The Applications and Gaming Tab - Port Range Forward

The Applications and Gaming Tab allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

To forward a port, enter the information on each line for the criteria required. Descriptions of each criteria are described here.

Application. In this field, enter the name you wish to give the application. Each name can be up to 12 characters.

Start/End. This is the port range. Enter the number that starts the port range under **Start** and the number that ends the range under **End**.

Protocol. Enter the protocol used for this application, either **TCP** or **UDP**, or **Both**.

IP Address. For each application, enter the IP Address of the PC running the specific application.

Enable. Click the **Enable** checkbox to enable port forwarding for the relevant application.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

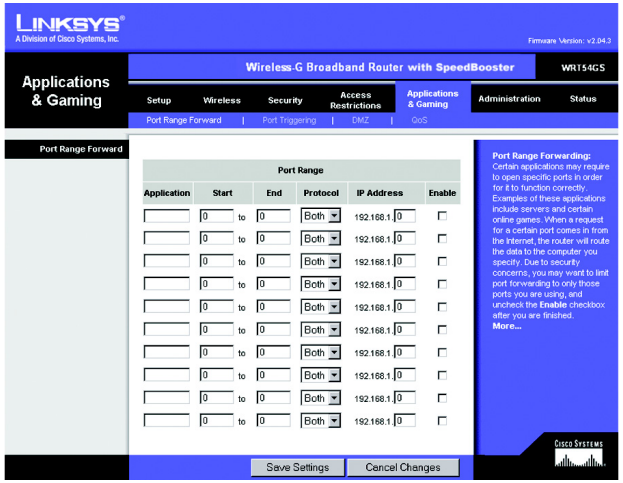

Figure 6-31: Applications and Gaming Tab - Port Range Forward

***tcp**: a network protocol for transmitting data that requires acknowledgement from the recipient of data sent*

***udp**: a network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.*

***ip** (internet protocol): a protocol used to send data over a network*

***ip address** : the address used to identify a computer or device on a network*

The Applications & Gaming Tab - Port Triggering

The *Port Triggering* screen allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

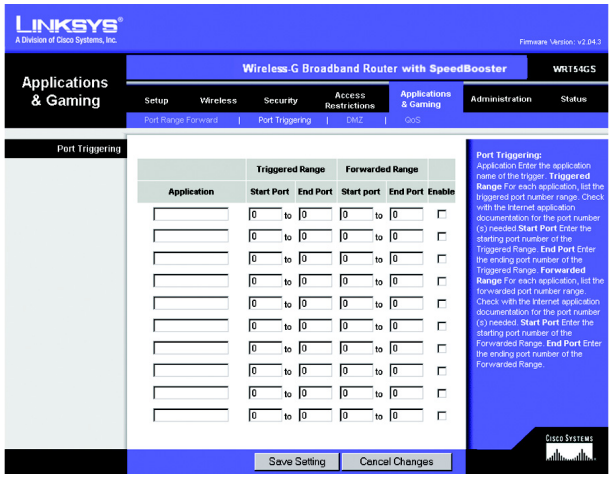

Figure 6-32: Applications and Gaming Tab - Port Triggering

Port Triggering

Application. Enter the application name of the trigger.

Triggered Range

For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed.

Start Port. Enter the starting port number of the Triggered Range.

End Port. Enter the ending port number of the Triggered Range.

Forwarded Range

For each application, list the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.

Start Port. Enter the starting port number of the Forwarded Range.

End Port. Enter the ending port number of the Forwarded Range.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

The Applications and Gaming Tab - DMZ

The DMZ feature allows one network user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forward feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.

Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

To expose one PC, select **Enable**. Then, enter the computer's IP address in the *DMZ Host IP Address* field.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

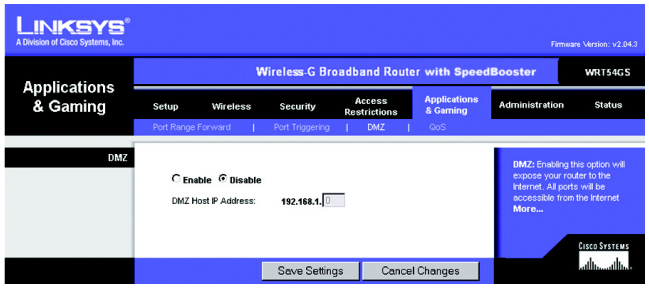

Figure 6-33: Applications and Gaming Tab - DMZ

QoS

Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing.

