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**.

AP Isolation This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, select **On**. AP Isolation is turned **Off** by default.

SecureEasySetup This feature allows you to enable or disable the SecureEasySetup feature. Select **Disabled** to disable the feature and turn off the button's light. The feature is **Enabled** by default.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Security > Firewall

The *Security* > *Firewall* screen is used to configure a firewall that can filter out various types of unwanted traffic on the Router's local network.

Security > Firewall

Firewall

Firewall Protection To use firewall protection, keep the default selection, **Enable**. To turn off firewall protection, select **Disable**.

Block WAN Requests

Block Anonymous Internet Requests This feature makes it more difficult for outside users to work their way into your network. This feature is selected by default. Deselect the feature to allow anonymous Internet requests.

Filter Multicast Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. This feature is selected by default. Deselect this feature to disable it.

Filter Internet NAT Redirection This feature uses port forwarding to block access to local servers from local networked computers. Select **Filter Internet NAT Redirection** to filter Internet NAT redirection. This feature is not selected by default.

Filter IDENT (Port 113) This feature keeps port 113 from being scanned by devices outside of your local network. This feature is selected by default. Deselect this feature to disable it.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Security > VPN Passthrough

The *Security* > *VPN Passthrough* screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.

Security > VPN Passthrough

VPN Passthrough

IPSec Passthrough Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the Router, keep the default, **Enable**.

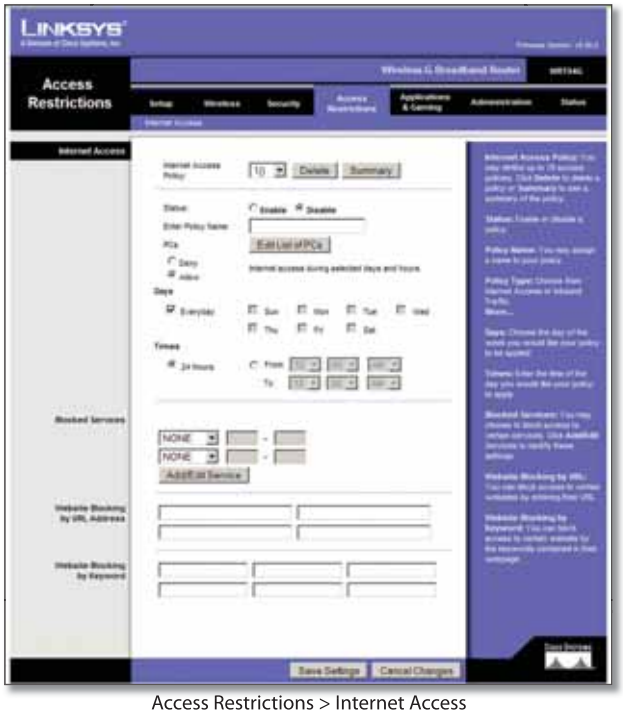
PPTP Passthrough Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, keep the default, **Enable**.

L2TP Passthrough Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, **Enable**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Access Restrictions > Internet Access

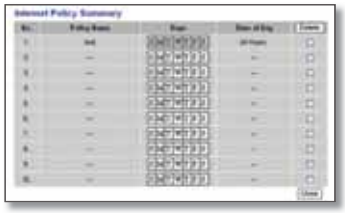
The *Access Restrictions* > *Internet Access* screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites during specific days and times.



Access Restrictions > Internet Access

Internet Access

Internet Access Policy Access can be managed by a policy. Use the settings on this screen to establish an access policy (after **Save Settings** 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 **Delete**. To view all the policies, click **Summary**. (Policies can be deleted from the *Summary* screen by selecting the policy or policies and clicking **Delete**. To return to the Internet Access tab, click **Close**.)



Internet Policy Summary

Status Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and select **Enable**.

To create an Internet Access policy:

1. Select a number from the *Internet Access Policy* drop-down menu.
2. To enable this policy, select **Enable**.
3. Enter a Policy Name in the field provided.
4. Click **Edit List of PCs** to select which PCs will be affected by the policy. The *List of PCs* screen appears. 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 **Save Settings** to apply your changes or **Cancel Changes** to cancel your changes. Then click **Close**.

