Router's ability to catch all Wireless-G transmissions but will severely decrease performance. If you do not want to use CTS Protection Mode at all, select **Disabled**.

Frame Burst Mode. Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. If you are not sure how to use this option, keep the default, **Enabled**.

Beacon Interval. The default value is **100**. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network.

DTIM Interval. This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

Fragmentation Threshold. This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

RTS Threshold. Should you encounter inconsistent data flow, only minor reduction of the default value, **2347**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of **2347**.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

The Security Tab - Firewall

The *Firewall* screen offers the Block Anonymous Internet Requests feature. The use of this feature enhances the security of your network.

Firewall

Block Anonymous Requests. When enabled, this feature keeps your network from being "pinged," or detected, by other Internet users. It also reinforces your network security by hiding your network ports. Both functions of this feature make it more difficult for outside users to work their way into your network. This feature is enabled by default. Select **Disabled** to allow anonymous Internet requests.

Change this setting as described here and click the **Save Settings** button to apply your change or **Cancel Changes** to cancel your change. Help information is shown on the right-hand side of the screen.

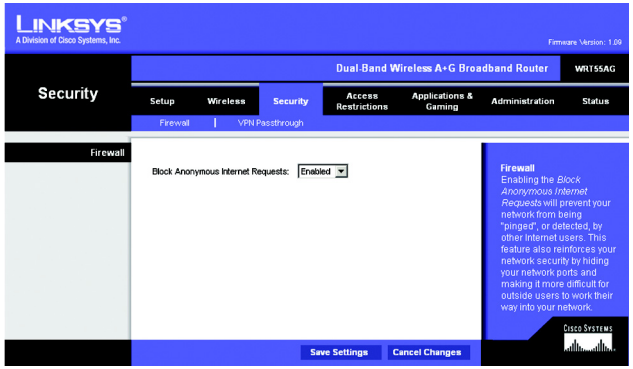

Figure 5-16: Security Tab - Firewall

The Security Tab - VPN Passthrough

Use the settings on this tab to allow VPN tunnels using IPSec, L2TP, or PPTP protocols to pass through the Router's firewall.

VPN Passthrough

IPSec Passthrough. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Pass-Through is enabled by default. To disable IPSec Passthrough, select **Disabled**.

L2TP Passthrough. Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Pass-Through is enabled by default. To disable L2TP Passthrough, select **Disabled**.

PPTP Passthrough. Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Pass-Through is enabled by default. To disable PPTP Passthrough, select **Disabled**.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

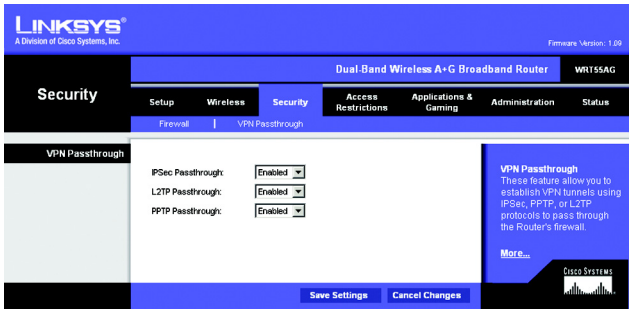

Figure 5-17: Security Tab - VPN Passthrough

***vpn**: a security measure to protect data as it leaves one network and goes to another over the Internet.*

***ipsec**: a VPN protocol used to implement secure exchange of packets at the IP layer.*

***pptp**: a VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.*

The Access Restrictions Tab - Internet Access Policy

The *Internet Access Policy* screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated applications, websites, and inbound traffic during specific days and times.

Internet Access Policy

Access Policy. Access can be managed by a policy. Use the settings on this screen to establish an access policy (after the **Save Settings** button is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click the **Delete This Policy** button. To view all the policies, click the **Summary** button.

On the *Summary* screen, the policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled). You can change the type of access, days, and times of a policy. To activate a policy, click the **Enabled** checkbox. To delete a policy, click its **Delete** button. Click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to cancel your changes. To return to the Internet Access Policy tab, click the **Close** button. To view the list of PCs for a specific policy, click the **Edit List** button.

On the *List of PCs* screen, you can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Click the **Close** button to exit this screen.

To create an Internet Access policy:

1. Select a number from the *Access Policy* drop-down menu.
2. Enter a Policy Name in the field provided.
3. To enable this policy, select **Enabled** from the *Status* drop-down menu.

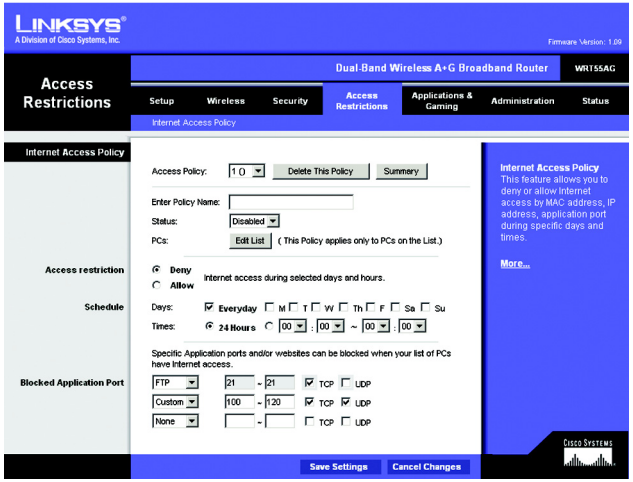

Figure 5-18: Access Restrictions Tab - Internet Access Policy

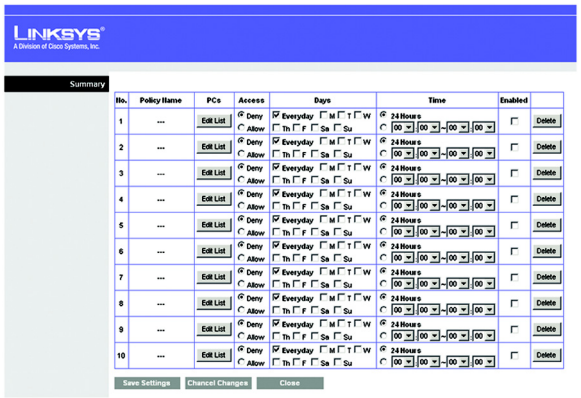

Figure 5-19: Summary

4. Click the **Edit List** button to select which PCs will be affected by the policy. The *List of PCs* screen will appear. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Then click the **Close** button.

5. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.

6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.

7. You can filter access to various applications accessed over the Internet, such as FTP or telnet, by selecting up to three applications from the drop-down menus next to *Blocked Application Port*.

   Each drop-down menu offers a choice of ten preset applications (select **None** if you do not want to use any of the applications). For the preset applications you select, the appropriate range of ports will automatically be displayed.

   If the application you want to block is not listed or you want to edit an application's settings, then select **Custom** from the drop-down menu. Enter the port range you want to block. Then select its protocol(s), **TCP** and/or **UDP**.

8. Click the **Save Settings** button to save the policy's settings. To cancel the policy's settings, click the **Cancel Changes** button.

Help information is shown on the right-hand side of the screen. For additional information, click **More**.

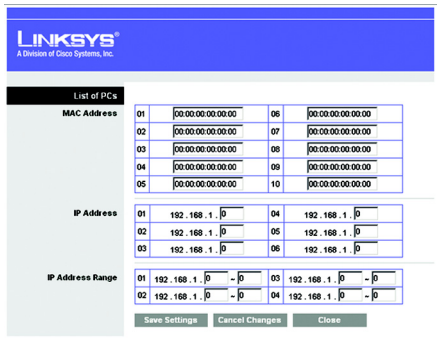

Figure 5-20: List of PCs

***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.*

The Applications and Gaming Tab - Port Range Forwarding

The *Port Range Forwarding* screen 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.)

Before using forwarding, you should assign static IP addresses to the designated PCs.

Port Range Forwarding

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

Application Name. Each drop-down menu offers a choice of ten preset applications (select **None** if you do not want to use any of the preset applications). Select up to five preset applications. For custom applications, enter the name of your application in one of the available fields.

The preset applications are among the most widely used Internet applications. They include the following:

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.

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.

DNS (Domain Name System). The way that Internet domain names are located and translated into IP addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

TFTP (Trivial File Transfer Protocol). A version of the TCP/IP FTP protocol that has no directory or password capability.

Finger. A UNIX command widely used on the Internet to find out information about a particular user, such as a telephone number, whether the user is currently logged on, and the last time the user was logged on. The person being "fingered" must have placed his or her profile on the system in order for the information to be available. Fingering requires entering the full user@domain address.

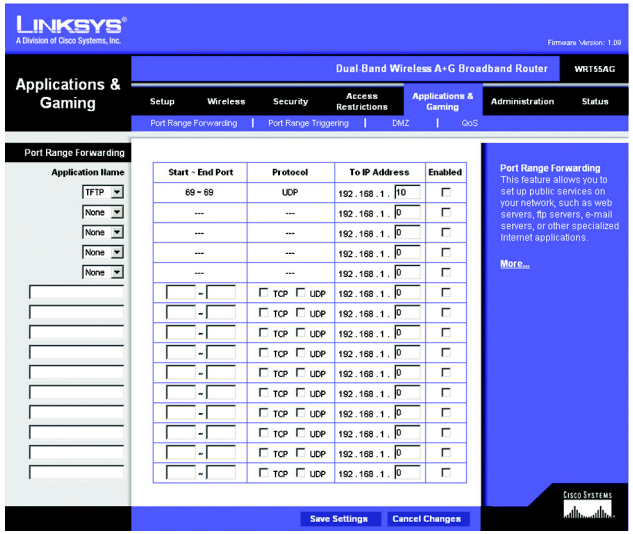

Figure 5-21: Applications and Gaming Tab - Port Range Forwarding

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.

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.

NNTP (Network News Transfer Protocol). The protocol used to connect to Usenet groups on the Internet. Usenet newsreaders support the NNTP protocol.

SNMP (Simple Network Management Protocol). A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).

Start/End. This is the port range. Enter the port number or range of external ports used by the server or Internet application. Check with the software documentation of the Internet application for more information.

Protocol. Select the protocol(s) used for this application, **TCP** and/or **UDP**.

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

Enabled. Click the **Enabled** 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. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

The Applications & Gaming Tab - Port Range Triggering

The *Port Range 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 5-22: Applications and Gaming Tab - Port Triggering

Port Range Triggering

Application Name. 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. In the first field, enter the starting port number of the Triggered Range. In the second field, 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. In the first field, enter the starting port number of the Forwarded Range. In the second field, enter the ending port number of the Forwarded Range.

Enabled. Click the **Enabled** checkbox to enable port range triggering 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. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

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 Forwarding 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.

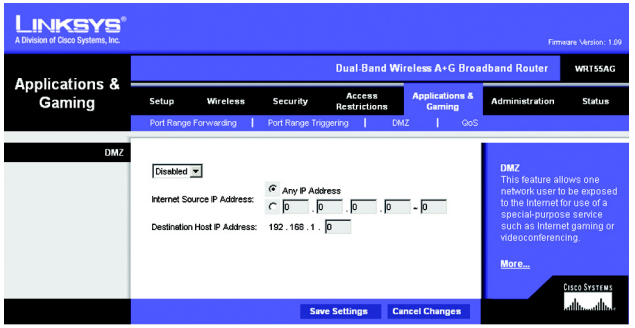

Figure 5-23: Applications and Gaming Tab - DMZ

DMZ

To expose one PC, select **Enabled**.

Internet Source IP Address. If you want to allow any Internet IP address to access the exposed computer, select **Any IP Address**. If you want to allow a specific IP address or range of IP addresses to access the exposed computer, select the second option and enter the IP address or range of IP addresses in the fields provided.

