A Division of Cisco Systems, Inc.

USER GUIDE

Wireless-G Router for Mobile Broadband

Model No: **WRT54G3GV2-ST**

About This Guide

Icon Descriptions

While reading through the User Guide you may see various icons that call attention to specific items. Below is a description of these icons:

✓ **NOTE:** This check mark indicates that there is a note of interest and is something that you should pay special attention to while using the product.

⚠ **WARNING:** This exclamation point indicates that there is a caution or warning and it is something that could damage your property or product.

WEB: This globe icon indicates a noteworthy website address or e-mail address.

Online Resources

Website addresses in this document are listed without **http://** in front of the address because most current web browsers do not require it. If you use an older web browser, you may have to add **http://** in front of the web address.

Resource	Website
Sprint	www.sprint.com
Linksys	www.linksys.com
Linksys International	www.linksys.com/international
Glossary	www.linksys.com/glossary
Network Security	www.linksys.com/security

Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2007 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

Appendix D: Regulatory Information 37

Appendix E: Contact Information 43

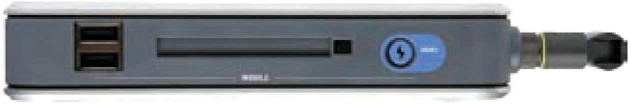
Chapter 1: Product Overview

Thank you for choosing the Linksys Wireless-G Router for Mobile Broadband. The Router lets you access the Internet through either your mobile broadband service (requires a mobile broadband data card or USB adapter, available separately), or your cable or DSL broadband service. This access can be shared via a wireless connection or through one of the Router's four switched ports.

A variety of security features help to protect your data and your privacy while online. Security features include WPA2 (Wi-Fi Protected Access 2) security, a Stateful Packet Inspection (SPI) firewall, and NAT technology. Configuring the Router is easy using the Setup Wizard or provided browser-based utility.

Top Panel

If you have a mobile broadband USB adapter, use the Mobile USB port(s). If you have a mobile broadband data card, use the Mobile slot.

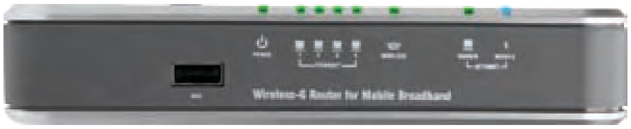


Mobile USB Ports If the Router will connect to a mobile broadband service, insert the mobile broadband USB adapter (available separately) into the USB port(s). For more information, refer to the documentation of the mobile broadband USB adapter.

Mobile Slot If the Router will connect to a mobile broadband service, insert the mobile broadband data card (available separately) into this slot. After the data card is inserted, the eject button will pop up. To remove the data card, press the eject button.

Mobile Connect/Disconnect Button Press this button to connect to and disconnect from the mobile network. (You can also use the *Basic Setup* screen of the Router's web-based utility.)

Side Panel



USB Port Reserved for future use.

Power (Green) The Power LED lights up and stays on while the Router is powered on.

Ethernet 1-4 (Green) These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. It flashes to indicate network activity over that port.

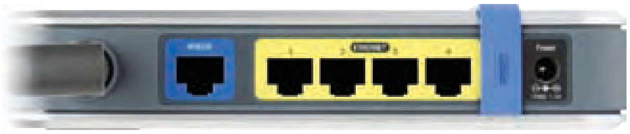
Wireless (Green) The Wireless LED lights up when the wireless feature is enabled. It flashes when the Router is actively sending or receiving data over the wireless network.

Modem Internet (Green) The Modem LED lights up and stays on when there is a connection made through the Modem port. It flashes to indicate network activity over the Modem port.

Mobile Internet (Blue) The Mobile LED flashes as the Router connects to the mobile network. When the LED stops flashing and stays on, then the connection is active.

If the LED flashes quickly, the Router is not connected to the mobile network. Before you press the Mobile Connect/Disconnect button, make sure the mobile broadband data card or USB adapter is already installed.

Opposite Side Panel with Antenna



Modem The Modem port is where you will connect your cable or DSL modem.

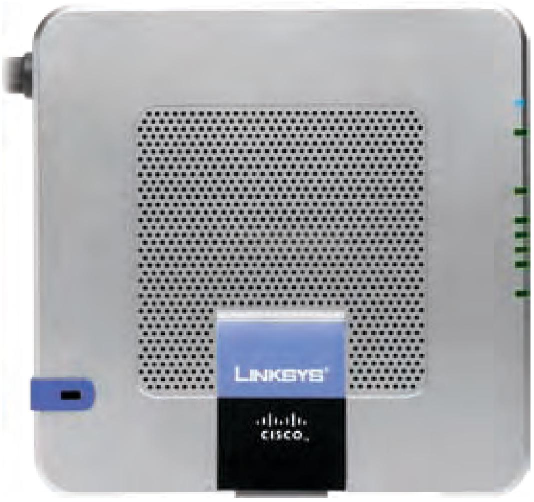
Ethernet 1, 2, 3, 4 These Ethernet ports (1, 2, 3, 4) connect the Router to wired computers and other Ethernet network devices.

Security Bracket The security bracket labeled "Reset" clips onto the Router. It covers the Reset button and the security slot on the Router's top panel. You can remove the security bracket to access the Reset button.

Reset There are two ways to reset the Router's factory defaults. Either press and hold the Reset button for approximately five seconds, or restore the defaults from the *Administration > Factory Defaults* screen of the Router's web-based utility.

Power The Power port is where you will connect the power adapter.

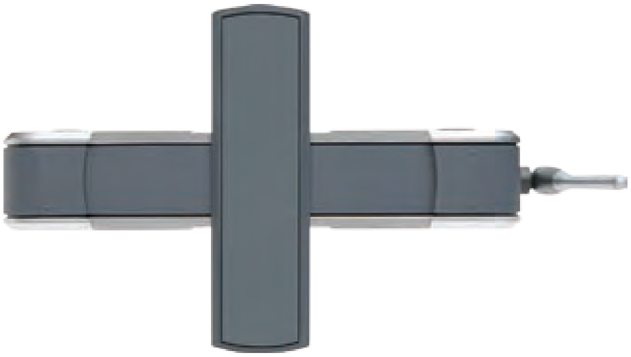
Front Panel



Security Slot To protect the Router from theft, you can attach a lock to the Router using the security slot.

Bottom Panel

To place the Router in a vertical position, rotate the stand 90 degrees.



Placement Positions

There are three ways to physically install the Router. The first way is to place the Router horizontally on a surface. The second way is to stand the Router vertically on a surface. The third way is to mount the Router on a wall.

Horizontal Placement

The Router has four rubber feet on its bottom panel. Place the Router on a level surface near an electrical outlet.

Vertical Placement

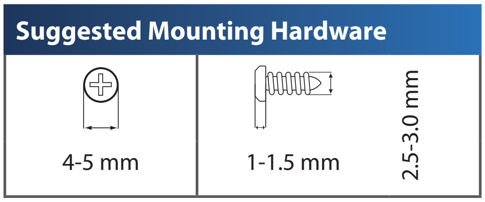
The Router has a stand on the panel opposite to the antenna. Rotate the stand 90 degrees, and place the Router on a level surface near an electrical outlet.

Wall-Mounting Placement

The Router has four wall-mount slots on its back panel. The distance between two adjacent slots is 68 mm (2.68 inches).

Two screws are needed to mount the Router.

