LINKSYS®

A Division of Cisco Systems, Inc.

2.4 GHz

Wireless-N

Gigabit Router with Storage Link

WIRELESS

User Guide

CISCO SYSTEMS

Model No. **WRT350N**

Copyright and Trademarks

WARNING: This product contains chemicals, including lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. ***Wash hands after handling.***

How to Use This User Guide

This User Guide has been designed to make understanding networking with the Wireless-N Gigabit Router with Storage Link easier than ever. Look for the following items when reading this User Guide:

This checkmark means there is a note of interest and is something you should pay special attention to while using the Wireless-N Gigabit Router with Storage Link.

This exclamation point means there is a caution or warning and is something that could damage yoGigabit Router with Storage Linkur property or the Wireless-N Gigabit Router with Storage LinkWireless-N Gigabit Router with Storage Link.

This question mark provides you with a reminder about something you might need to do while using the Wireless-N Gigabit Router with Storage Link.

In addition to these symbols, there are definitions for technical terms that are presented like this:

word: *definition.*

Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this:

Figure 0-1: Sample Figure Description

Figure numbers and descriptions can also be found in the “List of Figures” section in the “Table of Contents”.

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

The Wireless-N Gigabit Router with Storage Link is really four devices in one box. First, there's the Wireless Access Point, which lets you connect to the network without wires. There's also a built-in 4-port full-duplex 10/100 Switch to connect your wired-Ethernet devices together. The Router function ties it all together and lets your whole network share a high-speed cable or DSL Internet connection.

We've also included a Storage Link that lets you easily add gigabytes of storage space onto your network using readily available USB 2.0 hard drives -- or plug in a USB flash disk for a convenient way to access your portable data files. The built-in Media Server streams music, video, and photos from the attached storage device to any UPnP compatible media adapter. And you can get to your files from anywhere in the world through the Internet.

The Access Point built into the Router uses the very latest wireless networking technology, Wireless-N (draft 802.11n). By overlaying the signals of multiple radios, Wireless-N's "Multiple In, Multiple Out" (MIMO) technology multiplies the effective data rate. Unlike ordinary wireless networking technologies that are confused by signal reflections, MIMO actually uses these reflections to increase the range and reduce "dead spots" in the wireless coverage area. The robust signal travels farther, maintaining wireless connections up to 4 times farther than standard Wireless-G.

With Wireless-N, the farther away you are, the more speed advantage you get. It works great with standard Wireless-G and -B equipment, but when both ends of the wireless link are Wireless-N, the router can increase the throughput even more by using twice as much radio band, yielding speeds up to 12 times as fast as standard Wireless-G. But unlike other speed-enhanced technologies, Wireless-N can dynamically enable this double-speed mode for Wireless-N devices, while still connecting to other wireless devices at their respective fastest speeds. In congested areas, the "good neighbor" mode ensures that the Router checks for other wireless devices in the area before gobbling up the radio band.

To help protect your data and privacy, the Router can encode all wireless transmissions with industrial-strength 256-bit encryption. It can serve as your network's DHCP Server, has a powerful SPI firewall to protect your PCs against intruders and most known Internet attacks, and supports VPN pass-through. Configuration is a snap with the web browser-based configuration utility.

The incredible speed of Wireless-N makes it ideal for media-centric applications like streaming video, gaming, and Voice over IP telephony, and gives you plenty of headroom to run multiple media-intense data streams through the network at the same time, with no degradation in performance. With the Linksys Wireless-N Gigabit Router with Storage Link at the center of your home or office network, you can easily add storage, share a high-speed Internet connection, files, printers and multi-player games, and run media-intensive applications at faster than 10/100 wired network speeds, without the hassle of stringing wires!

spi *(stateful packet inspection)* ***firewall****: a technology that inspects incoming packets of information before allowing them to enter the network.*

firewall*: Security measures that protect the resources of a local network from intruders.*

nat *(network address translation): NAT technology translates IP addresses of a local area network to a different IP address for the Internet.*

lan *(local area network): The computers and networking products that make up the network in your home or office.*

What's in this User Guide?

This user guide covers the steps for setting up and using the Wireless-N Gigabit Router with Storage Link.

- Chapter 1: Introduction
  This chapter describes the Router's applications and this User Guide.

- Chapter 2: Planning Your Wireless Network
  This chapter describes the basics of wireless networking.

- Chapter 3: Getting to Know the Wireless-N Gigabit Router with Storage Link
  This chapter describes the physical features of the Router.

- Chapter 4: Connecting the Wireless-N Gigabit Router with Storage Link
  This chapter instructs you on how to connect the Router to your network.

- Chapter 5: Configuring the Wireless-N Gigabit Router with Storage Link
  This chapter explains how to use the Web-based Utility to configure the settings on the Wireless-N Gigabit Router with Storage Link.

- Appendix A: Troubleshooting
  This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-N Gigabit Router with Storage Link.

- Appendix B: Wireless Security
  This appendix explains the risks of wireless networking and some solutions to reduce the risks.

- Appendix C: Upgrading Firmware
  This appendix instructs you on how to upgrade the firmware on the Router should you need to do so.

- Appendix D: Windows Help
  This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.

- Appendix E: Finding the MAC Address and IP Address for your Ethernet Adapter
  This appendix describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Router.

- Appendix F: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.

- Appendix G: Specifications
  This appendix provides the technical specifications for the Router.

- Appendix H: Warranty Information
  This appendix supplies the warranty information for the Router.

- Appendix I: Regulatory Information
  This appendix supplies the regulatory information regarding the Router.

- Appendix J: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning Your Wireless Network

Network Topology

A wireless local area network (WLAN) is exactly like a regular local area network (LAN), except that each computer in the WLAN uses a wireless device to connect to the network. Computers in a WLAN share the same frequency channel and SSID, which is an identification name shared by the wireless devices belonging to the same wireless network.

ssid *(service set identifier): your wireless network's name.*

Ad-Hoc versus Infrastructure Mode

Unlike wired networks, wireless networks have two different modes in which they may be set up: infrastructure and ad-hoc. An infrastructure configuration is a WLAN and wired LAN communicating to each other through an access point. An ad-hoc configuration is wireless-equipped computers communicating directly with each other. Choosing between these two modes depends on whether or not the wireless network needs to share data or peripherals with a wired network or not.

infrastructure*: a wireless network that is bridged to a wired network via an access point.*

ad-hoc*: a group of wireless devices communicating directly to each other (peer-to-peer) without the use of an access point.*

If the computers on the wireless network need to be accessible by a wired network or need to share a peripheral, such as a printer, with the wired network computers, the wireless network should be set up in Infrastructure mode. The basis of Infrastructure mode centers around a wireless router or an access point, such as the Wireless-N Gigabit Router with Storage Link, which serves as the main point of communications in a wireless network. The Router transmits data to PCs equipped with wireless network adapters, which can roam within a certain radial range of the Router. You can arrange the Router and multiple access points to work in succession to extend the roaming range, and you can set up your wireless network to communicate with your Ethernet hardware as well.

If the wireless network is relatively small and needs to share resources only with the other computers on the wireless network, then the Ad-Hoc mode can be used. Ad-Hoc mode allows computers equipped with wireless transmitters and receivers to communicate directly with each other, eliminating the need for a wireless router or access point. The drawback of this mode is that in Ad-Hoc mode, wireless-equipped computers are not able to communicate with computers on a wired network. And, of course, communication between the wireless-equipped computers is limited by the distance and interference directly between them.

Network Layout

The Wireless-N Gigabit Router with Storage Link has been specifically designed for use with your Wireless-N, Wireless-G, and Wireless-B products. It will work with notebook adapters for your laptop computers, PCI adapters for your desktop computers, and USB adapters for your USB connectivity needs. The Router can also communicate with other devices, such as wireless print servers and bridges.

When you wish to connect your wireless network to your wired network, you can use the Router’s four local Ethernet ports. To add more ports, connect one of the Router's local ports to any Linksys switch.

With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys website at www.linksys.com for more information about products that work with the Wireless-N Gigabit Router with Storage Link.

Chapter 3: Getting to Know the Wireless-N Gigabit Router with Storage Link

The Back Panel

The Router's ports, where the cables are connected, and Reset button are located on the back panel.

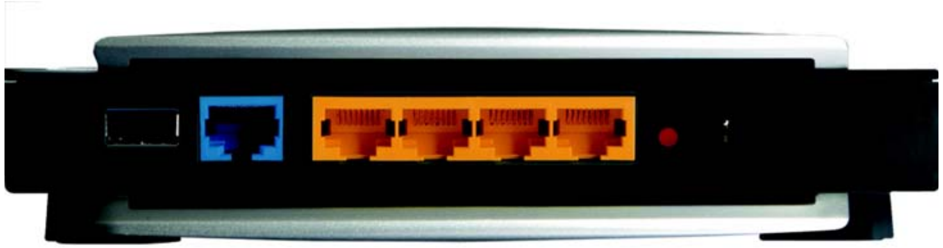


Figure 3-1: The Router's Back Panel

USB The USB port connects your Router to your wired PC or other USB network devices.

INTERNET The Internet port is where you will connect your broadband modem.

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

Reset Button There are two ways to reset the Router's factory defaults. Either press the **Reset** button, for approximately five seconds, or restore the defaults from the Administration - Factory Defaults tab of the Router's Web-based Utility.

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

⚠ **IMPORTANT:** Resetting the Router will erase all of your settings (Internet connection, wireless security, and other settings) and replace them with the factory defaults. Do not reset the Router if you want to retain these settings.

The Front Panel

The Router’s LEDs are located on the front panel.

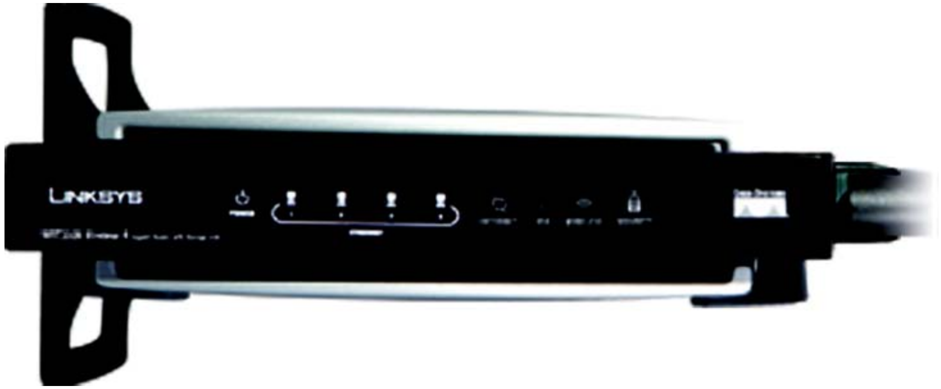


Figure 3-2: The Router’s Front Panel

POWER Green. The **POWER** LED lights up and will stay on while the Router is powered on.

ETHERNET 1, 2, 3, 4 Green, Orange. These numbered LEDs, corresponding with the numbered ports on the Router’s back panel, serve three purposes: (1) The green LED lights up when the Router is connected to a device through the corresponding port at 10/100, (2) The orange LED lights up when you are connected at 1,000 Mbps (1 Gigabit), and (3) If the LED is flashing, then the Router is sending or receiving data over that port.

INTERNET Green. The **INTERNET** LED lights up when there is a connection through the Internet port.

WIRELESS Green. The **WIRELESS** LED lights up when there is a wireless connection. If the LED is flashing, the Router is sending or receiving data over the wireless network.

USB Green. The **USB** LED lights up when a USB drive is connected through the USB port. If the LED is flashing, the Router is actively sending or receiving data over the USB connection.

SECURITY Green. The **SECURITY** LED indicates when wireless security is enabled.

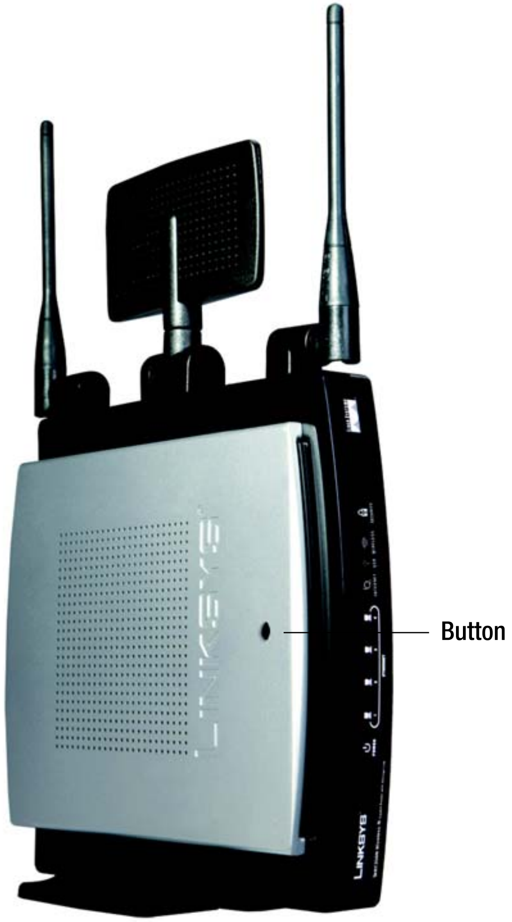


Figure 3-3: The Router’s Top Panel

The Top Panel

The Router has a button reserved for a future function.

