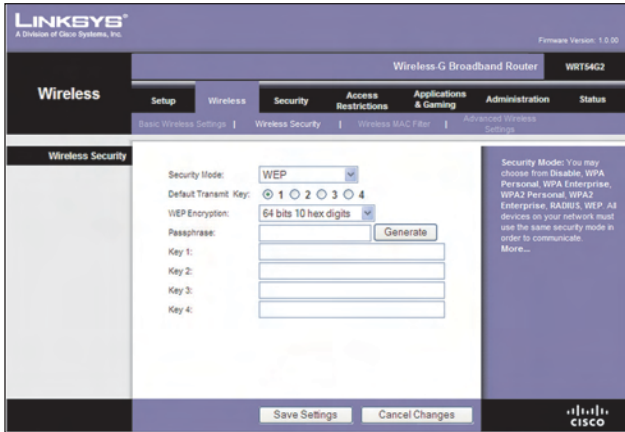


Passphrase Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

Key 1-4 If you did not enter a Passphrase, enter the WEP key(s) manually.

WEP

WEP is a basic encryption method, which is not as secure as WPA.



Security Mode > WEP

Default Transmit Key Select a Default Transmit Key (choose which Key to use). The default is 1.

WEP Encryption Select a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. The default is **64 bits 10 hex digits**.

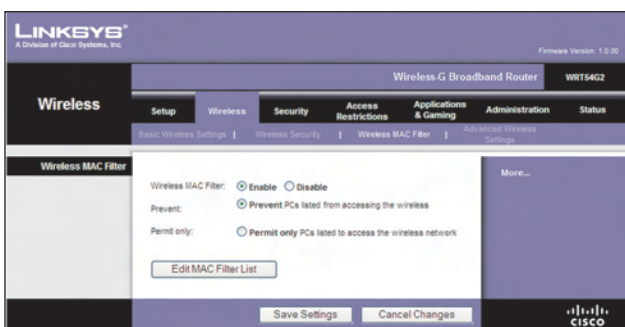
Passphrase Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

Key 1-4 If you did not enter a Passphrase, enter the WEP key(s) manually.

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

Wireless > Wireless MAC Filter

Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.



Wireless > Wireless MAC Filter

Wireless MAC Filter

Wireless MAC Filter To filter wireless users by MAC Address, either permitting or blocking access, click **Enable**. If you do not wish to filter users by MAC Address, keep the default setting, **Disable**.

Prevent Select this to block wireless access by MAC Address. This button is selected by default.

Permit Only Select this to allow wireless access by MAC Address. This button is not selected by default.

Edit MAC Filter List Click this to open the *MAC Address Filter List* screen. On this screen, you can list users, by MAC Address, to whom you wish to provide or block access. For easy reference, click **Wireless Client MAC List** to display a list of network users by MAC Address.



MAC Address Filter List

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

Wireless > Advanced Wireless Settings

This *Wireless > Advanced Wireless Settings* screen is used to set up the Router's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.



Wireless > Advanced Wireless Settings

Advanced Wireless

Authentication Type The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. With **Open System** authentication, the sender and the recipient do NOT use a WEP key for authentication. With **Shared Key** authentication, the sender and recipient use a WEP key for authentication.

Basic Rate The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, when the Router can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when the Router can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.

Transmission Rate The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.

CTS Protection Mode CTS (Clear-To-Send) Protection Mode should remain disabled unless you are having severe problems with your Wireless-G products not being able to transmit to the Router in an environment with heavy 802.11b traffic. This function boosts the Router's ability to catch all Wireless-G transmissions but will severely decrease performance.

Frame Burst Enabling this option should provide your network with greater performance, depending on the

manufacturer of your wireless products. To turn on the Frame Burst option, select **Enable**. The default is **Disable**.

Beacon Interval The default value is **100**. Enter a value between 1 and 65,535 milliseconds. 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, between 1 and 255, 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**.