Suggested Mounting Hardware

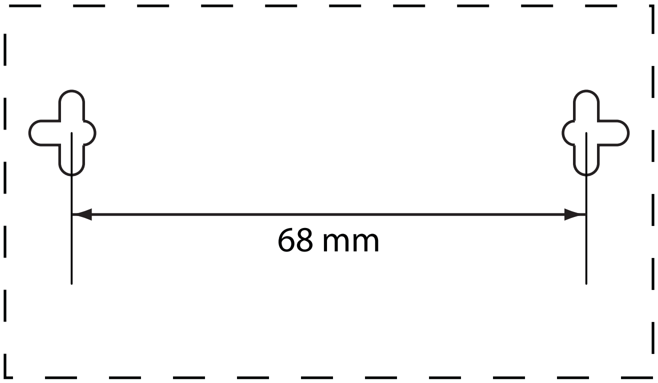


†Note: Mounting hardware illustrations are not true to scale.

> **NOTE:** Linksys is not responsible for damages incurred by insecure wall-mounting hardware.

Follow these instructions:

1. Determine where you want to mount the Router. Make sure that the wall you use is smooth, flat, dry, and sturdy. Also make sure the location is within reach of an electrical outlet.
2. Drill two holes into the wall. Make sure the holes are 68 mm (2.68 inches) apart.
3. Insert a screw into each hole and leave 3 mm (0.12 inches) of its head exposed.
4. Maneuver the Router so two of the wall-mount slots line up with the two screws.
5. Place the wall-mount slots over the screws and slide the Router down until the screws fit snugly into the wall-mount slots.



Print this page at 100% size. Cut along the dotted line, and place on the wall to drill precise spacing.

Wall Mounting Template

Chapter 2: Wireless Security Checklist

Wireless networks are convenient and easy to install, so homes with high-speed Internet access are adopting them at a rapid pace. Because wireless networking operates by sending information over radio waves, it can be more vulnerable to intruders than a traditional wired network. Like signals from your cellular or cordless phones, signals from your wireless network can also be intercepted. Since you cannot physically prevent someone from connecting to your wireless network, you need to take some additional steps to keep your network secure.

1. Change the default wireless network name or SSID

Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length. Linksys wireless products use **linksys** as the default wireless network name. You should change the wireless network name to something unique to distinguish your wireless network from other wireless networks that may exist around you, but do not use personal information (such as your Social Security number) because this information may be available for anyone to see when browsing for wireless networks.

2. Change the default password

For wireless products such as access points, routers, and gateways, you will be asked for a password when you want to change their settings. These devices have a default password set by the factory. The Linksys default password is **admin**. Hackers know these defaults and may try to use them to access your wireless device and change your network settings. To thwart any unauthorized changes, customize the device's password so it will be hard to guess.

3. Enable MAC address filtering

Linksys routers and gateways give you the ability to enable Media Access Control (MAC) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your home so that only those computers can access your wireless network.

4. Enable encryption

Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalency Privacy (WEP) offer different levels of security for wireless communication.

A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment.

WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA.

General Network Security Guidelines

Wireless network security is useless if the underlying network is not secure.

- Password protect all computers on the network and individually password protect sensitive files.
- Change passwords on a regular basis.
- Install anti-virus software and personal firewall software.
- Disable file sharing (peer-to-peer). Some applications may open file sharing without your consent and/or knowledge.

Additional Security Tips

- Keep wireless routers, access points, or gateways away from exterior walls and windows.
- Turn wireless routers, access points, or gateways off when they are not being used (at night, during vacations).
- Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary.

WEB: For more information on wireless security, visit **www.linksys.com/security**

Chapter 3: Advanced Configuration

After setting up the Router with the Setup Wizard (located on the CD-ROM), the Router will be ready for use. However, if you'd like to change its advanced settings, use the Router's web-based utility. This chapter describes each web page of the utility and each page's key functions. You can access the utility via a web browser on a computer connected to the Router.

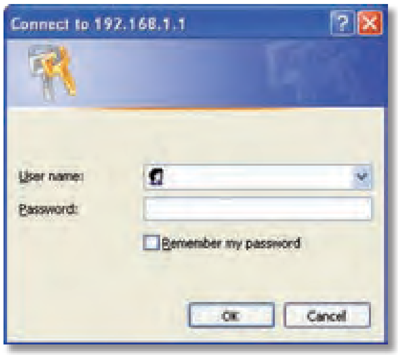
The web-based utility has these main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

> **NOTE:** When first installing the Router, you should use the Setup Wizard on the Setup CD-ROM. If you want to configure advanced settings, use this chapter to learn about the web-based utility.

How to Access the Web-Based Utility

To access the web-based utility, launch the web browser on your computer, and enter the Router's default IP address, **192.168.1.1**, in the *Address* field. Then, press **Enter**.

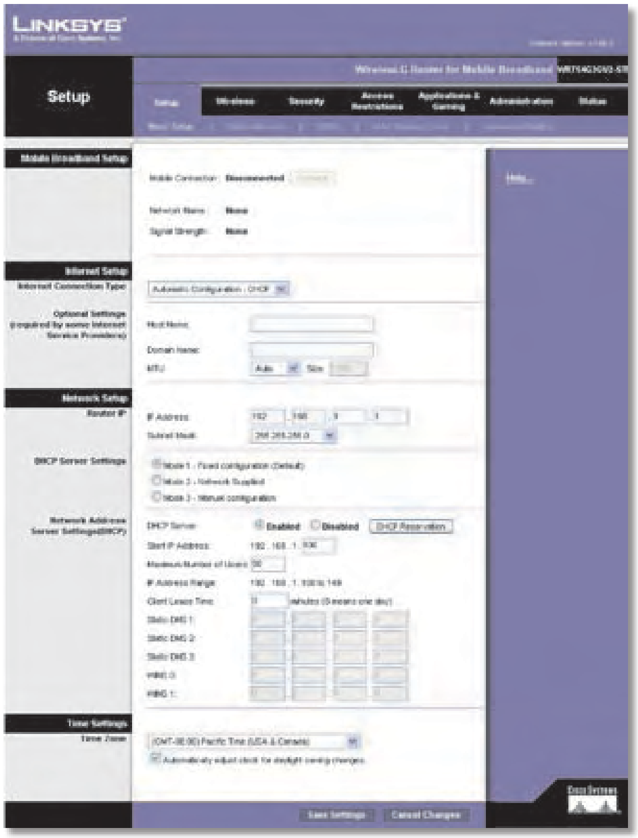
A login screen will appear. (Non-Windows XP users will see a similar screen.) Enter **admin** (the default) in both the *User name* and *Password* fields. (You can set a new password on the Administration tab's *Management* screen.) Click **OK** to continue.



Login Screen

Setup > Basic Setup

The first screen that appears is the *Basic Setup* screen. This allows you to change the Router's general settings.



Setup > Basic Setup

Internet Setup

The Internet Setup section configures the Router to your Internet connection. Most of this information can be obtained through your ISP.

Internet Connection Type

Select the type of Internet connection your ISP provides from the drop-down menu. These are the available types:

- Automatic Configuration - DHCP
- Static IP
- PPPoE
- PPTP
- L2TP
- Telstra Cable

Automatic Configuration - DHCP

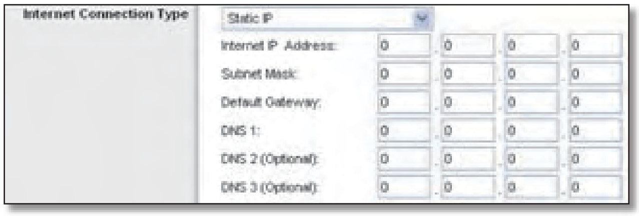
By default, the Router's Internet Connection Type is set to **Automatic Configuration - DHCP**, which should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address. (This option usually applies to cable connections.)

Internet Connection Type: Automatic Configuration - DHCP

Internet Connection Type > Automatic Configuration - DHCP

Static IP

If you are required to use a permanent IP address to connect to the Internet, select **Static IP**.



