
2 Reboot the NBG318S.
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 1.4 on page 33. If the NBG318S 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 NBG318S 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 NBG318S.
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.

26.4 Resetting the NBG318S to Its Factory Defaults

If you reset the NBG318S, you lose all of the changes you have made. The NBG318S 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 NBG318S,

1 Make sure the **PWR LED** is on and not blinking.

2 Press and hold the **RESET** button for five to ten seconds. Release the **RESET** button when the **PWR** LED begins to blink. The default settings have been restored.

If the NBG318S restarts automatically, wait for the NBG318S to finish restarting, and log in to the web configurator. The password is “1234”.

If the NBG318S does not restart automatically, disconnect and reconnect the NBG318S’s power. Then, follow the directions above again.

26.5 Wireless Router/AP Troubleshooting

?

I cannot access the NBG318S or ping any computer from the WLAN (wireless AP or router).

1 Make sure the wireless LAN is enabled on the NBG318S

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 NBG318S.

4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG318S.

5 Check that both the NBG318S 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 NBG318S.

7 Make sure you allow the NBG318S 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.

26.6 HomePlug AV Troubleshooting

I cannot start my powerline device.

Check your power supply is working. Powerline adapters operate from the power supplied by your home wiring and cannot operate without a working power supply. Remove the powerline adapter from the outlet. Then connect an electrical device that you know works into the same outlet. This checks the status of the power outlet.

The HomePlug light does not turn on.

1 Make sure that all your powerline adapters are HomePlug AV compliant. Check the package it came in or ask your vendor. This NBG318S can not detect earlier versions of HomePlug powerline adapters such as HomePlug 1.0 or 1.0.1. (Although they can coexist on the same electrical wiring without interfering with each other.)

2 Check all HomePlug AV adapters on your network have the latest firmware installed. The NBG318S cannot communicate with adapters using earlier versions of the firmware. See the documentation for your powerline product or visit your vendors website for more information on upgrading your HomePlug AV adapters.

3 Check the DAK password and MAC address for all powerline adapters are typed correctly in the utility. See Section 10.3 on page 124 for instructions on checking the DAK and MAC address.

4 Make sure that the powerline adapters on your network are all on the same electrical wiring. Connect another powerline adapter into an outlet close to your NBG318S's power outlet. They are probably now on the same electrical wiring. Check the HomePlug ⌂ light. If it now lights up your powerline adapter was probably previously on separate electrical wiring. Ask an electrician for more information on the electrical wiring in your building.

5 If your powerline network is using electrical wiring (not coaxial cable), check you do not have a power meter between powerline adapters. Powerline signals cannot pass this.

The signal on my powerline network may be weak for the following reasons.

1 Your powerline adapters may be connected to electrical surge protectors. Connect them to standard power outlets.

2 Your powerline adapters may be located close to large appliances such as refrigerators or air-conditioners that cause interference with the powerline signal. Move the adapters further away from such appliances to reduce interference.

3 Your powerline adapters may be placed close to electrical devices such as electrical insect-killers which produce radio waves. These may interfere with the powerline signals. Move the adapters further away from such electrical devices.

4 Your wiring may be old and/or low quality or with a long wiring path.

26.7 ENCRYPT Button Problems

This section applies only to NBG318Ss with the **ENCRYPT** button.

The HomePlug light is already on, but I haven't pressed the ENCRYPT button yet.

Your device has already connected to another powerline device. Press the **ENCRYPT** button for more than 10 seconds to release the connection.

The HomePlug light does not turn on.

- Ensure you have pressed the **ENCRYPT** button on **both** devices.
- Wait for about a minute while the devices set up a connection.
- If that does not work, try again with both devices connected to a power strip next to each other. If they now connect, then the devices were not on the same electrical circuit before.

The POWER lights on both devices finished blinking, but only one device's HomePlug light is on.

One device may have connected to a third powerline device. To check device A is connected to device B and not another device, disconnect device B from its power source. Device A's HomePlug (⌂) light will turn off if the connection is with Device B. Press the **ENCRYPT** button on **both** devices for more than 10 seconds, then try to reconnect, pressing the **ENCRYPT** button for less than 3 seconds on both devices.

I pressed the ENCRYPT button for more than 10 seconds, but the HomePlug light is still on.

The HomePlug light is on, indicating it is still connected to another powerline device. Try again, pressing the **ENCRYPT** button for more than 10 seconds.

26.8 Advanced Features

I can log in, but I cannot see some of the screens or fields in the Web Configurator.

You may be accessing the Web Configurator in Basic mode. Some screens and fields are available only in Advanced mode. Use the **Maintenance** > **Config** Mode screen to select Advanced mode.

I set up URL keyword blocking, but I can still access a Web site 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.

PART VI
Appendices and Index

A

Product Specifications and Wall-Mounting Instructions

The following tables summarize the NBG318S's hardware and firmware features.

Table 101 Hardware Features

Dimensions (W x D x H)	162 x 118 x 35 mm
Power Specification	120-240 VAC, 50/60 Hz
Ethernet ports	Auto-negotiating: This auto-negotiation feature allows the NBG318S to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. Auto-crossover: Use either crossover or straight-through Ethernet cables.
3-4 Port Switch	A combination of switch and router makes your NBG318S a cost-effective and viable network solution. You can add up to three computers to the NBG318S without the cost of a hub when connecting to the Internet through the WAN port. You can add up to four computers to the NBG318S when you connect to the Internet through a HomePlug connection. Add more than four computers to your LAN by using a hub.
ENCRYPT	Pressing this button in for less than 3 seconds begins the powerline connection setup process. Pressing this button in for more than 10 seconds resets the network name to a random value.
WPS button	The WPS (WI-Fi Protected Setup) button is built into the rear panel. Use this button to set up a WPS connection with another WPS enabled device. Note: Upgrade your firmware to install this feature on your device.
Reset Button	The reset button is built into the rear panel. Use this button to restore the NBG318S to its factory default settings. Press for 1 second to restart the device. Press for 5 seconds to restore to factory default settings.
Antenna	The NBG318S is equipped with a 2dBi detachable antenna to provide clear radio transmission and reception on the wireless network.
Operation Environment	Temperature: 0º C ~ 40º C Humidity: 20% ~ 90% RH (Non-condensing)
Storage Environment	Temperature: -20º C ~ 60º C Humidity: 20% ~ 90% RH (Non-condensing)
Distance between the centers of the holes on the device's back.	125 mm

Table 101 Hardware Features

Screw size for wall-mounting	M4
Certifications	Safety ANSI/UL-1950 3rd, CSA C22.2 No. 950 3rd, EN60950 (1992+A1+A2+A3+A4+A11), IEC 60950 3rd EMI FCC Part 15 Class B, EN55022 Class B, EN61000-3-2, EN61000-3-3 EMS EN61000-4-2/3/4/5/6/8/11

Table 102 Firmware Features

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.33 to 192.168.1.64
Device Management	Use the web configurator to easily configure the rich range of features on the NBG318S.
Wireless Functionality	Allows IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the NBG318S wirelessly. IEEE 802.11g clients can connect using the Super G function. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network. Note: The NBG318S may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.
Powerline Functionality	The HomePlug AV standard specifies how network devices communicate using standard electrical wiring. It supports a data transfer rate of up to 200Mbps. Data is encrypted using 128-bit AES (Advanced Encryption Standard). HomePlug AV compatible devices co-exist with HomePlug 1.0 devices but do not detect each other. The range of a HomePlug AV network is 300 meters/984 feet in optimal conditions. HomePlug AV is compatible with all OSs Maximum number of devices connected to a powerline adapter is 64 Maximum number of powerline devices on a single network is 64. Maximum number of powerline networks on one electrical circuit is 4.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the NBG318S. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the NBG318S's configuration and put it back on the NBG318S later if you decide you want to revert back to an earlier configuration.

Table 102 Firmware Features

FEATURE	DESCRIPTION
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert a single public IP address to multiple private IP addresses for the computers on your network.
Firewall	You can configure firewall on the ZyXEL Device for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.
Content Filter	The NBG318S blocks or allows access to web sites that you specify and blocks access to web sites with URLs that contain keywords that you specify. You can define time periods and days during which content filtering is enabled. You can also include or exclude particular computers on your network from content filtering. You can also subscribe to category-based content filtering that allows your NBG318S to check web sites against an external database.
Bandwidth Management	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Time and Date	Get the current time and date from an external server when you turn on your NBG318S. You can also set the time manually. These dates and times are then used in logs.
Port Forwarding	If you have a server (mail or web server for example) on your network, then use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the NBG318S assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP Multicast is used to send traffic to a specific group of computers. The NBG318S supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
IP Alias	IP Alias allows you to subdivide a physical network into logical networks over the same Ethernet interface with the NBG318S itself as the gateway for each subnet.
Logging and Tracing	Use packet tracing and logs for troubleshooting. You can send logs from the NBG318S to an external UNIX syslog server.
PPPoE	PPPoE mimics a dial-up over Ethernet Internet access connection.
PPTP Encapsulation	Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The NBG318S supports one PPTP connection at a time.
Universal Plug and Play (UPnP)	The NBG318S can communicate with other UPnP enabled devices in a network.