Destination Host IP Address. Enter the IP address of the computer you want to expose.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

The Applications and Gaming Tab - QoS

QoS (Quality of Service) manages information as it is transmitted and received. It ensures better service to high-priority types of Internet traffic, which may involve demanding, real-time applications, such as videoconferencing. QoS can also prioritize traffic for a specific device or the Router's LAN ports.

Qos (Quality of Service)

There are three types of QoS available, Application Port Priority, MAC Address Priority, and LAN Port Priority.

Application Port Priority

Depending on the settings of the *QoS* screen, this feature will assign information a specific priority for up to five preset applications and up to five additional applications that you specify.

Application Name. Each drop-down menu offers a choice of ten preset applications (select **None** if you do not want to use any of the preset applications). Select up to five preset applications. For custom applications, enter the name of your application in one of the available fields.

The preset applications are among the most widely used Internet applications. They include the following:

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.

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.

DNS (Domain Name System). The way that Internet domain names are located and translated into IP addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

TFTP (Trivial File Transfer Protocol). A version of the TCP/IP FTP protocol that has no directory or password capability.

Finger. A UNIX command widely used on the Internet to find out information about a particular user, such as a telephone number, whether the user is currently logged on, and the last time the user was logged on. The person being "fingered" must have placed his or her profile on the system in order for the information to be available. Fingering requires entering the full user@domain address.

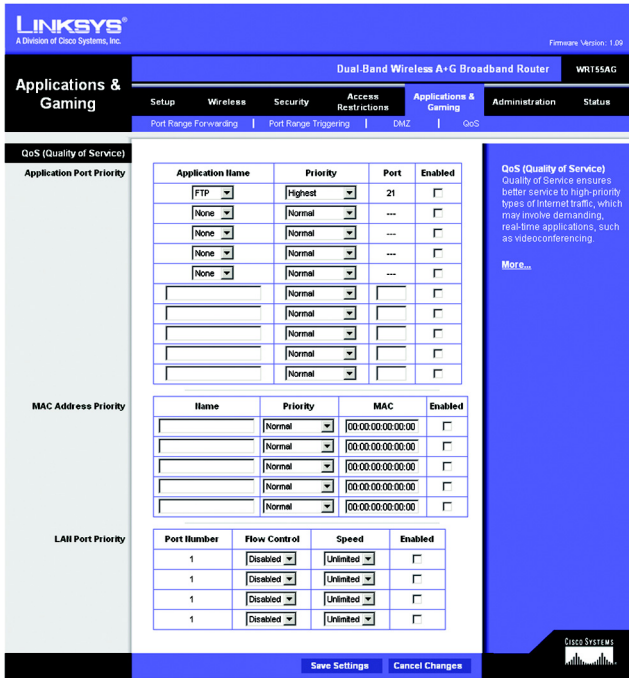

Figure 5-24: Applications and Gaming Tab - QOS

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.

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.

NNTP (Network News Transfer Protocol). The protocol used to connect to Usenet groups on the Internet. Usenet newsreaders support the NNTP protocol.

SNMP (Simple Network Management Protocol). A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).

Priority. Select one of these priority levels: **Highest**, **High**, **Above Normal**, or **Normal**.

Port. For preset applications, the port number is automatically displayed. For custom applications, enter the appropriate port number in the *Port* field.

Enabled. Click the **Enabled** checkbox to enable QoS for the relevant application.

MAC Address Priority

Depending on the settings of the *QoS* screen, this feature will assign a specific priority for up to five network devices.

Name. Enter the name of your network device.

Priority. Select one of these priority levels: **Highest**, **High**, **Above Normal**, or **Normal**.

MAC. Enter the MAC address of the device.

Enabled. Click the **Enabled** checkbox to enable QoS for the appropriate MAC address.

LAN Port Priority

QoS allows you to prioritize performance for the Router's LAN Ports (1-4). It does not require support from your ISP because the prioritized ports are LAN ports going out to your network.

Port Number. The Router's LAN port numbers are automatically displayed here.

Flow Control. For each port, if you want the Router to control the transmission of data between network devices, select **Enabled**. To disable this feature, select **Disabled**.

Speed. This setting limits the speed possible for each port. To use this feature, select **50M**, **20M**, **10M**, **5M**, **2M**, **1M**, **512k**, or **256k** (M stands for Mbps, while k stands for kbps). If you do not want to use this feature, keep the default, **Unlimited**.

Enabled. Click the **Enabled** checkbox to enable QoS for the appropriate LAN port.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

The Administration Tab - Management

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

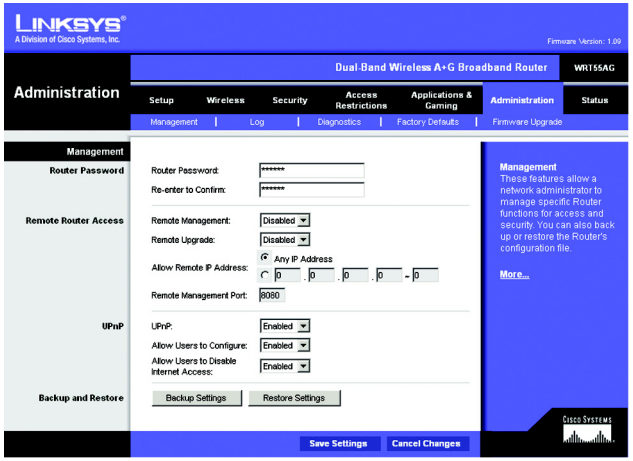

Figure 5-25: Administration Tab - Management

Management

Router Password

Router Password and Re-enter to Confirm. 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.

Remote Router Access

Remote Management. To access the Router remotely, from outside the local network, select **Enabled**. Otherwise, keep the default setting, **Disabled**.

Remote Upgrade. If you want to be able to upgrade the Router remotely, from outside the local network, select **Enabled**. (You must have the Remote Management feature enabled as well.) Otherwise, keep the default setting, **Disabled**.