Chapter 4: Connecting the Wireless-N Gigabit Router with Storage Link

Hardware Installation

1. Make sure that all of your hardware is powered off, including the broadband modem and PCs.
2. Connect your USB cable tot he Router's USB port.
3. Connect your broadband modem's Ethernet cable to the Router's Internet port.
4. Connect one end of an Ethernet network cable to one of the numbered ports on the back of the Router. Connect the other end to an Ethernet port on a network device, e.g., a PC, print server, or switch.

   Repeat this step to connect more PCs or other network devices to the Router.
5. Power on the broadband modem.
6. Connect the included power adapter to the Router's Power port, and then plug the power adapter into an electrical outlet. The Power LED on the front panel will light up when the adapter is connected properly.
7. Power on your PC(s).
8. Locate an optimum location for the Router. The best place for the Router is usually at the center of your wireless network, with line of sight to all of your wireless devices.

Proceed to "Chapter 5: Configuring the Wireless-N Gigabit Router with Storage Link".

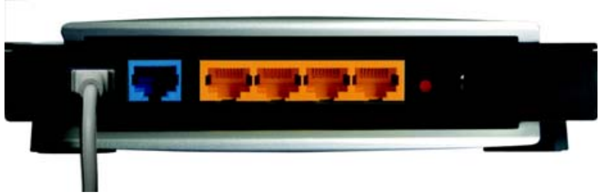


Figure 4-1: Connect the USB cable

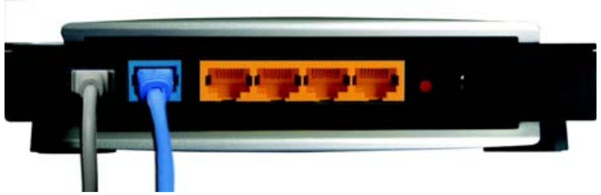


Figure 4-2: Connect the internet

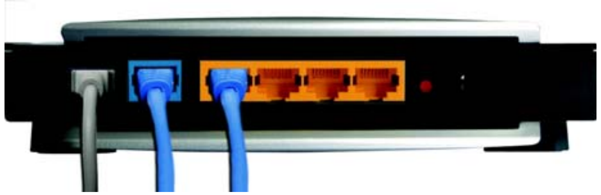


Figure 4-3: Connect the ethernet

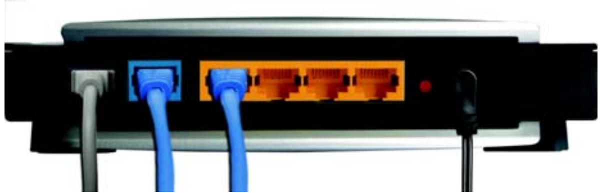


Figure 4-4: Connect the power

IMPORTANT: Make sure you use the power adapter that is supplied with the Router. Use of a different power adapter could damage the Router.

Chapter 5: Configuring the Wireless-N Gigabit Router with Storage Link

Overview

Linksys recommends using the Setup CD-ROM for first-time installation of the Router. If you do not wish to run the Setup Wizard on the Setup CD-ROM, then you can use the Web-based Utility to configure the Router. For advanced users, you may configure the Router's advanced settings through the Web-based Utility.

This chapter will describe each web page on the Utility and each page's key functions. The Utility can be accessed via your web browser through use of a computer connected to the Router. For a basic network setup, most users only have to use the following screens of the Utility:

- Basic Setup. On the *Basic Setup* screen, enter the Internet connection settings provided by your Internet Service Provider (ISP). If you do not have this information, you can call your ISP to request the settings. When you have the setup information, then you can configure the Router.

- Management. Click the **Administration** tab and then the **Management** tab. The Router's default password is **admin**. To secure the Router, change the Password from its default.

- Wireless. On the Basic Wireless Settings screen, set the basic configuration for your wireless network.

There are eight main tabs: Setup, Wireless, Security, Storage, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

Setup

- Basic Setup. Enter the Internet connection and network settings on this screen.

- DDNS. Enable the Router's Dynamic Domain Name System (DDNS) feature on this screen.

- MAC Address Clone. If you need to clone a MAC address onto the Router, use this screen.

- Advanced Routing. Use this screen to alter dynamic and static routing configurations.

Wireless

- Basic Wireless Settings. Enter the basic settings for your wireless network on this screen.
- Wireless Security. Enable and configure the security settings for your wireless network.
- Wireless MAC Filter. Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.
- Advanced Wireless Settings. For advanced users, you can alter data transmission settings on this screen.

Security

- Firewall. You can enable or disable the Router's firewall, as well as various filters.
- VPN Passthrough. To enable or disable IPSec, L2TP, and/or PPTP Passthrough, use this screen.

Storage

- Disk. Describes the disk currently attached to the Router.
- Share. Controls access to the partition of the disk attached to the Router.
- Administration. Manages the user and groups of users that can access the shares.
- Media Server. Scans for contents using a built-in media server.
- FTP Server. Creates an FTP server that can be accessed through the Internet.

Access Restrictions

Internet Access Policy. Create policies to control Internet access for your local network users.

Applications & Gaming

- Single Port Forwarding. This allows you to do port mapping and forwarding for a single service port.
- Port Range Forwarding. Set up public services or other specialized Internet applications on your network.
- Port Range Triggering. Configure the Router to watch outgoing data for specific port numbers.

- DMZ. Click this tab to allow one local user to be exposed to the Internet for use of special-purpose services.
- QoS. Quality of Service (QoS) ensures better service to high-priority types of network traffic.

Administration

- Management. On this screen, alter the Router's password, access privileges, and UPnP settings. You can also use this screen to back up and restore the Router's configuration file.
- Log. If you want to view or save activity logs, click this tab.
- Diagnostics. If you want to run a ping or traceroute test, then use this screen.
- Factory Defaults. If you want to restore the Router's factory defaults, then use this screen.
- Firmware Upgrade. Click this tab if you want to upgrade the Router's firmware.

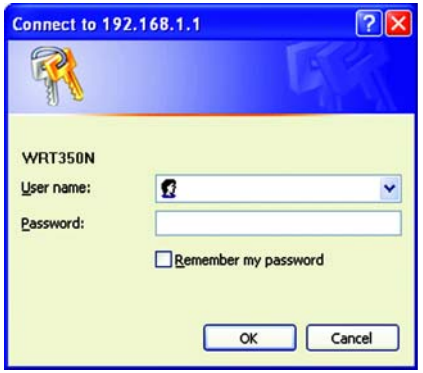
Status

- Router. This screen provides status information about the Router.
- Local Network. This provides status information about the local network.
- Wireless Network. This provides status information about the wireless network.

How to Access the Web-based Utility

To access the Web-based Utility of the Router, launch Internet Explorer or Netscape Navigator, and enter the Router's default IP address, **192.168.1.1**, in the *Address* field. Press the **Enter** key.

A screen will appear asking you for your User name and Password. Leave the *User Name* field blank. Enter **admin** in the *Password* field. Then click the **OK** button.



Connect to 192.168.1.1

WRT350N

User name:

Password:

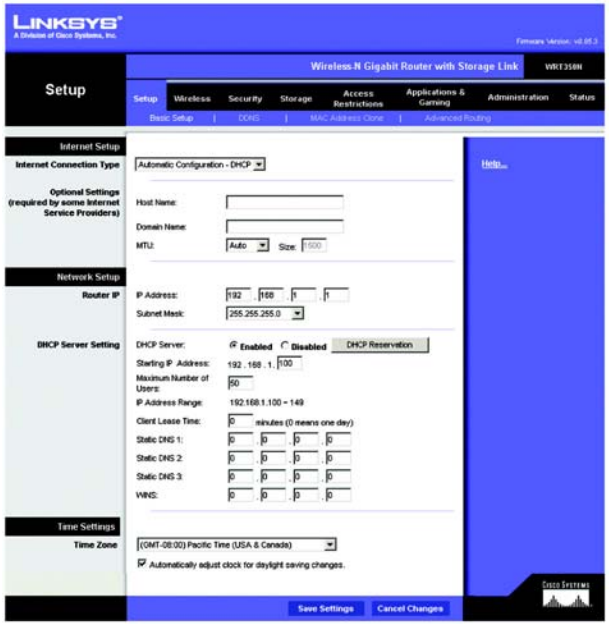
□ Remember my password

Figure 5-1: Router Login

Make the necessary changes through the Utility. When you have finished making changes to a screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For information on a tab, click **Help**.

The Setup Tab - Basic Setup

The *Basic Setup* screen is the first screen you see when you access the Web-based Utility.



LINKSYS®
A Division of Cisco Systems, Inc.
Wireless-N Gigabit Router with Storage Link
WRT350N
Setup
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Basic Setup | DDNS | MAC Address Clone | Advanced Routing
Help...
Cisco Systems

Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some Internet Service Providers)

Host Name:

Domain Name:

MTU: Auto Size: 1500

Network Setup

Router IP

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

DHCP Server Setting

DHCP Server: ● Enabled ○ Disabled DHCP Reservation

Starting IP Address: 192 . 168 . 1. 100

Maximum Number of Users: 50

IP Address Range: 192.168.1.100 ~ 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

Time Settings

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

☑ Automatically adjust clock for daylight saving changes.

Figure 5-2: Setup Tab - Basic Setup (Automatic Configuration - DHCP)

NOTE: Some of these connection types may not be available in your area.

Internet Setup

The Internet Setup section configures the Router for your Internet connection type. This information can be obtained from your ISP.

Internet Connection Type

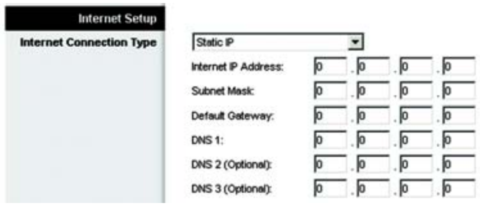
The Router supports six connection types: Automatic Configuration - DHCP, Static IP, PPPoE, PPTP, Telstra Cable, and L2TP. Each *Basic Setup* screen and available features will differ depending on what kind of connection type you select.

Automatic Configuration - DHCP

By default, the Router's Internet Connection Type is set to **Automatic Configuration - DHCP**, and it should be used only if your ISP supports DHCP or you are connecting through a dynamic IP address.

Static IP

If you are required to use a permanent IP address, then select **Static IP**.



Internet Setup

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

Figure 5-3: Static IP

***static ip address**: a fixed address assigned to a computer or device connected to a network.*

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

***default gateway**: a device that forwards Internet traffic from your local area network*

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

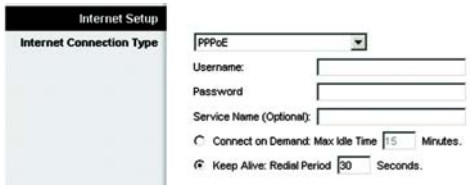
Subnet Mask. This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway. Your ISP will provide you with the Default Gateway Address.

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 for end-users. If you use a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable it.



Internet Setup

Internet Connection Type: PPPoE

Username:

Password

Service Name (Optional):

○ Connect on Demand: Max Idle Time 15 Minutes.

● Keep Alive: Redial Period 30 Seconds.

Figure 5-4: PPPoE

***pppoe**: a type of broadband connection that provides authentication (username and password) in addition to data transport*

User Name and Password. Enter the User Name and Password provided by your ISP.

IMPORTANT: For DSL users, if you need to enable PPPoE support, remember to remove any PPPoE applications that are installed on your PCs.