The following list, which is not exhaustive, illustrates the standards supported in the NBG318S.

Table 103 Standards Supported

	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol.
RFC 1112	IGMP v1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2766	Network Address Translation - Protocol
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
Microsoft PPTP	MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)
HomePlug AV	The HomePlug AV standard specifies how network devices communicate using standard electrical wiring.

Wall-mounting Instructions

Do the following to hang your NBG318S on a wall.

See the product specifications appendix for the size of screws to use and how far apart to place them.

1 Locate a high position on a wall that is free of obstructions. Use a sturdy wall.

2 Drill two holes for the screws. Make sure the distance between the centers of the holes matches what is listed in the product specifications appendix.

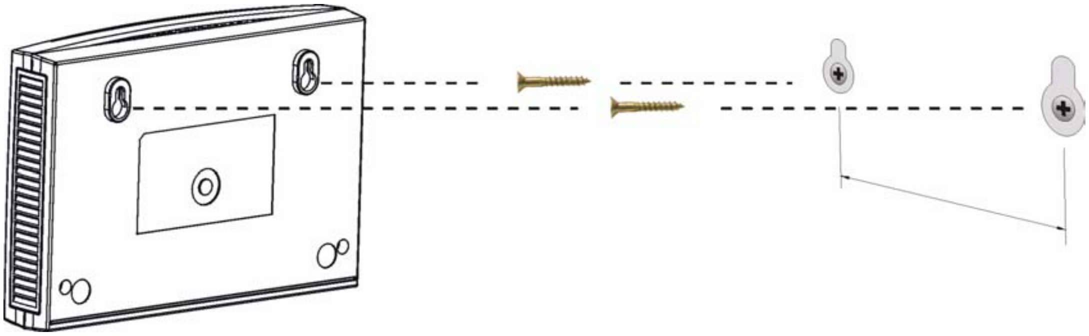
Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

3 Do not screw the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.

4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the NBG318S with the connection cables.

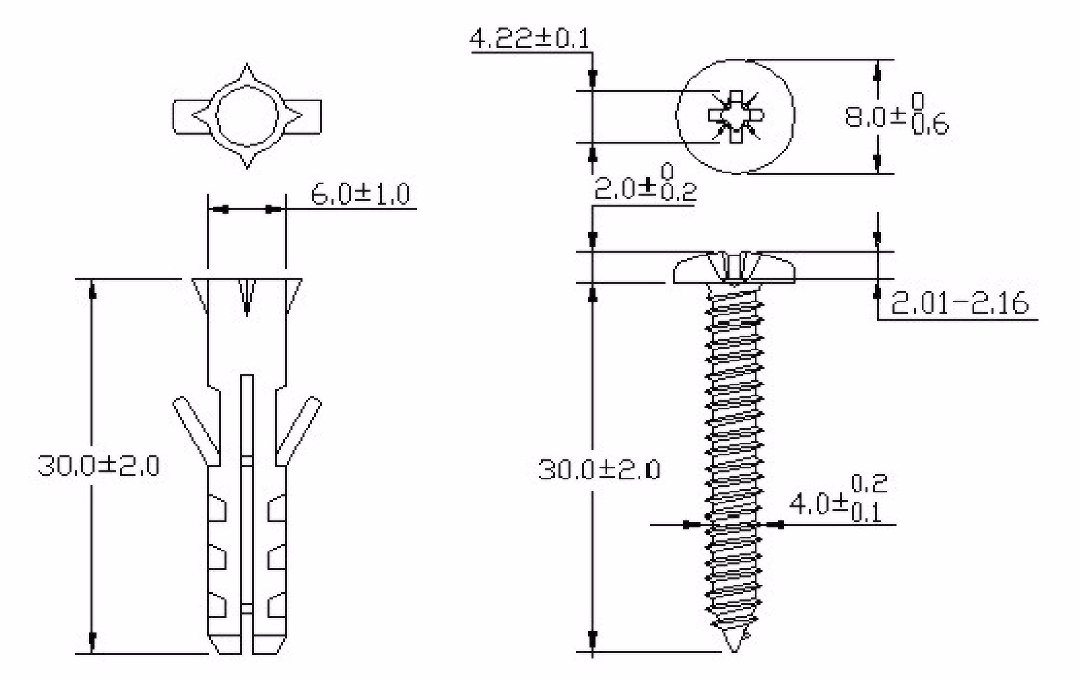
5 Align the holes on the back of the NBG318S with the screws on the wall. Hang the NBG318S on the screws.

Figure 135 Wall-mounting Example



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

Figure 136 Masonry Plug and M4 Tap Screw



B

Pop-up Windows, JavaScripts and Java Permissions

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

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

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

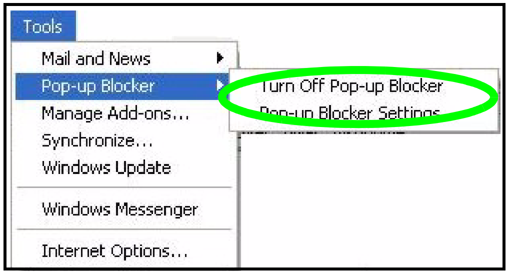
You may have to disable pop-up blocking to log into your device.

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

Disable pop-up Blockers

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

Figure 137 Pop-up Blocker

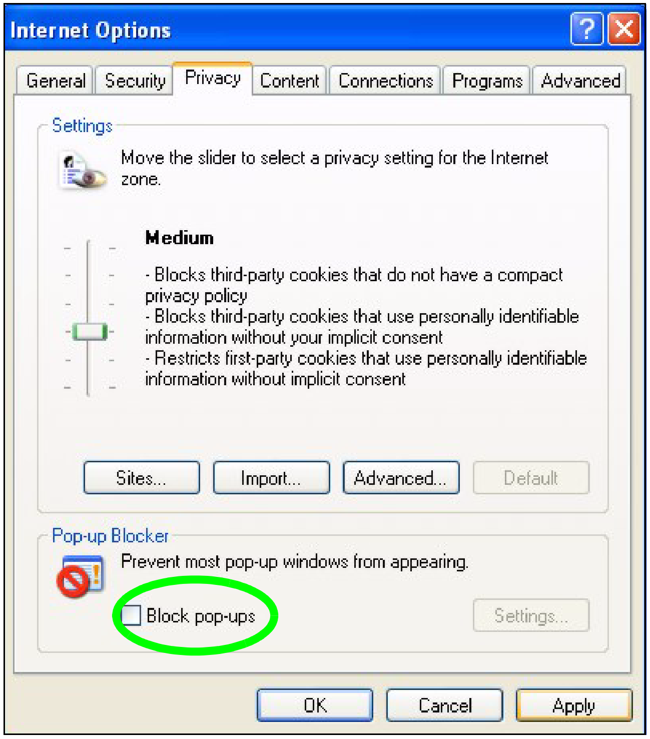


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 138 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

☐ Block pop-ups

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

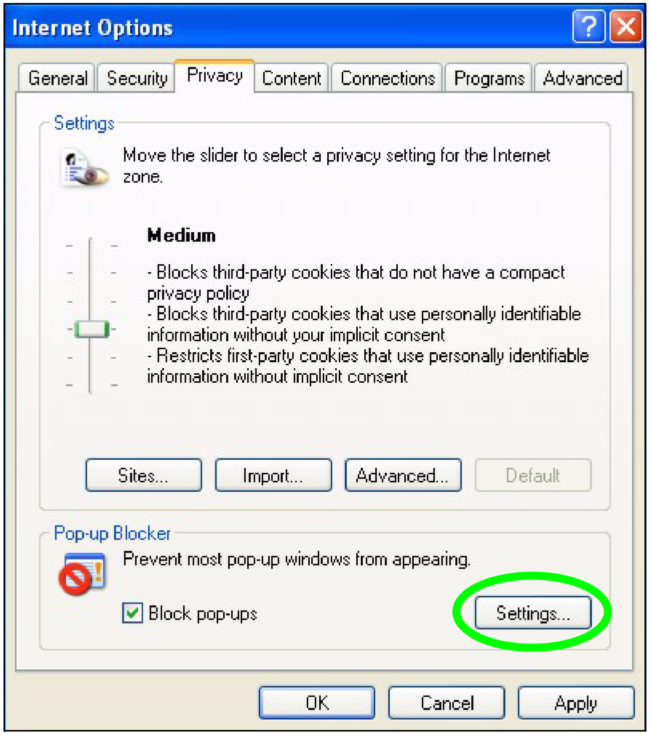
Enable pop-up Blockers with Exceptions

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

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 139 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