Internet Connection Type
Static IP
Internet IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Default Gateway: 0 . 0 . 0 . 0
DNS 1: 0 . 0 . 0 . 0
DNS 2 (Optional): 0 . 0 . 0 . 0
DNS 3 (Optional): 0 . 0 . 0 . 0

Internet Connection Type > Static IP

Internet IP Address This is the Router's IP address, when seen from the Internet. Your ISP will provide you with the IP address you need to specify here.

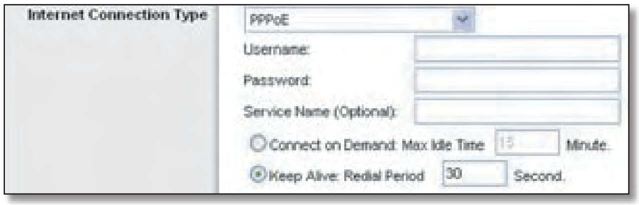
Subnet Mask This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Your ISP will provide you with the IP address of the ISP server.

DNS 1-3 Your ISP will provide you with at least one DNS (Domain Name System) server IP address.

PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable **PPPoE**.



Internet Connection Type
PPPoE
Username:
Password:
Service Name (Optional):
○ Connect on Demand: Max Idle Time 15 Minute.
● Keep Alive: Redial Period 30 Second.

Internet Connection Type > PPPoE

Username and Password Enter the Username and Password provided by your ISP.

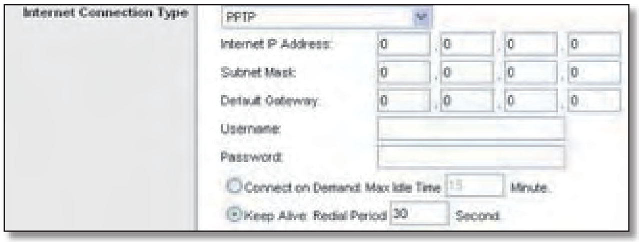
Service Name If provided by your ISP, enter the Service Name.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **15** minutes.

Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select **Keep Alive**. In the *Redial Period* field, specify how often you want the Router to check the Internet connection. The default Redial Period is **30** seconds.

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only.



Internet Connection Type
PPTP
Internet IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Default Gateway: 0 . 0 . 0 . 0
Username:
Password:
○ Connect on Demand: Max Idle Time 15 Minute.
● Keep Alive: Redial Period 30 Second.

Internet Connection Type > PPTP

Server IP Address This is the Router's IP address, as seen from the Internet. Your ISP will provide you with the IP address you need to specify here.

Subnet Mask This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Your ISP will provide you with the IP address of the ISP server.

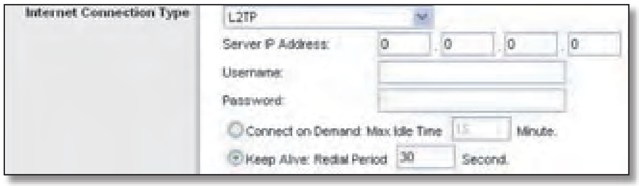
Username and Password Enter the Username and Password provided by your ISP.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **15** minutes.

Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select **Keep Alive**. In the *Redial Period* field, specify how often you want the Router to check the Internet connection. The default Redial Period is **30** seconds.

L2TP

L2TP is a service that applies to connections in Israel only.


Internet Connection Type: L2TP
Server IP Address: 0 . 0 . 0 . 0
Username:
Password:
○ Connect on Demand: Max Idle Time 15 Minute.
● Keep Alive: Redial Period 30 Second.

Internet Connection Type > L2TP

Server IP Address This is the IP address of the L2TP Server. Your ISP will provide you with the IP address you need to specify here.

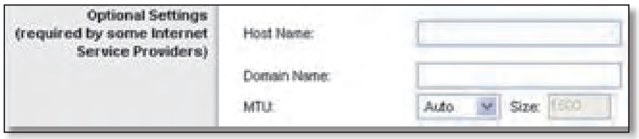
Username and Password Enter the Username and Password provided by your ISP.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **15** minutes.

Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select **Keep Alive**. In the *Redial Period* field, specify how often you want the Router to check the Internet connection. The default Redial Period is **30** seconds.

Optional Settings

Some of these settings may be required by your ISP. Verify with your ISP before making any changes.


Optional Settings (required by some Internet Service Providers)
Host Name:
Domain Name:
MTU: Auto Size: 1500

Optional Settings

Host Name and Domain Name These fields allow you to supply a host and domain name for the Router. Some ISPs, usually cable ISPs, require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select Manual if you want to manually enter the largest packet size that is transmitted. To have the Router select the best MTU for your Internet connection, keep the default, **Auto**.

Size When Manual is selected in the *MTU* field, this option is enabled. Leave this value in the 1200 to 1500 range. The default size depends on the Internet Connection Type:

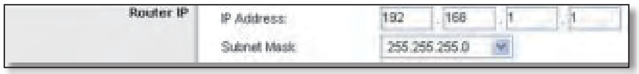
- DHCP, Static IP, or Telstra: **1500**
- PPPoE: **1492**
- PPTP or L2TP: **1460**

Network Setup

The Network Setup section changes the settings on the network connected to the Router's Ethernet ports. Wireless setup is performed through the Wireless tab.

Router IP

This presents both the Router's IP Address and Subnet Mask as seen by your network.


Router IP
IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255.255.255.0

Router IP

DHCP Server Settings

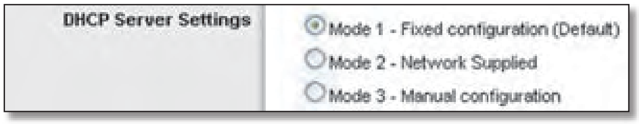
This setting determines how the clients (network devices) use DNS/WINS.

Mode 1 - Fixed configuration (Default) Select this option if you want the Router to advertise itself as the DNS server to use and handle upstream changes automatically.

Mode 2 - Network Supplied Select this option if you want the Router to pass through the DNS server values (learned from the Modem port or mobile network) to the client, depending on how the Router is currently connected.

NOTE: If the upstream DNS servers change between connections, the clients may become unable to resolve addresses because they have valid DHCP leases that use the old server values.

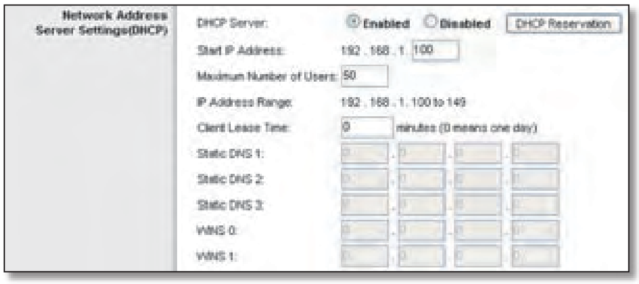
Mode 3 - Manual configuration Select this option if you want to set arbitrary DNS/WINS values for the clients to use. These values are not validated by the Router.


DHCP Server Settings
● Mode 1 - Fixed configuration (Default)
○ Mode 2 - Network Supplied
○ Mode 3 - Manual configuration

DHCP Server Settings

Network Address Server Settings (DHCP)

The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Router’s DHCP server option, make sure there is no other DHCP server on your network.



Network Address Server Settings(DHCP)

DHCP Server: ● Enabled ○ Disabled [DHCP Reservation]

Start IP Address: 192 . 168 . 1 . 100

Maximum Number of Users: 50

IP Address Range: 192 . 168 . 1 . 100 to 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS 0: 0 . 0 . 0 . 0

WINS 1: 0 . 0 . 0 . 0

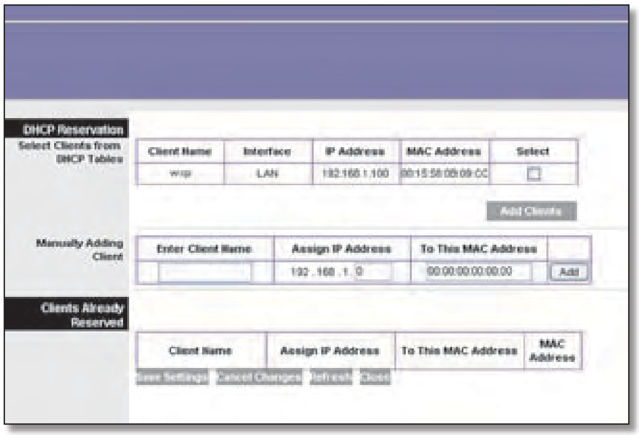
Network Address Server Settings (DHCP)

DHCP Server DHCP is enabled by factory default. If you already have a DHCP server on your network, or you don’t want a DHCP server, then select **Disabled** (no other DHCP features will be available).