There are three types of QoS available, Device Priority, Application Priority, and Ethernet Port Priority.

Enabled/Disabled. To limit outgoing bandwidth for the QoS policies in use, select **Enable**. Otherwise, select **Disable**.

Upstream Bandwidth. Select the bandwidth to be used from the drop-down menu.This setting allows you to limit the outgoing bandwidth for the QoS policies in use, so you can control how much bandwidth a particular application is allowed to use.

Device Priority

Enter the name of your network device in the *Device name* field, enter its MAC Address, then select its priority from the drop-down menu.

Ethernet Port Priority

Ethernet Port Priority QoS allows you to prioritize performance for four of the Router's ports, LAN Ports 1-4. For each of these ports, select **High** or **Low** for *Priority*. For Flow Control, if you want the Router to control the transmission of data between network devices, select **Enable**. To disable this feature, select **Disable**. The

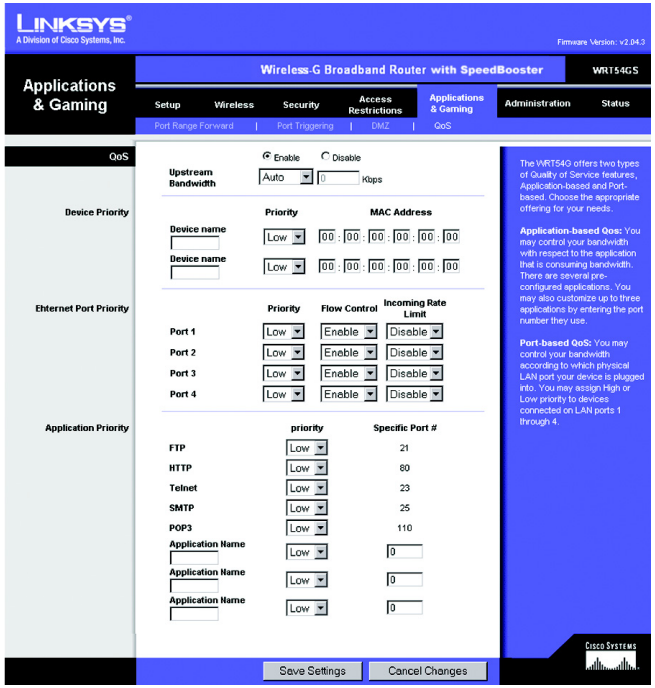

Figure 6-34: Applications and Gaming Tab - QOS

Router's other four ports will be automatically assigned low priority. Incoming Rate Limit limits the incoming bandwidth. To use this feature, select **8M**, **4M**, **2M**, **1M**, **512K**, **256K**, or **128K** (M stands for Mbps, while K stands for kbps). If you do not want to use this feature, keep the default, **Disable**.

Ethernet Port Priority QoS does not require support from your ISP because the prioritized ports are LAN ports going out to your network.

Application Port Priority

Application Port Priority QoS manages information as it is transmitted and received. Depending on the settings of the *QoS* screen, this feature will assign information a high or low priority for the five preset applications and three additional applications that you specify. For each application, select **High** or **Low** for *Priority*. For Specific Port#, you can add three additional applications by entering their respective port numbers in the *Specific Port#* fields.

FTP (File Transfer Protocol). A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the web server using FTP.

HTTP (HyperText Transport Protocol). The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client web browser.

Telnet. A terminal emulation protocol commonly used on Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

SMTP (Simple Mail Transfer Protocol). The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

POP3 (Post Office Protocol 3). A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are downloaded at the same time. POP3 uses the SMTP messaging protocol.

Application Name. You can add three additional applications by entering their names in the *Application Name* fields.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

The Administration Tab - Management

This section of the Administration tab allows the network's administrator to manage specific Router functions for access and security.

Local Router Access. You can change the Router's password from here. Enter a new Router password and then type it again in the *Re-enter to confirm* field to confirm.

Web Access. HTTP (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web. HTTPS - Uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. Select **HTTP** or **HTTPS**. Wireless Access Web - If you are using your Wireless Router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the router's web-based utility. You will only be able to access the web-based utility via a wired connection if you disable the setting. Select **Enable** to enable wireless access to the Router's web-based utility or **Disable** to disable wireless access to the utility.