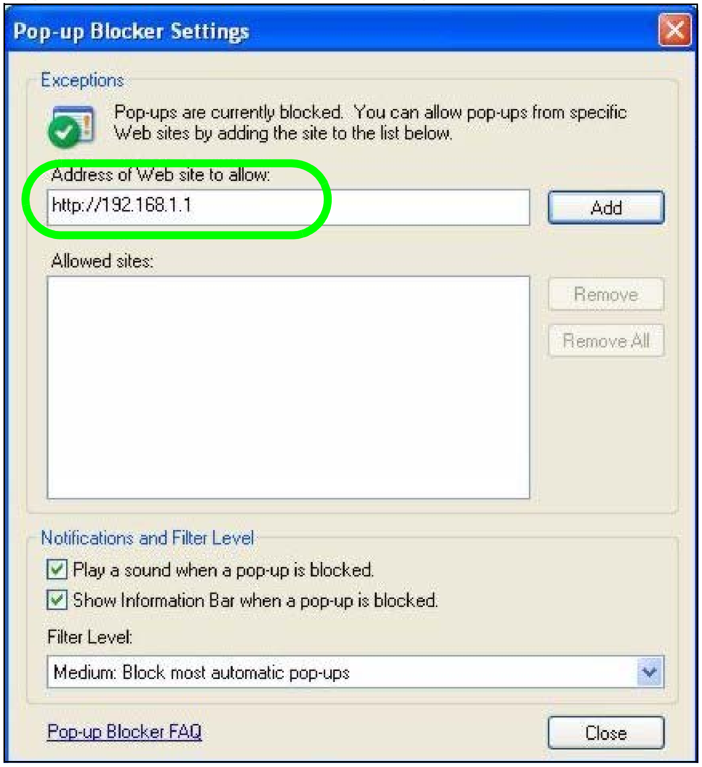
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 140 Pop-up Blocker Settings



Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow: http://192.168.1.1

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

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

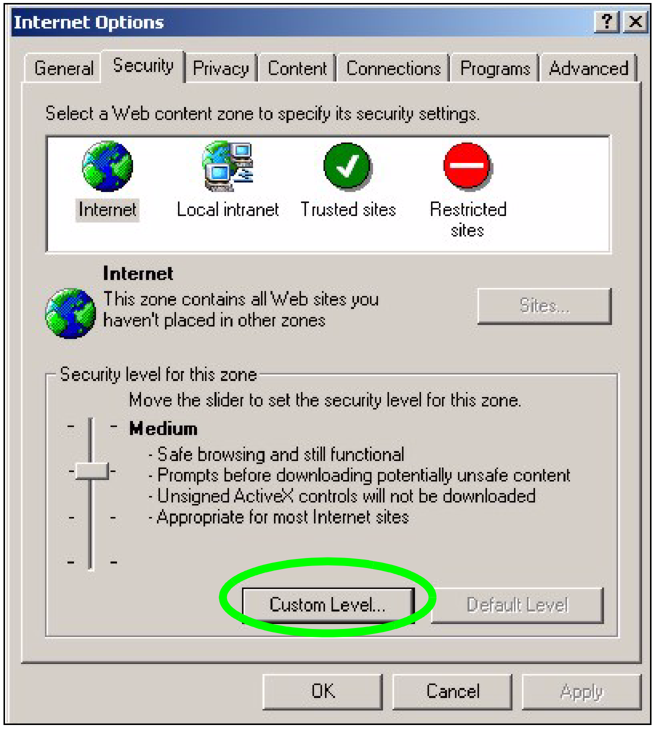
6 Click **Apply** to save this setting.

JavaScripts

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

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

Figure 141 Internet Options: Security



Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Move the slider to set the security level for this zone.

Medium
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

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

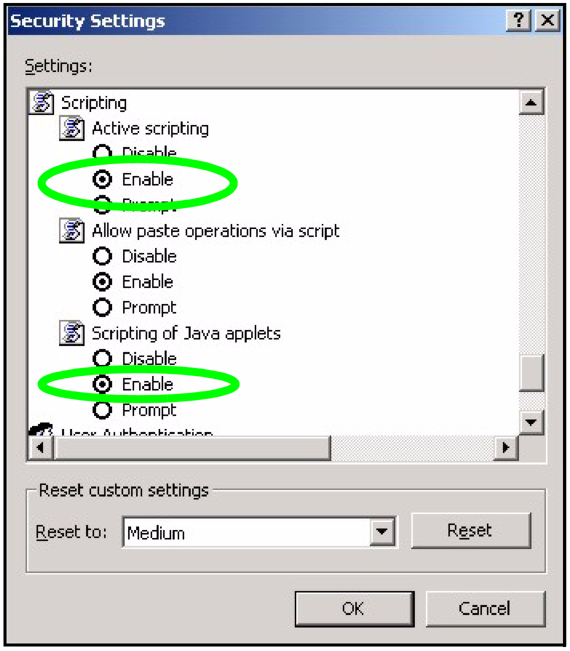
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 142 Security Settings - Java Scripting



Settings:

Scripting
- Active scripting
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Allow paste operations via script
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Scripting of Java applets
  - ○ Disable
  - ● Enable
  - ○ Prompt

User Authentication

Reset to: Medium

Java Permissions

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

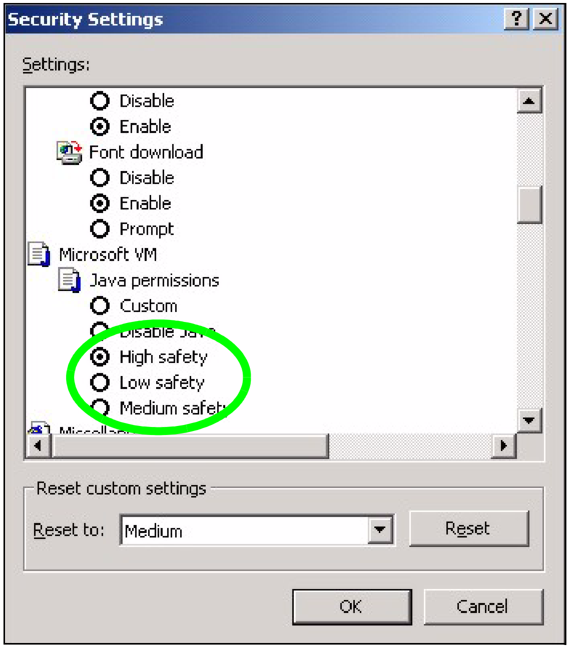
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 143 Security Settings - Java



Settings:

- ○ Disable
- ● Enable

Font download
- ○ Disable
- ● Enable
- ○ Prompt

Microsoft VM
- Java permissions
  - ○ Custom
  - ○ Disable Java
  - ● High safety
  - ○ Low safety
  - ○ Medium safety

Miscellaneous

Reset to: Medium

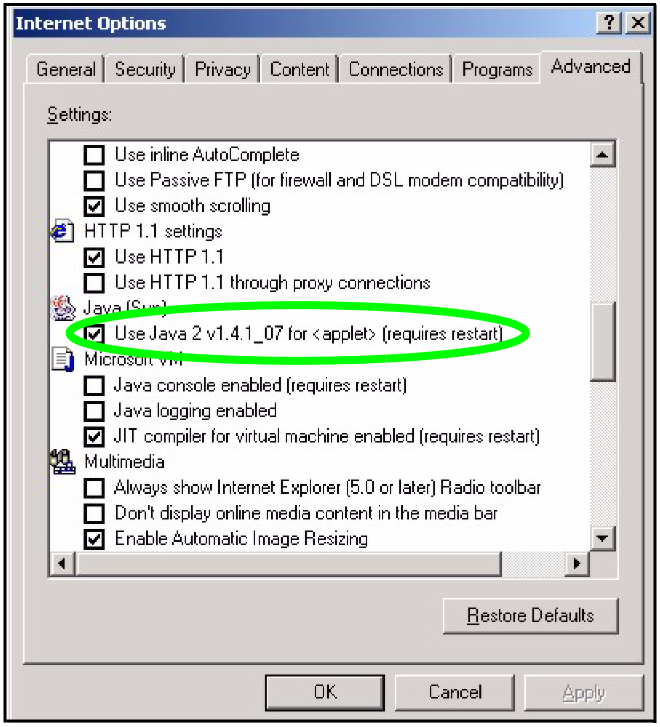
JAVA (Sun)

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

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 144 Java (Sun)



Settings:

- □ Use inline AutoComplete
- □ Use Passive FTP (for firewall and DSL modem compatibility)
- ☑ Use smooth scrolling

HTTP 1.1 settings

- ☑ Use HTTP 1.1
- □ Use HTTP 1.1 through proxy connections

Java (Sun)

- ☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)

Microsoft VM

- □ Java console enabled (requires restart)
- □ Java logging enabled
- ☑ JIT compiler for virtual machine enabled (requires restart)

Multimedia

- □ Always show Internet Explorer (5.0 or later) Radio toolbar
- □ Don't display online media content in the media bar
- ☑ Enable Automatic Image Resizing

C

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.