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

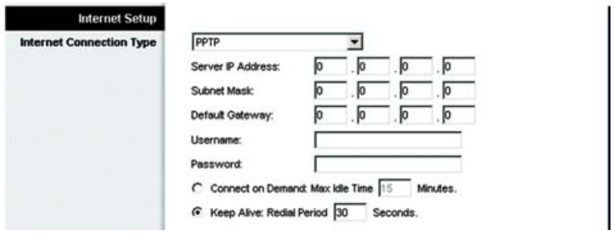
Connect on Demand and Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specific period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use Connect on Demand, click the radio button. If you want your Internet connection to remain on at all times, enter **0** in the *Max Idle Time* field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

Keep Alive and Redial Period. This option keeps your Internet access connected indefinitely, even when it sits idle. If you select this option, the Router will periodically check your Internet connection. If the connection is down, then the Router will automatically re-establish the connection. To use this option, click the radio button next to *Keep Alive*. The default Redial Period is **30** seconds.

Click the **Save Settings** button. Then click the **Status** tab, and click the **Connect** button.

PPTP

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



PPTP

Server 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 Minutes.

● Keep Alive: Redial Period 30 Seconds.

Figure 5-5: PPTP

Server IP Address. This is the IP address that the Router has, 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 external 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 Default Gateway Address.

User Name and Password. Enter the User Name and Password provided by your ISP.

Connect on Demand and Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specific 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 Connect on Demand, click the radio button. If you want your Internet connection to remain on at all times, enter **0** in the *Max Idle Time* field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

Keep Alive and Redial Period. This option keeps your Internet access connected indefinitely, even when it sits idle. If you select this option, the Router will periodically check your Internet connection. If the connection is down, then the Router will automatically re-establish the connection. To use this option, click the radio button next to *Keep Alive*. The default Redial Period is **30** seconds.

Click the **Save Settings** button. Then click the **Status** tab, and click the **Connect** button.

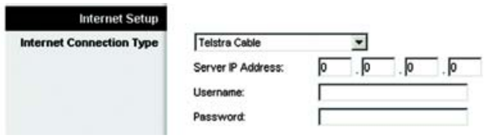
Telstra Cable

Telstra Cable is a service used in Australia only. Check with your ISP for the necessary setup information.

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

User Name and Password. Enter the User Name and Password provided by your ISP.

Click the **Save Settings** button. Then click the **Status** tab, and click the **Connect** button.



Internet Setup

Internet Connection Type: Telstra Cable

Server IP Address: 0 . 0 . 0 . 0

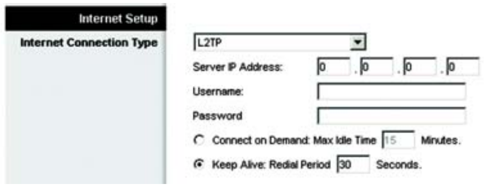
Username:

Password:

Figure 5-6: Telstra Cable

L2TP

Layer 2 Tunneling Protocol (L2TP) is a service that tunnels Point-to-Point Protocol (PPP) across the Internet. It is used mostly in European countries. Check with your ISP for the necessary setup information.



Internet Setup

Internet Connection Type: L2TP

Server IP Address: 0 . 0 . 0 . 0

Username:

Password

○ Connect on Demand: Max Idle Time 15 Minutes.

● Keep Alive: Redial Period 30 Seconds.

Figure 5-7: L2TP

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

User Name and Password. Enter the User Name and Password provided by your ISP.

Connect on Demand and Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specific 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 Connect on Demand, click the radio button. If you want your Internet connection to remain on at all times, enter **0** in the *Max Idle Time* field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

Keep Alive and Redial Period. This option keeps your Internet access connected indefinitely, even when it sits idle. If you select this option, the Router will periodically check your Internet connection. If the connection is down, then the Router will automatically re-establish the connection. To use this option, click the radio button next to *Keep Alive*. The default Redial Period is **30** seconds.

***packet**: a unit of data sent over a network.*

Click the **Save Settings** button. Then click the **Status** tab, and click the **Connect** button.

Optional Settings

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

Host Name and Domain Name. Some 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. The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. To manually set a value, select **Manual** and enter the value desired in the *Size* field. You should leave this value in the 1200 to 1500 range. Most DSL users should use the value 1492. The default is **Auto**, which allows the Router to select the best MTU for your Internet connection.

Network Setup

The Network Setup section allows you to change the Router's local network settings.

Router IP

The Router's Local IP Address and Subnet Mask are shown here. In most cases, you should keep the defaults.

Local IP Address. The default value is **192.168.1.1**.

Subnet Mask. The default value is **255.255.255.0**.

DHCP Server Setting

The Router can be used as a Dynamic Host Configuration Protocol (DHCP) server for your network. A DHCP server automatically assigns an IP address to each computer on your network. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server.

DHCP Server. DHCP is enabled by factory default. If you already have a DHCP server on your network, set the Router's DHCP option to **Disabled**. If you disable DHCP, remember to assign a static IP address to the Router.

Start IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the Router is 192.168.1.1, the Start IP Address must be 192.168.1. 2 or greater, but smaller than 192.168.1.254. The default Start IP Address is **192.168.1.100**.

dynamic ip address*: a temporary IP address assigned by a DHCP server.*

Maximum Number of Users (Optional). 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**.

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 dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **0** minutes, which means one day.

Static DNS 1-3. 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. You can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

WINS. The Windows Internet Naming Service (WINS) converts NetBIOS names to IP addresses. If you use a WINS server, enter that server's IP address here. Otherwise, leave this field blank.

DHCP Reservation. Click the **DHCP Reservation** button if you want to assign a fixed local IP address to a MAC address. You will see a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address. Click the **Select** checkbox to reserve a client's IP address. Then click the **Add Clients** button.

If you want 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. Click the **Add** button.

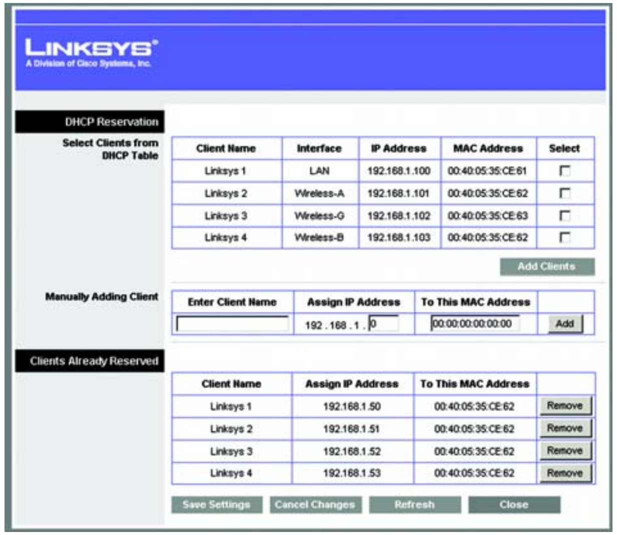
A list of DHCP clients and their fixed local IP addresses will be displayed at the bottom of the screen. If you want to remove a client from this list, click the **Remove** button.

When you have finished your changes, click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel your changes. To view the most up-to-date information, click the **Refresh** button. To exit this screen, click the **Close** button.

Time Setting

Time Zone. Select the time zone in which your network functions. If you want the Router to automatically adjust the clock for daylight savings, then select the checkbox.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



DHCP Reservation

Select Clients from DHCP Table

Client Name	Interface	IP Address	MAC Address	Select
Linksys 1	LAN	192.168.1.100	00:40:05:35:CE:61	□
Linksys 2	Wireless-A	192.168.1.101	00:40:05:35:CE:62	□
Linksys 3	Wireless-G	192.168.1.102	00:40:05:35:CE:63	□
Linksys 4	Wireless-B	192.168.1.103	00:40:05:35:CE:62	□

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	
Linksys 1	192.168.1.50	00:40:05:35:CE:62	Remove
Linksys 2	192.168.1.51	00:40:05:35:CE:62	Remove
Linksys 3	192.168.1.52	00:40:05:35:CE:62	Remove
Linksys 4	192.168.1.53	00:40:05:35:CE:62	Remove

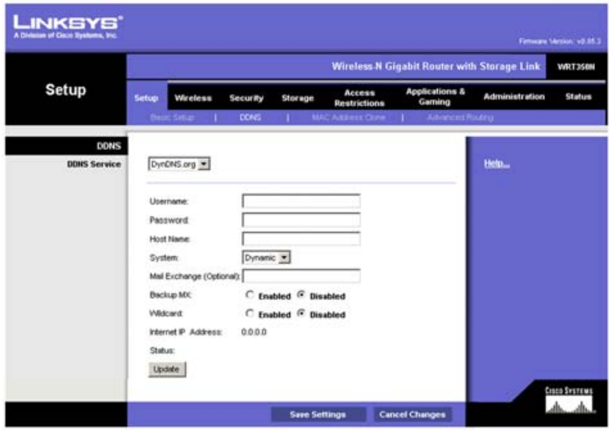
Figure 5-8: DHCP Reservation

NOTE: To test your settings, connect to the Internet now.

The Setup Tab - 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 at one of two DDNS service providers, DynDNS.org or TZO.com. If you do not want to use this feature, keep the default setting, **Disable**.



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:

Figure 5-9: Setup Tab - DynDDNS.org

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

Username, Password, and Host Name. Enter the settings of the account you set up with DynDNS.org.

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

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 enable this feature, keep the default, **Enabled**. To disable the feature, select **Disabled**. If you are not sure which setting to select, keep the default, **Enabled**.

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 enable wildcards, keep the default, **Enabled**. To disable wildcards, select **Disabled**. If you are not sure which setting to select, keep the default, **Enabled**.

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

Update. To manually trigger an update, click this button.

TZO.com

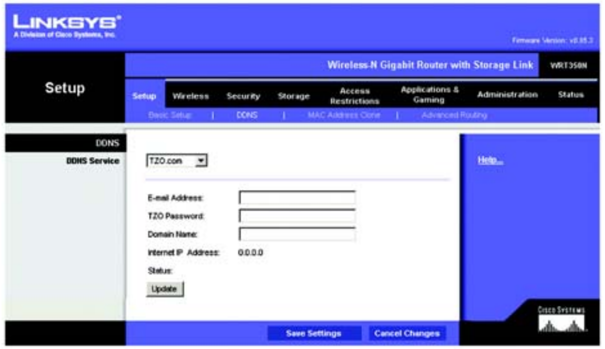
E-mail Address, TZO Password, and Domain Name. Enter the settings of the account you set up with TZO.

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.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



DDNS Service: TZO.com

E-mail Address:

TZO Password:

Domain Name:

Internet IP Address: 0.0.0.0

Status:

Figure 5-10: Setup Tab - TZO.com

The Setup Tab - MAC Address Clone

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification, like a social security number. 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.

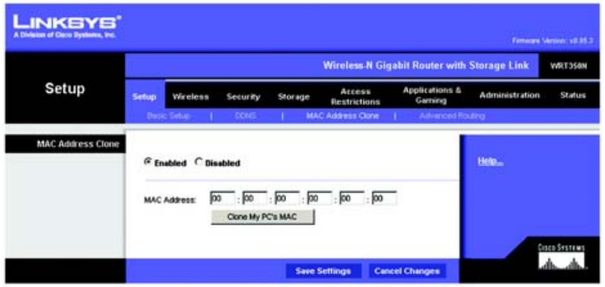
MAC Address Clone

To use MAC address cloning, select **Enabled**. Otherwise, keep the default, **Disabled**.

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

Clone My PC's MAC. If you want to clone the MAC address of the PC you are currently using to configure the Router, then click this button. The Router will automatically detect your PC's MAC address, so you do NOT have to call your ISP to change the registered MAC address to the Router's MAC address. It is recommended that the PC registered with the ISP is used to open the *MAC Address Clone* screen.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



● Enabled ○ Disabled

MAC Address: 00 : 00 : 00 : 00 : 00 : 00

Figure 5-11: Setup Tab - MAC Clone

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

The Setup Tab - Advanced Routing

The *Advanced Routing* screen allows you to configure the dynamic and static routing settings.

Advanced Routing

NAT

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

Dynamic Routing

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. To use dynamic routing, select **Enabled**. Otherwise, select **Disabled**. When the NAT setting is disabled, dynamic routing will be enabled.

Static Routing

A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Use this feature to set up a static route between the Router and another network (you can have up to 20 static routes). To create a static route, alter the following settings:

Route Entries. Select the number of the static route from the drop-down menu.

