USER GUIDE

Simultaneous Dual-N Band Wireless Router

Model: WRT610N

About This Guide

Icon Descriptions

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

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

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

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

Online Resources

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

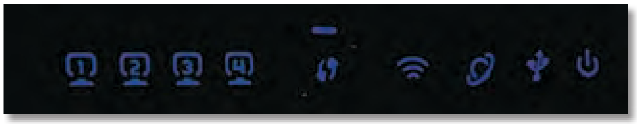
Resource	Website
Linksys	www.linksys.com
Linksys International	www.linksys.com/international
Glossary	www.linksys.com/glossary
Network Security	www.linksys.com/security

Copyright and Trademarks

Chapter 1: Product Overview

Thank you for choosing the Dual-Band Wireless-N Gigabit Router with Storage Link. The Router lets you access the Internet via a wireless connection or through one of its four switched ports. With the built-in storage link, you can easily add gigabytes of storage space onto your network using USB 2.0 hard drives, or plug in a USB flash disk 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. Configuring the Router is easy using the provided browser-based utility.

Front Panel



1, 2, 3, 4 (Green/Blue) These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. A flashing LED indicates network activity over that port. The LED lights up Green when it is connected to 10/100 port and Blue when it is connected to a gigabit port.

Wi-Fi Protected Setup Button If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup to automatically configure wireless security for your wireless network(s).

To use Wi-Fi Protected Setup, run the Linksys Easy Link Advisor (LELA) , or refer to the "Wireless > Basic Wireless Settings" section of "Chapter 3: Advanced Configuration".

Wi-Fi Protected Setup (WPS) LED (Blue/Amber) The LED flashes blue for two minutes during the WPS process and lights up blue when the WPS process is successful.

The LED lights up amber if there is an error during the Wi-Fi Protected Setup process. Make sure the client device supports Wi-Fi Protected Setup. Wait until the LED is off, and then try again.

The LED flashes when a Wi-Fi Protected Setup session is active. The Router supports one session at a time. Wait until the LED is solidly lit, or off before starting the next Wi-Fi Protected Setup session.

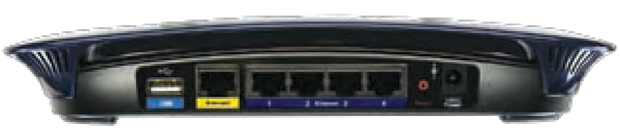
Wireless (Blue) The Wireless LED lights up when the wireless feature is enabled. If the LED is flashing, the Router is actively sending or receiving data over the network.

Internet (Green/Blue) The Internet LED lights up when there is a connection made through the Internet port. A flashing LED indicates network activity over the Internet port. The LED lights up Green when it is connected to 10/100 port and Blue when it is connected to a gigabit port.

USB (Blue) The USB LED lights up when a USB device is attached. If the LED is flashing, the data is being sent or received through this device.

Power (Blue) The Power LED lights up and will stay on while the Router is powered on. When the Router goes through its self-diagnostic mode during every boot-up, this LED will flash. When the diagnostic is complete, the LED will be solidly lit.

Back Panel



USB Port For use with an external hard drive.

Internet The Internet port is where you will connect your cable or DSL Internet connection.

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

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

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

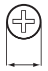
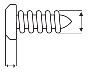
Horizontal Placement

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

Wall-Mounting Placement

The Router has two wall-mount slots on its bottom panel. The distance between the slots is 175.56 mm (6.91 inches).

Two screws are needed to mount the Router.

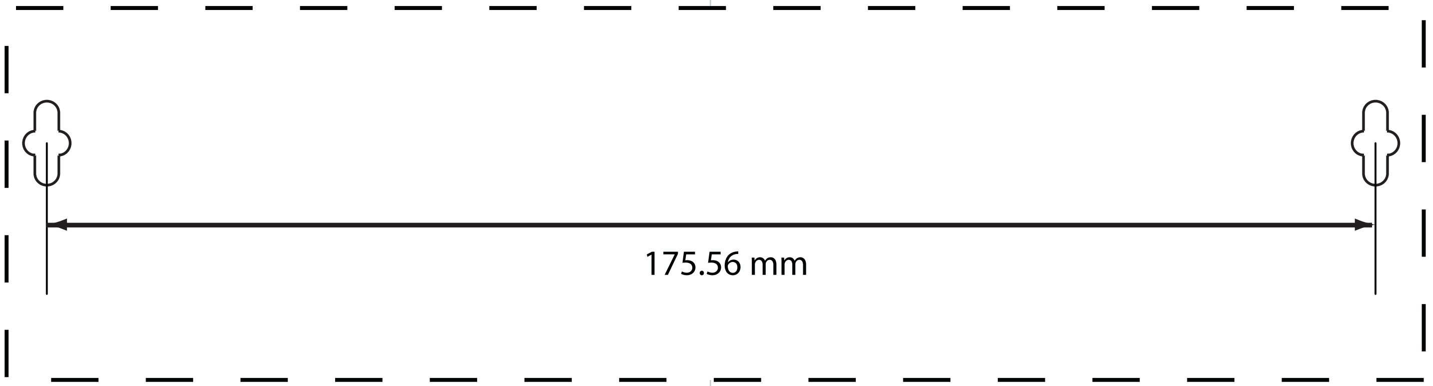
Suggested Mounting Hardware	
 4-5 mm	 1-1.5 mm 2.5-3.0 mm

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

NOTE: Linksys is not responsible for damages incurred by unsecure wall-mounting hardware.

Follow these instructions:

1. Determine where you want to mount the Router. Make sure that the wall you use is smooth, flat, dry, and sturdy. Also make sure the location is within reach of an electrical outlet.
2. Drill two holes into the wall. Make sure the holes are 175.56 mm (6.91 inches) apart.
3. Insert a screw into each hole and leave 3 mm (0.12 inches) of its head exposed.
4. Maneuver the Router so the wall-mount slots line up with the two screws.
5. Place the wall-mount slots over the screws and slide the Router down until the screws fit snugly into the wall-mount slots.



Chapter 2: Wireless Security Checklist

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

1. Change the default wireless network name or SSID

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

2. Change the default password

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

3. Enable MAC address filtering

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

4. Enable encryption

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

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

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

General Network Security Guidelines

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

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

Additional Security Tips

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

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

Chapter 3: Advanced Configuration

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

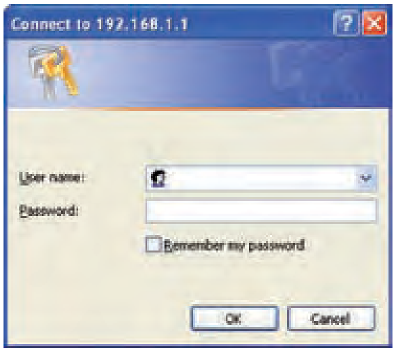
The web-based utility has these main tabs: Setup, Wireless, Security, Storage, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

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

How to Access the Web-Based Utility

To access the web-based utility, launch the web browser on your computer, and enter the Router's default IP address, **192.168.1.1** or **http://wrt160n.com** in the *Address* field. Then, press **Enter**.

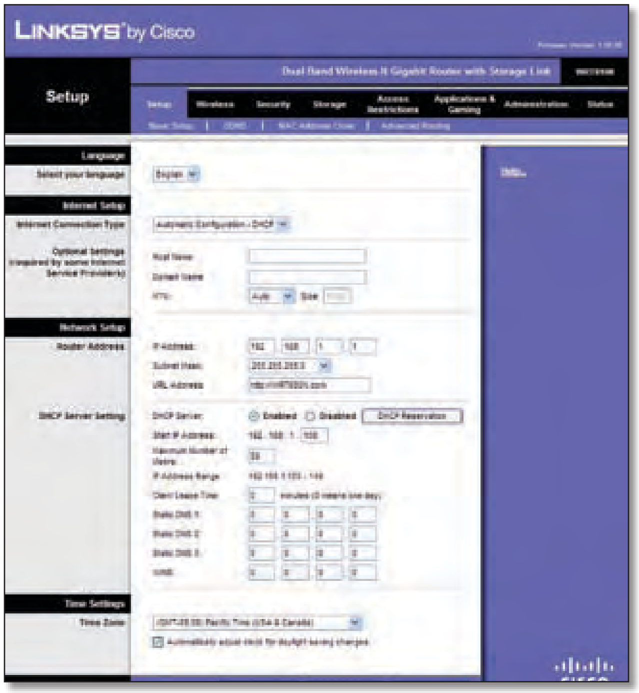
A password request screen will appear. (Non-Windows XP users will see a similar screen.) Leave the *User name* field blank. The first time you open the web-based utility, use the default password **admin**. (You can set a new password on the Administration > Management screen.) Click **OK** to continue.



Password Screen

Setup > Basic Setup

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



Setup > Basic Setup

Language

Language To use a different language, select one from the drop-down menu. The language of the web-based utility will change five seconds after you select another language.

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

Internet Setup

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

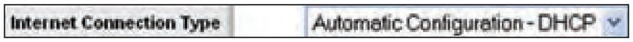
Internet Connection Type

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

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

Automatic Configuration - DHCP

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

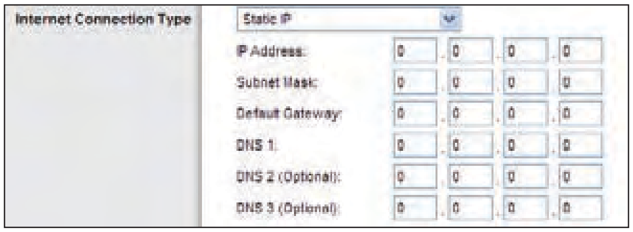


Internet Connection Type: Automatic Configuration - DHCP

Internet Connection Type > Automatic Configuration - DHCP

Static IP

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



Internet Connection Type: Static IP

IP Address:	0	0	0	0
Subnet Mask:	0	0	0	0
Default Gateway:	0	0	0	0
DNS 1:	0	0	0	0
DNS 2 (Optional):	0	0	0	0
DNS 3 (Optional):	0	0	0	0

Internet Connection Type > Static IP

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

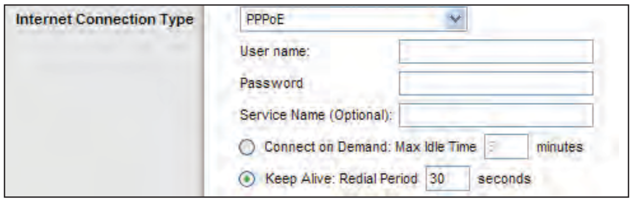
Subnet Mask This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Your ISP will provide you with the Gateway Address, which is the ISP server's IP address.