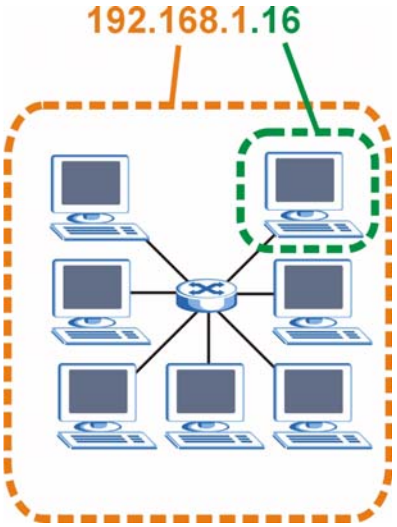
Structure

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 145 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 104 Subnet Mask - Identifying Network Number

		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 105 Subnet Masks

					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 106 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		
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 107 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

Table 107 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

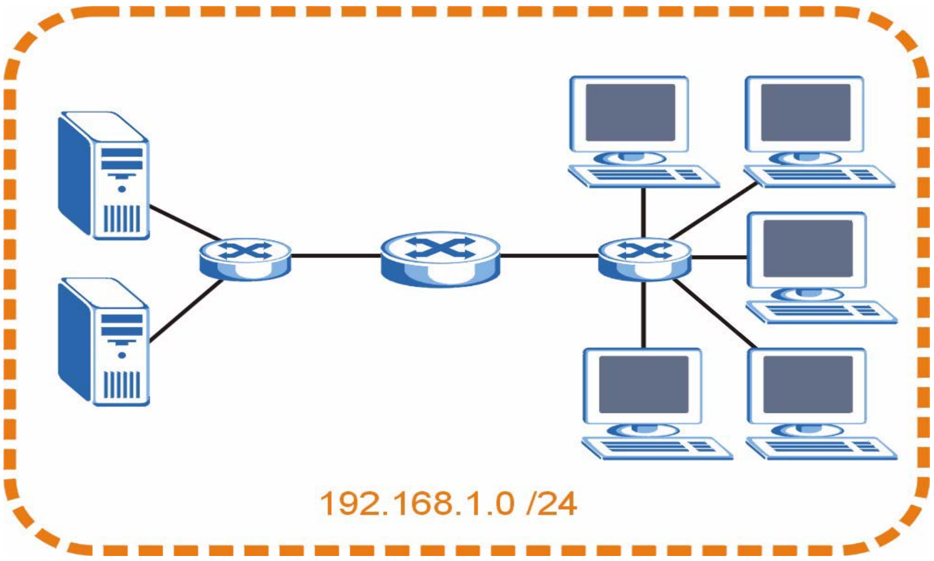
Subnetting

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

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

The following figure shows the company network before subnetting.

Figure 146 Subnetting Example: Before Subnetting

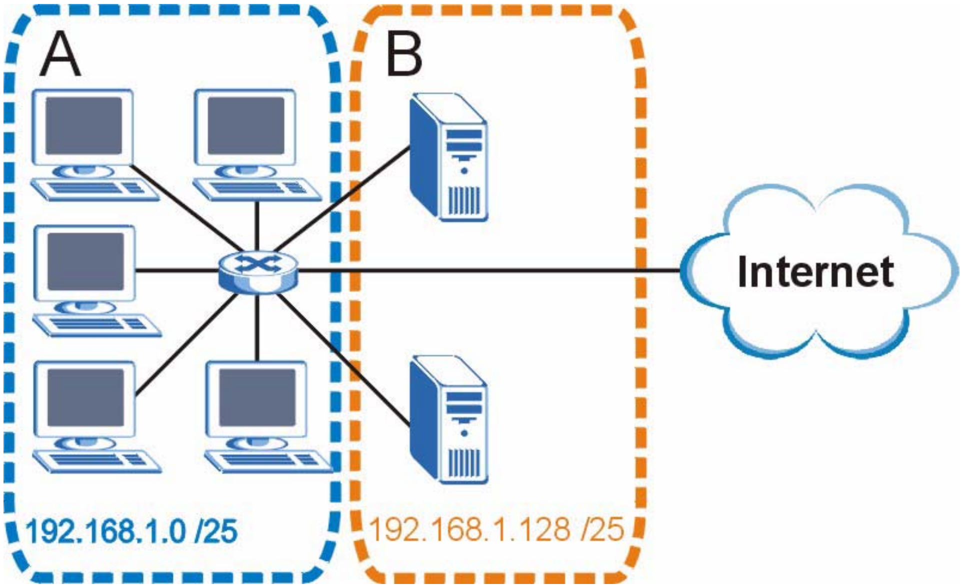


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 147 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 108 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 109 Subnet 2

	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 110 Subnet 3

	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 111 Subnet 4

	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 112 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

Table 112 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
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 113 24-bit Network Number Subnet Planning

	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 114 16-bit Network Number Subnet Planning

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

Table 114 16-bit Network Number Subnet Planning (continued)

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
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 NBG318S.

Once you have decided on the network number, pick an IP address for your NBG318S 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 NBG318S 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 NBG318S 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.*

D

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

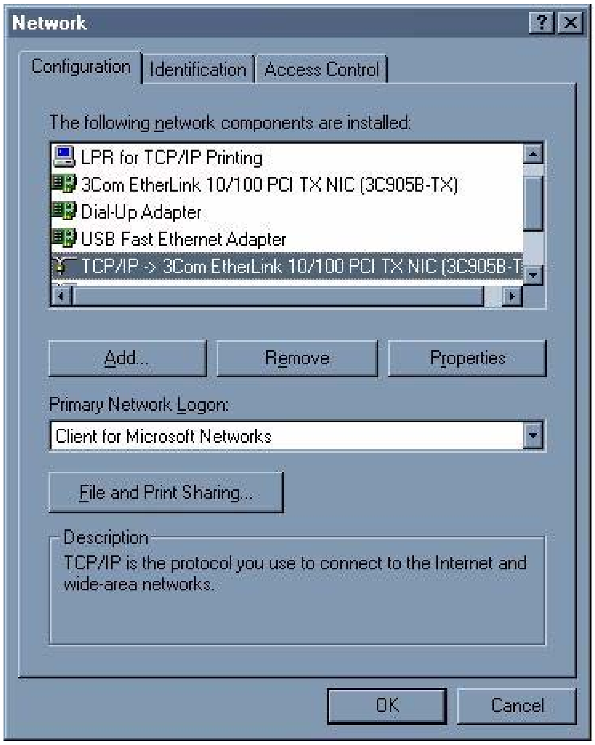
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 148 WIndows 95/98/Me: Network: Configuration



Network

Configuration | Identification | Access Control

The following network components are installed:

- LPR for TCP/IP Printing
- 3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
- Dial-Up Adapter
- USB Fast Ethernet Adapter
- TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.
2 Select **Adapter** and then click **Add**.
3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.
2 Select **Protocol** and then click **Add**.
3 Select **Microsoft** from the list of **manufacturers**.
4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.
2 Select **Client** and then click **Add**.
3 Select **Microsoft** from the list of manufacturers.
4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
5 Restart your computer so the changes you made take effect.