DHCP Reservation Click this button if you want to assign a fixed local IP address to a MAC address.

DHCP Reservation

You will see a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address.



DHCP Reservation

Select Clients from DHCP Tables

Client Name	Interface	IP Address	MAC Address	Select
wip	LAN	192.168.1.100	00:15:58:08:09:CC	□

[Add Clients]

Manually Adding Client

Enter Client Name	Assign IP Address	To This MAC Address	
	192 . 168 . 1 . 0	00:00:00:00:00:00	[Add]

Clients Already Reserved

Client Name	Assign IP Address	To This MAC Address	MAC Address

[Save Settings] [Cancel Changes] [Refresh] [Close]

DHCP Reservation

- **Select Clients from DHCP Table** Click the **Select** check box to reserve a client’s IP address. Then click **Add Clients**.
- **Manually Adding Client** To manually assign an IP address, enter the client’s name in the *Enter Client Name* field. Enter the IP address you want it to have in the *Assign IP Address* field. Enter its MAC address in the *To This MAC Address* field. Then click **Add**.

Clients Already Reserved

A list of DHCP clients and their fixed local IP addresses will be displayed at the bottom of the screen. If you want to remove a client from this list, click **Remove**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. To view the most up-to-date information, click **Refresh**. To exit this screen, click **Close**.

Start IP Address Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router’s default IP address is 192.168.1.1, the Start IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.253. The default is **192.168.1.100**.

Maximum Number of Users Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is **50**.

IP Address Range Displayed here is the range of available IP addresses.

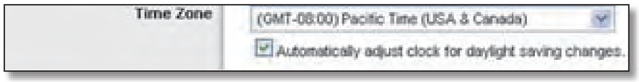
Client Lease Time The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be “leased” this dynamic IP address. After the time is up, the user will be automatically assigned a new dynamic IP address. The default is **0** minutes, which means one day.

Static DNS 1-3 These settings are available if you selected Mode 3 - Manual configuration for the DHCP Server Setting. The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS server IP address. If you wish to use another, enter that IP address in one of these fields. You can enter up to three DNS server IP addresses here. The Router will use these for quicker access to functioning DNS servers.

WINS 0-1 These settings are available if you selected Mode 3 - Manual configuration for the DHCP Server Setting. The Windows Internet Naming Service (WINS) manages each PC’s interaction with the Internet. If you use a WINS server, enter that server’s IP address. You can enter up to two WINS server IP addresses here. Otherwise, leave these fields blank.

Time Setting

Time Zone Select the time zone in which your network functions from this drop-down menu. (You can even automatically adjust for daylight saving time.)



Time Zone: (GMT-08:00) Pacific Time (USA & Canada)

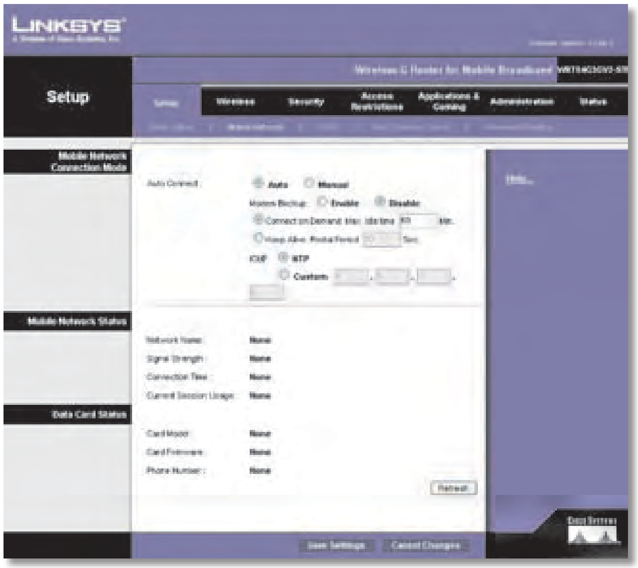
☑ Automatically adjust clock for daylight saving changes.

Time Setting

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

Setup > Mobile Network

Configure mobile network settings and view mobile broadband status information for the Router. Some of these settings will be automatically configured by the Router and, in most cases, should not be changed unless you are instructed to do so.



Auto Connect: ● Auto ○ Manual
Modem Backup: ○ Enable ● Disable
● Connect on Demand: Max Idle time 15 Min.
○ Keep Alive: Redial Period Sec.
ICMP ● NTP
○ Custom . . .

Network Name: None
Signal Strength: None
Connection Time: None
Current Session Usage: None

Card Model: None
Card Firmware: None
Phone Number: None

Setup > Mobile Network

Mobile Network Connection Mode

Auto Connect If you want the Router to automatically connect to the default mobile network when it powers on, keep the default, **Auto**. To manually connect to a mobile network, select **Manual**. You can use the Mobile Connect/Disconnect button on the Router to connect and disconnect from the mobile network.

Modem Backup To use the cable/DSL WAN broadband modem as your backup, select **Enable**. Otherwise, keep the default, **Disable**.

Connect on Demand: Max Idle Time You can configure the Router to cut the mobile network connection after it has been inactive for a specified period of time (Max Idle Time). If your mobile network connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your mobile network connection terminates. The default Max Idle Time is **15** minutes.

Keep Alive: Redial Period If you select this option, the Router will periodically check your mobile network connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select **Keep Alive**. In the *Redial Period* field, specify how often you want the Router to check the mobile network connection. The default Redial Period is **30** seconds.

ICMP To use the default Network Time Protocol (NTP) server, keep the default, **NTP**. To use a different time server, select **Custom**, and enter its IP address.

Mobile Network Status

Network Name The name of the mobile network the Router uses is displayed.

Signal Strength The strength of the mobile broadband signal that the Router receives is displayed.

Connection Time The length of time the Router has been connected to the mobile network since your last connection is displayed.

Current Session Usage The amount of data that has been sent to and received from the mobile network since your last connection is displayed.

Data Card Status

Card Model The model number of your mobile data card or USB adapter is displayed.

Card Firmware The firmware version of your mobile data card or USB adapter is displayed.

Phone Number The phone number of your mobile broadband account is displayed.

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

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

Setup > DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router.

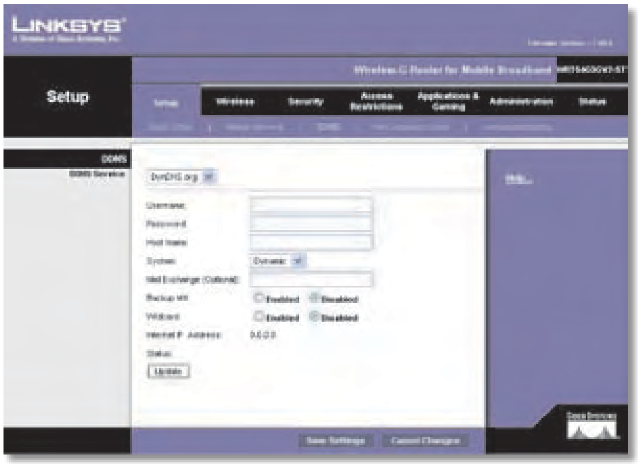
Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, www.dyndns.org or www.TZO.com. If you do not want to use this feature, keep the default, **Disabled**.