DNS Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

PPPoE

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



Internet Connection Type: PPPoE

User name:

Password

Service Name (Optional):

○ Connect on Demand: Max Idle Time 5 minutes

● Keep Alive: Redial Period 30 seconds

Internet Connection Type > PPPoE

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

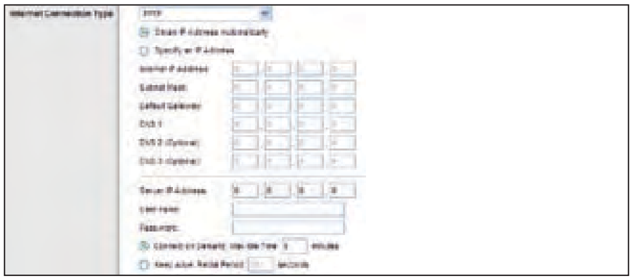
Service Name (optional) If provided by your ISP, enter the Service Name.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes.

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

PPTP

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



Internet Connection Type: PPTP

● Obtain IP Address Automatically

○ Specify an IP Address

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
Server IP Address:	0	0	0	0

User name:

Password:

● Connect on Demand: Max Idle Time 5 minutes

○ Keep Alive: Redial Period 30 seconds

Internet Connection Type > PPTP

If your ISP supports DHCP or you are connecting through a dynamic IP address, then select **Obtain an IP Address Automatically**. If you are required to use a permanent IP address to connect to the Internet, then select **Specify an IP Address**. Then configure the following:

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

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

Default Gateway Your ISP will provide you with the Gateway Address, which is the ISP server's IP address.

DNS Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

Server IP Address Your ISP will provide you with the Server IP Address.

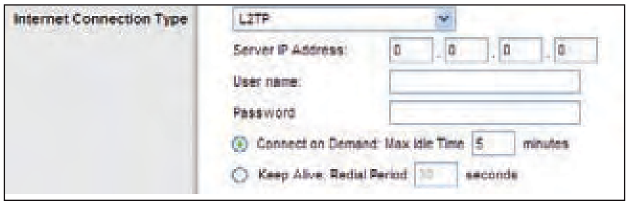
User Name and Password Enter the User Name and Password provided by your ISP.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes.

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

L2TP

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



Internet Connection Type

L2TP

Server IP Address: 0 . 0 . 0 . 0

User name:

Password

● Connect on Demand: Max Idle Time 5 minutes

○ Keep Alive: Redial Period 30 seconds

Internet Connection Type > L2TP

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

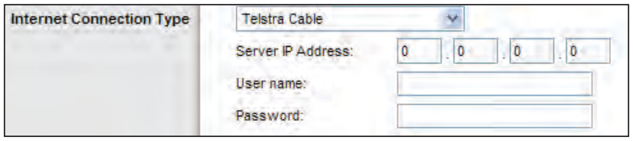
User Name and Password Enter the User Name and Password provided by your ISP.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes

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

Telstra Cable

Telstra Cable is a service that applies to connections in Australia only.



Internet Connection Type

Telstra Cable

Server IP Address: 0 . 0 . 0 . 0

User name:

Password:

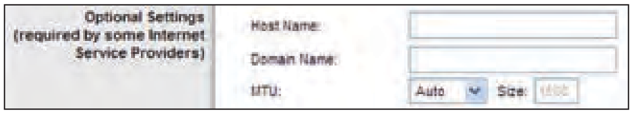
Internet Connection Type > Telstra Cable

Server IP Address This is the IP address of the Telstra Cable. 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.

Optional Settings

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



Optional Settings (required by some Internet Service Providers)

Host Name:

Domain Name:

MTU: Auto Size: 1500

Optional Settings

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

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

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

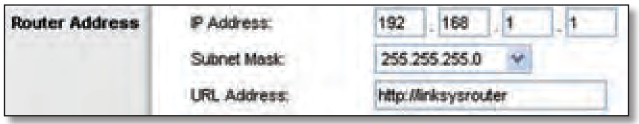
- DHCP, Static IP, or Telstra: **1500**
- PPPoE: **1492**
- PPTP or L2TP: **1460**

Network Setup

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

Router Address

This presents both the Router's IP Address, Subnet Mask, and URL Address as seen by your network. The default Router IP address is **192.168.1.1** and URL address is **http://WRT610N.com**.

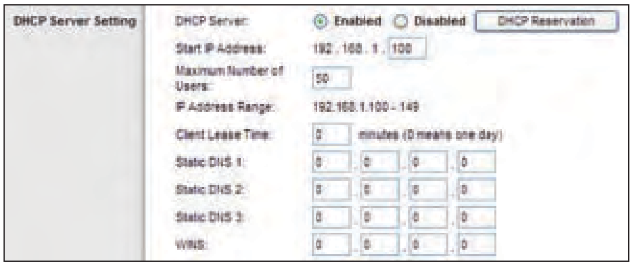


Router Address	IP Address:	192 . 168 . 1 . 1
	Subnet Mask:	255.255.255.0
	URL Address:	http://linksysrouter

Router IP Address

Network Address Server Settings (DHCP)

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



DHCP Server Setting	DHCP Server:	● Enabled ○ Disabled DHCP Reservation
	Start IP Address:	192 . 168 . 1 . 100
	Maximum Number of Users:	50
	IP Address Range:	192.168.1.100 - 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

Network Address Server Settings (DHCP)

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

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

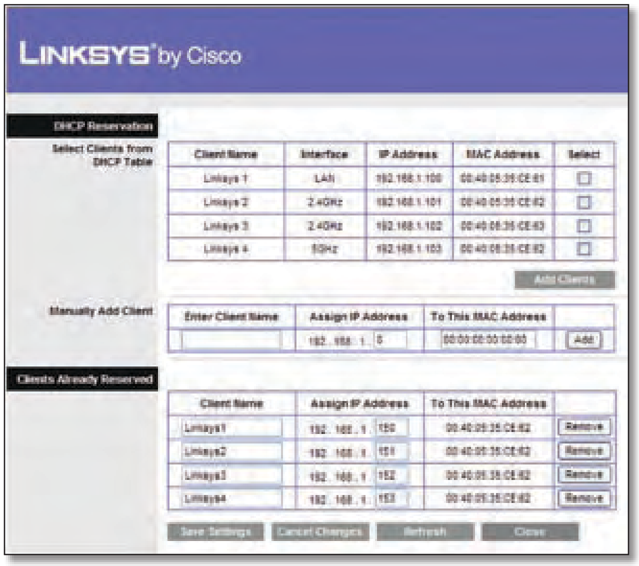
Maximum Number of DHCP Users Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is **50**.

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

Static DNS (1-3) The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, enter that IP Address in one of these fields. You can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

WINS The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

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



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:81	□
Linksys 2	2.4GHz	192.168.1.101	00:40:05:35:CE:82	□
Linksys 3	2.4GHz	192.168.1.102	00:40:05:35:CE:83	□
Linksys 4	5GHz	192.168.1.103	00:40:05:35:CE:82	□

Manually Add 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	
Linksys1	192 . 168 . 1 . 150	00:40:05:35:CE:82	Remove
Linksys2	192 . 168 . 1 . 151	00:40:05:35:CE:82	Remove
Linksys3	192 . 168 . 1 . 152	00:40:05:35:CE:82	Remove
Linksys4	192 . 168 . 1 . 153	00:40:05:35:CE:82	Remove

DHCP Reservation

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 **Add Clients**.

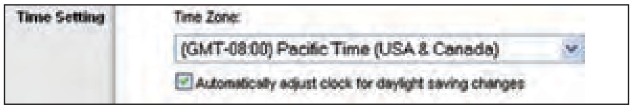
If you want to manually assign an IP address, enter the client's name in the *Enter Client Name* field. Enter the IP address you want it to have in the *Assign IP Address* field. Make sure the IP address is between the starting DHCP server's IP address and maximum number of DHCP users range. Enter its MAC Address in the *To This MAC Address* field. Click **Add**.

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

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

Time Setting

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



Time Setting

Time Zone:

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

☑ Automatically adjust clock for daylight saving changes

Time Setting

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

Setup > DDNS

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

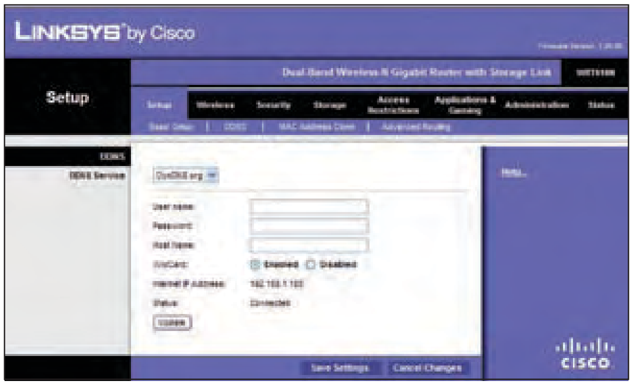
Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, www.dyndns.org or www.TZO.com. If you do not want to use this feature, keep the default setting, **Disabled**.

DDNS

DDNS Service

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

DynDNS.org



DDNS

DDNS Service: DynDNS.org

User name:

Password:

Host Name:

WildCard: ● Enabled ○ Disabled

Internet IP Address: 192.168.1.100

Status: Connected

Update

Setup > DDNS > DynDNS

User Name Enter the User Name for your DDNS account.