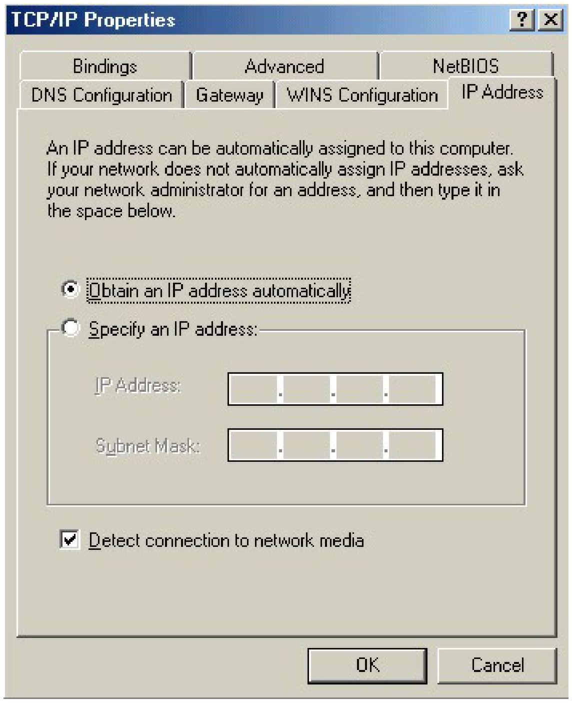
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 149 Windows 95/98/Me: TCP/IP Properties: IP Address



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

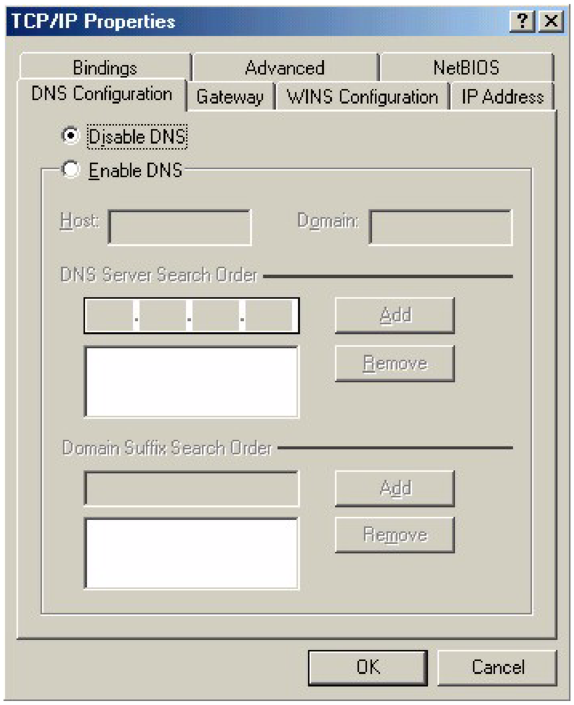
Subnet Mask: . . .

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 150 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS
○ Enable DNS

4 Click the **Gateway** tab.
   - If you do not know your gateway’s IP address, remove previously installed gateways.
   - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
5 Click **OK** to save and close the **TCP/IP Properties** window.
6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7 Turn on your Prestige and restart your computer when prompted.

Verifying Settings

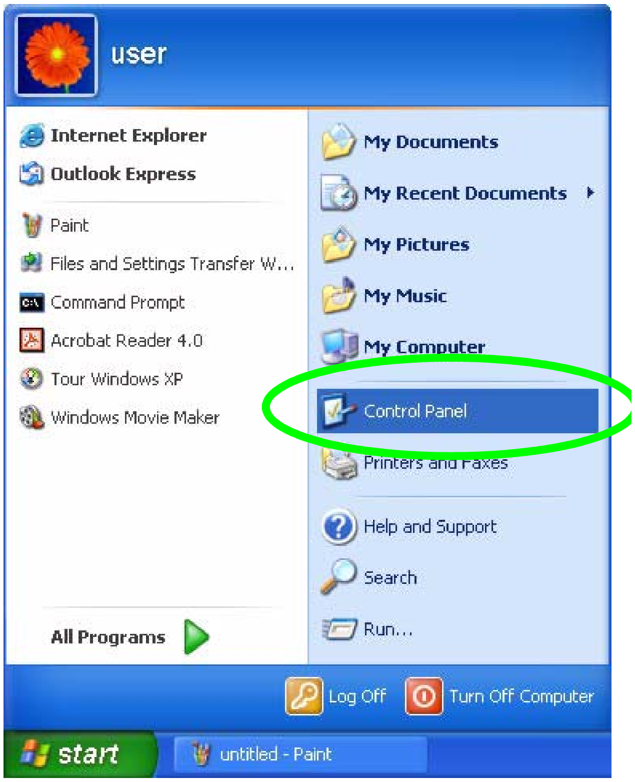
1 Click **Start** and then **Run**.
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

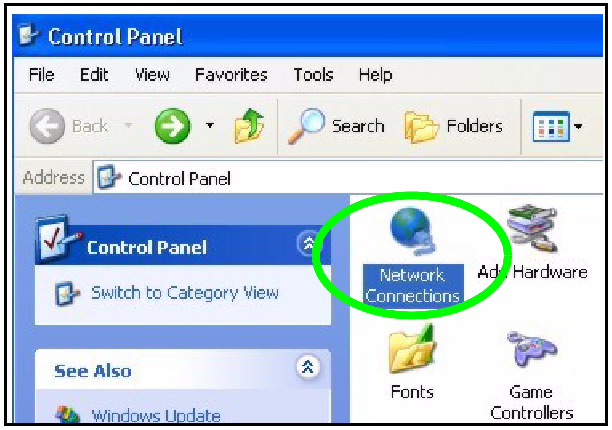
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 151 Windows XP: Start Menu



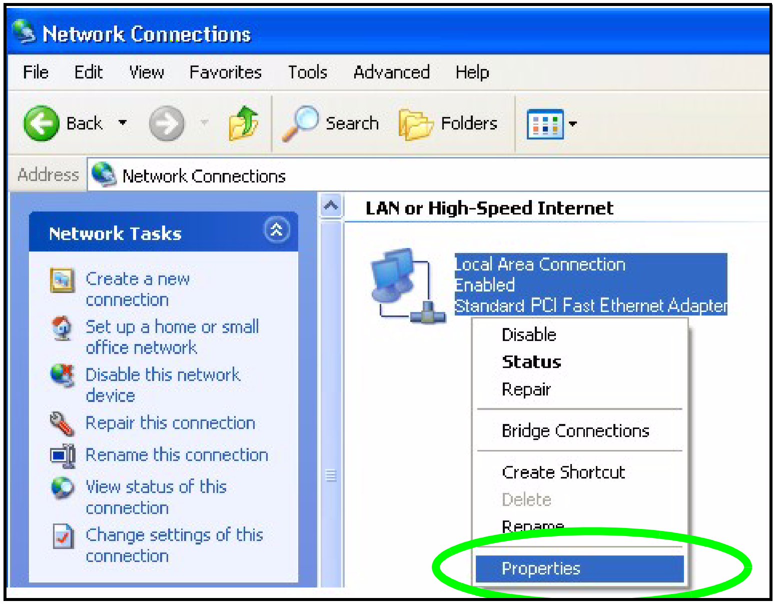
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 152 Windows XP: Control Panel



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

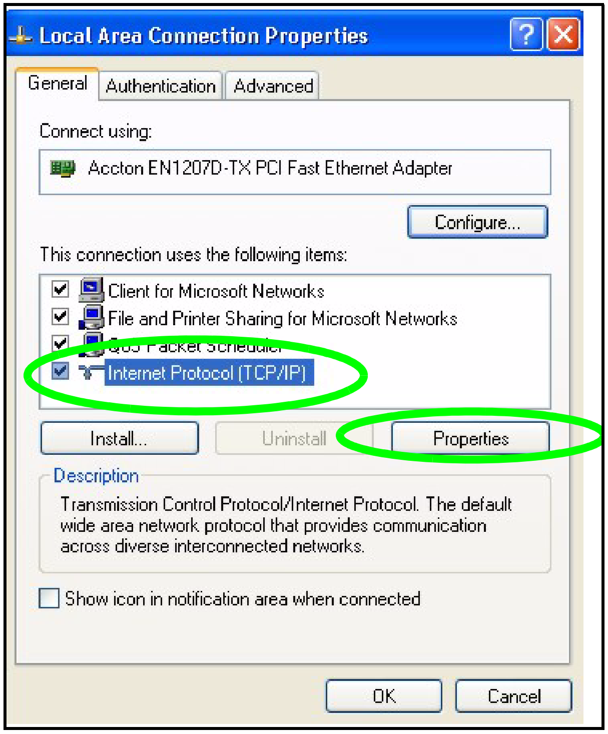
Figure 153 Windows XP: Control Panel: Network Connections: Properties



Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter

4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 154 Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

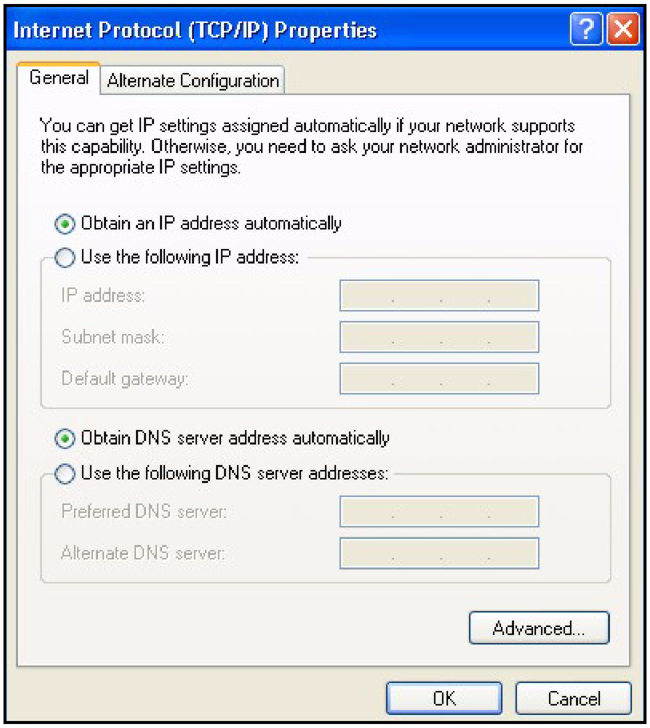
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 155 Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