DDNS

DDNS Service

If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** from the drop-down menu. If your DDNS service is provided by TZO, then select **TZO.com**. The features available on the *DDNS* screen will vary, depending on which DDNS service provider you use.

DynDNS.org



DDNS Service: DynDNS.org

Username:

Password:

Host Name:

System: Dynamic

Mail Exchange (Optional):

Backup MX ○ Enabled ● Disabled

Wildcard ○ Enabled ● Disabled

Internet IP Address: 0.0.0.0

Status:

Update

Setup > DDNS > DynDNS

Username Enter the Username for your DDNS account.

Password Enter the Password for your DDNS account.

Host Name This is the DDNS URL assigned by the DDNS service.

System Select the DynDNS service you use: **Dynamic**, **Static**, or **Custom**. The default is **Dynamic**.

Mail Exchange (Optional) Enter the address of your mail exchange server, so e-mails to your DynDNS address go to your mail server.

Backup MX This feature allows the mail exchange server to be a backup. To disable this feature, keep the default, **Disabled**. To enable the feature, select **Enabled**. If you are not sure which setting to select, keep the default, **Disabled**.

Wildcard This setting enables or disables wildcards for your host. For example, if your DDNS address is *myplace.dyndns.org* and you enable wildcards, then *x.myplace.dyndns.org* will work as well (x is the wildcard). To disable wildcards, keep the default, **Disabled**. To enable wildcards, select **Enabled**. If you are not sure which setting to select, keep the default, **Disabled**.

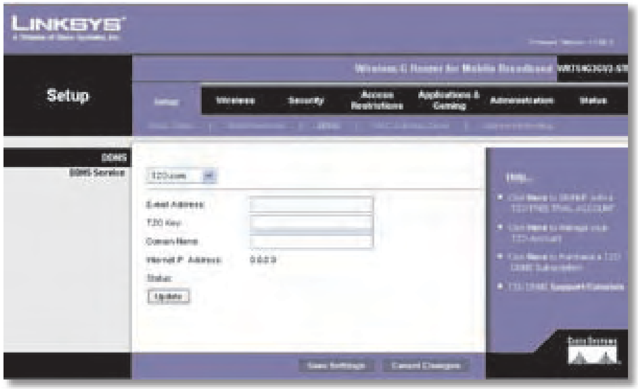
Internet IP Address The Router's Internet IP address is displayed here. Because it is dynamic, it will change.

Status The status of the DDNS service connection is displayed here.

Update To manually trigger an update, click this button.

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

TZO.com



DDNS Service: TZO.com

E-mail Address:

TZO Key:

Domain Name:

Internet IP Address: 0.0.0.0

Status:

Update

Setup > DDNS > TZO

E-mail Address, TZO Key, and Domain Name Enter the settings of the account you set up with TZO.

Internet IP Address The Router's Internet IP address is displayed here. Because it is dynamic, it will change.

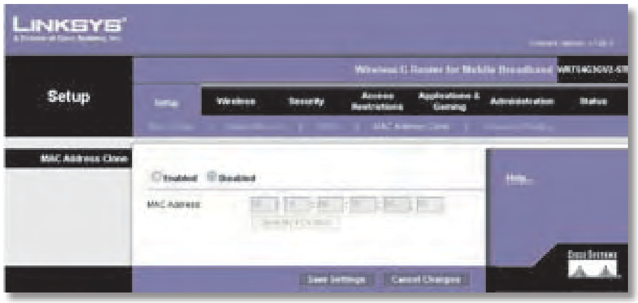
Status The status of the DDNS service connection is displayed here.

Update To manually trigger an update, click this button.

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

Setup > MAC Address Clone

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Router with the MAC Address Clone feature.



MAC Address Clone ○ Enabled ● Disabled

MAC Address:

Setup > MAC Address Clone

MAC Address Clone

Enabled/Disabled To have the MAC Address cloned, select **Enabled**.

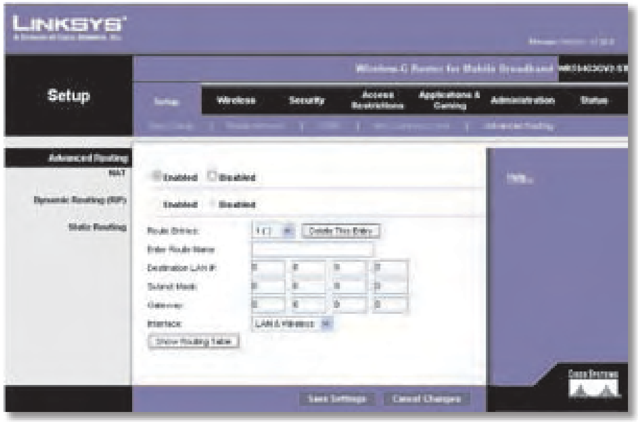
MAC Address Enter the MAC Address registered with your ISP here.

Clone My PC's MAC Click this button to clone the MAC address of the computer you are using.

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

Setup > Advanced Routing

This screen is used to set up the Router's advanced functions. Operating Mode allows you to select the type(s) of advanced functions you use. Dynamic Routing automatically adjusts how packets travel on your network. Static Routing sets up a fixed route to another network destination.



NAT: ● Enabled ○ Disabled

Dynamic Routing (RIP): ○ Enabled ○ Disabled

Route Entries: 1 ( ) Delete This Entry

Enter Route Name:

Destination LAN IP: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Gateway: 0 . 0 . 0 . 0

Interface: LAN & Wireless

Show Routing Table

Setup > Advanced Routing

Advanced Routing

NAT

Enabled/Disabled If this Router is hosting your network's connection to the Internet, keep the default, **Enabled**. If another router exists on your network, select **Disabled**. When the NAT setting is disabled, dynamic routing will be enabled.

Dynamic Routing (RIP)

Enabled/Disabled This feature enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s). The Router determines the network packets' route based on the fewest number of hops between the source and the destination. When the NAT setting is enabled, the Dynamic Routing feature is automatically disabled. When the NAT setting is disabled, this feature is available. Select **Enabled** to use the Dynamic Routing feature.

Static Routing

A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Enter the information described below to set up a new static route.

Route Entries To set up a static route between the Router and another network, select a number from the drop-down list. Click **Delete This Entry** to delete a static route.

Enter Route Name Enter a name for the Route here, using a maximum of 25 alphanumeric characters.

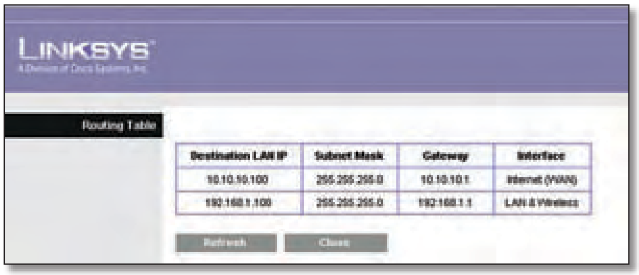
Destination LAN IP The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.

Subnet Mask The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion.

Gateway This is the IP address of the gateway device that allows for contact between the Router and the remote network or host.

Interface This interface tells you whether the Destination IP address is on the **LAN & Wireless** (Ethernet and wireless networks) or the **WAN (Internet)**.

Click **Show Routing Table** to view the static routes you have already set up.