Password Enter the Password for your DDNS account.

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

WildCard Select **Enabled** to enable this feature or **Disabled** to disable it.

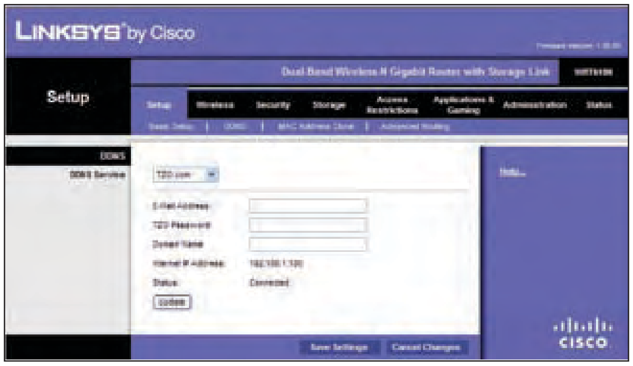
Internet IP Address The Router's Internet IP address is displayed here. Because it is dynamic, it will change.

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

Update To manually trigger an update, click **Update**.

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

TZO.com



DDNS

DDNS Service: TZO.com

E-Mail Address:

TZO Password:

Domain Name:

Internet IP Address: 192.168.1.100

Status: Connected

Update

Setup > DDNS > TZO

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.

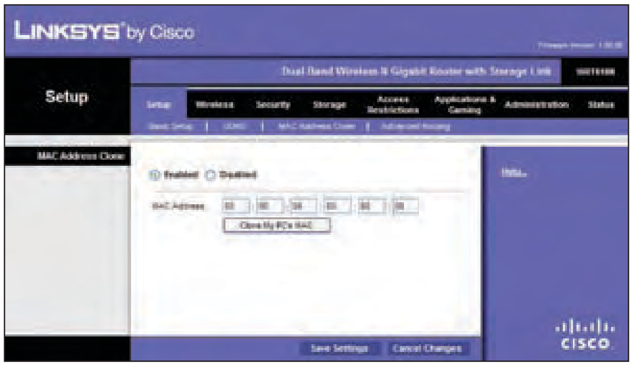
Status The status of the DDNS service connection is displayed here.

Update To manually trigger an update, click **Update**.

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

Setup > MAC Address Clone

Every computere hardware device, including the network adapter of your computer has a unique code called a MAC address. Some Internet Service Providers (ISPs) require you to register this address with them 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.


LINKSYS by Cisco
Dual-Band Wireless-N Gigabit Router with Storage Link
Setup
Setup | Wireless | Security | Storage | Access Restrictions | Applications & Gaming | Administration | Status
Basic Setup | DDNS | MAC Address Clone | Advanced Routing
MAC Address Clone
Help...
Save Settings
Cancel Changes
CISCO

◉ Enabled ○ Disabled

MAC Address

Clone My PC's MAC

Setup > MAC Address Clone

MAC Address Clone

Enabled/Disabled To enable MAC Address cloning, select **Enabled**.

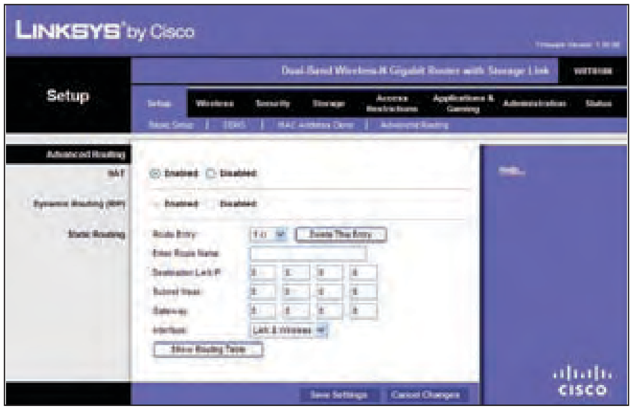
User Defined Entry Enter the MAC Address registered with your ISP here.

Clone Your PC's MAC Clicking this button will clone the MAC address of the computer you are using.

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

Setup > Advanced Routing

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


LINKSYS by Cisco
Dual-Band Wireless-N Gigabit Router with Storage Link
Setup
Setup | Wireless | Security | Storage | Access Restrictions | Applications & Gaming | Administration | Status
Basic Setup | DDNS | MAC Address Clone | Advanced Routing
Advanced Routing
Help...
Delete This Entry
Show Routing Table
Save Settings
Cancel Changes
CISCO

NAT ◉ Enabled ○ Disabled

Dynamic Routing (RIP) ○ Enabled ○ Disabled

Static Routing

Route Entry: 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

Setup > Advanced Routing

Advanced Routing

NAT If this Router is hosting your network's connection to the Internet, select **Enabled**. When NAT is disabled, **Dynamic Routing (RIP)** will be available as an option.

Dynamic Routing (RIP) 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. This feature is **Disabled** by default.

Static Routing

Select Route Entry number To set up a static route between the Router and another network, select a number from the drop-down list. (A static route is a pre-determined pathway that network information must travel to reach a specific host or network.) Enter the information described below to set up a new static route. (Click **Delete This Entry** to delete a static route.)

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

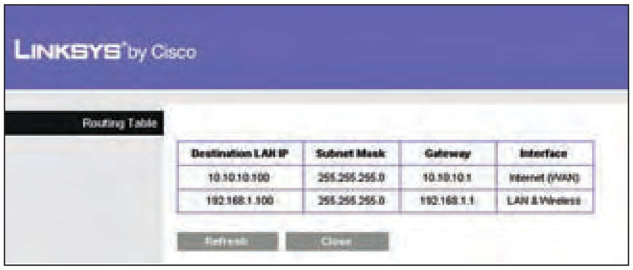
Destination LAN IP The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.

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

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

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

Click **Show Routing Table** to view the Static Routes you have already set up.



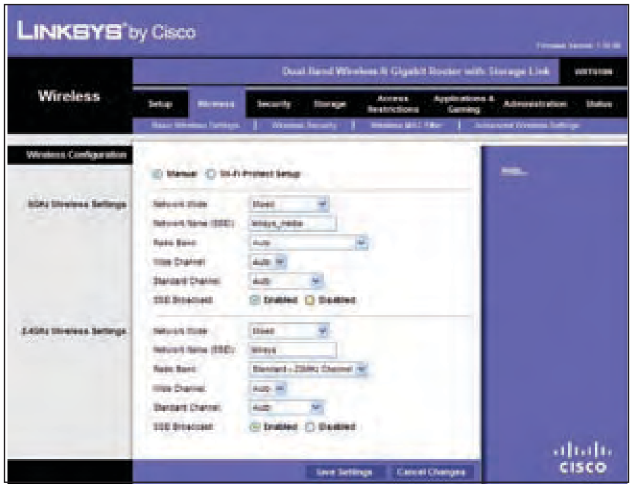
Destination LAN IP	Subnet Mask	Gateway	Interface
10.10.10.100	255.255.255.0	10.10.10.1	Internet (WAN)
192.168.1.100	255.255.255.0	192.168.1.1	LAN & Wireless

Routing Table

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

Wireless > Basic Wireless Settings

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



● Manual ○ Wi-Fi Protect Setup

5GHz Wireless Settings

Network Mode: Mixed
Network Name (SSID): linksys_media
Radio Band: Auto
Wide Channel: Auto
Standard Channel: Auto
SSID Broadcast: ● Enabled ○ Disabled

2.4GHz Wireless Settings

Network Mode: Mixed
Network Name (SSID): linksys
Radio Band: Standard - 20MHz Channel
Wide Channel: Auto
Standard Channel: Auto
SSID Broadcast: ● Enabled ○ Disabled

Wireless > Basic Wireless Settings

Wireless Configuration

Wireless Configuration Keep the default selection, **Wi-Fi Protected Setup** to configure your network using Wi-Fi Protected Setup. Select **Manual** to set up your wireless network your wireless network manually.

Manual

If you set the *Wireless Configuration* to **Manual**, the *Basic Wireless Settings* screen displays the following fields.

Network Mode (5 GHz) From this drop-down menu, you can select the wireless standards running on your network. If you have both Wireless-A and Wireless-N (5GHz) devices in your network, keep the default setting, **Mixed**. If you have only Wireless-A devices, select **Wireless-A Only**. If you have only Wireless-N (5GHz) devices, select **Wireless-N Only.** If you do not have any Wireless-A and Wireless-N (5GHz) devices in your network, select **Disabled**.

Network Mode (2.4 GHz) From this drop-down menu, you can select the wireless standards running on your network. If you have both Wireless-B, Wireless-G and Wireless-N (2.4GHz) devices in your network, keep the default setting, **Mixed**. If you have only Wireless-B devices, select **Wireless-B Only**. If you have only Wireless-G devices, select **Wireless-G Only**. If you have only Wireless-N (2.4GHz) devices, select **Wireless-N Only**. If you do not have any Wireless-B, Wireless-G and Wireless-N (2.4GHz) devices in your network, select **Disabled**.

Wireless 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 keyboard characters. Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID to a unique name.

Radio Band (5 GHz) For best performance in a network using Wireless-A and Wireless-N (5GHz) devices, keep the default, **Auto**.

Radio Band (2.4 GHz) For best performance in a network using Wireless-B, Wireless-G and Wireless-N (2.4GHz) devices, select **Auto**. The default is **Standard - 20MHz Channel**.

Wide Channel (5 GHz) If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N (5GHz) channel. If you are not sure which channel to select, keep the default, **Auto (DFS)**.

Wide Channel (2.4 GHz) If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N (2.4GHz) channel. If you are not sure which channel to select, keep the default, **Auto**.

Standard Channel (5 GHz) Select the channel for Wireless-A and Wireless-N (5GHz) networking. If you selected Wide – 40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N (5GHz). If you are not sure which channel to select, keep the default, **Auto (DFS)**.