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

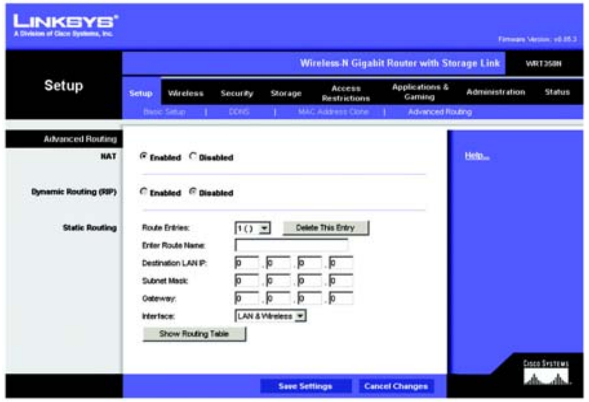
Destination LAN IP. The Destination LAN IP Address is the address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route.

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

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

Interface. Select **LAN & Wireless** or **WAN (Internet)**, depending on the location of the final destination.

Delete This Entry. To delete a route, select its number from the drop-down menu, and click this button.



NAT ● Enabled ○ Disabled

Dynamic Routing (RIP) ○ Enabled ● Disabled

Static Routing

Route Entries: 1 ( )

Enter Route Name:

Destination LAN IP: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

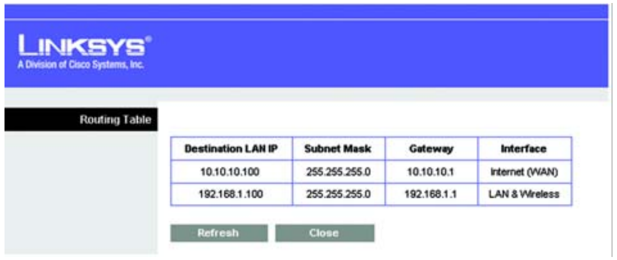
Gateway: 0 . 0 . 0 . 0

Interface: LAN & Wireless

Figure 5-12: Setup Tab - Advanced Routing

Show Routing Table. Click the **Show Routing Table** button to open a screen displaying how data is routed through your local network. For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click the **Refresh** button to update the information. Click the **Close** button to exit this screen.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



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

Figure 5-13: Routing Table

The Wireless Tab - Basic Wireless Settings

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

Basic Wireless Settings

Network Mode. If you have wireless devices in your network, keep the default setting, **Mixed**. If you do not have any wireless devices in your network, select **Disable**.

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.

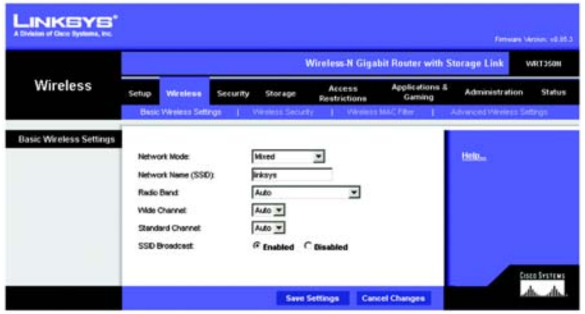
Radio Band. For best performance in a network using Wireless-N, Wireless-G and Wireless-B devices, keep the default, **Wide - 40MHz Channel**. For Wireless-G and Wireless-B networking only, select **Standard - 20MHz Channel**.

Wide Channel. If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N channel. Select any channel from the drop-down menu.

Standard Channel. Select the channel for Wireless-N, Wireless-G, and Wireless-B networking. If you selected Wide – 40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N. If you are not sure which channel to select, keep the default, **Auto**.

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 setting, **Enabled**. If you do not want to broadcast the Router's SSID, then select **Disabled**.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.


LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: v0.85.3
Wireless-N Gigabit Router with Storage Link
WRT350N
Wireless
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Help...
Save Settings
Cancel Changes
Cisco Systems

Basic Wireless Settings

Network Mode: Mixed

Network Name (SSID): linksys

Radio Band: Auto

Wide Channel: Auto

Standard Channel: Auto

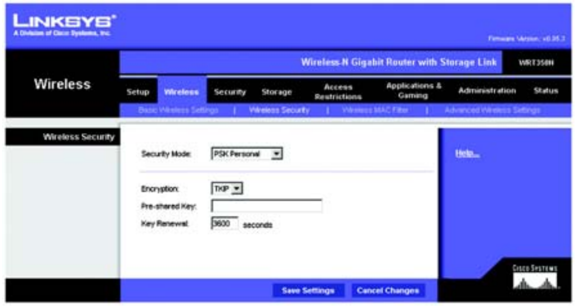
SSID Broadcast: ● Enabled ○ Disabled

Figure 5-14: Wireless Tab - Basic Wireless Settings

NOTE: If you select Wide - 40MHz Channel for the Radio Band setting, then Wireless-N can use two channels: a primary one (Wide Channel) and a secondary one (Standard Channel). This will enhance Wireless-N performance.

The Wireless Tab - Wireless Security

These settings configure the security of your wireless network. There are six wireless security modes supported by the Router: PSK-Personal, PSK2-Personal, PSK-Enterprise, PSK2-Enterprise, RADIUS, and WEP. (PSK stands for Pre-Shared Key, which is stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) For details on configuring wireless security for the Router, turn to "Appendix B: Wireless Security." If you do not want to use wireless security, select **Disabled**.



Security Mode: PSK Personal

Encryption: TKIP

Pre-shared Key:

Key Renewal: 3600 seconds

Figure 5-15: Wireless Tab - Wireless Security (PSK-Personal)

Wireless Security

Security Mode. Select the mode you want to use: **PSK-Personal**, **PSK2-Personal**, **PSK-Enterprise**, **PSK2-Enterprise**, **RADIUS**, or **WEP**. PSK2 is a more advanced, more secure version of PSK.

Follow the instructions for the security method you want to use.

PSK-Personal

Encryption. Select the algorithm you want to use, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

Pre-shared Key. Enter the key shared by the Router and your other network devices. It must have 8-63 characters.

Key Renewal. Enter the Key Renewal period, which tells the Router how often it should change encryption keys.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.

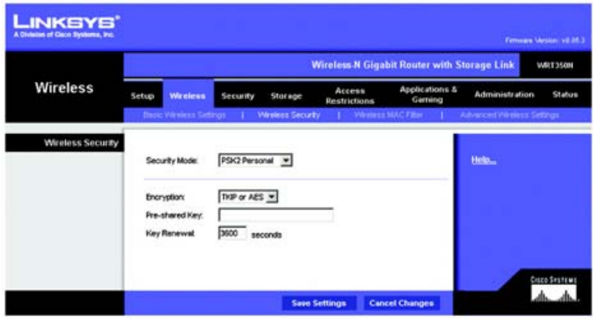
PSK2-Personal

Encryption. Select the algorithm(s) you want to use, **AES** or **TKIP or AES**. (AES is a stronger encryption method than TKIP.)

Pre-shared Key. Enter the key shared by the Router and your other network devices. It must have 8-63 characters.

Key Renewal. Enter the Key Renewal period, which tells the Router how often it should change encryption keys.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



Security Mode: PSK2 Personal

Encryption: TKIP or AES

Pre-shared Key:

Key Renewal: 3600 seconds

Figure 5-16: Wireless Security - PSK2-Personal

PSK-Enterprise

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

Encryption. Select the algorithm(s) you want to use, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

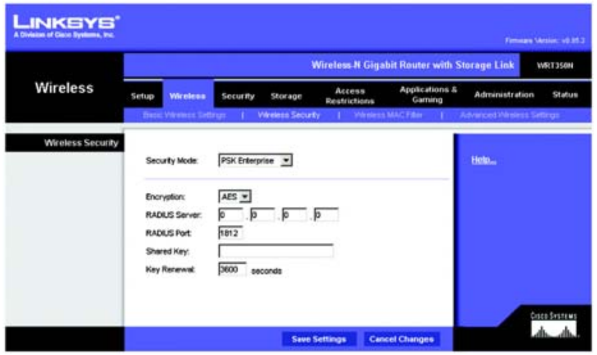
RADIUS Server. Enter the IP address of your RADIUS server.

RADIUS Port. Enter the port number of your RADIUS server.

Shared Key. Enter the key shared by the Router and RADIUS server.

Key Renewal. Enter the Key Renewal period, which tells the Router how often it should change encryption keys.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



Security Mode: PSK Enterprise

Encryption: AES

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Key:

Key Renewal: 3600 seconds

Figure 5-17: Wireless Security - PSK-Enterprise

PSK2-Enterprise

This option features PSK2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

Encryption. Select the algorithm(s) you want to use, **AES** or **TKIP or AES**. (AES is a stronger encryption method than TKIP.)

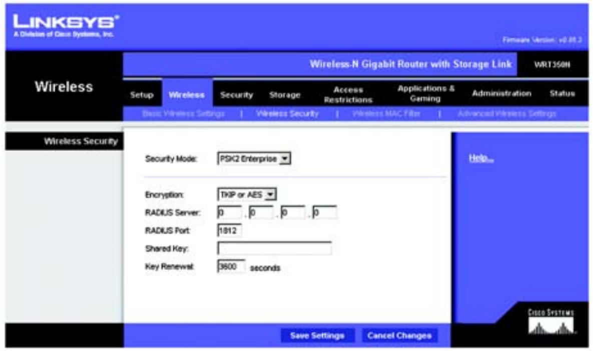
RADIUS Server. Enter the IP address of your RADIUS server.

RADIUS Port. Enter the port number of your RADIUS server.

Shared Key. Enter the key shared by the Router and RADIUS server.

Key Renewal. Enter the Key Renewal period, which tells the Router how often it should change encryption keys.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



Security Mode: PSK2 Enterprise

Encryption: TKIP or AES

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Key:

Key Renewal: 3600 seconds

Figure 5-18: Wireless Security - PSK2-Enterprise

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.)

RADIUS Server. Enter the IP address of your RADIUS server.

RADIUS Port. Enter the port number of your RADIUS server.

Shared Key. Enter the key shared by the Router and RADIUS server.

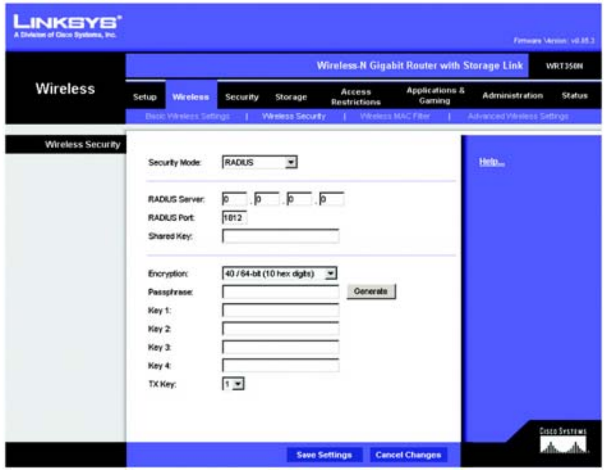
Encryption. Select the appropriate level of encryption, **40/64-bit (10 hex digits)** or **128-bit (26 hex digits)**, which is stronger encryption than 40/64 bit encryption.

Passphrase. To automatically generate keys, enter your passphrase. Then click the **Generate** button.

Key 1-4. If you want to manually enter the WEP keys, then enter them in the *Key 1-4* fields.

TX Key. To indicate which WEP key to use, select a transmit key number.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



Security Mode: RADIUS

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Key:

Encryption: 40 / 64-bit (10 hex digits)

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

TX Key: 1

Figure 5-19: Wireless Security - RADIUS

WEP

WEP is a basic encryption method offering two levels of encryption; 128-bit is stronger than 40/64-bit encryption.

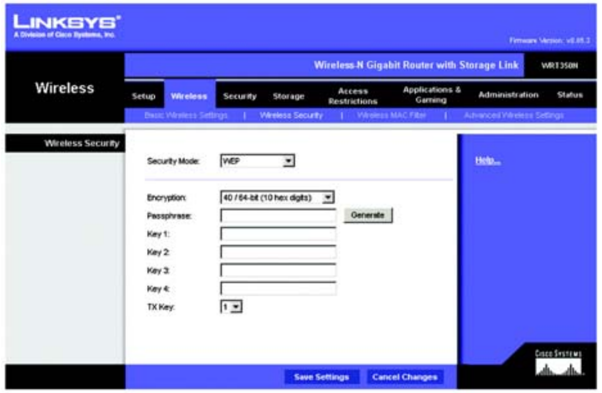
Encryption. Select the appropriate level of encryption, **40/64-bit (10 hex digits)** or **128-bit (26 hex digits)**.

Passphrase. To automatically generate keys, enter your passphrase. Then click the **Generate** button.

Key 1-4. If you want to manually enter the WEP keys, then enter them in the *Key 1-4* fields.