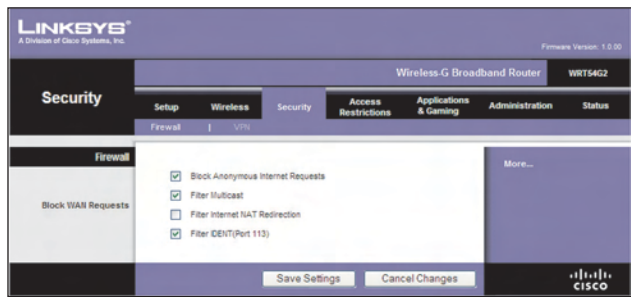
AP Isolation This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, select **On**. AP Isolation is turned **Off** by default.

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.

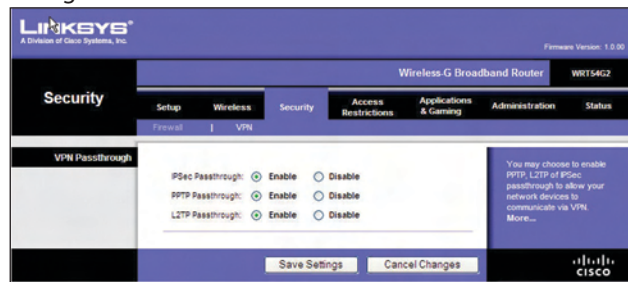
Filter Internet NAT Redirection This feature uses port forwarding to block access to local servers from local networked computers. Select **Filter Internet NAT Redirection** to filter Internet NAT redirection. This feature is not selected by default.

Filter IDENTITY (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**.)

No.	Policy Name	Days	Times of Day	Column
1.	test	[Sun] [Mon] [Tue] [Wed] [Thu] [Fri] [Sat]	24 hours	<input type="checkbox"/>
2.	---	[Sun] [Mon] [Tue] [Wed] [Thu] [Fri] [Sat]	---	<input type="checkbox"/>
3.	---	[Sun] [Mon] [Tue] [Wed] [Thu] [Fri] [Sat]	---	<input type="checkbox"/>
4.	---	[Sun] [Mon] [Tue] [Wed] [Thu] [Fri] [Sat]	---	<input type="checkbox"/>
5.	---	[Sun] [Mon] [Tue] [Wed] [Thu] [Fri] [Sat]	---	<input type="checkbox"/>
6.	---	[Sun] [Mon] [Tue] [Wed] [Thu] [Fri] [Sat]	---	<input type="checkbox"/>
7.	---	[Sun] [Mon] [Tue] [Wed] [Thu] [Fri] [Sat]	---	<input type="checkbox"/>
8.	---	[Sun] [Mon] [Tue] [Wed] [Thu] [Fri] [Sat]	---	<input type="checkbox"/>
9.	---	[Sun] [Mon] [Tue] [Wed] [Thu] [Fri] [Sat]	---	<input type="checkbox"/>
10.	---	[Sun] [Mon] [Tue] [Wed] [Thu] [Fri] [Sat]	---	<input type="checkbox"/>

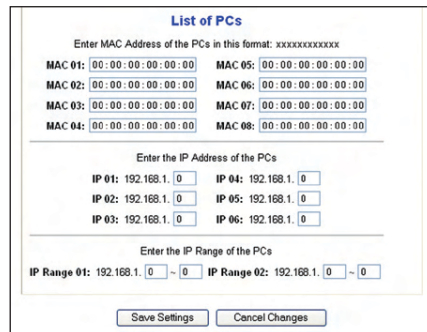
Internet Policy Summary

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**.



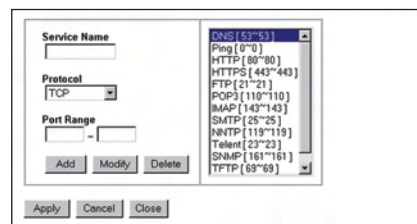
List of PCs

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**.