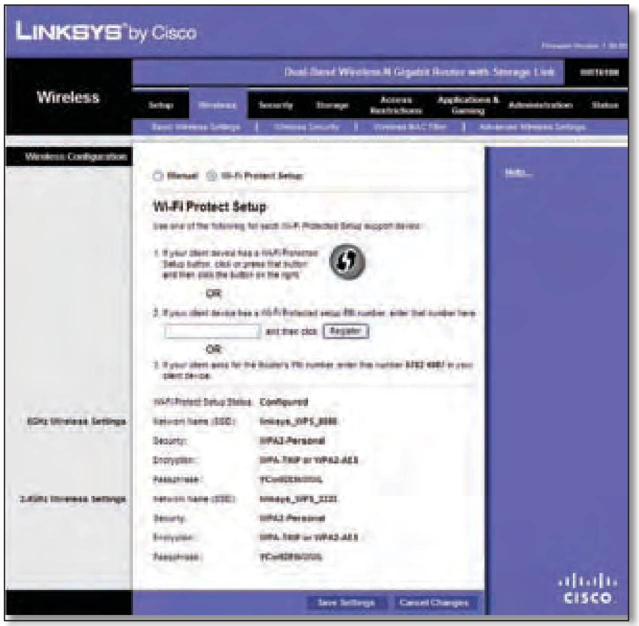
Standard Channel (2.4 GHz) Select the channel for Wireless-B, Wireless-G and Wireless-N (2.4GHz) networking. If you selected Wide – 40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N (2.4GHz). If you are not sure which channel to select, keep 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**.

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

Wi-Fi Protected Setup

There are three methods available. Use the method that applies to the client device you are configuring.



○ Manual ● Wi-Fi Protect Setup

Wi-Fi Protect Setup

1. [illegible]

OR

2. [illegible]

OR

3. [illegible]

Wi-Fi Protect Setup Status: Configured

5GHz Wireless Settings
Network Name (SSID): [illegible]
Security: WPA2-Personal
Encryption: WPA-TKIP or WPA2-AES
Passphrase: [illegible]

2.4GHz Wireless Settings
Network Name (SSID): [illegible]
Security: WPA2-Personal
Encryption: WPA-TKIP or WPA2-AES
Passphrase: [illegible]

Wireless > Basic Wireless Settings (Wi-Fi Protected Setup)

NOTE: Wi-Fi Protected Setup configures one client device at a time. Repeat the instructions for each client device that supports Wi-Fi Protected Setup.

Method #1

Use this method if your client device has a Wi-Fi Protected Setup button.

1. Click or press the **Wi-Fi Protected Setup** button on the client device.
2. Click the **Wi-Fi Protected Setup** button on this screen.
3. After the client device has been configured, click the **OK** button. Then refer back to your client device or its documentation for further instructions.

Method #2

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

1. Enter the PIN number from the client device in the field on this screen.
2. Click the **Register** button.
3. After the client device has been configured, click the **OK** button. Then refer back to your client device or its documentation for further instructions.

Method #3

Use this method if your client device asks for the Router's PIN number.

1. Enter the PIN number listed on this screen. (It is also listed on the label on the bottom of the Router.)
2. After the client device has been configured, click the **OK** button. Then refer back to your client device or its documentation for further instructions.

The Wi-Fi Protected Setup Status, Network Name (SSID), Security, Encryption, and Passphrase are displayed at the bottom of the screen.

NOTE: If you have client devices that do not support Wi-Fi Protected Setup, note the wireless settings, and then manually configure those client devices.

Wireless > Wireless Security

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

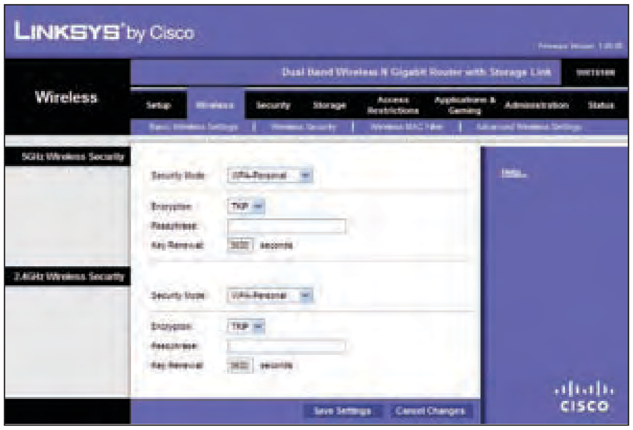
Wireless Security

Security Mode

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

WPA Personal

NOTE: If you are using WPA or WPA2, each device in your wireless network MUST use the same WPA or WPA2 method and shared key, or else the network will not function properly.



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

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

WPA Personal

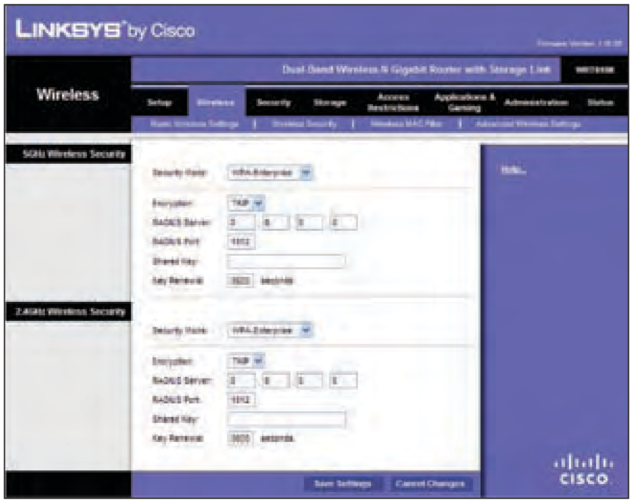
Encryption WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. The default is **TKIP**.

Passphrase Enter a passphrase of 8-63 characters.

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

WPA Enterprise

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



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

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

WPA Enterprise

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

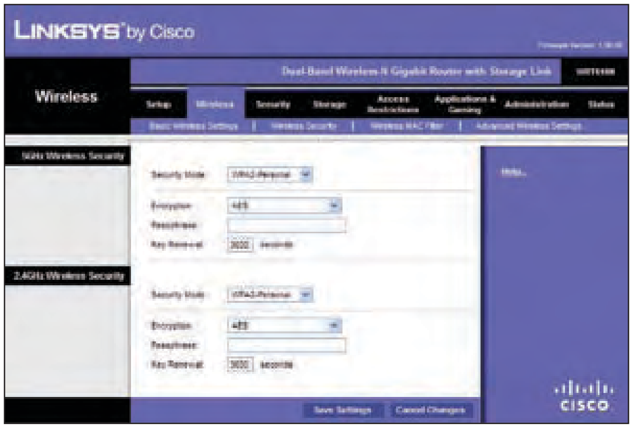
RADIUS Server Enter the IP Address of the RADIUS server.

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

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

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

WPA2 Personal



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

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

WPA2 Personal

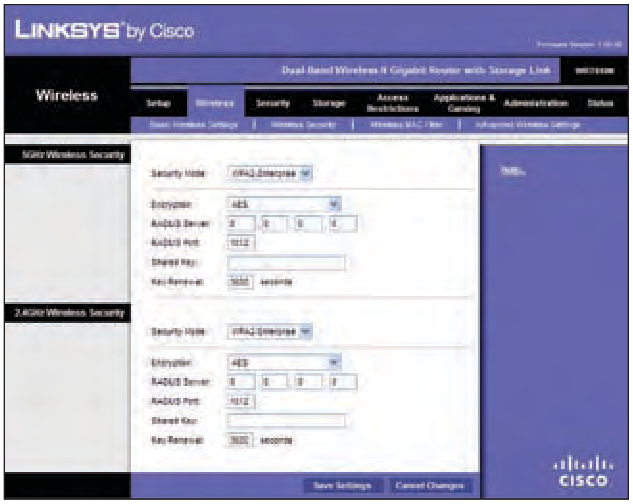
Encryption WPA2 supports two encryption methods with dynamic encryption keys; AES or WPA-TKIP/WPA2-AES. You must select **WPA-TKIP** or **WPA2-AES** to connect to the Router.

Passphrase Enter a passphrase of 8-63 characters.

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

WPA2 Enterprise

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



5GHz Wireless Security

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

2.4GHz Wireless Security

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

WPA2 Enterprise

Encryption WPA2 supports two encryption methods with dynamic encryption keys; AES or WPA-TKIP/WPA2-AES. You must select **WPA-TKIP** or **WPA2-AES** to connect to the Router.

RADIUS Server Enter the IP Address of the RADIUS server.

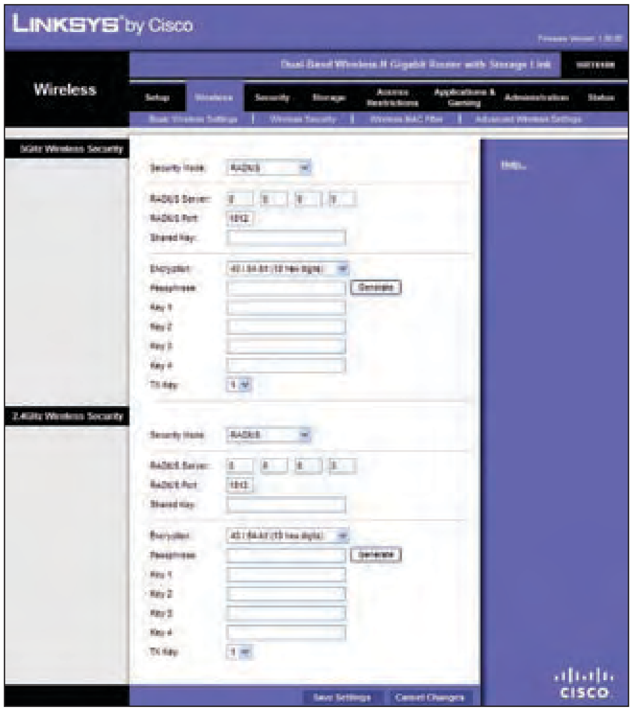
RADIUS Port Enter the port number of the RADIUS server. The default value is **1812**.