Remote Router Access. To access the Router remotely, from outside the network, verify that **Enable** is selected. Then, enter the port number that will be open to outside access. You will need to enter the Router's password when accessing the Router this way, as usual.

UPnP. When using UPnP features, select **Enable**. Because allowing this may present a risk to security, this feature is disabled by default.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

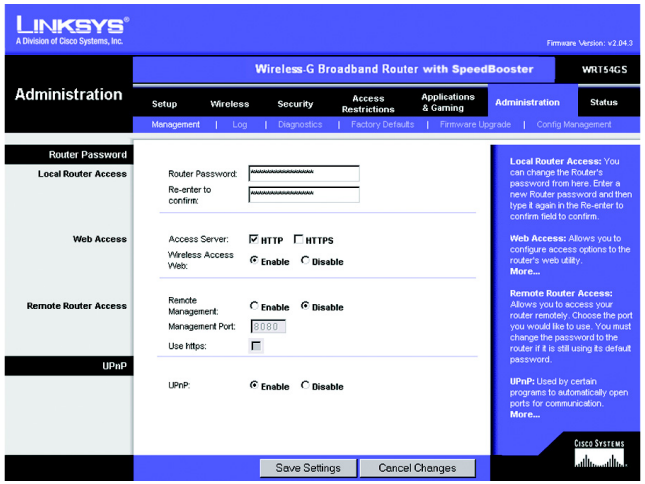

Figure 6-35: Administration Tab - Management

The Administration Tab - Log

The Router can keep logs of all traffic for your Internet connection. To disable the Log function, keep the default setting, **Disable**. To monitor traffic between the network and the Internet, select **Enable**. When you wish to view the logs, click **Incoming Log** or **Outgoing Log**, depending on which you wish to view.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

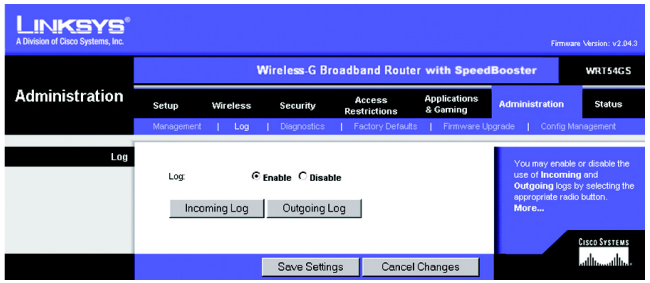

Figure 6-36: Administration Tab - Log

The Administration Tab - Diagnostics

The diagnostic tests (Ping and Traceroute) allow you to check the connections of your network components.

Ping Test. The Ping test will check the status of a connection. Click the **Ping** button to open the *Ping Test* screen. Enter the address of the PC whose connection you wish to test and how many times you wish to test it. Then, click the **Ping** button. The Ping Test screen will show if the test was successful. To stop the test, click the **Stop** button. Click the **Clear Log** button to clear the screen. Click the **Close** button to return to the *Diagnostics* screen.

Traceroute Test. To test the performance of a connect, click the **Traceroute** button. Enter the address of the PC whose connection you wish to test and click the **Ping** button. The Traceroute Test screen will show if the test was successful. To stop the test, click the **Stop** button. Click the **Clear Log** button to clear the screen. Click the **Close** button to return to the *Diagnostics* screen.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