TX Key. To indicate which WEP key to use, select a transmit key number.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



Security Mode: WEP

Encryption: 40 / 64-bit (10 hex digits)

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

TX Key: 1

Figure 5-20: Wireless Security - WEP

The Wireless Tab - 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

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

Access Restrictions

Prevent. Click this button to block wireless access from the devices listed on this screen.

Permit. Click this button to allow wireless access by the devices listed on this screen.

MAC Address Filter List

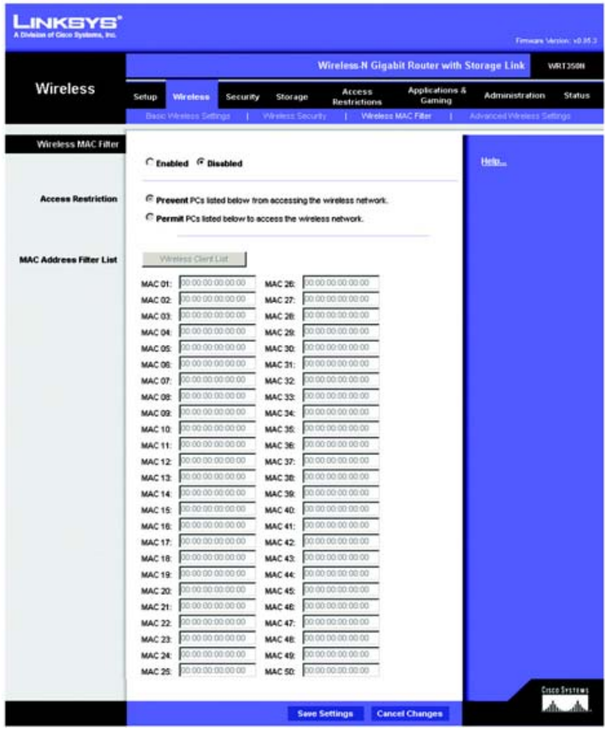
Click the **Wireless Client List** button to display the Wireless Client List. It shows computers and other devices on the wireless network. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Status. Click the **Save to MAC Address Filter List** checkbox for any device you want to add to the MAC Address Filter List. Then click the **Add** button. To retrieve the most up-to-date information, click the **Refresh** button. To exit this screen and return to the *Wireless MAC Filter* screen, click the **Close** button.

Then click the *Enable MAC Filter* checkbox for any device you want to add to the MAC Address Filter List. To update the information on this list, click the **Refresh** button. When you have finished making changes to the *Wireless Client MAC List* screen, click the **Update Filter List** button to save the changes. Click the **Close** button to return to the *Wireless MAC Filter* screen.

When you have finished making changes to the *MAC Address Filter List* screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes.

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

When you have finished making changes to the *Wireless MAC Filter* screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.


LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: v0.95.3
Wireless-N Gigabit Router with Storage Link
WRT350N
Wireless
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Help...
Cisco Systems

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.

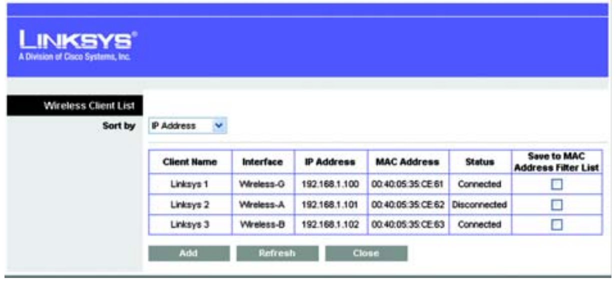
MAC Address Filter List

Wireless Client List

MAC 01:	00:00:00:00:00:00	MAC 26:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 06:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00
MAC 07:	00:00:00:00:00:00	MAC 32:	00:00:00:00:00:00
MAC 08:	00:00:00:00:00:00	MAC 33:	00:00:00:00:00:00
MAC 09:	00:00:00:00:00:00	MAC 34:	00:00:00:00:00:00
MAC 10:	00:00:00:00:00:00	MAC 35:	00:00:00:00:00:00
MAC 11:	00:00:00:00:00:00	MAC 36:	00:00:00:00:00:00
MAC 12:	00:00:00:00:00:00	MAC 37:	00:00:00:00:00:00
MAC 13:	00:00:00:00:00:00	MAC 38:	00:00:00:00:00:00
MAC 14:	00:00:00:00:00:00	MAC 39:	00:00:00:00:00:00
MAC 15:	00:00:00:00:00:00	MAC 40:	00:00:00:00:00:00
MAC 16:	00:00:00:00:00:00	MAC 41:	00:00:00:00:00:00
MAC 17:	00:00:00:00:00:00	MAC 42:	00:00:00:00:00:00
MAC 18:	00:00:00:00:00:00	MAC 43:	00:00:00:00:00:00
MAC 19:	00:00:00:00:00:00	MAC 44:	00:00:00:00:00:00
MAC 20:	00:00:00:00:00:00	MAC 45:	00:00:00:00:00:00
MAC 21:	00:00:00:00:00:00	MAC 46:	00:00:00:00:00:00
MAC 22:	00:00:00:00:00:00	MAC 47:	00:00:00:00:00:00
MAC 23:	00:00:00:00:00:00	MAC 48:	00:00:00:00:00:00
MAC 24:	00:00:00:00:00:00	MAC 49:	00:00:00:00:00:00
MAC 25:	00:00:00:00:00:00	MAC 50:	00:00:00:00:00:00

Save Settings Cancel Changes

Figure 5-21: Wireless Tab - Wireless MAC Filter



Wireless Client List

Sort by: IP Address

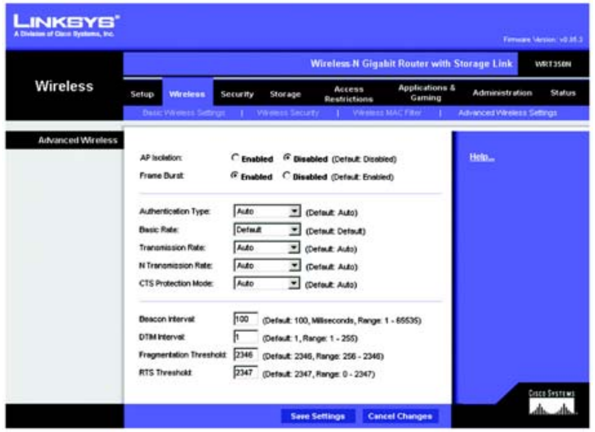
Client Name	Interface	IP Address	MAC Address	Status	Save to MAC Address Filter List
Linksys 1	Wireless-G	192.168.1.100	00:40:05:35:CE:61	Connected	□
Linksys 2	Wireless-A	192.168.1.101	00:40:05:35:CE:62	Disconnected	□
Linksys 3	Wireless-B	192.168.1.102	00:40:05:35:CE:63	Connected	□

Add Refresh Close

Figure 5-22: Wireless Client List

The Wireless Tab - Advanced Wireless Settings

This tab 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.


LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: v0.95.3
Wireless
Wireless-N Gigabit Router with Storage Link
WRT350N
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Advanced Wireless
Help...
Save Settings
Cancel Changes
Cisco Systems

AP Isolation: ○ Enabled ● Disabled (Default: Disabled)
Frame Burst: ● Enabled ○ Disabled (Default: Enabled)

Authentication Type: Auto (Default: Auto)
Basic Rate: Default (Default: Default)
Transmission Rate: Auto (Default: Auto)
N Transmission Rate: Auto (Default: Auto)
CTS Protection Mode: Auto (Default: Auto)

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)

Figure 5-23: Wireless Tab - 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, click **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. If you are not sure how to use this option, keep the default, **Disable**.

Authentication Type. The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. Select **Shared Key** if you only want to use 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.

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 setting is **Auto**.

N Transmission Rate. The rate of data transmission should be set depending on the speed of your Wireless-N networking. 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 setting is **Auto**.

CTS Protection Mode. CTS (Clear-To-Send) Protection Mode’s default setting is **Auto**. The Router will automatically use CTS 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.

Beacon Interval. Enter a value between 20-1000 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 value 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 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, **2346**, 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. In most cases, keep its default value of **2346**.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.

The Security Tab - Firewall

The *Firewall* screen offers a firewall and filters that block specific Internet data types.

Firewall

Firewall Protection. A firewall enhances network security and uses Stateful Packet Inspection (SPI) for more detailed review of data packets entering your network. Select **Enabled** to use a firewall, or **Disabled** to disable it.

Internet Filter

Filter Anonymous Internet Requests. When enabled, this feature keeps your network from being "pinged," or detected, by other Internet users. It also hides your network ports. Both make it more difficult for outside users to enter your network. This filter is enabled by default. Select **Disabled** 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 **Enabled** to filter multicasting, or **Disabled** to disable this feature.

Filter Internet NAT Redirection. This feature uses port forwarding to block access to local servers from local networked computers. Select **Enabled** to filter Internet NAT redirection, or **Disabled** to disable this feature.

Filter IDENT (Port 113). This feature keeps port 113 from being scanned by devices outside of your local network. Select **Enabled** to filter port 113, or **Disabled** to disable this feature.

Web Filter

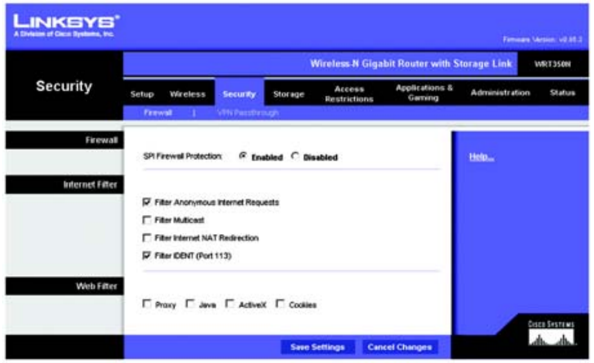
Proxy. Use of WAN proxy servers may compromise the Gateway's security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click the checkbox.

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. To enable Java filtering, click the checkbox.

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. To enable ActiveX filtering, click the checkbox.

Cookies. A cookie is data stored on your computer and used by Internet sites when you interact with them. To enable cookie filtering, click the checkbox.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



SPI Firewall Protection: ● Enabled ○ Disabled

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

☐ Proxy ☐ Java ☐ ActiveX ☐ Cookies

Figure 5-24: Security Tab - Firewall

The Security Tab - VPN Passthrough

The *VPN Passthrough* screen allows you to allow VPN tunnels using IPSec, L2TP, or PPTP protocols to pass through the Router.

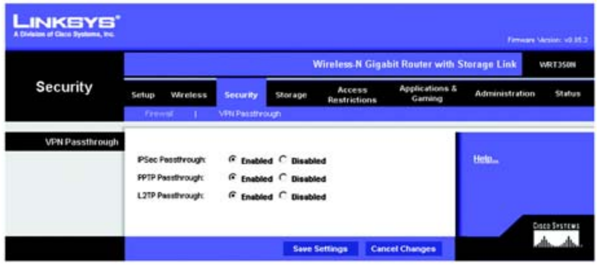
VPN Passthrough

IPSec Passthrough. IPSec (Internet Protocol Security) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec Passthrough, click the **Enabled** button. To disable IPSec Passthrough, click the **Disabled** button.

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, click the **Enabled** button. To disable L2TP Passthrough, click the **Disabled** button.

PPTP Passthrough. PPTP (Point-to-Point Tunneling Protocol) Passthrough allows the Point-to-Point (PPP) to be tunneled through an IP network. To allow PPTP Passthrough, click the **Enabled** button. To disable PPTP Passthrough, click the **Disabled** button.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



IPSec Passthrough: ● Enabled ○ Disabled
PPTP Passthrough: ● Enabled ○ Disabled
L2TP Passthrough: ● Enabled ○ Disabled

Figure 5-25: VPN Passthrough

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

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

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

The Storage Tab - Disk

You can attach a USB flash drive or hard disk to the Router. The *Disk* screen describes the disk currently attached to the Router. Using this screen, you can format a blank disk, safely remove a disk, or erase a disk.

Disk Management

Disk Detail

If a blank disk is attached to the Router, the Disk, Make and Model, and Physical Size columns describe the disk.

Claim. For a blank disk, click the **Claim** button to create a partition that will be formatted as FAT32. On the *Claim Disk* screen, enter a name for the partition. Click the **Claim** button to save the new name, or click the **Clear** button to clear the *New Partition Name* field. Click the **Cancel** button to cancel the changes.

Safely Remove. Before physically disconnecting a disk from the Router, click the **Safely Remove** button first. This ensures that the disk is not removed while data is being transferred to or from the disk; otherwise, data may be lost.