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

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

RADIUS

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



5GHz Wireless Security

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

2.4GHz Wireless Security

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

RADIUS

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

RADIUS Server Enter the IP Address of the RADIUS server.

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

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

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

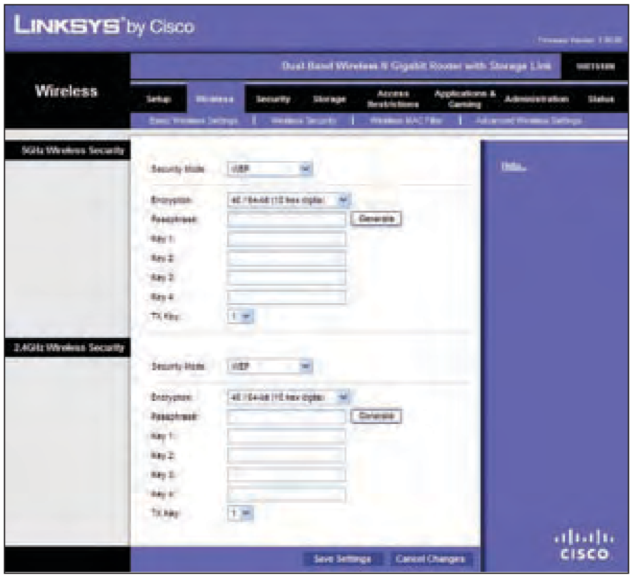
Passphrase Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

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

Tx Key Select a key from the drop-down menu.

WEP

WEP is a basic encryption method that is not as secure as WPA.



WEP

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

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

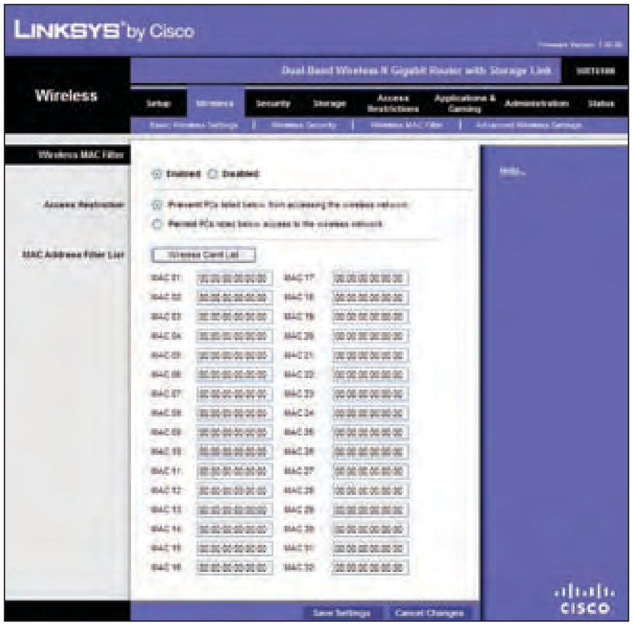
Key 1-4 If you did not enter a Passphrase, enter the WEP key(s) manually.

Tx Key Select a key from the drop-down menu.

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

Wireless > Wireless MAC Filter

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



Wireless > Wireless MAC Filter

Wireless MAC Filter

Access Restriction

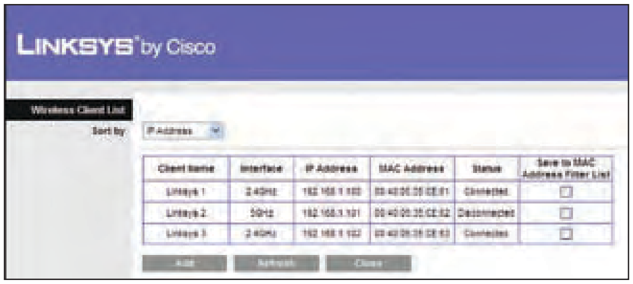
Wireless MAC Filter To filter wireless users by MAC Address, either permitting or blocking access, click **Enabled**. If you do not wish to filter users by MAC Address, keep the default setting, **Disabled**.

Prevent PCs listed below from accessing the wireless network Select this to block wireless access by MAC Address. This option is selected by default.

Permit PCs listed below to the wireless network Select this to allow wireless access by MAC Address. This option is not selected by default.

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. 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.



Sort by: IP Address

Client Name	Interface	IP Address	MAC Address	Status	Save to MAC Address Filter List
Linksys 1	2.4GHz	192.168.1.100	00:40:05:35:CE:01	Connected	☐
Linksys 2	5GHz	192.168.1.101	00:40:05:35:CE:02	Disconnected	☐
Linksys 3	2.4GHz	192.168.1.102	00:40:05:35:CE:03	Connected	☐

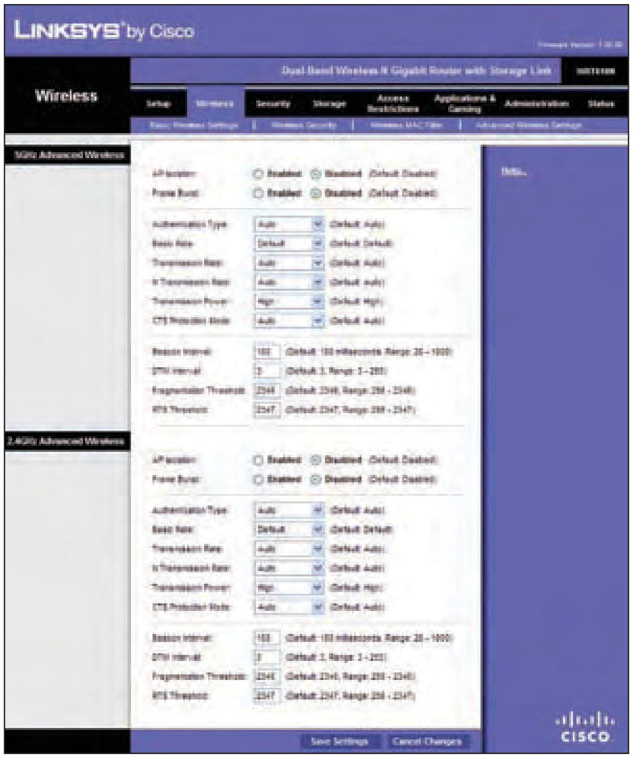
Wireless Client List

MAC XX Enter the MAC addresses of the devices whose wireless access you want to control.

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

Wireless > Advanced Wireless Settings

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



5GHz Advanced Wireless

AP Isolation: ○ Enabled ● Disabled (Default: Disabled)
Frame Burst: ○ Enabled ● Disabled (Default: Disabled)
Authentication Type: Auto (Default: Auto)
Basic Rate: Default (Default: Default)
Transmission Rate: Auto (Default: Auto)
N Transmission Rate: Auto (Default: Auto)
Transmission Power: High (Default: High)
CTS Protection Mode: Auto (Default: Auto)
Beacon Interval: 100 (Default: 100 milliseconds, Range: 20 - 1000)
DTIM Interval: 3 (Default: 3, Range: 1 - 255)
Fragmentation Threshold: 2346 (Default: 2346, Range: 256 - 2346)
RTS Threshold: 2347 (Default: 2347, Range: 256 - 2347)

2.4GHz Advanced Wireless

AP Isolation: ○ Enabled ● Disabled (Default: Disabled)
Frame Burst: ○ Enabled ● Disabled (Default: Disabled)
Authentication Type: Auto (Default: Auto)
Basic Rate: Default (Default: Default)
Transmission Rate: Auto (Default: Auto)
N Transmission Rate: Auto (Default: Auto)
Transmission Power: High (Default: High)
CTS Protection Mode: Auto (Default: Auto)
Beacon Interval: 100 (Default: 100 milliseconds, Range: 20 - 1000)
DTIM Interval: 3 (Default: 3, Range: 1 - 255)
Fragmentation Threshold: 2346 (Default: 2346, Range: 256 - 2346)
RTS Threshold: 2347 (Default: 2347, Range: 256 - 2347)

Wireless > Advanced Wireless Settings

Advanced Wireless

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

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

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

Basic Rate The Basic Rate setting is not one, but a series of rates at which the Router can transmit. (The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.) 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..

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

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

Beacon Interval A beacon is a packet broadcast by the Router to synchronize the wireless network. Enter a value between 20 and 1000 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon.The default value is **100**.

DTIM Interval This value, between 3 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 **3**.

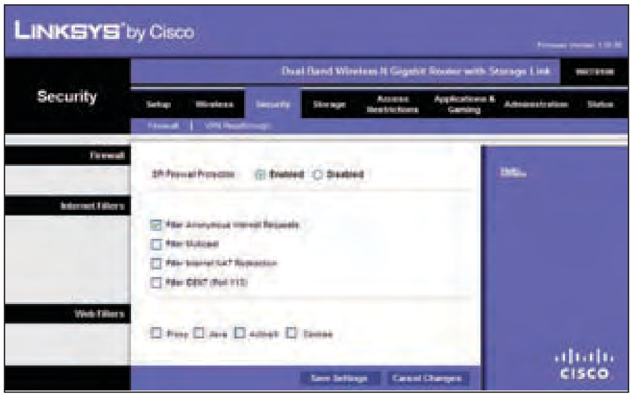
Fragmentation Threshold This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance.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

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

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

Security > Firewall

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



SPI Firewall Protection ● Enabled ○ Disabled

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

☐ Proxy ☐ Java ☐ ActiveX ☐ Cookies

Security > Firewall

Firewall

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

Internet Filters

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

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

Filter Internet NAT Redirection This feature is used to prevent a local computer from using a URL or Internet address to access the local server. Select **Filter Internet NAT Redirection** to filter Internet NAT redirection. It is not selected by default.

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

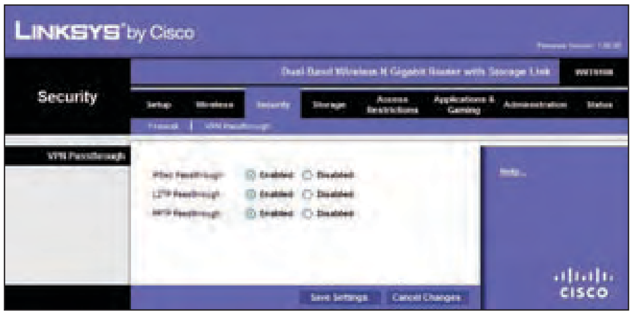
Web Filters

Filters Select to filter Proxy, Java, ActiveX, and Cookies.

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

Security > VPN Passthrough

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



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

Security > VPN Passthrough

VPN Passthrough

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

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

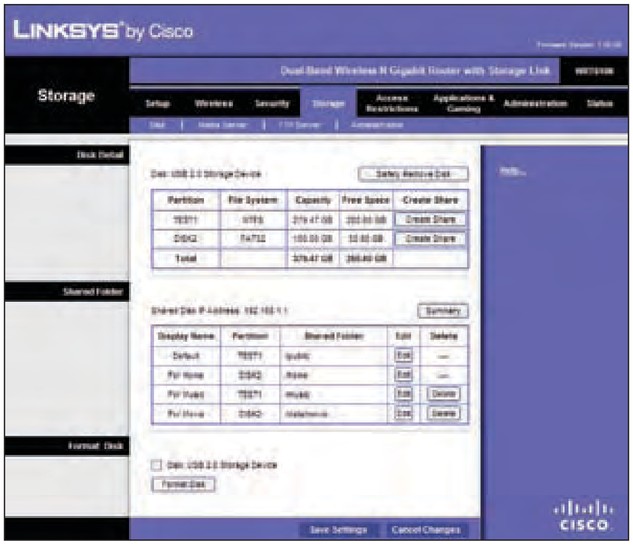
L2TP Passthrough Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, **Enabled**.

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

Storage > Disk

An external USB hard drive or USB disk must be connected to the USB Port of the Router to use the storage feature.

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: USB 2.0 Storage Device

Partition	File System	Capacity	Free Space	Create Share
TEST1	NTFS	279.47 GB	[illegible]	Create Share
DISK2	FAT32	100.00 GB	[illegible]	Create Share
Total		379.47 GB	[illegible]	

Shared Disk IP Address: 192.168.1.1

Display Name	Partition	Shared Folder	Edit	Delete
Default	TEST1	/public	Edit	—
For Home	DISK2	/home	Edit	—
For Music	TEST1	/music	Edit	Delete
For Movie	DISK2	[illegible]	Edit	Delete

□ Disk: USB 2.0 Storage Device

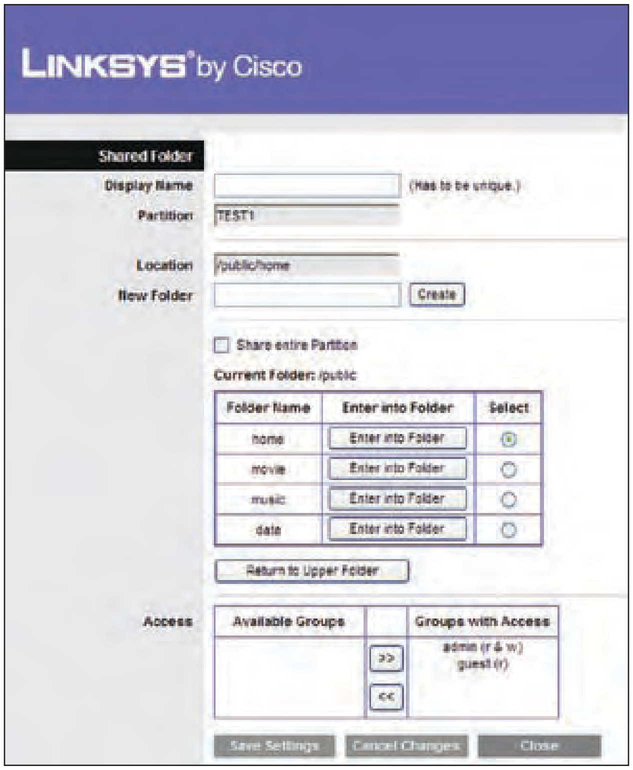
Storage > Disk

Disk Detail

If a formatted disk is attached to the Router, you can view the Partition, File System, Capacity, and Free Space information for each partition of the disk. Click **Create Share** to create a shared folder.

Safely Remove Disk Before physically disconnecting a disk from the Router, click **Safely Remove** first. This prevents the possible loss of data, if the disk is removed while data is transferring to or from the disk.

If you click **Create Share**, the *Shared Folder* screen appears.



Display Name: (Has to be unique.)

Partition: TEST1

Location: /public/home

New Folder:

□ Share entire Partition

Current Folder: /public

Folder Name	Enter into Folder	Select
home	Enter into Folder	●
movie	Enter into Folder	○
music	Enter into Folder	○
data	Enter into Folder	○

Access

Available Groups		Groups with Access
	>> <<	admin (r & w) guest (r)

Shared Folder Screen

Shared Folder Screen

Use this screen to add a Shared folder.

Display Name Enter a display name that will appear in the Shared Folder table of the *Disk* screen.

Partion The name of the Partion to share, that you selected in the *Shared Folder* will appear here.

Location The location of the shared folder is displayed.

New Folder To create a new folder, enter a name for the folder and click **Create**.

Share entire Partion To share the entire partition, click the check box for **Share entire Partion**.

If you don't want to share the entire partition, you can specify the folder you do want to share. Select a folder name to share. To see a sub-folder, click **Enter into Folder**. To return to the previous folder, click **Return to Upper Folder**. To create a new folder, enter a name in the *New Folder* field, then click **Create**.

Access Select the right Access arrows to allow access to a group or the left arrows to remove access to a group. You can allow Read and Write or Read Only access. To add more groups, go to the Storage > Administration s

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Close** to exit the screen.

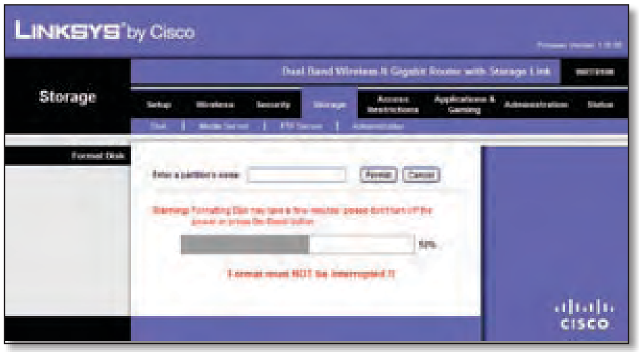
Shared Folder

Each Display Name you created on the *Shared Folder* screen will be listed with its partition and shared folder, which you can edit or delete. Select **Edit** to edit an item or **Delete** to delete the item.

If you click the **Edit**, the *Shared Folder* screen appears. Refer to the "Shared Folder Screen" section above.

Format Disk

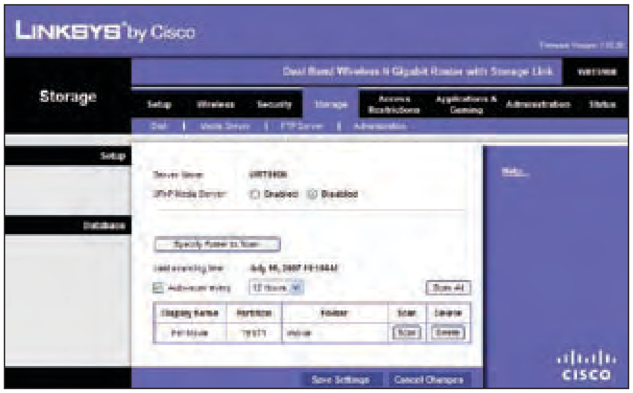
Select the disk you want to format, then click **Format Disk** to format the disk and create a new partition. If your hard drive is formatted with multiple partitions, it will delete them and create a single partition. Enter the name of the partition you want to format. Select **Format** to start the formatting or **Cancel** to cancel it before it begins.



Format Disk

Storage > Media Server

An external USB hard drive or USB disk must be connected to the USB Port of the Router to use the storage feature.



Storage > Media Server

Setup

Server Name The name of the router's media server is displayed here. It can be changed on the Storage > Administration screen.

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

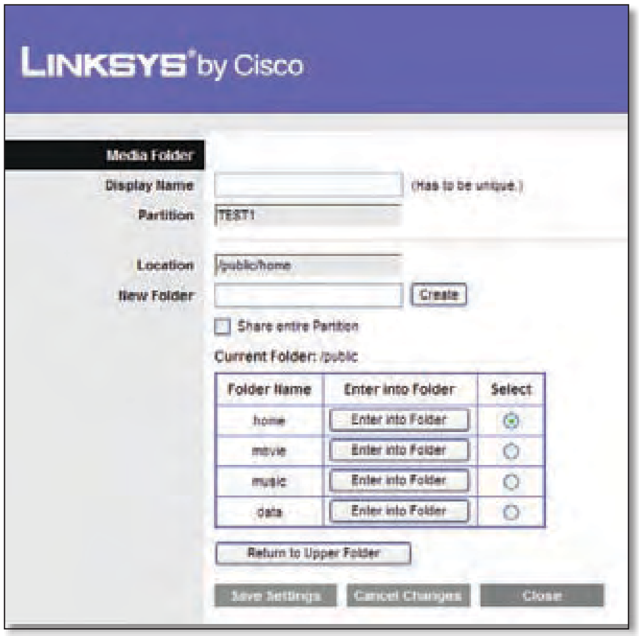
Database

This section lets you select content to add to the database of the Router's media server. Click **Specify Folder to Scan** to add a media folder to the Database table.

If you click **Specify Folder to Scan**, the *Media Folder* screen appears.

Media Folder Screen

Use this screen to add a Media folder.



Display Name (Has to be unique.)
Partition TEST1
Location /public/home
New Folder
□ Share entire Partition
Current Folder: /public

Folder Name	Enter into Folder	Select
home	Enter into Folder	●
movie	Enter into Folder	○
music	Enter into Folder	○
data	Enter into Folder	○

Media Folder

Display Name Enter a display name that will appear in the Database table of the *Media Server* screen.

Partion The name of the Partion to share, that you selected in the *Shared Folder* will appear here.

Location The location of the shared folder is displayed.

New Folder To create a new folder, enter a name for the folder and click **Create**.

Share entire Partion To share the entire partition, click the check box for **Share entire Partion**.

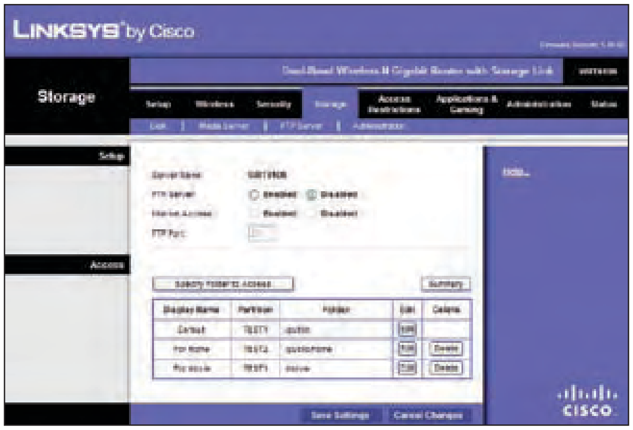
If you don't want to share the entire partition, you can specify the folder you do want to share. Select a folder name to share. To see a sub-folder, click **Enter into Folder**. To return to the previous folder, click **Return to Upper Folder**. To create a new folder, enter a name in the *New Folder* field, then click **Create**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. For more information, click **Help**.

Storage > FTP Server

An external USB hard drive or USB disk must be connected to the USB Port of the Router to use the storage feature.

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



Storage> FTP Server

Setup

Server Name The name of the Router's FTP server is displayed here. It can be changed on the Storage > Administration screen.

FTP Server Select **Enabled** to set this Router as an FTP Server. Otherwise, select **Disabled** to turn the service off. An external USB hard drive or USB disk must be connected to the USB Port to use this service.

Internet Access Select **Enabled** to allow access of the FTP Server from the Internet. Otherwise, select **Disabled** to only allow local network access.

FTP Port Enter the FTP Port number to use. The default port is **21**.

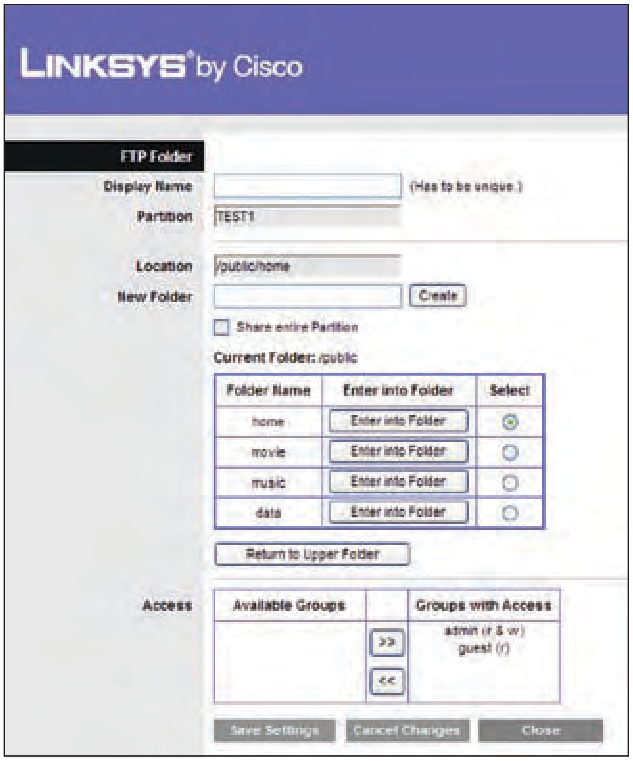
Access

This section lets you add FTP folders that can be accessed through the FTP client. Click **Specify Folder to Access** to add a FTP folder to the Access table.

If you click **Specify Folder to Access**, the *FTP Folder* screen appears.

FTP Folder Screen

Use this screen to add an FTP folder.



Display Name (Has to be unique.)

Partition TEST1

Location /public/home

New Folder

□ Share entire Partition

Current Folder: /public

Folder Name	Enter into Folder	Select
home	Enter into Folder	●
movie	Enter into Folder	○
music	Enter into Folder	○
data	Enter into Folder	○

Access

Available Groups	Groups with Access
	admin (r & w) guest (r)

FTP Folder Screen

Display Name Enter a display name that will appear in the Access table of the *FTP Server* screen.

Partion The name of the Partion to share, that you selected in the *Shared Folder* will appear here.

Location The location of the shared folder is displayed.

New Folder To create a new folder, enter a name for the folder and click **Create**.

Share entire Partion To share the entire partition, click the check box for **Share entire Partion**.

If you don't want to share the entire partition, you can specify the folder you do want to share. Select a folder name to share. To see a sub-folder, click **Enter into Folder**. To return to the previous folder, click **Return to Upper Folder**. To create a new folder, enter a name in the *New Folder* field, then click **Create**.

Access Select the right Access arrows to allow access to a group or the left arrows to remove access to a group. You can allow Read and Write or Read Only access. To add more groups, go to the Storage > Administration screen.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Close** to close the screen.

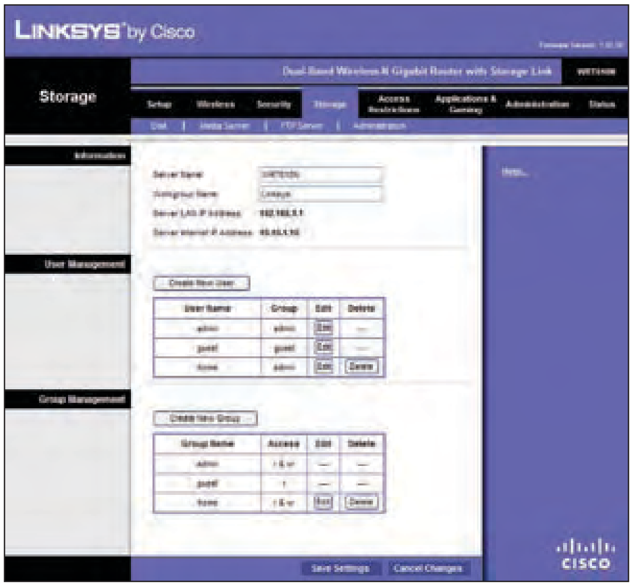
Each Display Name you created on the *FTP Folder* screen will be listed with its partition and folder, which you can edit or delete. Select **Edit** to edit an item or **Delete** to delete the item.

If you click **Edit**, the *FTP Folder* screen appears. Refer to the "FTP Folder Screen" section above.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. For more information, click **Help**.

Storage > Administration

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



Server Name: [illegible]
Workgroup Name: Linksys
Server LAN IP Address: 192.168.1.1
Server Internet IP Address: [illegible]

User Name	Group	Edit	Delete
admin	admin	Edit	—
guest	guest	Edit	—
home	admin	Edit	Delete

Group Name	Access	Edit	Delete
admin	r & w	—	—
guest	r	—	—
home	r & w	Edit	Delete

Storage > Administration

Information

Server Name Enter a name that will be used for the network storage FTP and Media server. Punctuation, spaces, and other special characters (e.g., * / | \) cannot be used in the name.

Workgroup Name Enter the Workgroup Name of your Router in the local network.

The (FTP and Media) Server LAN IP Address and the (FTP) Server Internet IP Address are displayed here.

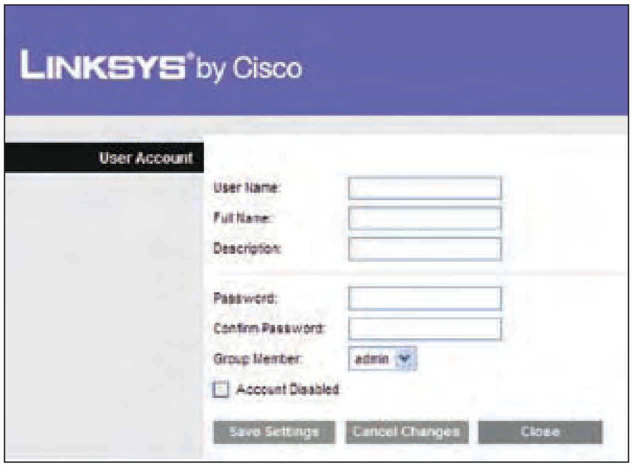
User Management

The available users are listed in the User Management table. The two default users, **Admin** (read and write access) and **Guest** (read-only access) cannot be deleted. Click **Create New User** to create a new user.

If you click **Create New User**, the *User Account* screen appears.

Each user you created on the *User Account* screen will be listed with its group, which you can edit or delete. Select **Edit** to edit a user or **Delete** to delete the user.

If you click **Edit**, the *User Account* screen appears. Refer to the "User Account Screen" section.



User Name:
Full Name:
Description:
Password:
Confirm Password:
Group Member: admin
☐ Account Disabled

User Account

User Account Screen

Users can be added, edited or deleted through the *User Account* screen:

1. Enter a user name for the user.
2. Enter the full name and description for the user.
3. Enter a password and enter it again in the *Confirm Password* field.
4. Select **Admin** or **Guest** from the *Group Member* drop-down menu. You can create a new group in the Group Management section.
5. Click **Save Settings** to save the new changes, or click **Cancel Changes** to cancel the changes. Click **Close** to close the screen.