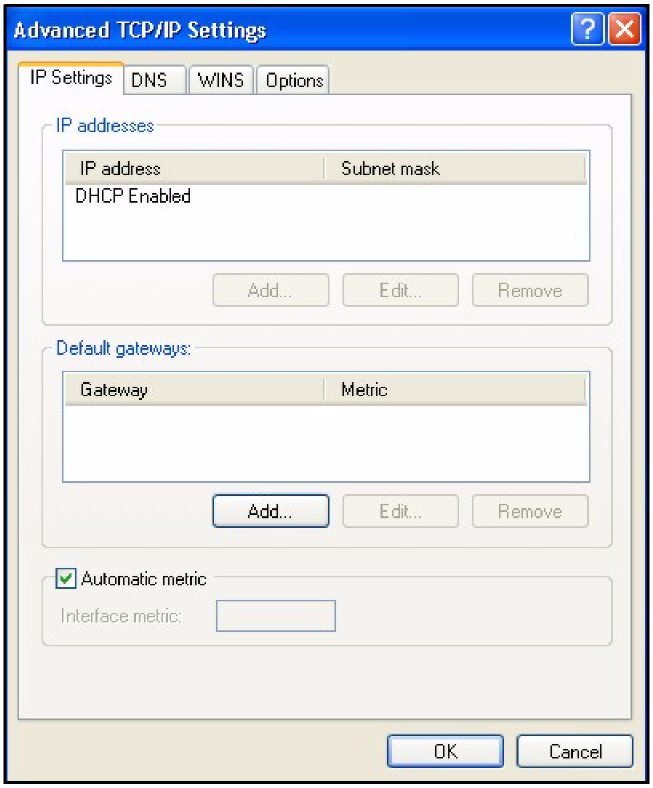
Alternate DNS server: . . .

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 156 Windows XP: Advanced TCP/IP Properties



Advanced TCP/IP Settings

IP Settings | DNS | WINS | Options

IP addresses

IP address	Subnet mask
DHCP Enabled	

Add... Edit... Remove

Default gateways:

Gateway	Metric

Add... Edit... Remove

☑ Automatic metric

Interface metric:

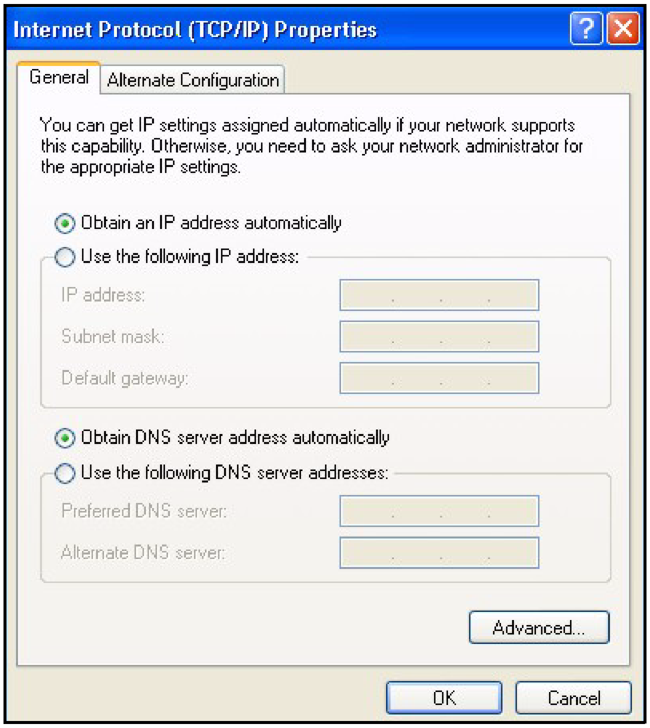
OK Cancel

7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 157 Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

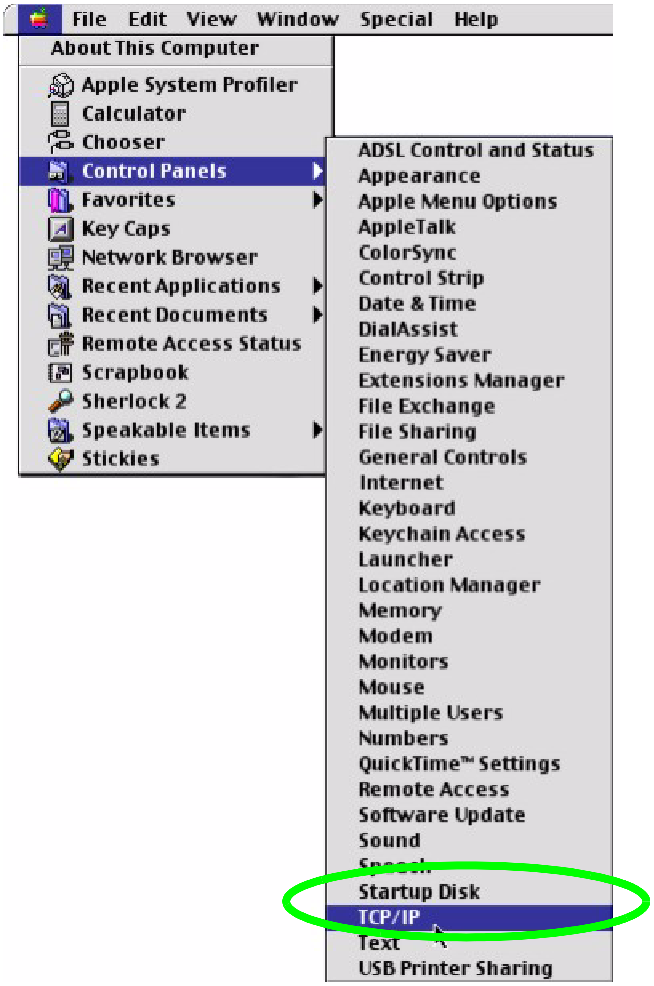
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

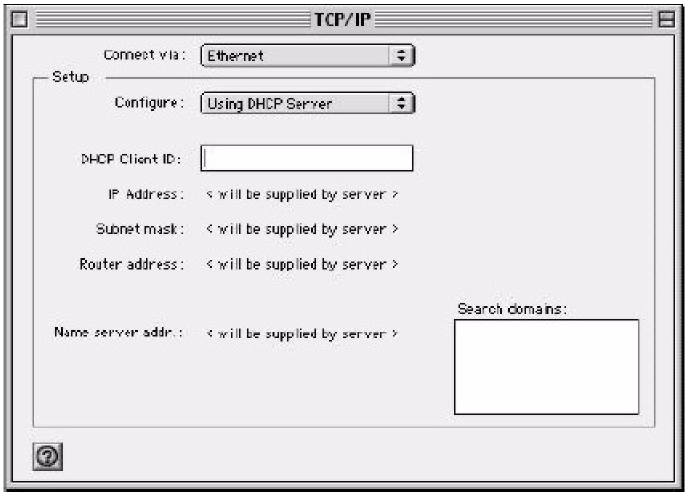
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 158 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 159 Macintosh OS 8/9: TCP/IP



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Search domains:

Name server addr.: < will be supplied by server >

3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your Prestige and restart your computer (if prompted).