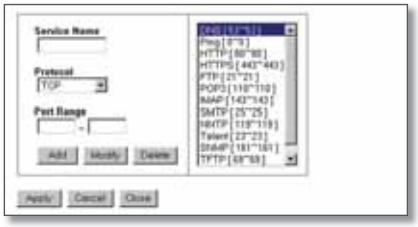
List of PCs

5. Select 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. Select any Blocked Services or Website Blocking you wish to use.
8. Click **Save Settings** to save the policy's settings, or click **Cancel Changes** to cancel the policy's settings.

Blocked Services

You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting services from the drop-down menus next to *Blocked Services*. (You can block up to 20 services.) Then enter the range of ports you want to filter.

If the service you want to block is not listed or you want to edit a service's settings, then click **Add/Edit Service**. Then the *Port Services* screen will appear.



Port Services

To add a service, enter the service's name in the *Service Name* field. Select its protocol from the *Protocol* drop-down menu, and enter its range in the *Port Range* fields. Then click **Add**.

To modify a service, select it from the list on the right. Change its name, protocol setting, or port range. Then click **Modify**.

To delete a service, select it from the list on the right. Then click **Delete**.

When you are finished making changes on the *Port Services* screen, click **Apply** to save the changes. If you want to cancel your changes, click **Cancel**. To close the *Port Services* screen and return to the *Access Restrictions* screen, click **Close**.

Website Blocking by URL Address

If you want to block websites with specific URL addresses, enter each URL in a separate field next to *Website Blocking by URL Address*.

Website Blocking by Keyword

If you want to block websites using specific keywords, enter each keyword in a separate field next to *Website Blocking by Keyword*.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications and Gaming > Port Range Forward

The *Applications & Gaming > Port Range Forward* 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.)

Applications and Gaming > Port Range Forward

Port Range Forward

To forward a port, enter the information on each line for the criteria required.

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 in the Start column and the number that ends the range in the End column.

Protocol Select 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 Select **Enable** to enable port forwarding for the relevant application.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications & Gaming > Port Triggering

The *Applications & Gaming > 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.

Applications and Gaming > 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.

Enable Select **Enable** to enable port triggering for the applicable application.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications and Gaming > DMZ

The DMZ feature allows one network computer 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.

Applications and Gaming > DMZ

DMZ

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. This feature is disabled by default.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications and Gaming > QoS

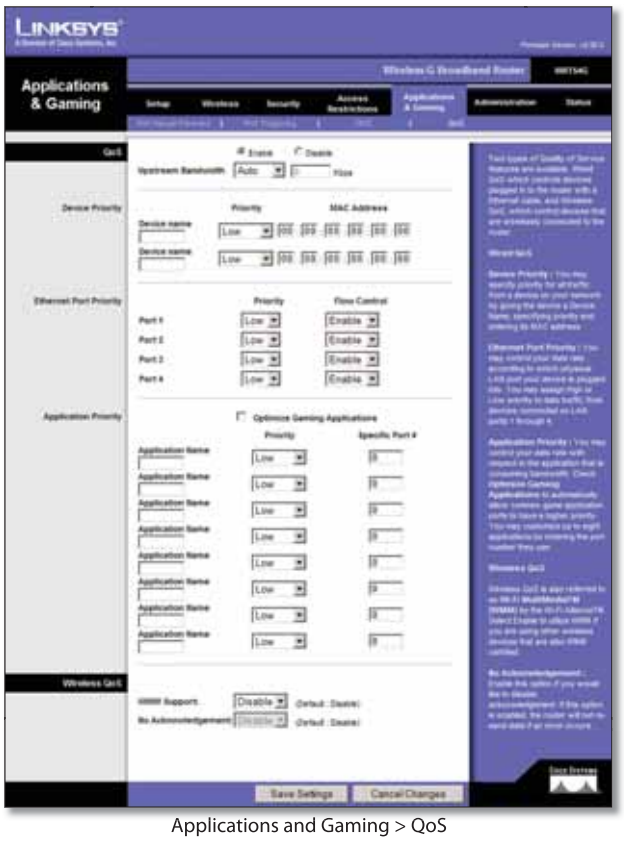
Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing.

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

QoS

Enable/Disable To enable QoS, select **Enable**. Otherwise, select **Disable**. QoS is disabled by default.

Upstream Bandwidth Select **Auto** or **Manual** from the drop-down menu. Manual allows you to specify the maximum outgoing bandwidth that applications can utilize.



Applications and Gaming > QoS

Device Priority

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

Ethernet Port Priority

Ethernet Port Priority QoS allows you to prioritize performance for the Router's four ports, LAN Ports 1-4. For each port, select the priority and flow control setting.