Destination LAN IP	Subnet Mask	Gateway	Interface
10.10.10.100	255.255.255.0	10.10.10.1	Internet (WAN)
192.168.1.100	255.255.255.0	192.168.1.1	LAN & Wireless

Advanced Routing > Routing Table

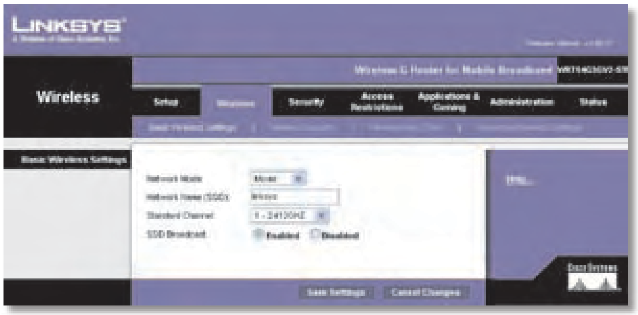
Routing Table

For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click **Refresh** to update the information. Click **Close** to exit this screen.

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

Wireless > Basic Wireless Settings

The basic settings for wireless networking are set on this screen.



Network Mode: Mixed
Network Name (SSID): linksys
Standard Channel: 1 - 2.412GHZ
SSID Broadcast: ● Enabled ○ Disabled

Wireless > Basic Wireless Settings

Basic Wireless Settings

Network Mode From this drop-down menu, you can select the wireless standards running on your network. If you have Wireless-G and Wireless-B devices in your network, keep the default, **Mixed**. If you have only Wireless-G devices, select **G-Only**. If you have only Wireless-B devices, select **B-Only**. If you do not have any wireless devices in your network, select **Disabled**.

Network Name (SSID) The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID (**linksys**) to a unique name.

Standard Channel Select the channel you want to use for wireless networking.

SSID Broadcast When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default, **Enabled**. If you do not want to broadcast the Router's SSID, then select **Disabled**.

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

Wireless > Wireless Security

The *Wireless Security* screen configures the security of your wireless network. There are six wireless security mode options supported by the Router: WPA Personal, WPA2 Personal, WPA Enterprise, WPA2 Enterprise, RADIUS, and WEP. (WPA stands for Wi-Fi Protected Setup, which is a security method stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) These six are briefly discussed here. For detailed instructions on configuring wireless security for the Router, refer to "Chapter 2: Wireless Security."

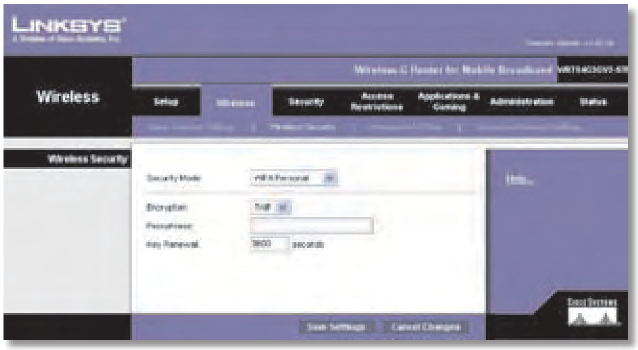
Wireless Security

Security Mode

Select the security method for your wireless network. If you do not want to use wireless security, keep the default, **Disabled**.

WPA Personal

NOTE: If you are using WPA, always remember that each device in your wireless network MUST use the same WPA method and passphrase, or else the network will not function properly.



Security Mode: WPA Personal
Encryption: TKIP
Passphrase:
Key Renewal: 3600 seconds

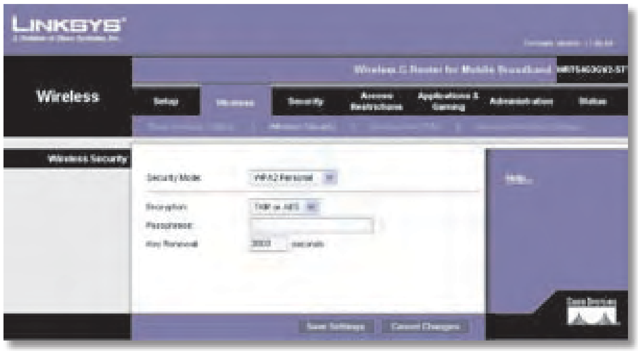
Security Mode > WPA Personal

Encryption WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. The default is **TKIP**.

Passphrase Enter a Passphrase of 8-63 characters.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default is **3600** seconds.

WPA2 Personal



Security Mode: WPA2 Personal
Encryption: TKIP or AES
Passphrase:
Key Renewal: 3600 seconds

Security Mode > WPA2 Personal

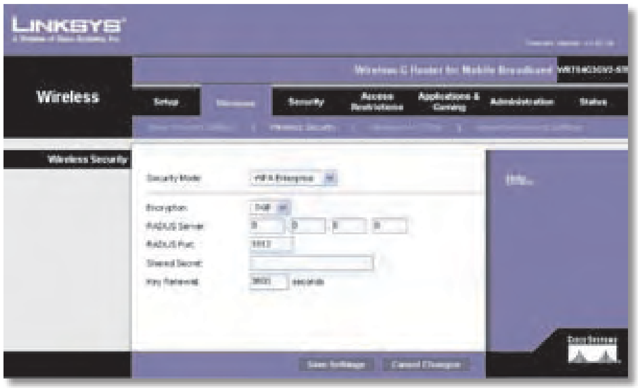
Encryption WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **AES** or **AES or TKIP**. The default is **AES or TKIP**.

Passphrase Enter a Passphrase of 8-63 characters.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default is **3600** seconds.

WPA Enterprise

This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)



Security Mode: WPA Enterprise
Encryption: TKIP
RADIUS Server: 0 . 0 . 0 . 0
RADIUS Port: 1812
Shared Secret:
Key Renewal: 3600 seconds

Security Mode > WPA Enterprise

Encryption WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. The default is **TKIP**.

RADIUS Server Enter the IP address of the RADIUS server.

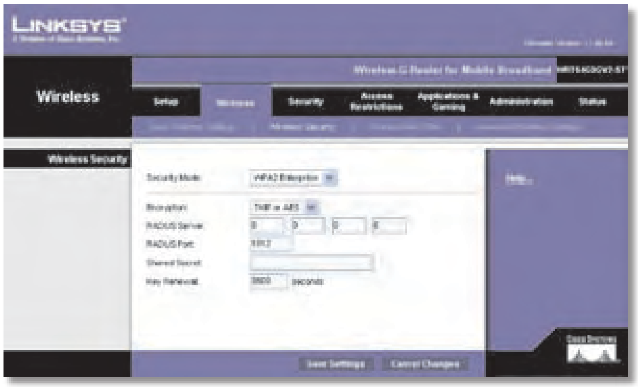
RADIUS Port Enter the port number of the RADIUS server. The default is **1812**.

Shared Secret Enter the key shared between the Router and the server.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default Key Renewal period is **3600** seconds.

WPA2 Enterprise

This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)



Security Mode: WPA2 Enterprise
Encryption: TKIP or AES
RADIUS Server: 0 . 0 . 0 . 0
RADIUS Port: 1812
Shared Secret:
Key Renewal: 3600 seconds

Security Mode > WPA2 Enterprise

Encryption WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **AES** or **AES or TKIP**. The default is **AES or TKIP**.

RADIUS Server Enter the IP address of the RADIUS server.

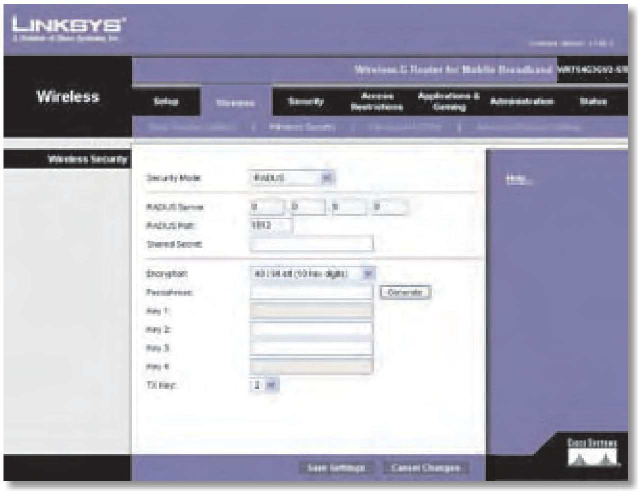
RADIUS Port Enter the port number of the RADIUS server. The default is **1812**.