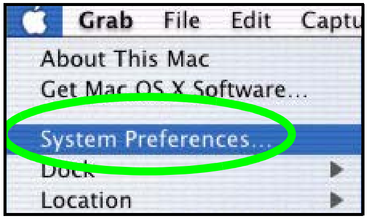
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 160 Macintosh OS X: Apple Menu

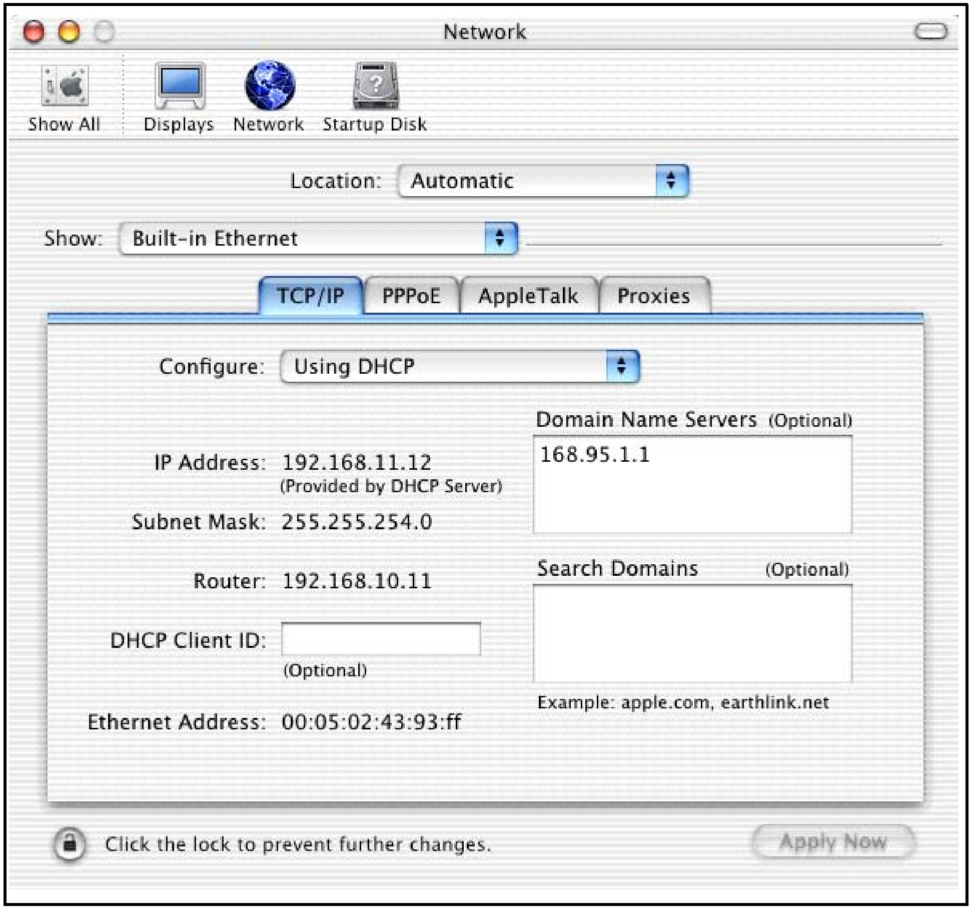


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 161   Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

4 For statically assigned settings, do the following:
    - From the **Configure** box, select **Manually**.
    - Type your IP address in the **IP Address** box.
    - Type your subnet mask in the **Subnet mask** box.
    - Type the IP address of your Prestige in the **Router address** box.
5 Click **Apply Now** and close the window.
6 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

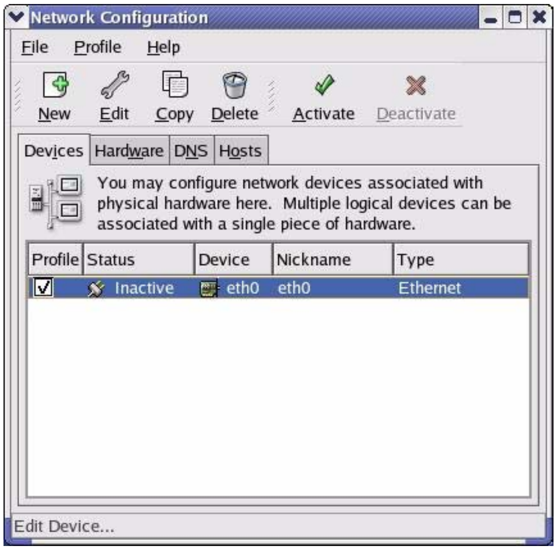
Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 162 Red Hat 9.0: KDE: Network Configuration: Devices

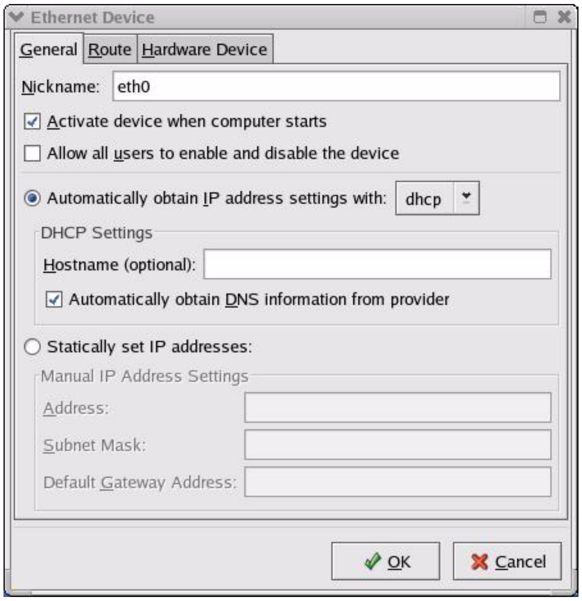


You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

Profile	Status	Device	Nickname	Type
☑	Inactive	eth0	eth0	Ethernet

2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Figure 163 Red Hat 9.0: KDE: Ethernet Device: General



Nickname: eth0

☑ Activate device when computer starts

□ Allow all users to enable and disable the device

● Automatically obtain IP address settings with: dhcp

DHCP Settings

Hostname (optional):

☑ Automatically obtain DNS information from provider

○ Statically set IP addresses:

Manual IP Address Settings

Address:

Subnet Mask:

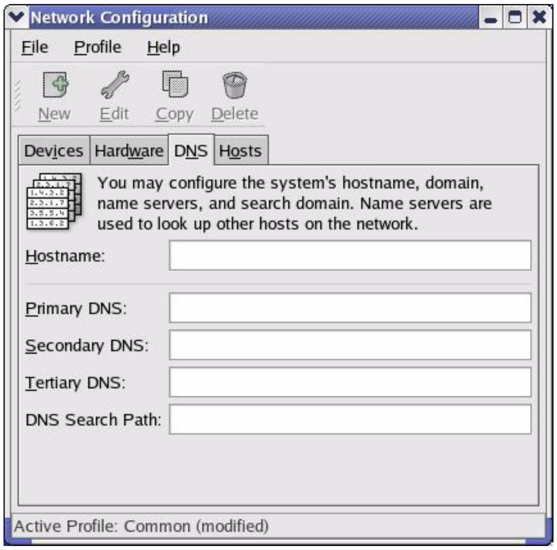
Default Gateway Address:

- If you have a dynamic IP address click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 164 Red Hat 9.0: KDE: Network Configuration: DNS



You may configure the system's hostname, domain, name servers, and search domain. Name servers are used to look up other hosts on the network.

Hostname:

Primary DNS:

Secondary DNS:

Tertiary DNS:

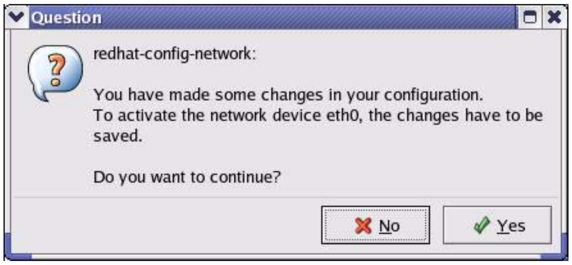
DNS Search Path:

Active Profile: Common (modified)

5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 165 Red Hat 9.0: KDE: Network Configuration: Activate



redhat-config-network:

You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.

Do you want to continue?