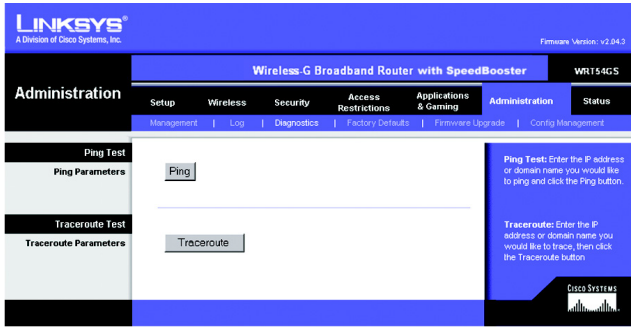

Figure 6-37: Administration Tab - Diagnostics

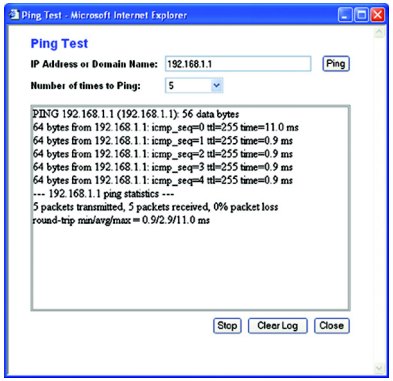

Figure 6-38: The Ping Test

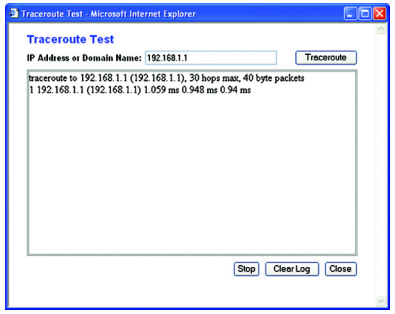

Figure 6-39: The Traceroute Test

The Administration Tab - Factory Defaults

Click the **Yes** button to reset all configuration settings to their default values, and then click the **Save Settings** button. Any settings you have saved will be lost when the default settings are restored. This feature is disabled by default.

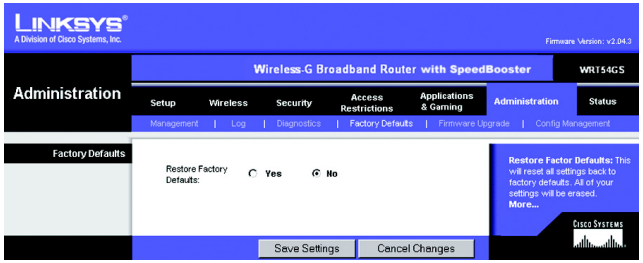

Figure 6-40: Administration Tab - Factory Defaults

The Administration Tab - Firmware Upgrade

Firmware can be upgraded by clicking the **Upgrade** button after browsing for the firmware, which you can download from the Linksys website. Do not upgrade your firmware unless you are experiencing problems with the Router. For more information about upgrading firmware, refer to “Appendix C: Upgrading Firmware”.

Figure 6-41: Administration Tab - Firmware Upgrade

***firmware**: the programming code that runs a networking device*

***upgrade**: to replace existing software or firmware with a newer version*

***download**: to receive a file transmitted over a networ*

The Administration Tab - Config Management

This screen is used to back up or restore the Router's configuration file.

To back up the Router's configuration file, click the **Backup** button. Then follow the on-screen instructions.

To restore the Router's configuration file, click the **Browse** button to locate the file, and follow the on-screen instructions. After you have selected the file, click the **Restore** button.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes

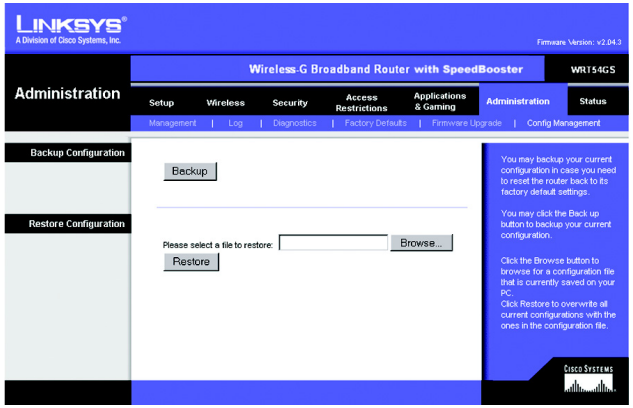

Figure 6-42: Administration Tab - Config Management

The Status Tab - Router

The *Router* screen on the Status Tab displays the Router's current status.

Firmware Version. This is the Router's current firmware.

Current Time. This shows the time, as you set on the Setup Tab.

MAC Address. This is the Router's MAC Address, as seen by your ISP.

Router Name. This is the specific name for the Router, which you set on the Setup Tab.

Host Name. If required by your ISP, this would have been entered on the Setup Tab.

Domain Name. If required by your ISP, this would have been entered on the Setup Tab.

Configuration Type. This shows the information required by your ISP for connection to the Internet. This information was entered on the Setup Tab. You can **Connect** or **Disconnect** your connection here by clicking on that button.