Allow Remote IP Address. If you want to be able to access the Router from any external IP address, select **Any IP Address**. If you want to specify an external IP address or range of IP addresses, then select the second option and complete the fields provided.

Remote Management Port. Enter the port number that will be open to outside access.

Note: When you are in a remote location and wish to manage the Router, enter *http://<Internet IP Address>: port*. Enter the Router's specific Internet IP address in place of *<Internet IP Address>*, and enter the Administration Port number in place of the word *port*.

UPnP

Universal Plug and Play (UPnP) allows Windows Me and XP to automatically configure the Router for various Internet applications, such as gaming and videoconferencing.

UPnP. If you want to use UPnP, keep the default setting, **Enabled**. Otherwise, select **Disabled**.

Allow Users to Configure. Keep the default setting, **Enabled**, if you want to be able to make manual changes to the Router while using the UPnP feature. Otherwise, select **Disabled**.

Allow Users to Disable Internet Access. Keep the default setting, **Enabled**, if you want to be able to prohibit any and all Internet connections. Otherwise, select **Disabled**.

Backup and Restore

Backup Settings. To back up the Router's configuration, click this button and follow the on-screen instructions.

Restore Settings. To restore the Router's configuration, click this button and follow the on-screen instructions. (You must have previously backed up the Router's configuration.)

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

The Administration Tab - Log

The Router can keep logs of all traffic for your Internet connection.

Log

To disable the Log function, keep the default setting, **Disabled**. To monitor traffic between the network and the Internet, select **Enabled**.

Logviewer IP Address. For a permanent record of the Router's activity logs, Logviewer software must be used. This software can be downloaded from the Linksys website, *www.linksys.com*. The Log viewer saves all incoming and outgoing activity in a permanent file on your PC's hard drive. In the *Logviewer IP Address* field, enter the fixed IP address of the PC running the Log viewer software. The Router will now send updated logs to that PC.

View Log. When you wish to view the logs, click **View Log**. A new screen will appear. Select **Incoming Log** or **Outgoing Log** from the *Type* drop-down menu. The Incoming Log will display a temporary log of the Source IP Addresses and Destination Port Numbers for the incoming Internet traffic. Click the **Save the Log** button to save this information to a file on your PC's hard drive. Click the **Refresh** button to update the log. Click the **Clear** button to clear all the information that is displayed.

The Outgoing Log will display a temporary log of the LAN IP Addresses, Destination URLs or IP Addresses, and Service or Port Numbers for the outgoing Internet traffic. Click the **Save the Log** button to save this information to a file on your PC's hard drive. Click the **Refresh** button to update the log. Click the **Clear** button to clear all the information that is displayed.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

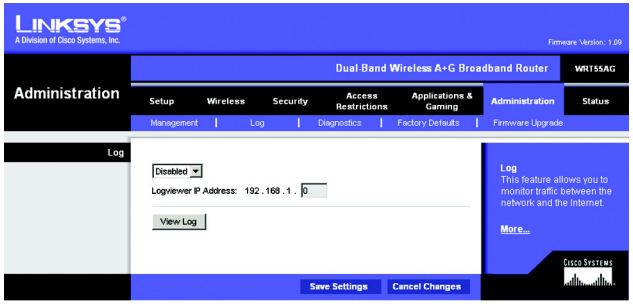

Figure 5-26: Administration Tab - Log

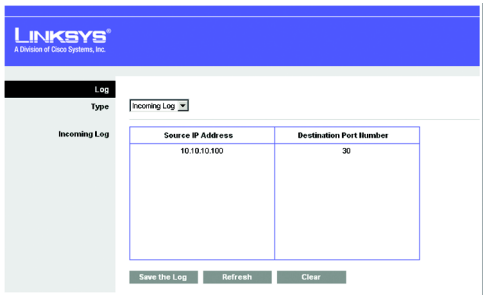

Figure 5-27: Incoming Log

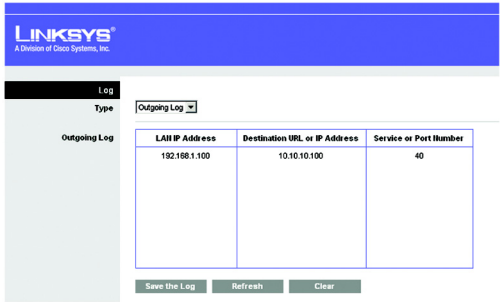

Figure 5-28: Outgoing Log

The Administration Tab - Diagnostics

The Ping test allows you to check the status of your Internet connection.

Diagnostics

Ping Test

To IP or URL Address. Enter the IP address or URL that you want to ping.

Packet Size. Enter the size of the packet you want to use.

Times to Ping. Select the number of times you wish to ping: **5**, **10**, **15**, or **Unlimited**.

Start to Ping. Click this button to begin the test. A new screen will appear and display the test results. 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. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

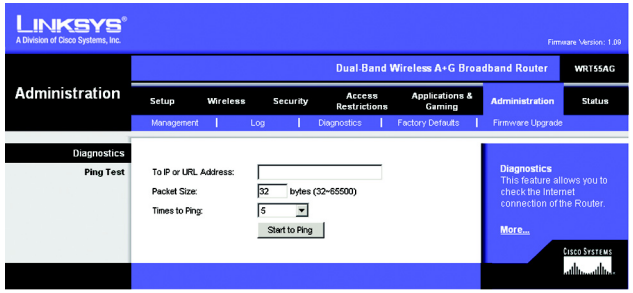

Figure 5-29: Administration Tab - Diagnostics

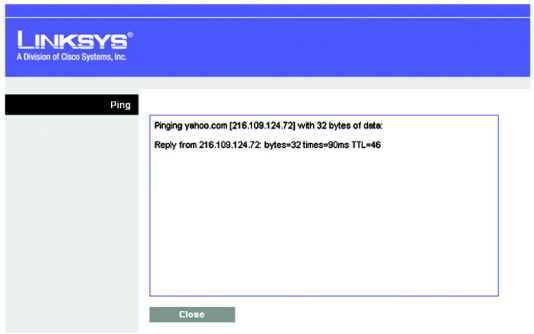

Figure 5-30: Ping

The Administration Tab - Factory Defaults

This screen allows you to restore the Router's configuration to its factory default settings.