Shared Secret Enter the key shared between the Router and the server.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default is **3600** seconds.

RADIUS

This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)



Security Mode: RADIUS
RADIUS Server: 0 . 0 . 0 . 0
RADIUS Port: 1812
Shared Secret:
Encryption: 40 / 64-bit (10 hex digits)
Passphrase:
Key 1:
Key 2:
Key 3:
Key 4:
TX Key: 1

Security Mode > RADIUS

IMPORTANT: If you are using WEP encryption, always remember that each device in your wireless network MUST use the same WEP encryption method and encryption key, or else your wireless network will not function properly.

RADIUS Server Enter the IP address of the RADIUS server.

RADIUS Port Enter the port number of the RADIUS server. The default is **1812**.

Shared Key Enter the key shared between the Router and the server.

Encryption Select a level of WEP encryption, **40/64 bits (10 hex digits)** or **104/128 bits (26 hex digits)**. The default is **40/64 bits (10 hex digits)**.

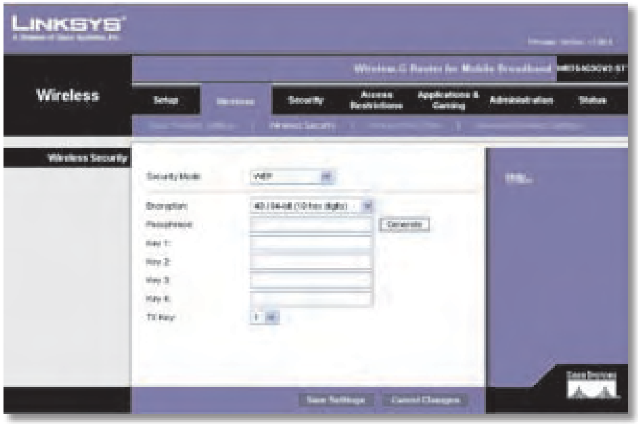
Passphrase Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

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

TX Key Select which TX (Transmit) Key to use. The default is **1**.

WEP

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



Security Mode: WEP
Encryption: 40 / 64-bit (10 hex digits)
Passphrase: Generate
Key 1:
Key 2:
Key 3:
Key 4:
TX Key: 1

Security Mode > WEP

Encryption Select a level of WEP encryption, **40/64 bits (10 hex digits)** or **104/128 bits (26 hex digits)**. The default is **40/64 bits (10 hex digits)**.

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

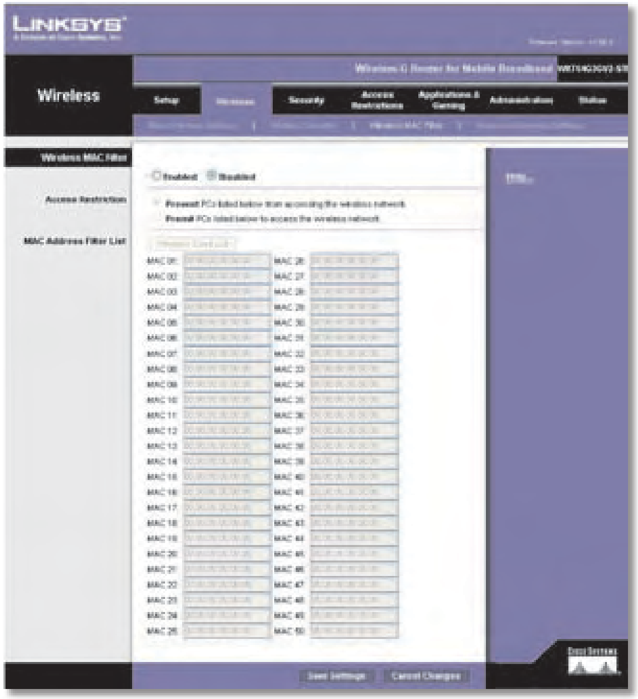
Key 1-4 If you did not enter a Passphrase, enter the WEP key(s) manually.

TX Key Select which TX (Transmit) Key to use. The default is **1**.

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 MAC Filter: ○ Enabled ● Disabled
Access Restriction: ● Prevent PCs listed below from accessing the wireless network
○ Permit PCs listed below to access the wireless network
MAC Address Filter List: Wireless Client List
MAC 01: … MAC 25:
MAC 26: … MAC 50:

Wireless > Wireless MAC Filter

Wireless MAC Filter

Enabled/Disabled To filter wireless users by MAC Address, either permitting or blocking access, select **Enabled**. If you do not wish to filter users by MAC Address, keep the default, **Disabled**.

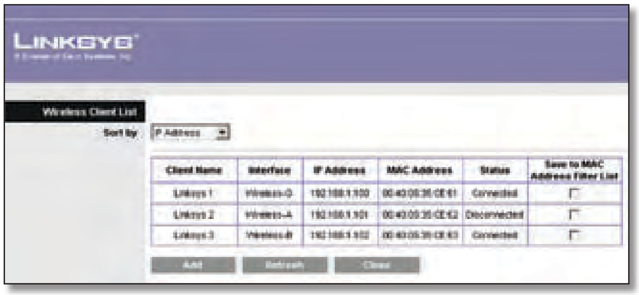
Access Restriction

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

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

MAC Address Filter List

Wireless Client List Click this to open the *Wireless Client List* screen.



Sort by: IP Address

Client Name	Interface	IP Address	MAC Address	Status	Save to MAC Address Filter List
Linksys 1	Wireless-G	192.168.1.100	00:40:05:35:CE:61	Connected	□
Linksys 2	Wireless-A	192.168.1.101	00:40:05:35:CE:62	Disconnected	□
Linksys 3	Wireless-B	192.168.1.102	00:40:05:35:CE:63	Connected	□

Wireless Client List

Wireless Client List

This screen shows computers and other devices on the wireless network. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Status.

Select **Save to MAC Address Filter List** for any device you want to add to the MAC Address Filter List. Then click **Add**.

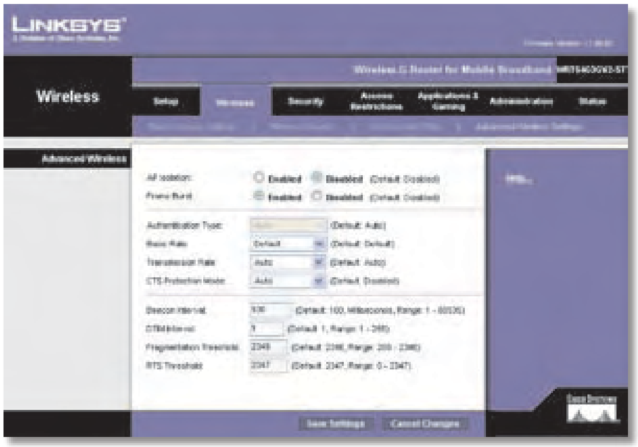
To retrieve the most up-to-date information, click **Refresh**. To exit this screen and return to the *Wireless MAC Filter* screen, click **Close**.

MAC 01-50 Enter the MAC addresses of the devices whose wireless access you want to block or allow.

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

Wireless > Advanced Wireless Settings

This *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.



AP Isolation: ○ Enabled ● Disabled (Default: Disabled)
Frame Burst: ● Enabled ○ Disabled (Default: Disabled)
Authentication Type: Auto (Default: Auto)
Basic Rate: Default (Default: Default)
Transmission Rate: Auto (Default: Auto)
CTS Protection Mode: Auto (Default: Disabled)
Beacon Interval: 100 (Default: 100, Milliseconds, Range: 1 - 65535)
DTIM Interval: 1 (Default: 1, Range: 1 - 255)
Fragmentation Threshold: 2346 (Default: 2346, Range: 256 - 2346)
RTS Threshold: 2347 (Default: 2347, Range: 0 - 2347)

Wireless > Advanced Wireless Settings

Advanced Wireless

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 **Enabled**. AP Isolation is disabled by default.