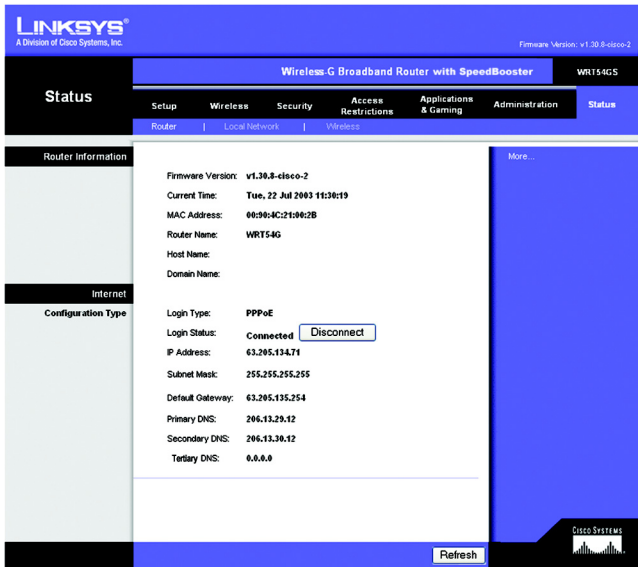

Figure 6-43: Status Tab - Router

***mac address**: the unique address that a manufacturer assigns to each networking device.*

***isp**: your internet provider*

***domain**: a specific name for a network of computers*

The Status Tab - Local Network

The *Local Network* screen on the Status Tab displays the status of your network.

MAC Address. This is the Router's MAC Address, as seen on your local, Ethernet network.

IP Address. This shows the Router's IP Address, as it appears on your local, Ethernet network.

Subnet Mask. When the Router is using a Subnet Mask, it is shown here.

DHCP Server. If you are using the Router as a DHCP server, that will be displayed here.

Start IP Address. For the range of IP Addresses used by devices on your local, Ethernet network, the beginning of that range is shown here.

End IP Address. For the range of IP Addresses used by devices on your local, Ethernet network, the end of that range is shown here.

DHCP Clients Table. Clicking this button will open a screen to show you which PCs are utilizing the Router as a DHCP server. You can delete PCs from that list, and sever their connections, by checking a **Delete** box and clicking the **Delete** button.

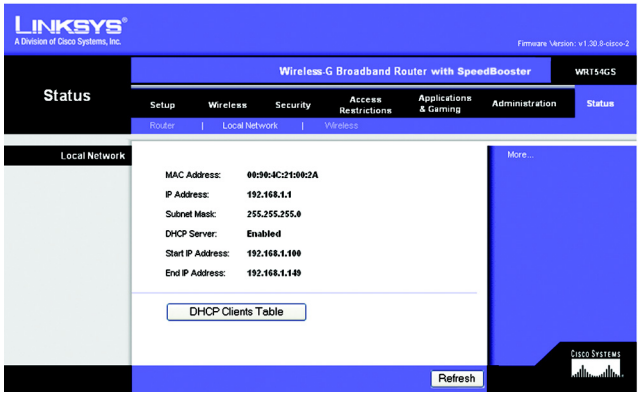

Figure 6-44: Status Tab - Local Network

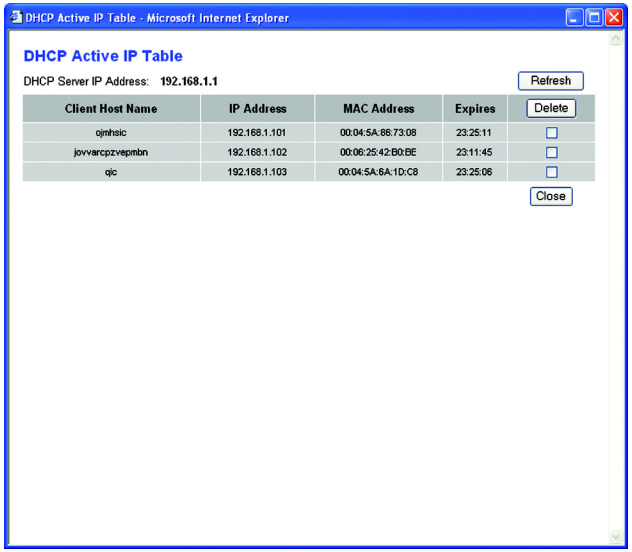

Figure 6-45: DHCP Clients Table

***subnet mask**: an address code that determines the size of the network*