Priority Select **High** or **Low** in the Priority column. The Router's four ports have been assigned low priority by default.

Flow Control If you want the Router to control the transmission of data between network devices, select **Enabled**. To disable this feature, select **Disabled**. Ethernet Port Priority QoS does not require support from your ISP because the prioritized ports LAN ports 1-4 are in your network. This feature is enabled by default.

Application Priority

Application 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 applications that you specify.

Optimize Gaming Applications Select this to automatically allow common game application ports to have a higher priority. These games include, but are not limited to: *Counter-Strike*, *Half-Life*, *Age of Empires*, *Everquest*, *Quake2/Quake3*, and *Diablo II*. The default setting is unselected.

Application Name Enter the name you wish to give the application in the *Application Name* field.

Priority Select **High** or **Low** to assign priority to the application. The default selection is **Low**.

Specific Port # Enter the port number for the application.

Wireless QoS

WMM Support Wi-Fi Multimedia (WMM), formerly known as Wireless Multimedia Extensions (WME), is a Wi-Fi Alliance certified feature, based on the IEEE 802.11e standard. This feature provides QoS to wireless networks. It is especially suitable for voice, music and video applications; for example, Voice over IP (VoIP), video streaming, and interactive gaming. If you have other devices on your wireless network that support WMM, select **Enabled**. Otherwise, keep the default, **Disabled**.

No Acknowledgement This feature prevents the Router from re-sending data if an error occurs. To use this feature, select **Enabled**. Otherwise, keep the default setting, **Disabled**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Administration > Management

The *Administration* > *Management* screen allows the network's administrator to manage specific Router functions for access and security.

Administration > Management

Router Password

Local Router Access

Router Password Enter a new Password for the Router.

Re-enter to confirm Enter the Password again to confirm.

Web Access

Access Server HTTP (HyperText Transport Protocol) is 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.** The default selection is **HTTP**.

Wireless Access Web If you are using the 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. Keep the default, **Enable**, to enable wireless access to the Router's web-based utility, or select **Disable** to disable wireless access to the utility.

Remote Router Access

Remote Management To access the Router remotely, from outside the network, select **Enable**.

Management Port 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.

Use https To require the use of HTTPS for remote access, select this feature.

UPnP

UPnP Keep the default, **Enable** to enable the UPnP feature; otherwise, select **Disable**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Administration > Log

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

Administration > Log

Log

Log 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.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Administration > Diagnostics

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

Administration > Diagnostics

Ping Test

Ping The Ping test checks the status of a connection. Click **Ping** 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 **Ping**. The *Ping Test* screen will show if the test was successful. To stop the test, click **Stop**. Click **Clear Log** to clear the screen. Click **Close** to return to the *Diagnostics* screen.

The Ping Test

Traceroute Test

Traceroute To test the performance of a connection, click **Traceroute** to open the *Traceroute Test* screen. Enter the address of the PC whose connection you wish to test

and click **Traceroute**. The *Traceroute Test* screen will show if the test was successful. To stop the test, click **Stop**. Click **Clear Log** to clear the screen. Click **Close** to return to the *Diagnostics* screen.

The Traceroute Test

Administration > Factory Defaults

The *Administration* > *Factory Defaults* screen allows you to restore the Router's configuration to its factory default settings.

Factory Defaults

Restore Factory Defaults To reset the Router's settings to the default values, select **Yes**, and then click **Save Settings**. Any settings you have saved will be lost when the default settings are restored.

Administration > Factory Defaults

Administration > Upgrade Firmware

The *Administration* > *Upgrade Firmware* 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.

Administration > Upgrade Firmware

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

Upgrade Firmware

Please select a file to upgrade Click **Browse** and select the extracted firmware upgrade file. Then click **Upgrade** and follow the on-screen instructions.

Administration > Config Management

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

Administration > Config Management

Backup Configuration

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

Restore Configuration

Please select a file to restore Click **Browse** and select the configuration file. Then click **Restore**.

Status > Router

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

Status > Router

Router Information

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.

Internet

Configuration Type

This section shows the current network information stored in the Router. The information varies depending on the Internet connection type selected on the *Setup* > *Basic Setup* screen.

Click **Refresh** to update the on-screen information.

Status > Local Network

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

Status > Local Network

Local 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 This shows the current subnet mask being configured for your local network.

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.

DHCP Clients Table

Click **Refresh** to update the on-screen information.