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 166 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **`static`** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 167 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 168 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 169 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                   [OK]
Shutting down loopback interface:               [OK]
Setting network parameters:                     [OK]
Bringing up loopback interface:                 [OK]
Bringing up interface eth0:                     [OK]
```

26.8.1 Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 170 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

Wireless LANs

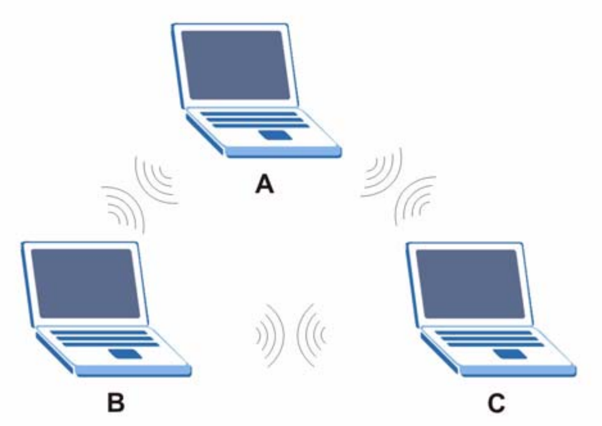
Wireless LAN Topologies

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 stations (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 171 Peer-to-Peer Communication in an Ad-hoc Network

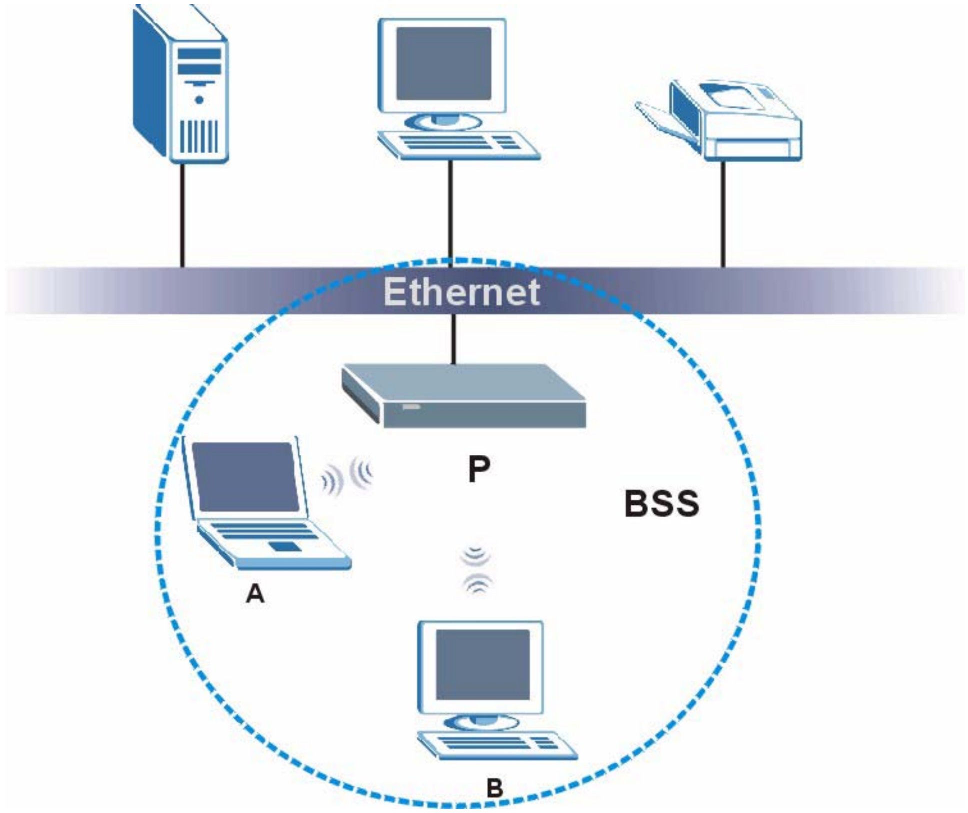


BSS

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

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

Figure 172 Basic Service Set



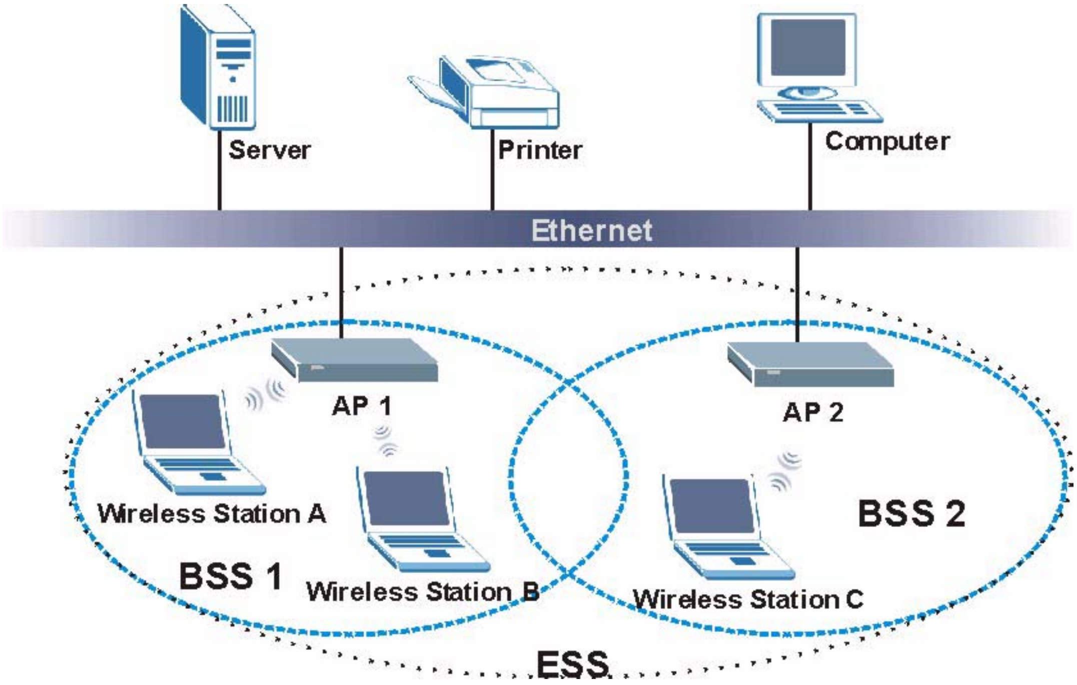
ESS

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 stations within the same ESS must have the same ESSID in order to communicate.

Figure 173 Infrastructure WLAN



Channel

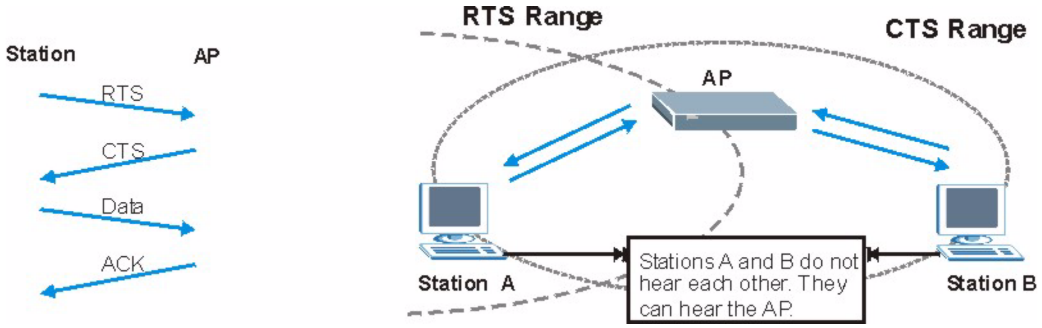
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs 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 174 RTS/CTS


Station
AP
RTS
CTS
Data
ACK
RTS Range
CTS Range
AP
Station A
Station B
Stations A and B do not hear each other. They can hear the AP.

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

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

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

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

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

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

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

Fragmentation Threshold

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

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

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

Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

The AP and the wireless stations MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

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

Table 115 IEEE 802.11g

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

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 stations.

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 station 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 Authentication

This appendix discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station ‘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 stations 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 screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

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 116 Comparison of EAP Authentication Types

		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(2)

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(2) and WEP are improved data encryption and user authentication.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. In addition to TKIP, WPA2 also uses Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes 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.

TKIP regularly changes and rotates 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 pair-wise key 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.

WPA2 AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael.

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), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

User Authentication

WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

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.

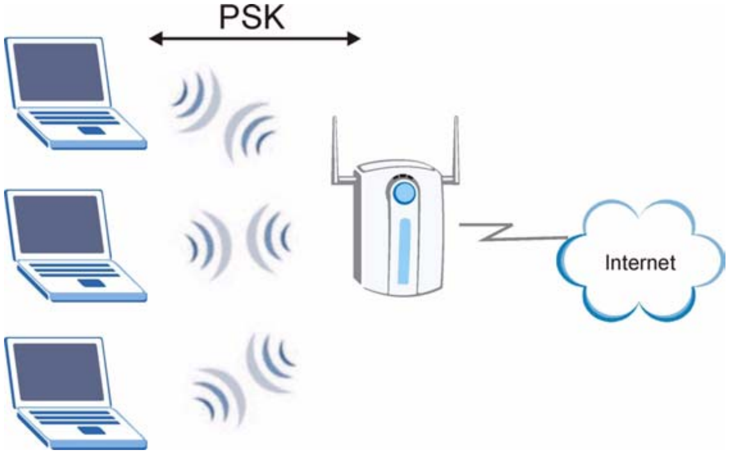
Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

26.8.2 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 (including spaces and symbols).
2. The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 175 WPA(2)-PSK Authentication



26.8.3 WPA(2) with RADIUS Application Example

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. 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 pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Security Parameters Summary

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

Table 117 Wireless Security Relational Matrix

	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	No	Enable
WPA-PSK	TKIP	Yes	Enable
WPA2	AES	No	Enable
WPA2-PSK	AES	Yes	Enable

F

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **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**.
  - 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 118 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
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 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 (e.g. 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.

Table 118 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast 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.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks’ messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
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).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.

Table 118 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
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	The Simple File Transfer Protocol is an old way of transferring files between computers.
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.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
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.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
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.

Table 118 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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 UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

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.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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

FCC Radiation Exposure Statement

- 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.
- 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.

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。

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.

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 materials or workmanship for a period of up to two years from the date of purchase. 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 ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

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

H

Customer Support

Please have the following information ready when you contact customer support.

Required Information

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

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- FTP: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz

- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com

- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index