Note: Do not restore the factory defaults unless you are having difficulties with the Router and have exhausted all other troubleshooting measures. Once the Router is reset, you will have to re-enter all of your configuration settings.

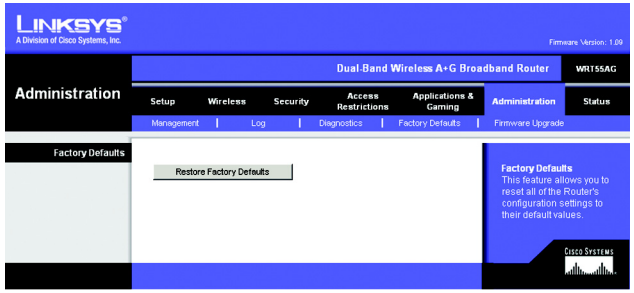

Figure 5-31: Administration Tab - Factory Defaults

Factory Defaults

Restore Factory Defaults. Click this button to reset all configuration settings to their default values. Any settings you have saved will be lost when the default settings are restored.

Help information is shown on the right-hand side of the screen.

The Administration Tab - Firmware Upgrade

This screen allows you to upgrade the Router's firmware. Do not upgrade the firmware unless you are experiencing problems with the Router or the new firmware has a feature you want to use.

Note: The Router will lose all of the settings you have customized. Before you upgrade its firmware, write down all of your custom settings. After you upgrade its firmware, you will have to re-enter all of your configuration settings.

Figure 5-32: Administration Tab - Firmware Upgrade

Firmware Upgrade

Before upgrading the firmware, download the Router's firmware upgrade file from the Linksys website, *www.linksys.com*. Then extract the file.

Please select a file to upgrade. In the field provided, enter the name of the extracted firmware upgrade file, or click the **Browse** button to find this file.

Start to Upgrade. After you have selected the appropriate file, click this button, and follow the on-screen instructions.

Help information is shown on the right-hand side of the screen.

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

***download**: to receive a file transmitted over a network.*

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

The Status Tab - Router

The *Router* screen on the Status Tab displays information about the Router and its current settings. The on-screen information will vary depending on the Internet Connection Type you use.

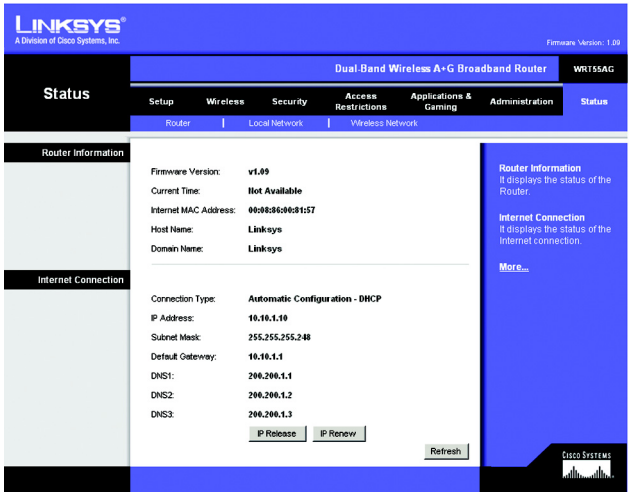

Figure 5-33: Status Tab - Router

Router Information

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

Current Time. This shows the time, based on the time zone you selected on the Setup Tab.

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

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.

Internet Connection

Connection Type. This indicates the type of Internet connection you are using.

Login Status. The status of the connection is displayed only for a PPPoE connection. For this dial-up style connection, click the **Connect** button to click if there is no connection and you want to establish an Internet connection. When your PPPoE connection is active, you can click the **Disconnect** button to end the connection.

IP Address. The Router's Internet IP Address is displayed here.

Subnet Mask and Default Gateway. The Router's Subnet Mask and Default Gateway address are displayed here for DHCP and static IP connections.

DNS1-3. Shown here are the DNS (Domain Name System) IP addresses currently used by the Router.

IP Release. Available for a DHCP connection, click this button to release the current IP address of the device connected to the Router's Internet port.

IP Renew. Available for a DHCP connection, click this button to replace the current IP address—of the device connected to the Router's Internet port—with a new IP address.

Click the **Refresh** button to update the on-screen information. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

The Status Tab - Local Network

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

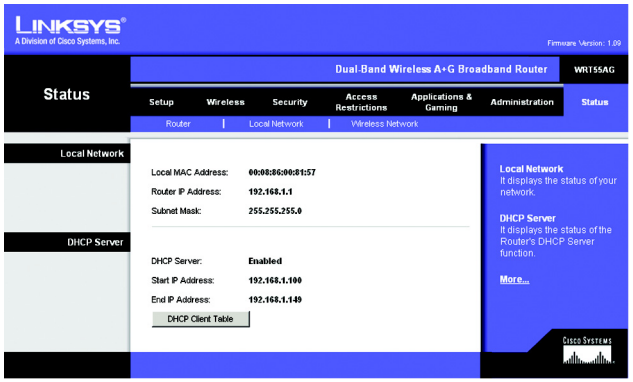

Figure 5-34: Status Tab - Local Network

Local Network

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

Router 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

DHCP Server. The status of the Router's use as a DHCP server is 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 Client Table. Clicking this button will open a screen showing you which PCs are utilizing the Router as a DHCP server. On the *DHCP Client Table* screen, you will see a list of DHCP clients (PCs and other network devices) with the following information: Client Names, Interfaces, IP Addresses, MAC Addresses, and the length of time before their assigned IP addresses expire. From the *To Sort by* drop-down menu, you can sort the table by Client Name, Interface, IP Address, or MAC Address. To remove a DHCP client from this list and sever its network connection, click its **Delete** button. To view the most up-to-date information, click the **Refresh** button. To exit this screen, click the **Close** button.