If a formatted disk is attached to the Router, the Partition, File System, Total Space, and Free Space columns describe the partition(s) of the disk.

Create Share. Shares control access to the partition(s) of the disk. To create shares, click the **Create Share** button. Proceed to the next page for descriptions of the *Share* screen.

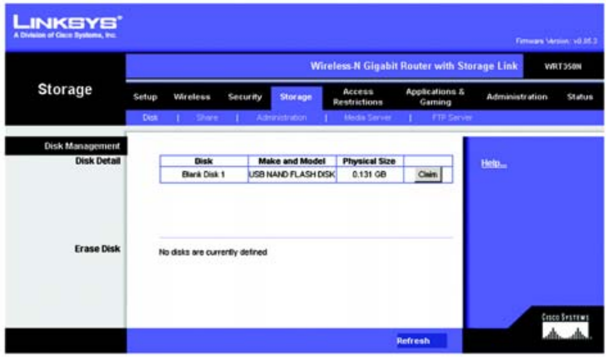
Erase Disk

To erase a disk, click the checkbox next to the name of the disk.

Quick Erase. To quickly free up space on the disk, click the **Quick Erase** button to remove the table of contents from the disk. (This is less secure than the Full Erase option.)

Full Erase. Click the **Full Erase** button to initiate complete removal of data from the disk. Once the removal is complete, the data cannot be recovered. The Full Erase option is recommended if the disk holds sensitive data.

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


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v0.85.3
Wireless-N Gigabit Router with Storage Link
WRT350N
Storage
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Disk | Share | Administration | Media Server | FTP Server
Help...
Refresh
Cisco Systems

Disk Management

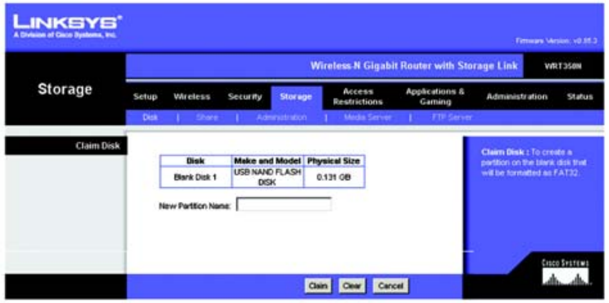
Disk Detail

Disk	Make and Model	Physical Size	
Blank Disk 1	USB NAND FLASH DISK	0.131 GB	Claim

Erase Disk

No disks are currently defined

Figure 5-26: Storage Tab - Disk


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v0.85.3
Wireless-N Gigabit Router with Storage Link
WRT350N
Storage
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Disk | Share | Administration | Media Server | FTP Server
Claim
Clear
Cancel
Cisco Systems

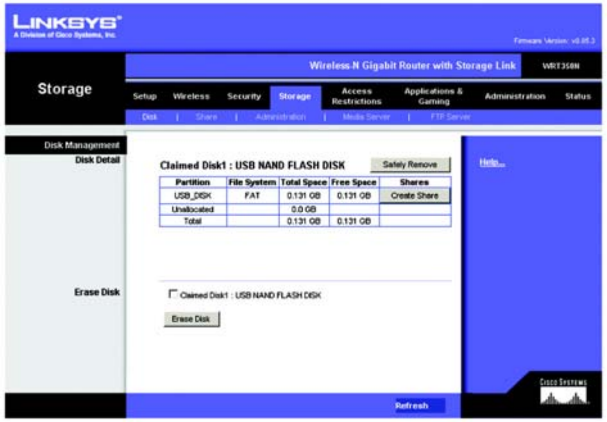
Claim Disk

Disk	Make and Model	Physical Size
Blank Disk 1	USB NAND FLASH DISK	0.131 GB

New Partition Name:

Claim Disk : To create a partition on the blank disk that will be formatted as FAT32.

Figure 5-27: Storage Tab - Claim Disk


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v0.85.3
Wireless-N Gigabit Router with Storage Link
WRT350N
Storage
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Disk | Share | Administration | Media Server | FTP Server
Help...
Refresh
Cisco Systems

Disk Management

Disk Detail

Claimed Disk1 : USB NAND FLASH DISK — Safely Remove

Partition	File System	Total Space	Free Space	Shares
USB_DISK	FAT	0.131 GB	0.131 GB	Create Share
Unallocated		0.0 GB		
Total		0.131 GB	0.131 GB	

Erase Disk

□ Claimed Disk1 : USB NAND FLASH DISK

Erase Disk

Figure 5-28: Storage Tab - Claimed Disk

The Storage Tab - Share

Shares control access to the partition(s) of the disk attached to the Router. The *Share* screen describes the current shares. Using this screen, you can create new shares, modify share properties, or delete shares.

Share Management

Shares

The Share Name, Partition, and Total Space columns describe the shares.

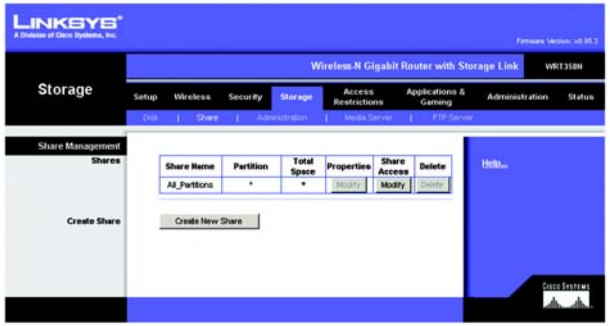
Properties - Modify. Click the **Modify** button to change the properties of a share. On the *Share Properties* screen, enter a different name for the share, and/or select a different partition from the *Resides in Partition* drop-down menu. Click the **Create Share** button to save the new properties, or click the **Clear** button to clear the changes. Click the **Cancel** button to cancel the changes.

Share Access - Modify. Click the **Modify** button to change the access privileges of a share. On the *Share Access* screen, groups with no access are listed in the Other Group column, and groups with access are listed in the Group with Access column. To give a group read-only access, select the group, and click the **>> Read Only** button. To give a group read/write access, select the group, and click the **>> Read/Write** button. To strip a group of its current access privileges, select the group, and click the **<< Remove** button. Click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to cancel the changes. Click the **Close** button to exit the *Share Access* screen.

Delete. Click the **Delete** button to remove a share.

Create Share

Create New Share. Click the **Create New Share** button to create a new share. On the *Share Properties* screen, enter a name for the share, and select a partition from the *Resides in Partition* drop-down menu. Click the **Create Share** button to save the new properties, or click the **Clear** button to clear the changes. Click the **Cancel** button to cancel the changes.



Share Name	Partition	Total Space	Properties	Share Access	Delete
All_Partitions	*	*	Modify	Modify	Delete

Figure 5-29: Storage Tab - Share Management

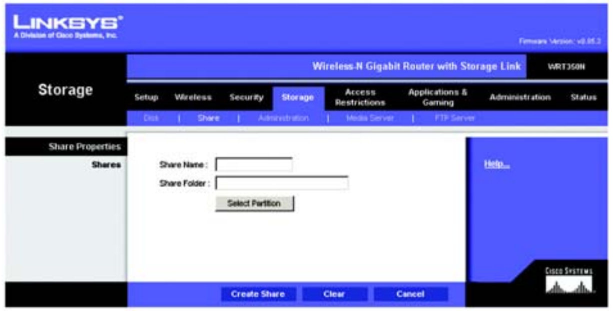


Figure 5-30: Share Properties

The Storage Tab - Administration

The *Administration* screen allows you to manage the users and groups of users that can access the shares.

Basic

Machine Name. Enter a name for the Router. Punctuation and other special characters (e.g., * / I \) cannot be used in the name.

Workgroup Name. Enter the Workgroup Name of your networked computers.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.

User Management

The users are listed in the User Management table. There are two default users, admin (read/write access) and guest (read-only access); these cannot be deleted.

Properties - Modify. Click the **Modify** button to change the properties of a user. On the *User Properties* screen, enter a different name for the user, change the password, and/or select a different group from the *Group* drop-down menu. Click the **Create User** button to save the new properties, or click the **Clear** button to clear the changes. Click the **Cancel** button to cancel the changes.

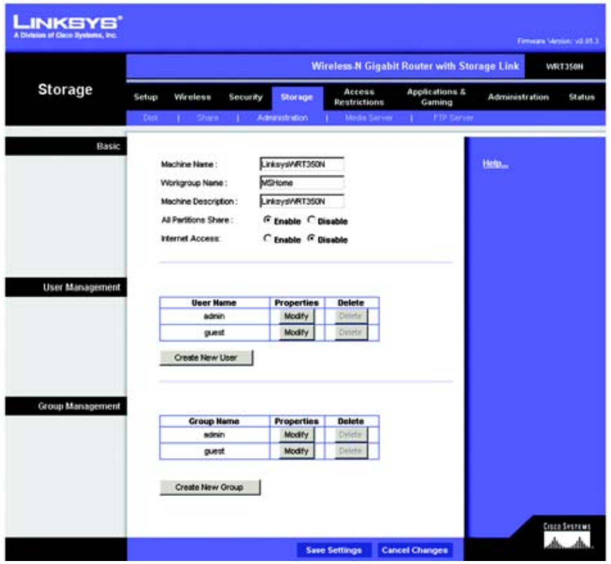
Delete. Click the **Delete** button to remove a user.

Create New User. Click the **Create New User** button to create a new user. On the *User Properties* screen, enter a name for the user. Then enter a password and enter it again in the *Re-enter to confirm* field. Select a group from the *Group* drop-down menu. Click the **Create User** button to save the new properties, or click the **Clear** button to clear the changes. Click the **Cancel** button to cancel the changes.

Group Management

The groups are listed in the Group Management table. There are two default groups, admin and guest; these cannot be deleted.

Properties - Modify. Click the **Modify** button to change the user membership of a group. On the *Group Properties* screen, users who are not members are listed in the Other Users column, and users who are members are listed in the Users in Group column. To add a user to the group, select the user, and click the **>> Join Group** button. To remove a user from the group, select the user, and click the **<< Remove** button. Click the **Save**

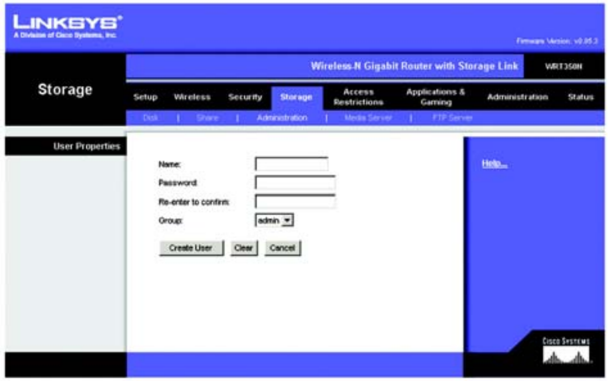


Machine Name : LinksysWRT350N
Workgroup Name : MSHome
Machine Description : LinksysWRT350N
All Partitions Share : ● Enable ○ Disable
Internet Access: ○ Enable ● Disable

User Name	Properties	Delete
admin	Modify	Delete
guest	Modify	Delete

Group Name	Properties	Delete
admin	Modify	Delete
guest	Modify	Delete

Figure 5-31: Storage Tab - Administration



Name:
Password:
Re-enter to confirm:
Group: admin

Figure 5-32: User Properties

Settings button to save the changes, or click the **Cancel Changes** button to cancel the changes. Click the **Close** button to exit the *Group Properties* screen.

Delete. Click the **Delete** button to remove a user.

Create New Group. Click the **Create New Group** button to create a new group. On the *Group Properties* screen, enter a name for the group. Click the **Create Group** button to save the new name, or click the **Clear** button to clear the change. Click the **Cancel** button to cancel the change.

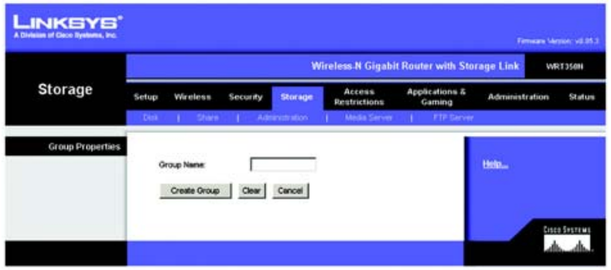


Figure 5-33: User Properties

The Storage Tab - Media Server

The Router has a built-in media server, so it can stream music, pictures, or video from the USB hard disk to a UPnP-compatible media adapter. The *Media Server* screen lets you select shares to scan for content.