Frame Burst Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. To use this option, keep the default, **Enabled**. Otherwise, select **Disabled**.

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. Select **Shared Key** to only use Shared Key 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 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 is **Auto**.

CTS Protection Mode The Router will automatically use CTS (Clear-To-Send) Protection Mode when your Wireless-N and Wireless-G products are experiencing severe problems and are not 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-N and Wireless-G transmissions but will severely decrease performance. The default is **Auto**.

Beacon Interval 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. The default is **100**.

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 is **1**.

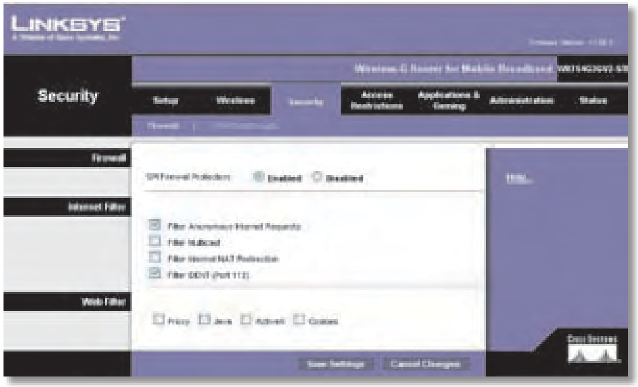
Fragmentation Threshold This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance.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

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

Security > Firewall

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



SPI Firewall Protection ● Enabled ○ Disabled

☑ Filter Anonymous Internet Requests
□ Filter Multicast
□ Filter Internet NAT Redirection
☑ Filter IDENT (Port 113)

□ Proxy □ Java □ ActiveX □ Cookies

Security > Firewall

Firewall

SPI Firewall Protection To use firewall protection, keep the default, **Enabled**. To turn off firewall protection, select **Disabled**.

Internet Filter

Filter 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. Select this feature to filter multicasting. This feature is not selected by default.

Filter Internet NAT Redirection This feature uses port forwarding to block access to local servers from local networked computers. Select this feature to filter Internet NAT redirection. It 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.

Web Filter

Proxy Use of WAN proxy servers may compromise the Gateway's security. Denying Proxy will disable access to any WAN proxy servers. Select this feature to enable proxy filtering. Deselect the feature to allow proxy access.

Java Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. Select this feature to enable Java filtering. Deselect the feature to allow Java usage.

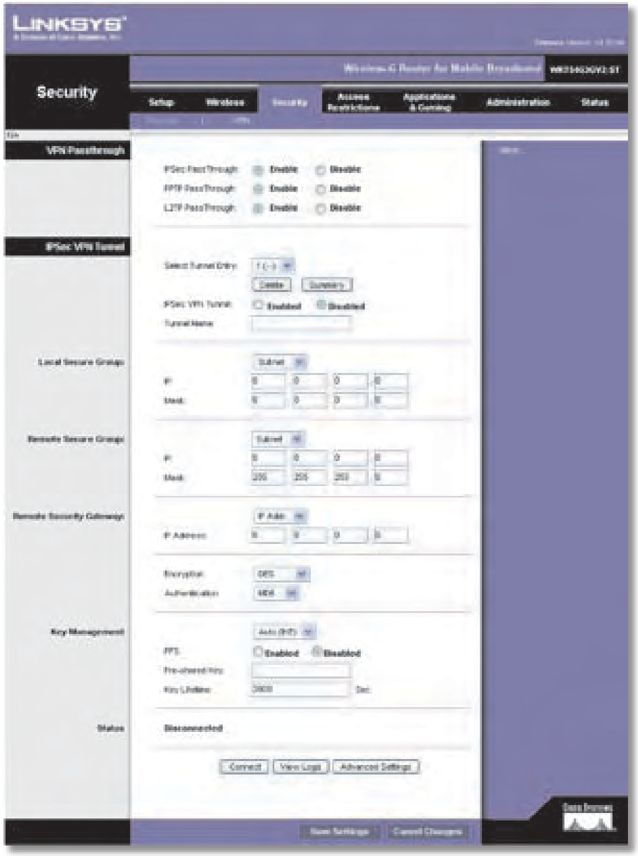
ActiveX ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. Select this feature to enable ActiveX filtering. Deselect the feature to allow ActiveX usage.

Cookies A cookie is data stored on your computer and used by Internet sites when you interact with them. Select this feature to filter cookies. Deselect the feature to allow cookie usage.

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

Security > VPN

The *VPN* screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall. You can also configure up to five IPSec VPN tunnels.



IPSec PassThrough: ● Enable ○ Disable
PPTP PassThrough: ● Enable ○ Disable
L2TP PassThrough: ● Enable ○ Disable

Select Tunnel Entry: 1 (-)
IPSec VPN Tunnel: ○ Enabled ● Disabled
Tunnel Name:

Local Secure Group: Subnet
IP: 0 . 0 . 0 . 0
Mask: 0 . 0 . 0 . 0

Remote Secure Group: Subnet
IP: 0 . 0 . 0 . 0
Mask: 255 . 255 . 255 . 0

Remote Security Gateway: IP Addr.
IP Address: 0 . 0 . 0 . 0

Encryption: DES
Authentication: MD5

Key Management: Auto (IKE)
PFS: ○ Enabled ● Disabled
Pre-shared Key:
Key Lifetime: 3600 Sec.

Status: Disconnected

Security > VPN

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, **Enabled**.

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, **Enabled**.

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, **Enabled**.

IPSec VPN Tunnel

The Router can create an IPSec tunnel or channel between two endpoints, so that the data or information between these endpoints is secure.

Select Tunnel Entry To establish this tunnel, select the tunnel you wish to create. It is possible to create up to five simultaneous tunnels.

To delete a tunnel entry, select the tunnel, and then click **Delete**. To view a summary of the settings, click **Summary**.

VPN Settings Summary

At the top of the screen is the WAN IP address of the Router. The screen also displays the No., Tunnel Name, Status, Local Group, Remote Group, Remote Gateway, and Security Method of the VPN tunnels. Click **Refresh** to update the information.

WAN IP: 0.0.0.0

No.	Tunnel Name	Status	Local Group	Remote Group	Remote Gateway	Security Method

VPN > VPN Settings Summary

IPSec VPN Tunnel Select **Enabled** to enable the IPSec VPN tunnel.

Tunnel Name Enter a descriptive name. This lets you identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

Local Secure Group

The Local Secure Group is the computer(s) on your network that can access the tunnel. Specify these computers using one of the following:

IP Addr. Select this option to specify a single host.

- **IP Address** Enter the host's IP address.

Subnet Select this option to give an entire local network access to the tunnel.

- **IP** Enter the IP address.
- **Mask** Enter the subnet mask.

Remote Secure Group

The Remote Secure Group is the computer(s) on the remote end of the tunnel that can access the tunnel. Specify these computers using one of the following:

IP Addr. Select this option to specify a single host.

- **IP Address** Enter the host's public IP address.

Subnet Select this option to give an entire remote subnet access to the tunnel.

- **IP** Enter the IP address.
- **Mask** Enter the subnet mask.

Host Select this option to use the Remote Security Gateway settings.

Any Select this option to have the Router accept requests from any IP address.

Remote Security Gateway

The Remote Security Gateway is the VPN device on the remote end of the VPN tunnel. The remote VPN device can be another router, a VPN Server, or a computer with VPN client software that supports IPSec. Specify the remote VPN device using one of the following: