Log action buttons are described in Table 5-2

Table 5-2. Log action buttons

Field	Description
Refresh	Click this button to refresh the log screen.
Clear Log	Click this button to clear the log entries.
Send Log	Click this button to E-mail the log immediately.

Configuring E-Mail Alert and Web Access Log Notifications

In order to receive logs and alerts by E-mail, you must provide your E-mail information in the E-Mail menu, shown below:

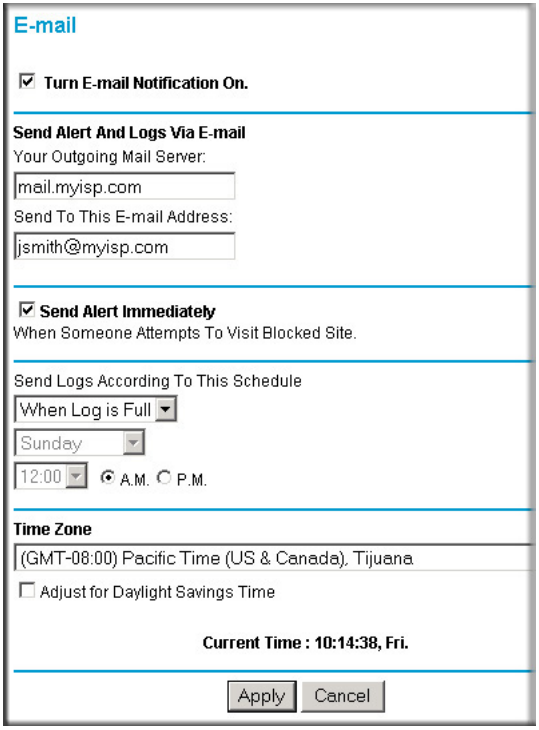

Figure 5-6: Email menu

- Turn e-mail notification on
  Check this box if you wish to receive e-mail logs and alerts from the router.
- Your outgoing mail server
  Enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. If you leave this box blank, log and alert messages will not be sent via e-mail.
- Send to this e-mail address
  Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.

You can specify that logs are automatically sent to the specified e-mail address with these options:

- Send alert immediately
  Check this box if you would like immediate notification of attempted access to a blocked site.
- Send logs according to this schedule
  Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
  - Day for sending log
    Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
  - Time for sending log
    Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

  If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer may fill up. In this case, the router overwrites the log and discards its contents.

The WGR624v3 router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must specify your Time Zone:

- Time Zone
  Select your local time zone. This setting will be used for the blocking schedule and for time-stamping log entries.
- Daylight Savings Time
  Check this box if your time zone is currently under daylight savings time.

Chapter 6
Maintenance

This chapter describes how to use the maintenance features of your 108 Mbps Wireless Firewall Router WGR624v3. These features can be found by clicking on the Maintenance heading in the Main Menu of the browser interface.

Viewing Wireless Router Status Information

The Router Status menu provides status and usage information. From the Main Menu of the browser interface, click on Maintenance, then select Router Status to view the System Status screen, shown below.

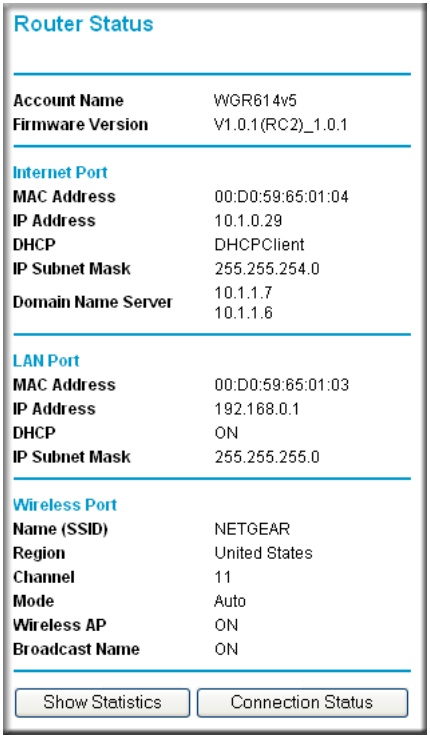

Figure 6-1: Router Status screen

This screen shows the following parameters:

Table 6-1. Wireless Router Status Fields

Field	Description
Account Name	This field displays the Host Name assigned to the router.
Firmware Version	This field displays the router firmware version.
Internet Port	These parameters apply to the Internet (WAN) port of the router.
MAC Address	This field displays the Media Access Control address being used by the Internet (WAN) port of the router.
IP Address	This field displays the IP address being used by the Internet (WAN) port of the router. If no address is shown, the router cannot connect to the Internet.
DHCP	If set to None, the router is configured to use a fixed IP address on the WAN. If set to Client, the router is configured to obtain an IP address dynamically from the ISP.
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (WAN) port of the router.
DNS	This field displays the Domain Name Server addresses being used by the router.
LAN Port	These parameters apply to the Local (LAN) port of the router.
MAC Address	This field displays the Media Access Control address being used by the LAN port of the router.
IP Address	This field displays the IP address being used by the Local (LAN) port of the router. The default is 192.168.0.1
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Local (LAN) port of the router. The default is 255.255.255.0
DHCP	Identifies if the router's built-in DHCP server is active for the LAN attached devices.

Table 6-1. Wireless Router Status Fields

Field	Description
Wireless Port	These parameters apply to the Wireless port of the router.
MAC Address	This field displays the Media Access Control address being used by the Wireless port of the router.
Name (SSID)	This field displays the wireless network name (SSID) being used by the wireless port of the router. The default is NETGEAR.
Region	This field displays the geographic region where the router being used. It may be illegal to use the wireless features of the router in some parts of the world.
Channel	Identifies the channel of the wireless port being used. See "Wireless Channels" on page D-2 for the frequencies used on each channel.

Click on the "Connection Status" button to display the connection status, as shown below.

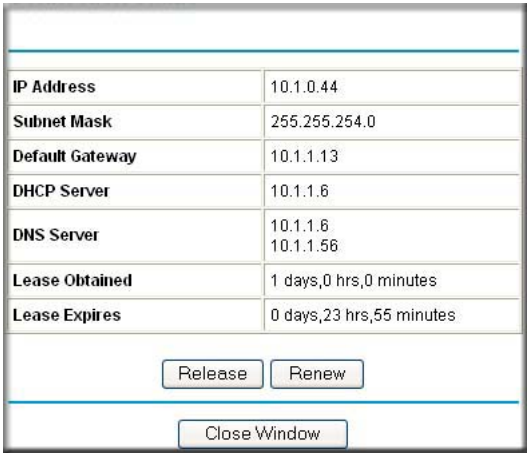

Figure 6-2: Connection Status screen

This screen shows the following statistics:.

Table 6-2: Connection Status Items

Item	Description
IP Address	The WAN (Internet) IP Address assigned to the router.
Subnet Mask	The WAN (Internet) Subnet Mask assigned to the router.

Table 6-2: Connection Status Items

Item	Description
Default Gateway	The WAN (Internet) default gateway the router communicates with.
DHCP Server	The IP address of the DHCP server which provided the IP configuration addresses.
DNS Server	The IP address of the DNS server which provides network name to IP address translation.
Lease Obtained	When the DHCP lease was obtained.
Lease Expires	When the DHCP lease was expires.
Release	Click the Release button to release the DHCP lease.
Renew	Click the Renew button to renew the DHCP lease.

Click on the “Show Statistics” button to display router usage statistics, as shown below.

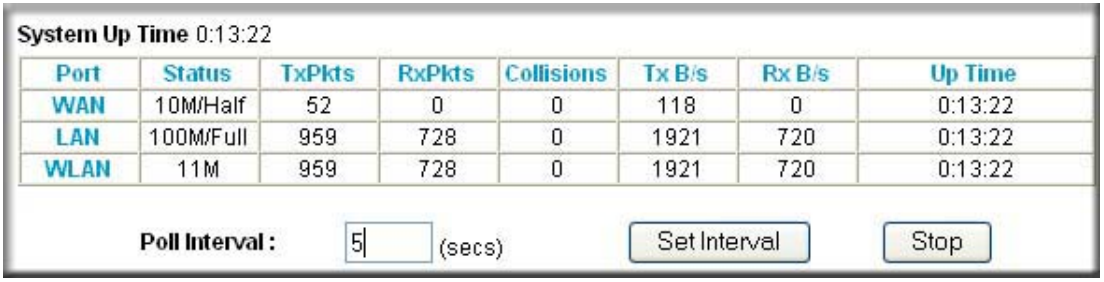

Figure 6-3: Router Statistics screen

This screen shows the following statistics:

Table 6-3: Router Statistics Items

Item	Description
Port	The statistics for the WAN (Internet) and LAN (local) ports. For each port, the screen displays:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current transmission (outbound) bandwidth used on the WAN and LAN ports.

Table 6-3: Router Statistics Items

Item	Description
Rx B/s	The current reception (inbound) bandwidth used on the WAN and LAN ports.
Up Time	The amount of time since the router was last restarted.
Up Time	The time elapsed since this port acquired the link.
Poll Interval	Specifies the intervals at which the statistics are updated in this window. Click on Stop to freeze the display.
Set Interval	Enter a time and click the button to set the polling frequency.
Stop	Click the Stop button to freeze the polling information.

Viewing a List of Attached Devices

The Attached Devices menu contains a table of all IP devices that the router has discovered on the local network. From the Main Menu of the browser interface, under the Maintenance heading, select Attached Devices to view the table, shown below.

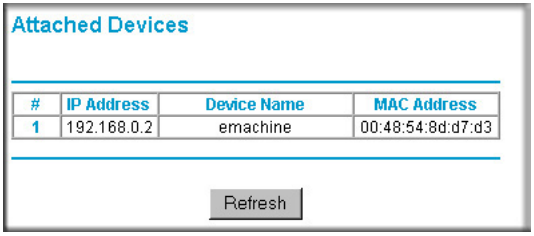

Figure 6-4: Attached Devices menu

For each device, the table shows the IP address, NetBIOS Host Name (if available), and Ethernet MAC address. Note that if the router is rebooted, the table data is lost until the router rediscovers the devices. To force the router to look for attached devices, click the Refresh button.

Configuration File Management

The configuration settings of the WGR624v3 router are stored within the router in a configuration file. This file can be saved (backed up) to a user's PC, retrieved (restored) from the user's PC, or cleared to factory default settings.

From the Main Menu of the browser interface, under the Maintenance heading, select the Settings Backup heading to bring up the menu shown below.

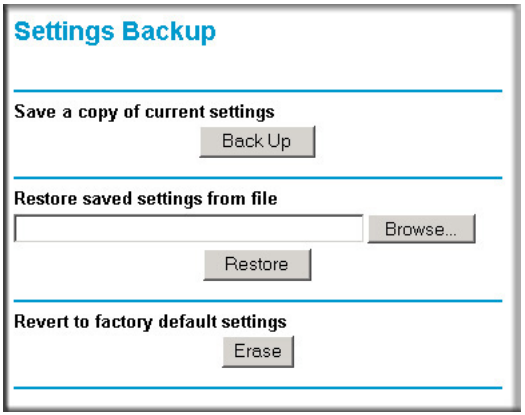

Figure 6-5: Settings Backup menu

Three options are available, and are described in the following sections.

Restoring and Backing Up the Configuration

The Restore and Backup options in the Settings Backup menu allow you to save and retrieve a file containing your router's configuration settings.

To save your settings, click the Backup button. Your browser will extract the configuration file from the router and will prompt you for a location on your PC to store the file. You can give the file a meaningful name at this time, such as pacbell.cfg.

To restore your settings from a saved configuration file, enter the full path to the file on your PC or click the Browse button to browse to the file. When you have located it, click the Restore button to send the file to the router. The router will then reboot automatically.

Warning: Do not interrupt the reboot process.

Erasing the Configuration

It is sometimes desirable to restore the router to original default settings. This can be done by using the Erase function, which will restore all factory settings. After an erase, the router's password will be **password**, the LAN IP address will be 192.168.0.1, and the router's DHCP client will be enabled.

To erase the configuration, click the Erase button.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the router. See "Restoring the Default Configuration and Password" on page 8-7.

Upgrading the Router Software

Note: Before upgrading the router software, use the router backup utility to save your configuration settings. Any router upgrade will revert the router settings back to the factory defaults. After completing the upgrade, you can restore your settings from the backup.

The routing software of the WGR624v3 router is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from the NETGEAR Web site. If the upgrade file is compressed (.ZIP file), you must first extract the file before sending it to the router. The upgrade file can be sent to the router using your browser.

Note: The Web browser used to upload new firmware into the WGR624v3 router must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer or Netscape Navigator 3.0 or above.

From the Main Menu of the browser interface, under the Maintenance heading, select the Router Upgrade link display the menu shown below.

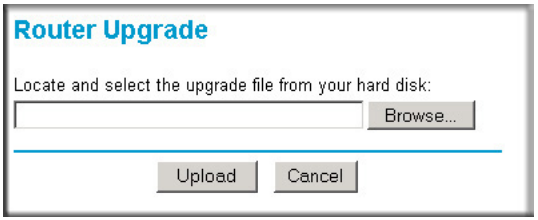

Figure 6-6: Router Upgrade menu

To upload new firmware:

1. Download and unzip the new software file from NETGEAR.
2. In the Router Upgrade menu, click the Browse button and browse to the location of the upgrade file
3. Click Upload.

   Note: When uploading software to the WGR624v3 router, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your router will automatically restart. The upgrade process will typically take about one minute.

In some cases, you may need to reconfigure the router after upgrading.

Changing the Administrator Password

	**Note:** Before changing the router password, use the router backup utility to save your configuration settings. If after changing the password, you forget the new password you assigned, you will have to reset the router back to the factory defaults to be able to log in using the default password of password. This means you will have to restore all the router configuration settings. If you ever have to reset the router back to the factory defaults, you can restore your settings from the backup.

The default password for the router's Web Configuration Manager is **password**. NETGEAR recommends that you change this password to a more secure password.

From the Main Menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown below.

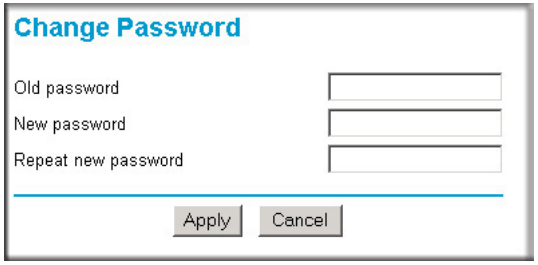

Figure 6-7: Set Password menu

To change the password, first enter the old password, then enter the new password twice. Click Apply.

Chapter 7
Advanced Configuration of the Router

This chapter describes how to configure the advanced features of your 108 Mbps Wireless Firewall Router WGR624v3. These features can be found under the Advanced heading in the Main Menu of the browser interface.

Note: If you are unfamiliar with networking and routing, refer to Appendix B, "Network, Routing, Firewall, and Basics," to become more familiar with the terms and procedures used in this chapter.

Configuring Port Triggering

Port Triggering is an advanced feature that can be used to easily enable gaming and other internet applications. Port Forwarding is typically used to enable similar functionality, but it is static and has some limitations.

Note: If you use applications such as multi-player gaming, peer-to-peer connections, real time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable UPnP according to the instructions at "Using Universal Plug and Play (UPnP)" on page 7-17.

Port Triggering opens an incoming port temporarily and does not require the server on the internet to track your IP address if it is changed by DHCP, for example.

Port Triggering monitors outbound traffic. When the router detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data and triggers the incoming port. Incoming traffic on the triggered port is then forwarded to the triggering computer.

Using the Port Triggering page, you can make local computers or servers available to the Internet for different services (for example, FTP or HTTP), to play Internet games (like Quake III), or to use Internet applications (like CUseeMe).

Port Forwarding is designed for FTP, Web Server or other server based services. Once port forwarding is set up, request from Internet will be forwarded to the proper server. On the contrary,

port triggering will only allow request from Internet after a designated port is 'triggered'. Port triggering applies to chat and Internet games.

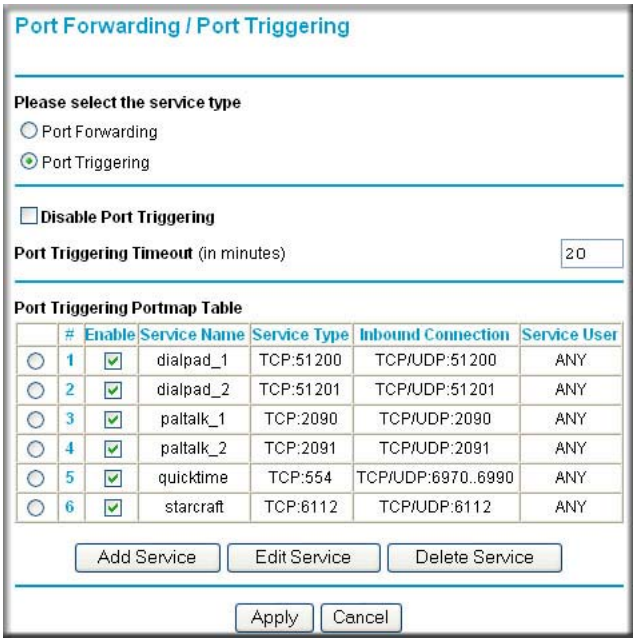

Figure 7-1: Port Triggering Menu

Note: If Disable Port Triggering box is checked after configuring port triggering, port triggering will be disabled but any port triggering configuration information you added to the router will be retained even though it will not be used.

- Port Triggering Timeout

  Enter a value up to 9999 minutes. The Port Triggering Timeout value controls the inactivity timer for the designated inbound port(s). The inbound port(s) will be closed when the inactivity timer expires.

- For Internet Games or Applications

  Before starting, you'll need to know which service, application or game you'll be configuring. Also, you'll need to have the outbound port (triggering port) address for this game or application.

Follow these steps to set up a computer to play Internet games or use Internet applications:

1. Click **Add**.

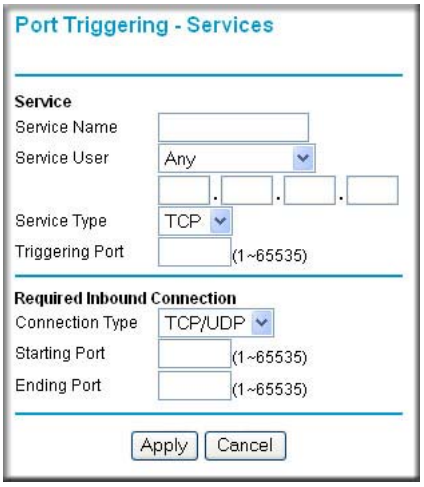

Figure 7-2: Add Port Trigger Menu

2. Enter a service name in the Service Name box.
3. Under Service User, selecting Any (default) will allow this service to be used by everyone in your network. Otherwise, select Single address and enter the IP address of one computer to restrict the service to a particular computer.
4. Select the Service Type.
5. Enter the outbound port number in Triggering Port box.
6. Enter the inbound connection port information such as Connection Type, Starting Port and Ending Port boxes. This information can be obtained from the game or applications manual or support Web site.
7. Click **Apply** to save your changes.

Configuring Port Forwarding to Local Servers

Although the router causes your entire local network to appear as a single machine to the Internet, you can make a local server (for example, a Web server or game server) visible and available to the Internet. This is done using the Port Forwarding menu. From the Main Menu of the browser

interface, under Advanced, click on Port Forwarding to view the port forwarding menu, shown below.

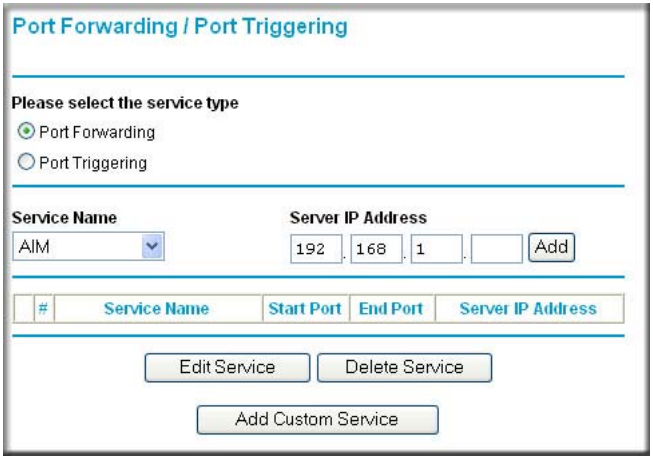

Figure 7-3: Port Forwarding Menu

Use the Port Forwarding menu to configure the router to forward incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a Default DMZ Server to which all other incoming protocols are forwarded. The DMZ Server is configured in the WAN Setup menu as discussed in "Configuring the WAN Setup Options" on page 7-7.

Before starting, you'll need to determine which type of service, application or game you'll provide and the IP address of the computer that will provide each service. Be sure the computer's IP address never changes. To configure port forwarding to a local server:

	Note: To assure that the same computer always has the same IP address, use the reserved IP address feature of your WGR624v3 router. See "Using Address Reservation" on page 7-12 for instructions on how to use reserved IP addresses.

1. From the Service & Game box, select the service or game that you will host on your network. If the service does not appear in the list, refer to the following section, "Adding a Custom Service".
2. Enter the IP address of the local server in the corresponding Server IP Address box.
3. Click the Add button.

Adding a Custom Service

To define a service, game or application that does not appear in the Services & Games list, you must determine what port numbers are used by the service. For this information, you may need to contact the manufacturer of the program that you wish to use. When you have the port number information, follow these steps:

1. Click the Add Custom Service button.

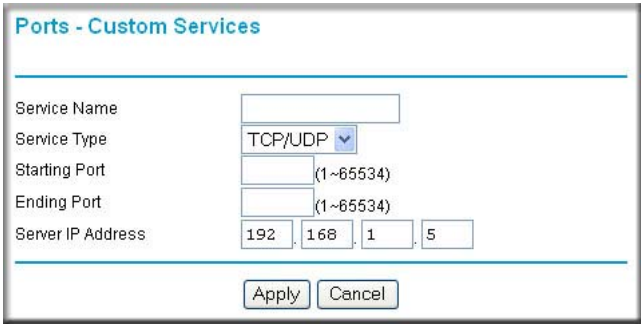

Figure 7-4: Ports - Custom Services Menu

2. Type the service name in the Service Name box.
3. Type the beginning port number in the Starting Port box.
   - If the application uses only a single port; type the same port number in the Ending Port box.
   - If the application uses a range of ports; type the ending port number of the range in the Ending Port box.
4. Type the IP address of the computer in the Server IP Address box.
5. Click **Apply** to save your changes.

Editing or Deleting a Port Forwarding Entry

To edit or delete a Port Forwarding entry, follow these steps.

1. In the table, select the button next to the service name.

2. Click Edit or Delete.

Local Web and FTP Server Example

If a local computer with a private IP address of 192.168.0.33 acts as a Web and FTP server, configure the Ports menu to forward HTTP (port 80) and FTP (port 21) to local address 192.168.0.33

In order for a remote user to access this server from the Internet, the remote user must know the IP address that has been assigned by your ISP. If this address is 172.16.1.23, for example, an Internet user can access your Web server by directing the browser to http://172.16.1.23. The assigned IP address can be found in the Maintenance Status Menu, where it is shown as the WAN IP Address.

Some considerations for this application are:

- If your account's IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires.
- If the IP address of the local computer is assigned by DHCP, it may change when the computer is rebooted. To avoid this, you can manually configure the computer to use a fixed address.
- Local computers must access the local server using the computers' local LAN address (192.168.0.33 in this example). Attempts by local computers to access the server using the external IP address (172.16.1.23 in this example) will fail.

Multiple Computers for Half Life, KALI or Quake III Example

To set up an additional computer to play Half Life, KALI or Quake III:

1. Click the button of an unused port in the table.
2. Select the game again from the Services/Games list.
3. Change the beginning port number in the Start Port box.
   For these games, use the supplied number in the default listing and add +1 for each additional computer. For example, if you've already configured one computer to play Hexen II (using port 26900), the second computer's port number would be 26901, and the third computer would be 26902.
4. Type the same port number in the End Port box that you typed in the Start Port box.
5. Type the IP address of the additional computer in the Server IP Address box.
6. Click Apply.

Some online games and videoconferencing applications are incompatible with NAT. The WGR624v3 router is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local computer can run the application properly if that computer's IP address is entered as the default in the PORTS Menu. If one local computer acts as a game or videoconferencing host, enter its IP address as the default.

Configuring the WAN Setup Options

The WAN Setup options let you configure a DMZ server, change the MTU size and enable the wireless router to respond to a Ping on the WAN port. These options are discussed below.

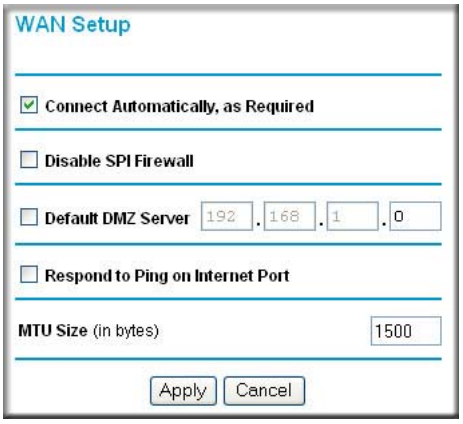

Figure 7-5: WAN Setup menu.

Connect Automatically, as Required

Normally, this option should be checked to enable it. An Internet connection will be made automatically after each timeout, whenever Internet-bound traffic is detected. This provides connection on demand and is potentially cost-saving in places in Europe for example where Internet services charge by the minute.

If disabled, you must connect manually, using the "Connection Status" button on the Router Status screen. This manual connection will stay up all the time without time outs.

Disabling the SPI Firewall

The SPI (Stateful Inspection) Firewall protects your LAN against Denial of Service attacks. This should only be disabled in special circumstances.

Setting Up a Default DMZ Server

The default DMZ server feature is helpful when using some online games and videoconferencing applications that are incompatible with NAT. The router is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local computer can run the application properly if that computer's IP address is entered as the default DMZ server.

Note: DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall, and is exposed to exploits from the Internet. If compromised, the DMZ server can be used to attack your network.

Incoming traffic from the Internet is normally discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports menu. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the Default DMZ Server.

The WAN Setup menu, shown below lets you configure a Default DMZ Server.

To assign a computer or server to be a Default DMZ server, follow these steps:

1. Click WAN Setup link on the Advanced section of the main menu.
2. Type the IP address for that server. To remove the default DMZ server, replace the IP address numbers with all zeros.
3. Click Apply.

Responding to Ping on Internet WAN Port

If you want the router to respond to a 'ping' from the Internet, click the 'Respond to Ping on Internet WAN Port' check box. This should only be used as a diagnostic tool, since it allows your router to be discovered. Don't check this box unless you have a specific reason to do so.