UPnP Media Server

Setup

Server Name. The name of the Router is displayed here.

UPnP Media Server. To use the Router's media server function, select **Enable**. Otherwise, select **Disable**.

Database

Select content to add to the database of the Router's media server.

Scan All Partitions. Click this button to scan all partitions of the USB hard disk for content.

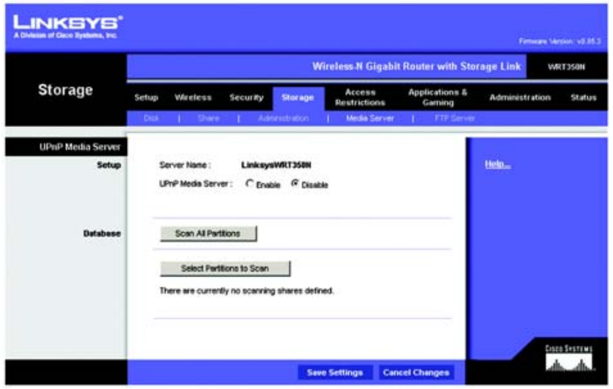
Select Partitions to Scan. Click this button to select specific partitions to scan for content.

The Partition and Folder columns describe the partitions of the USB hard disk.

Scan. Click the **Scan** button to scan a specific partition for content. The *Partition List* screen will appear. Click the **Select** button to select a partition for scanning. Click the **Up List** button to move up one level in the file structure. Click the **Refresh** button to update the on-screen information. Click the **Close** button to exit the *Partition List* screen.

Delete. Click the **Delete** button to delete a specific partition from the Router's database.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.

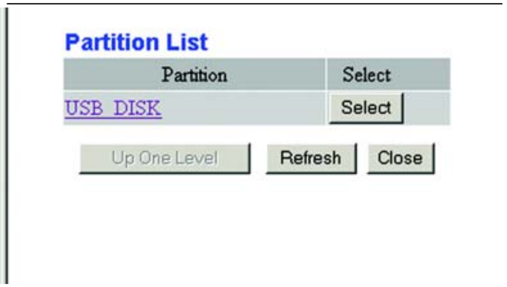


Server Name : LinksysWRT350N

UPnP Media Server : ○ Enable ● Disable

There are currently no scanning shares defined.

Figure 5-34: Storage Tab - UPnP Media Server



Partition	Select
USB_DISK	Select

Figure 5-35: Partition List

FTP Server

The FTP Server tab creates an FTP Server that can be accessed from the Internet or your local network.

Setup

Server Name. The name of the Router is displayed here.

FTP Server. Select **Enable** to set this Router as an FTP Server. Otherwise, select **Disable** to turn the service off. (Note: A USB drive or USB disk must be connected to the USB Port to use this service.)

Internet Access. Select **Enable** to allow access of the FTP Server from the Internet. Otherwise select **Disable** to only allow local network access.

Port. Select the Port service to use. The default port is 21.

Share

Select the partition or folder to share in the FTP Server.

All Partitions. Selects all partitions on the USB disk.

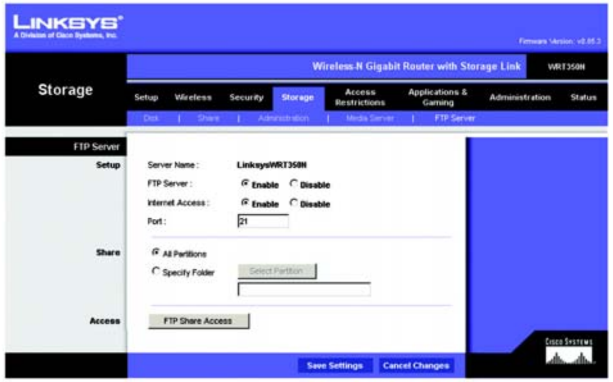
Specify Folder. If you want to share a specific folder, click **Select Partition** and locate the folder.

Access

Click **FTP Share Access** to grant specific rights to groups. You can grant Read Only or Read/Write permissions.

FTP Access. Select the group from the Other Group list and click either the Read Only or Read/Write button to move the group to the Group With Access column.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes. Click **Close** to exit this window.



Server Name : LinksysWRT350N

FTP Server : ● Enable ○ Disable

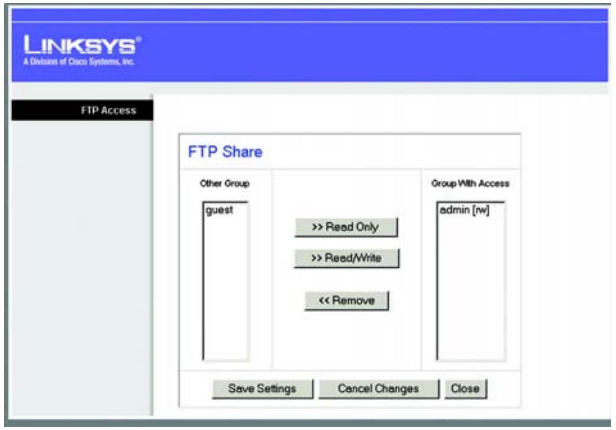
Internet Access : ● Enable ○ Disable

Port : 21

● All Partitions

○ Specify Folder

Figure 5-36: FTP Server



Other Group: guest

Group With Access: admin [rw]

Figure 5-37: FTP Access

The Access Restrictions Tab - Internet Access Policy

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

Internet Access Policy

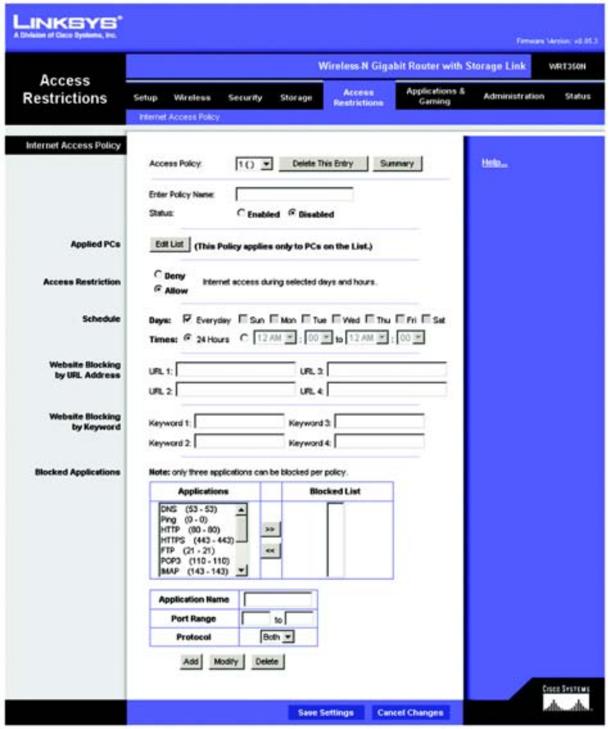
Access Policy. Access can be managed by a policy. Use the settings on this screen to establish an access policy (after the **Save Settings** button is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click the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

On the *Summary* screen, the policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled). To enable a policy, click the **Enabled** checkbox. To delete a policy, click its **Delete** button. Click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to cancel your changes. To return to the *Internet Access Policy* screen, click the **Close** button.

Status. Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and click the radio button beside *Enabled*.

To create a policy:

1. Select a number from the *Access Policy* drop-down menu.
2. Enter a Policy Name in the field provided.
3. To enable this policy, click the radio button beside *Enabled*.
4. Click the **Edit List** button to select which PCs will be affected by the policy. The *List of PCs* screen will appear. You can select a PC by MAC address or IP address. You can also enter a range of IP addresses if you want this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.
5. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.
6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.



Access Policy: 1 ()

Enter Policy Name:

Status: ○ Enabled ● Disabled

Applied PCs: (This Policy applies only to PCs on the List.)

Access Restriction: ○ Deny ● Allow Internet access during selected days and hours.

Schedule

Days: ☑ Everyday □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Times: ● 24 Hours ○ 12 AM : 00 to 12 AM : 00

Website Blocking by URL Address: URL 1: URL 2: URL 3: URL 4:

Website Blocking by Keyword: Keyword 1: Keyword 2: Keyword 3: Keyword 4:

Blocked Applications

Note: only three applications can be blocked per policy.

Applications:
DNS (53 - 53)
Ping (0 - 0)
HTTP (80 - 80)
HTTPS (443 - 443)
FTP (21 - 21)
POP3 (110 - 110)
IMAP (143 - 143)

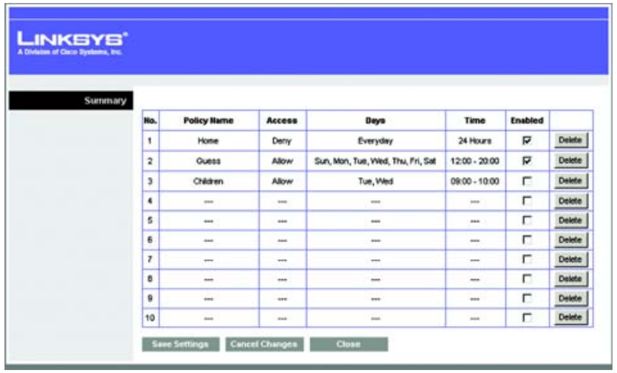
Blocked List

Application Name:

Port Range: to

Protocol: Both

Figure 5-38: Access Restrictions Tab - Internet Access Policy



No.	Policy Name	Access	Days	Time	Enabled	
1	Home	Deny	Everyday	24 Hours	☑	Delete
2	Guess	Allow	Sun, Mon, Tue, Wed, Thu, Fri, Sat	12:00 - 20:00	☑	Delete
3	Children	Allow	Tue, Wed	09:00 - 10:00	□	Delete
4	---	---	---	---	□	Delete
5	---	---	---	---	□	Delete
6	---	---	---	---	□	Delete
7	---	---	---	---	□	Delete
8	---	---	---	---	□	Delete
9	---	---	---	---	□	Delete
10	---	---	---	---	□	Delete

Figure 5-39: Summary

7. You can block websites with specific URL addresses. Enter each URL in a separate field next to *Website Blocking by URL Address*.

8. You can also block websites using specific keywords. Enter each keyword in a separate field next to *Website Blocking by Keyword*.

9. You can filter access to various services accessed over the Internet, such as FTP or telnet. (You can block up to three applications per policy.)

   From the Applications list, select the application you want to block. Then click the **>>** button to move it to the Blocked List. To remove an application from the Blocked List, select it and click the **<<** button.

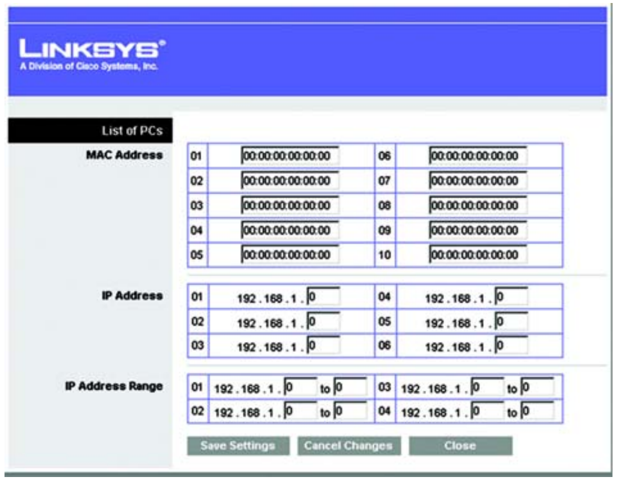
10. If the application you want to block is not listed or you want to edit a service's settings, enter the application's name in the *Application Name* field. Enter its range in the *Port Range* fields. Select its protocol from the *Protocol* drop-down menu. Then click the **Add** button.

    To modify a service, select it from the Application list. Change its name, port range, and/or protocol setting. Then click the **Modify** button.

    To delete a service, select it from the Application list. Then click the **Delete** button.

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

For more information, click **Help**.



List of PCs

MAC Address

01	00:00:00:00:00:00	06	00:00:00:00:00:00
02	00:00:00:00:00:00	07	00:00:00:00:00:00
03	00:00:00:00:00:00	08	00:00:00:00:00:00
04	00:00:00:00:00:00	09	00:00:00:00:00:00
05	00:00:00:00:00:00	10	00:00:00:00:00:00

IP Address

01	192 . 168 . 1 . 0	04	192 . 168 . 1 . 0
02	192 . 168 . 1 . 0	05	192 . 168 . 1 . 0
03	192 . 168 . 1 . 0	06	192 . 168 . 1 . 0

IP Address Range

01	192 . 168 . 1 . 0 to 0	03	192 . 168 . 1 . 0 to 0
02	192 . 168 . 1 . 0 to 0	04	192 . 168 . 1 . 0 to 0

Figure 5-40: List of PCs

The Applications & Gaming Tab - Single Port Forwarding

When you click the Applications & Gaming tab, you will see the *Single Port Forwarding* screen. You can customize port services for common applications on this screen.

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the *Basic Setup* screen).

Single Port Forwarding

Common applications are available for the first five entries. Select the appropriate application. Then enter the IP address of the server that should receive these requests. Click the **Enabled** checkbox to activate this entry.

For additional applications, complete the following fields:

Application Name. Enter the name of the application.

External Port. Enter the external port number used by the server or Internet application. Check with the Internet application documentation for more information.

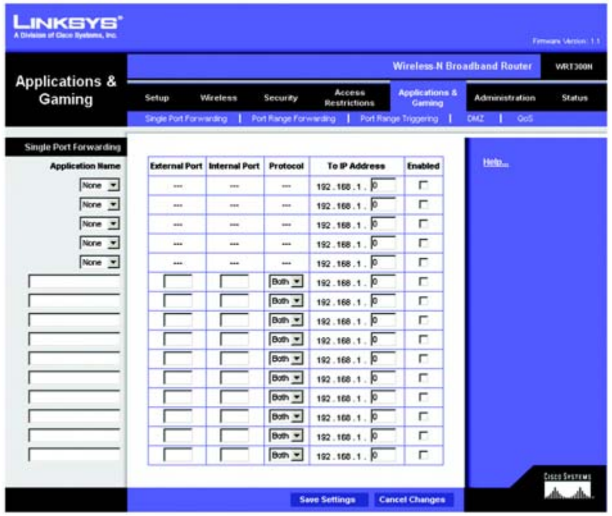
Internal Port. Enter the internal port number used by the server or Internet application. Check with the Internet application documentation for more information.

Protocol. Select the protocol **TCP** or **UDP**, or select **Both**.

To IP Address. Enter the IP address of the server that should receive the requests. To find the IP address, go to “Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter.” If you assigned a static IP address to the server, then you can click the **DHCP Reservation** button on the *Basic Setup* screen to look up its static IP address.

Enabled. Click the **Enabled** checkbox to enable the applications you have defined. This is disabled (unchecked) by default.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



Application Name	External Port	Internal Port	Protocol	To IP Address	Enabled
None	---	---	---	192.168.1. 0	□
None	---	---	---	192.168.1. 0	□
None	---	---	---	192.168.1. 0	□
None	---	---	---	192.168.1. 0	□
None	---	---	---	192.168.1. 0	□
			Both	192.168.1. 0	□
			Both	192.168.1. 0	□
			Both	192.168.1. 0	□
			Both	192.168.1. 0	□
			Both	192.168.1. 0	□
			Both	192.168.1. 0	□
			Both	192.168.1. 0	□
			Both	192.168.1. 0	□
			Both	192.168.1. 0	□
			Both	192.168.1. 0	□

Figure 5-41: Applications & Gaming Tab - Single Port Forwarding

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

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

The Applications & Gaming Tab - Port Range Forwarding

Port range forwarding sets 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.)

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the *Basic Setup* screen).

If you need to forward all ports to one PC, click the **DMZ** tab.

Port Range Forwarding

To add an application, complete the following fields:

Application Name. Enter the name of the application.

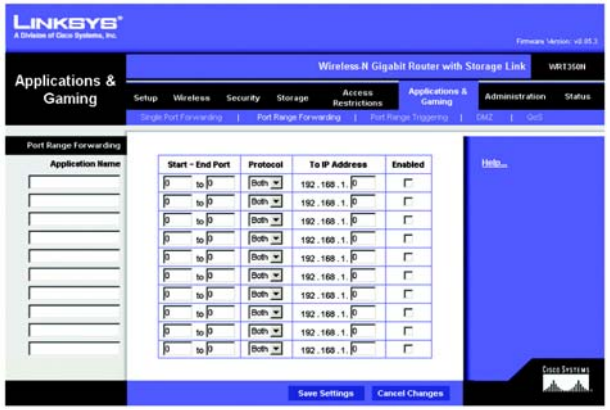
Start ~ End Port. Enter the number or range of port(s) used by the server or Internet application. Check with the Internet application documentation for more information.

Protocol. Select the protocol **TCP** or **UDP**, or select **Both**.

To IP Address. Enter the IP address of the server that you want the Internet users to be able to access. To find the IP address, go to "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter." If you assigned a static IP address to the server, then you can click the **DHCP Reservation** button on the *Basic Setup* screen to look up its static IP address.

Enabled. Click the **Enabled** checkbox to enable the applications you have defined. This is disabled (unchecked) by default.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



Application Name	Start - End Port	Protocol	To IP Address	Enabled
	0 to 0	Both	192 . 168 . 1 . 0	□
	0 to 0	Both	192 . 168 . 1 . 0	□
	0 to 0	Both	192 . 168 . 1 . 0	□
	0 to 0	Both	192 . 168 . 1 . 0	□
	0 to 0	Both	192 . 168 . 1 . 0	□
	0 to 0	Both	192 . 168 . 1 . 0	□
	0 to 0	Both	192 . 168 . 1 . 0	□
	0 to 0	Both	192 . 168 . 1 . 0	□
	0 to 0	Both	192 . 168 . 1 . 0	□
	0 to 0	Both	192 . 168 . 1 . 0	□

Figure 5-42: Applications & Gaming Tab - Port Range Forwarding

The Applications & Gaming Tab - Port Range Triggering

This screen instructs 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 sent to the proper computer by way of IP address and port mapping rules.

Port Range Triggering

To add an application, complete the following fields:

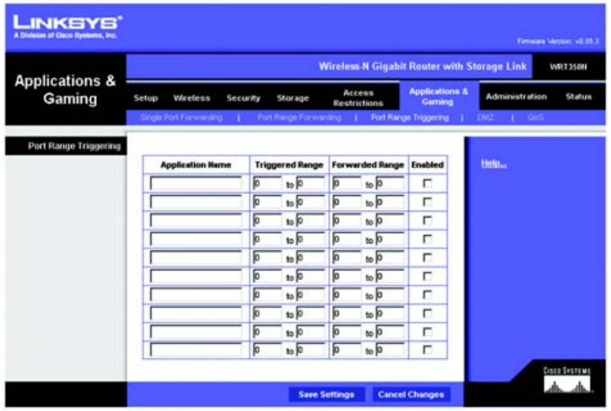
Application Name. Enter the name of the application.

Triggered Range. Enter the starting and ending port numbers of the triggered port range. Check with the Internet application documentation for the port number(s) needed.

Forwarded Range. Enter the starting and ending port numbers of the forwarded port range. Check with the Internet application documentation for the port number(s) needed.

Enabled. Click the **Enabled** checkbox to enable the applications you have defined. This is disabled (unchecked) by default.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



Application Name	Triggered Range	Forwarded Range	Enabled
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□

Figure 5-43: Applications & Gaming Tab - Port Range Triggering

The Applications & Gaming Tab - DMZ

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

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

DMZ

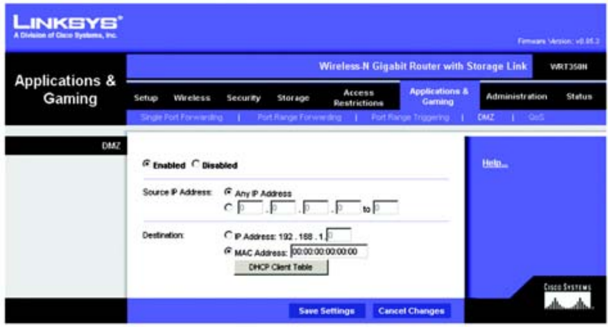
To use this feature, select **Enabled**. To disable DMZ hosting, select **Disabled**.

Source IP Address. If you want any IP address to be the source, select **Any IP Address**. If you want to specify an IP address or range of IP addresses as the designated source, click the second radio button, and enter the IP address(es) in the fields provided.

Destination. If you want to specify the DMZ host by IP address, select **IP Address** and complete the IP address in the field provided. If you want to specify the DMZ host by MAC address, select **MAC Address** and enter the MAC address in the field provided. To retrieve this information, click the **DHCP Client Table** button.

The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Router. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Expired Time (how much time is left for the current IP address). To select a DHCP client, click the **Select** button. To retrieve the most up-to-date information, click the **Refresh** button. To exit this screen and return to the *DMZ* screen, click the **Close** button.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.

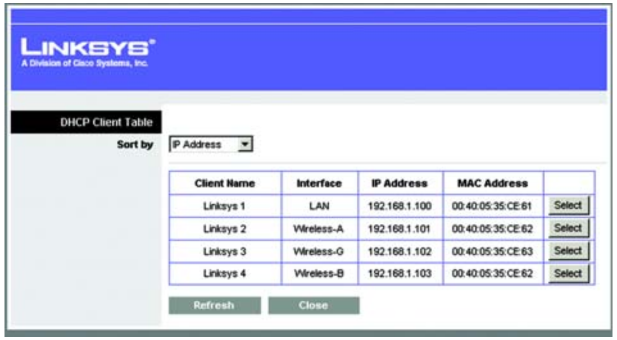


● Enabled ○ Disabled

Source IP Address: ● Any IP Address
○ 0 . 0 . 0 . 0 to 0

Destination: ○ IP Address: 192 . 168 . 1. 0
● MAC Address: 00:00:00:00:00:00

Figure 5-44: Applications & Gaming Tab - DMZ



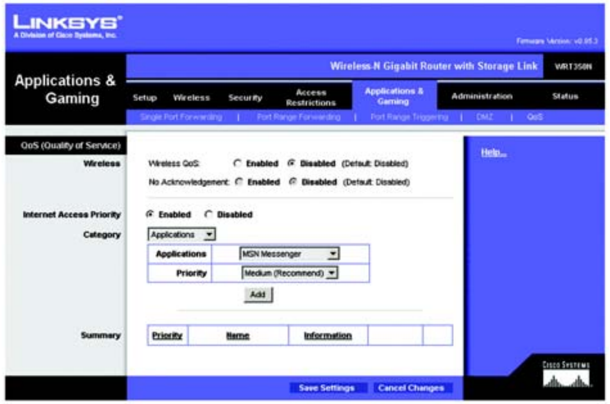
Sort by IP Address

Client Name	Interface	IP Address	MAC Address	
Linksys 1	LAN	192.168.1.100	00:40:05:35:CE:61	Select
Linksys 2	Wireless-A	192.168.1.101	00:40:05:35:CE:62	Select
Linksys 3	Wireless-G	192.168.1.102	00:40:05:35:CE:63	Select
Linksys 4	Wireless-B	192.168.1.103	00:40:05:35:CE:62	Select

Figure 5-45: DHCP Client Table

The Applications and Gaming Tab - 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.



Wireless

Wireless QoS: ○ Enabled ● Disabled (Default: Disabled)

No Acknowledgement: ○ Enabled ● Disabled (Default: Disabled)

Internet Access Priority: ● Enabled ○ Disabled

Category: Applications

Applications	MSN Messenger
Priority	Medium (Recommend)

Summary

Priority	Name	Information		

Figure 5-46: Applications & Gaming Tab - QoS (Applications)

QoS (Quality of Service)

Wireless

The Router features Wireless QoS. The No Acknowledgement feature is available only when the Wireless QoS Support feature is enabled.

Wireless QoS. If you have other devices on your network that support Wireless QoS, select **Enabled**. Otherwise, keep the default, **Disabled**.

No Acknowledgement. If you want to disable the Router’s Acknowledgement feature, so the Router will not re-send data if an error occurs, then keep the default, **Enabled**. Otherwise, select **Disabled**.

Internet Access Priority

In this section, you can set the bandwidth priority for a variety of applications and devices. There are four levels priority: High, Medium, Normal, or Low. When you set priority, do not set all applications to High, because this will defeat the purpose of allocating the available bandwidth. If you want to select below normal bandwidth, select **Low**. Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority.

Enabled/Disabled. To use the QoS policies you have set, select **Enabled**. Otherwise, select **Disabled**.

Category

There are four categories available. Select one of the following: **Applications**, **Online Games**, **MAC Address**, **Ethernet Port**, or **Voice Device**. Proceed to the instructions for your selection.

Applications

Applications. Select the appropriate application. If you select Add a New Application, follow the Add a New Application instructions.

Priority. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click the **Add** button to save your changes. Your new entry will appear in the Summary list.