Help information is shown on the right-hand side of the screen. For additional information, click **More**.

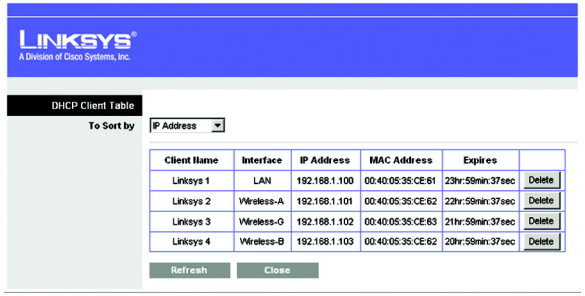

Figure 5-35: DHCP Client Table

The Status Tab - Wireless

The *Wireless* screen on the Status Tab displays the status of your Wireless-A and/or Wireless-G networks.

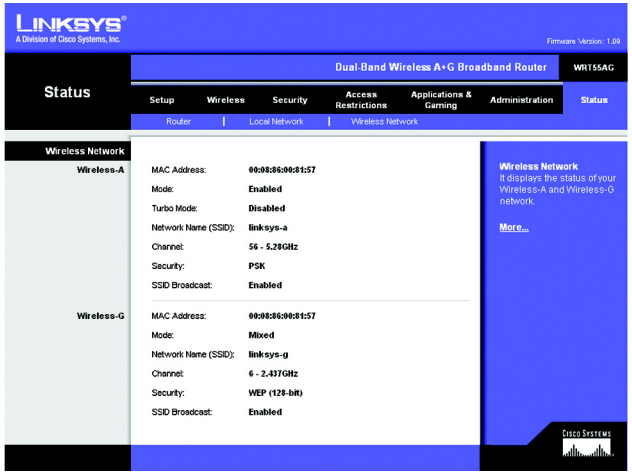

Figure 5-36: Status Tab - Wireless

Wireless Network

Wireless-A

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

Mode. As selected from the Wireless tab, this displays the status of the Router's Wireless-A networking mode.

Turbo Mode. As selected from the Wireless tab, this displays the status of the Router's Wireless-A Turbo Mode.

Network Name (SSID). As entered on the Wireless tab, this displays the wireless network name or SSID of your Wireless-A network.

Channel. As entered on the Wireless tab, this displays the channel on which your wireless network is broadcasting.

Security. As selected on the Wireless Security tab, this displays the wireless security method used by the Router.

SSID Broadcast. As selected on the Wireless tab, this displays the status of the Router's SSID Broadcast feature.

Wireless-G

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

Mode. As selected from the Wireless tab, this displays the status of the Router's Wireless-G networking mode.

Network Name (SSID). As entered on the Wireless tab, this displays the wireless network name or SSID of your Wireless-G network.

Channel. As entered on the Wireless tab, this displays the channel on which your wireless network is broadcasting.

Security. As selected on the Wireless Security tab, this displays the wireless security method used by the Router.

SSID Broadcast. As selected on the Wireless tab, this displays the status of the Router's SSID Broadcast feature.

Help information is shown on the right-hand side of the screen. For additional information, click **More**.

Appendix A: Troubleshooting

This appendix consists of two parts: "Common Problems and Solutions" and "Frequently Asked Questions." Provided are possible solutions to problems that may occur during the installation and operation of the Router. Read the descriptions below to help you solve your problems. If you can't find an answer here, check the Linksys website at *www.linksys.com*.

Common Problems and Solutions

1. ***I'm trying to access the Router's Web-based Utility, but I do not see the login screen. Instead, I see a screen saying, "404 Forbidden."***
   If you are using Windows Explorer, perform the following steps until you see the Web-based Utility's login screen (Netscape Navigator will require similar steps):
   1. Click **File**. Make sure *Work Offline* is NOT checked.
   2. Press **CTRL + F5**. This is a hard refresh, which will force Windows Explorer to load new webpages, not cached ones.
   3. Click **Tools**. Click **Internet Options**. Click the **Security** tab. Click the **Default level** button. Make sure the security level is Medium or lower. Then click the **OK** button.

2. ***I need to set a static IP address on a PC.***
   You can assign a static IP address to a PC by performing the following steps:
   - For Windows 98SE and Me:
     1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.
     2. In The following network components are installed box, select the TCP/IP-> associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the **Properties** button.
     3. In the TCP/IP properties window, select the **IP address** tab, and select **Specify an IP address**. Enter a unique IP address that is not used by any other computer on the network connected to the Router. Make sure that each IP address is unique for each PC or network device.
     4. Click the **Gateway** tab, and in the New Gateway prompt, enter **192.168.1.1**, which is the default IP address of the Router. Click the **Add** button to accept the entry.
     5. Click the **DNS** tab, and make sure the DNS Enabled option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
     6. Click the **OK** button in the TCP/IP properties window, and click **Close** or the **OK** button for the Network window.
     7. Restart the computer when asked.

- For Windows 2000:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
  2. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the **Properties** option.
  3. In the Components checked are used by this connection box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Select **Use the following IP address** option.
  4. Enter a unique IP address that is not used by any other computer on the network connected to the Router.
  5. Enter the Subnet Mask, **255.255.255.0**.
  6. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
  7. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
  8. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window, and click the **OK** button in the Local Area Connection Properties window.
  9. Restart the computer if asked.
- For Windows XP:

  The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.
  1. Click **Start** and **Control Panel**.
  2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
  3. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
  4. In the This connection uses the following items box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
  5. Enter a unique IP address that is not used by any other computer on the network connected to the Router.
  6. Enter the Subnet Mask, **255.255.255.0**.
  7. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
  8. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
  9. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window. Click the **OK** button in the Local Area Connection Properties window.

3. I want to test my Internet connection.

A Check your TCP/IP settings.

For Windows 98SE, Me, 2000, and XP:

- Make sure Obtain IP address automatically is selected in the settings. Refer to Windows Help for details.

B Open a command prompt.

For Windows 98SE and Me:

- Click **Start** and **Run**. In the Open field, type **command**. Press the **Enter** key or click the **OK** button.

For Windows 2000 and XP:

- Click **Start** and **Run**. In the Open field, type **cmd**. Press the **Enter** key or click the **OK** button. In the command prompt, type **ping 192.168.1.1** and press the **Enter** key.
- If you get a reply, the computer is communicating with the Router.
- If you do NOT get a reply, please check the cable, and make sure Obtain an IP address automatically is selected in the TCP/IP settings for your Ethernet adapter.

C In the command prompt, type **ping** followed by your Internet or WAN IP address and press the **Enter** key. The Internet or WAN IP Address can be found on the Status screen of the Router's web-based utility. For example, if your Internet or WAN IP address is 1.2.3.4, you would enter **ping 1.2.3.4** and press the **Enter** key.

- If you get a reply, the computer is connected to the Router.
- If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

D In the command prompt, type **ping www.yahoo.com** and press the **Enter** key.

- If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
- If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

4. I am not getting an IP address on the Internet with my Internet connection.

- Refer to "Problem #2, I want to test my Internet connection" to verify that you have connectivity.
- If you need to register the MAC address of your Ethernet adapter with your ISP, please see "Appendix E: Finding the MAC address and IP Address for Your Ethernet Adapter." If you need to clone the MAC address of your Ethernet adapter onto the Router, see the System section of "Chapter 5: Configuring the Dual-Band Wireless A+G Broadband Router" for details.
- Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of "Chapter 5: Configuring the Dual-Band Wireless A+G Broadband Router" for details on Internet connection settings.
- Make sure you have the right cable. Check to see if the Internet column has a solidly lit LED.
- Make sure the cable connecting from your cable or DSL modem is connected to the Router's Internet port. Verify that the Status page of the Router's web-based utility shows a valid IP address from your ISP.
- Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the Status tab of the Router's web-based utility to see if you get an IP address.

5. I am not able to access the Setup page of the Router's web-based utility.

- Refer to "Problem #2, I want to test my Internet connection" to verify that your computer is properly connected to the Router.
- Refer to "Appendix E: Finding the MAC Address and IP address for Your Ethernet Adapter" to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
- Set a static IP address on your system; refer to "Problem #1: I need to set a static IP address."
- Refer to "Problem #10: I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users)."

6. I need to set up a server behind my Router and make it available to the public.

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed.

Follow these steps to set up port forwarding through the Router's web-based utility. We will be setting up web, ftp, and mail servers.

1. Access the Router's web-based utility by going to http://192.168.1.1 or the IP address of the Router. Go to the Applications & Gaming => Port Range Forwarding tab.
2. Enter any name you want to use for the custom Application.
3. Enter the External Port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
4. Check the protocol you will be using, TCP and/or UDP.
5. Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
6. Check the **Enabled** option for the port services you want to use. Consider the example below:

Application	Start ~ End Port	Protocol	IP Address	Enabled
Web server	80 to 80	Both	192.168.1.100	X
FTP server	21 to 21	TCP	192.168.1.101	X
SMTP (outgoing)	25 to 25	Both	192.168.1.102	X
POP3 (incoming)	110 to 110	Both	192.168.1.102	X

When you have completed the configuration, click the **Save Settings** button.

7. I need to set up online game hosting or use other Internet applications.

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Router to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

1. Access the Router's web interface by going to http://192.168.1.1 or the IP address of the Router. Go to the Applications & Gaming => Port Range Forwarding tab.
2. Enter any name you want to use for the custom Application.
3. Enter the External Port range of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
4. Check the protocol you will be using, TCP and/or UDP.
5. Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
6. Check the **Enabled** option for the port services you want to use. Consider the example below:

Application	Start ~ End Port	Protocol	IP Address	Enabled
UT	7777 to 27900	Both	192.168.1.100	X
Halflife	27015 to 27015	Both	192.168.1.105	X
PC Anywhere	5631 to 5631	UDP	192.168.1.102	X
VPN IPSEC	500 to 500	UDP	192.168.1.100	X

When you have completed the configuration, click the **Save Settings** button.

8. I can't get the Internet game, server, or application to work.

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one PC to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the Router will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the Router will send the data to whichever PC or network device you set for DMZ hosting.)

Follow these steps to set DMZ hosting:

1. Access the Router's web-based utility by going to http://192.168.1.1 or the IP address of the Router. Go to the Applications & Gaming => Port Range Forwarding tab.
2. Disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
3. Go to the Applications & Gaming => DMZ tab.
4. Select **Enabled** next to DMZ. In the *Host IP Address* field, enter the IP address of the computer you want exposed to the Internet. This will bypass the NAT technology for that computer. Please refer to "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
5. Once completed with the configuration, click the **Save Settings** button.

9. I forgot my password, or the password prompt always appears when I am saving settings to the Router.

Reset the Router to factory default by pressing the Reset button for 10 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

1. Access the Router's web-based utility by going to http://192.168.1.1 or the IP address of the Router. Enter the default password admin, and click the Administrations => Management tab.
2. Enter a different password in the *Router Password* field, and enter the same password in the second field to confirm the password.
3. Click the **Save Settings** button.

10. I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.

If you have proxy settings, you need to disable these on your computer. Because the Router is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

- For Microsoft Internet Explorer 5.0 or higher:
  1. Click **Start, Settings**, and **Control Panel**. Double-click Internet Options.
  2. Click the **Connections** tab.
  3. Click the **LAN settings** button and remove anything that is checked.
  4. Click the **OK** button to go back to the previous screen.
  5. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.
- For Netscape 4.7 or higher:
  1. Start **Netscape Navigator**, and click **Edit**, **Preferences**, **Advanced**, and **Proxies**.
  2. Make sure you have Direct connection to the Internet selected on this screen.
  3. Close all the windows to finish.

11. To start over, I need to set the Router to factory default.

Hold the **Reset** button for 10 seconds and then release it. This will return the password, forwarding, and other settings on the Router to the factory default settings. In other words, the Router will revert to its original factory configuration.

12. I need to upgrade the firmware.

In order to upgrade the firmware with the latest features, you need to go to the Linksys website and download the latest firmware at *www.linksys.com*.

Follow these steps:

1. Go to the Linksys website at *www.linksys.com* and download the latest firmware.
2. To upgrade the firmware, follow the steps in "Appendix C: Upgrading Firmware."

13. The firmware upgrade failed, and/or the Power LED is flashing.

The upgrade could have failed for a number of reasons. Follow these steps to upgrade the firmware and/or make the Power LED stop flashing:

- If the firmware upgrade failed, use the TFTP program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.
- Set a static IP address on the PC; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:
  IP Address: 192.168.1.50
  Subnet Mask: 255.255.255.0
  Gateway: 192.168.1.1
- Perform the upgrade using the TFTP program or the Administration tab of the Router's web-based utility.

14. My DSL service's PPPoE is always disconnecting.

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet.

- There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.
  1. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the Router.
  2. Enter the password, if asked. (The default password is admin.)
  3. On the Setup screen, select the option **Keep Alive**, and set the Redial Period option at 20 (seconds).
  4. Click the **Save Settings** button.
  5. Click the **Status** tab, and click the **Connect** button.
  6. You may see the login status display as Connecting. Press the F5 key to refresh the screen, until you see the login status display as Connected.
- Click the **Save Settings** button to continue.
- If the connection is lost again, follow steps 1- 6 to re-establish connection.

15. I can't access my e-mail, web or I am getting corrupted data from the Internet.

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492.

- If you are having some difficulties, perform the following steps:
  1. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the Router.
  2. Enter the password, if asked. (The default password is admin.)
  3. Look for the MTU option, and select **Manual**. In the Size field, enter 1492.
  4. Click the **Save Settings** button to continue.
- If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:
  1462
  1400
  1362
  1300

16. The Power LED keeps flashing.

The Power LED flashes when the device is first powered up. Meantime, the system will boot up itself and check for proper operation. After finishing the checking procedure, the LED stays solid to show that the system is working fine. If the LED keeps flashing after this time, the device is not working properly. Try to flash the firmware by assigning a static IP address to the computer, and then upgrade the firmware. Try using the following settings, IP Address: 192.168.1.50 and Subnet Mask: 255.255.255.0.

17. When I enter a URL or IP address, I get a time-out error or am prompted to retry.

- Check if other PCs work. If they do, ensure that your workstation's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the PCs are configured correctly, but still not working, check the Router. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)
- If the Router is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Router to verify a direct connection.
- Manually configure the TCP/IP settings with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

Frequently Asked Questions

What is the maximum number of IP addresses that the Router will support?
The Router will support up to 253 IP addresses.

Is IPSec Pass-Through supported by the Router?
Yes, it is a built-in feature that the Router automatically enables.

Where is the Router installed on the network?
In a typical environment, the Router is installed between the cable/DSL modem and the LAN. Plug the Router into the cable/DSL modem's Ethernet port.

Does the Router support IPX or AppleTalk?
No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from the Internet to a LAN.

Does the Internet connection of the Router support 100Mbps Ethernet?
The Router's current hardware design supports up to 100Mbps Ethernet on its Internet port; however, the Internet connection speed will vary depending on the speed of your broadband connection. The Router also supports 100Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Router.

What is Network Address Translation and what is it used for?
Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Router to be used with low cost Internet accounts, such as DSL or cable modems, when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

Does the Router support any operating system other than Windows 98SE, Windows Millennium, Windows 2000, or Windows XP?
Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

Does the Router support ICQ send file?
Yes, with the following fix: click ICQ menu -> preference -> connections tab->, and check I am behind a firewall or proxy. Then set the firewall time-out to 80 seconds in the firewall setting. The Internet user can then send a file to a user behind the Router.

I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?
If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 ~ 27900. If you want to use the UT Server Admin, forward another port. (Port 8080 usually works well but is used for remote admin. You may have to disable this.) Then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Router from your ISP.

Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?
It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

How do I get Half-Life: Team Fortress to work with the Router?
The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. One problem: Version 1.0.1.6 won't let multiple computers with the same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

How can I block corrupted FTP downloads?
If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do?
Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at www.linksys.com for more information.

If all else fails in the installation, what can I do?
Reset the Router by holding down the reset button until the Power LED fully turns on and off. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys website, *www.linksys.com*.

How will I be notified of new Router firmware upgrades?
All Linksys firmware upgrades are posted on the Linksys website at www.linksys.com, where they can be downloaded for free. To upgrade the Router's firmware, use the Administration tab of the Router's web-based utility. If the Router's Internet connection is working well, there is no need to download a newer firmware version,

unless that version contains new features that you would like to use. Downloading a more current version of Router firmware will not enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

Will the Router function in a Macintosh environment?
Yes, but the Router's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.

I am not able to get the web configuration screen for the Router. What can I do?
You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

What is DMZ Hosting?
Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ Hosting. To get the LAN IP address, see "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter."

If DMZ Hosting is used, does the exposed user share the public IP with the Router?
No.

Does the Router pass PPTP packets or actively route PPTP sessions?
The Router allows PPTP packets to pass through.

Is the Router cross-platform compatible?
Any platform that supports Ethernet and TCP/IP is compatible with the Router.

How many ports can be simultaneously forwarded?
Theoretically, the Router can establish 520 sessions at the same time, but you can only forward 10 ranges of ports.

What are the advanced features of the Router?
The Router's advanced features include Advanced Wireless settings, Internet Access Policies, and Port Range Forwarding.