Group Management

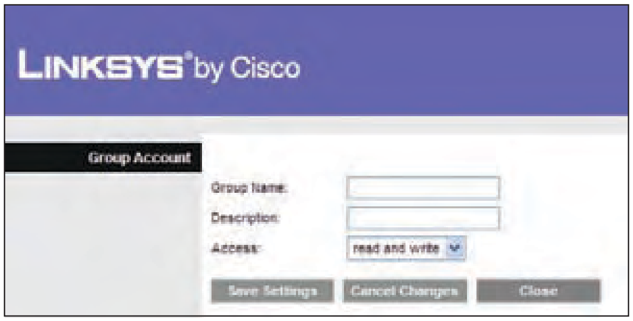
The groups are listed in the Group Management table. There are two default groups, **Admin** and **Guest**; these cannot be deleted. Click **Create New Group** to create a new group.

If you click **Create New Group**, the *Group Account* screen appears.

Each group you created on the *Group Account* screen will be listed with its access rights, which you can edit or delete. Select **Edit** to edit a user or **Delete** to delete the user.

If you click **Edit**, the *Group Account* screen appears. Refer to the "Group Account Screen" section.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. For more information, click **Help**.



Group Name:
Description:
Access: read and write

Group Account

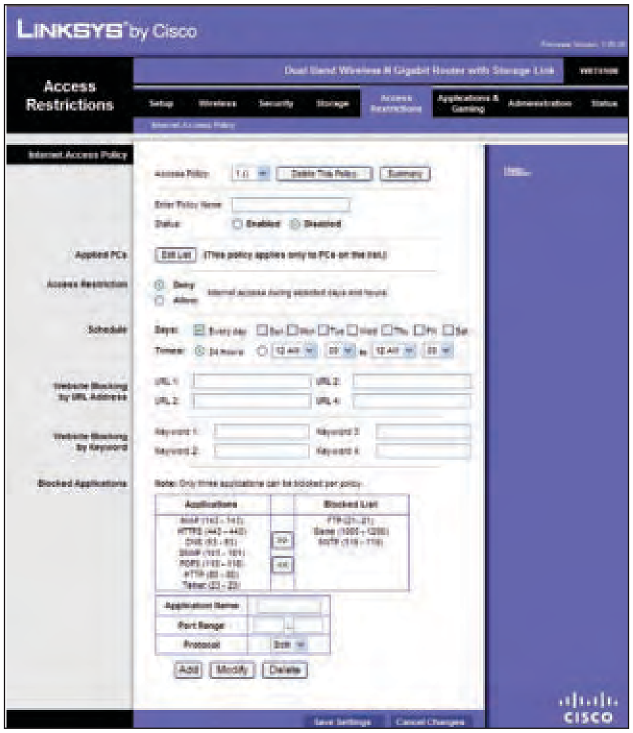
Group Account Screen

Groups can be added, edited or deleted:

1. Enter a name for the group.
2. Enter a description for the group.
3. Select **read and write** or **read only** access.
4. Click **Save Settings** to save the new changes, or click **Cancel Changes** to cancel the changes. Click **Close** to close the screen.

Access Restrictions > Internet Access

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



Internet Access Policy

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: ☑ Every day □ 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	Blocked List
IMAP (143 - 143) HTTPS (443 - 443) DNS (53 - 53) SNMP (161 - 161) POP3 (110 - 110) HTTP (80 - 80) Telnet (23 - 23)	FTP (21 - 21) Game (1000 - 1200) NNTP (119 - 119)

Application Name	
Port Range	~
Protocol	Both

Access Restrictions > Internet Access

Internet Access

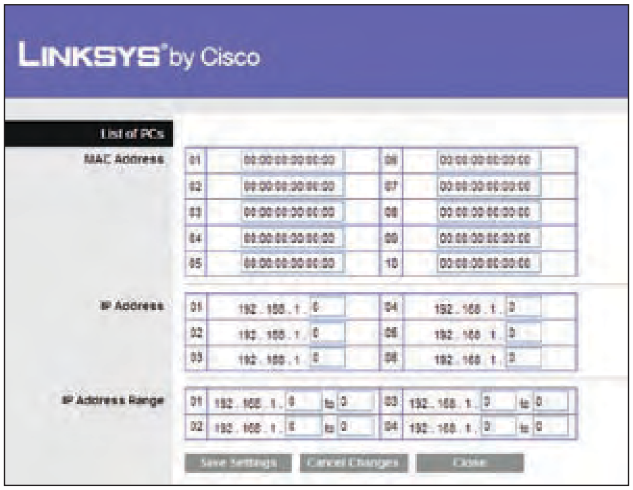
Internet Access Policy Internet Access can be managed by a policy. Use the settings on this screen to establish an access policy (after **Save Settings** is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click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

Deny or Allow If you select Deny, the PC on the Edit List will be denied Internet Access by the dates and times selected. PCs not on the list will still have Internet access. If you select Allow, the PCs on the Edit List will have Internet access by the dates and times selected. The PCs not on the Edit List will be denied Internet access. If there is a conflict with a policy, the lower numbered policy will have priority over a higher numbered policy.

To create an Internet Access Policy:

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

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



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	

List of PCs

5. Select the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.
6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.
7. Enter a URL address or Keyword for Website Blocking or select any Blocked Applications you wish to use. Using these features can slow down your Internet speed.
8. Click **Save Settings** to save the policy's settings, or click **Cancel Changes** to cancel the policy's settings.

Blocked Applications

You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting applications from the Applications List.

To add an application, 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 **Add**.

To modify an application, select it from the Application List. Change the application name, port range, or protocol setting. Then click **Modify**.

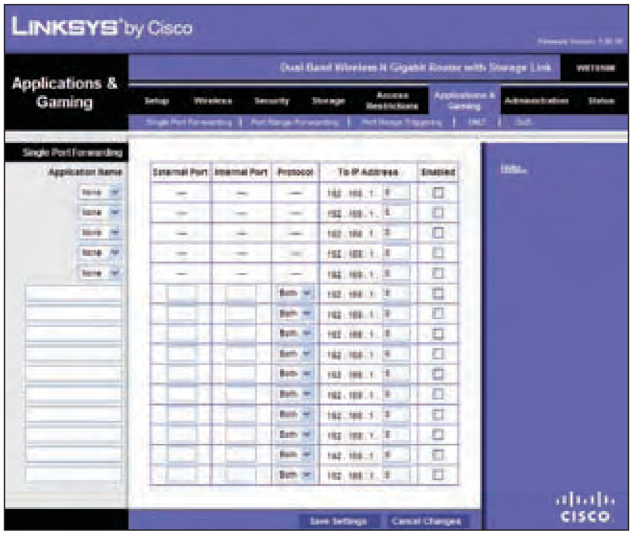
To delete an application, select it from the Application List. Then click **Delete**.

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

Applications and Gaming > Single Port Forwarding

The *Single Port Forwarding* screen allows you to customize port services for common applications.

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.



Applications and Gaming > Single Port Forwarding

Single Port Forwarding

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

Application Select a pre-configured application, or enter the name you wish to give the application. Each name can have up to 12 characters.

External and Internal Port Enter the external and internal port numbers.

Protocol Select the protocol used for this application, either **TCP** or **UDP**.

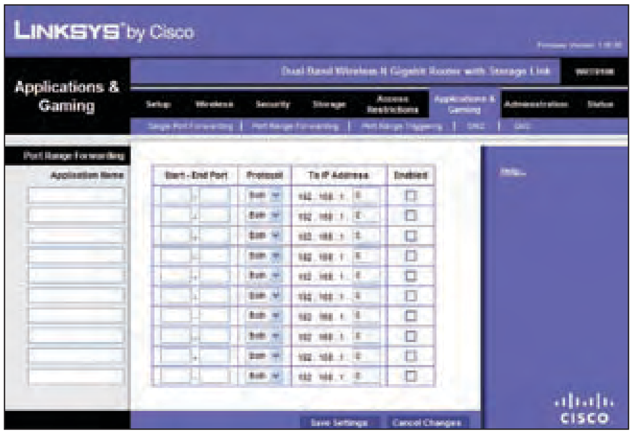
IP Address For each application, enter the IP address of the computer that should receive the requests.

Enabled For each application, select **Enabled** to enable port forwarding.

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

Applications and Gaming > Port Range Forwarding

The *Applications & Gaming > Port Range Forwarding* screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)



Applications and Gaming > Port Range Forwarding

Port Range Forwarding

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

Application In this field, enter the name you wish to give the application. Each name can be up to 12 characters.

Start/End This is the port range. Enter the number that starts the port range in the Start column and the number that ends the range in the End column.

Protocol Select the protocol used for this application, either **TCP** or **UDP**, or **Both**.

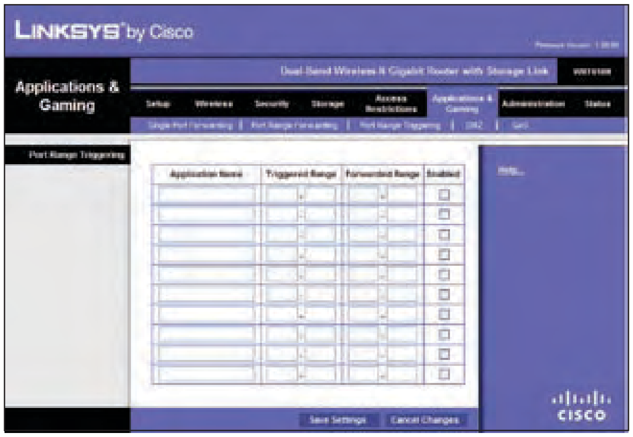
IP Address For each application, enter the IP Address of the PC running the specific application.

Enabled Select **Enabled** to enable port forwarding for the relevant application.

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

Applications & Gaming > Port Triggering

The *Applications & Gaming > Port Triggering* screen allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.



Applications and Gaming > Port Triggering

Port Triggering

Application Enter the application name of the trigger.

Triggered Range

For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed.

Start Port Enter the starting port number of the Triggered Range.

End Port Enter the ending port number of the Triggered Range.

Forwarded Range

For each application, list the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.

Start Port Enter the starting port number of the Forwarded Range.

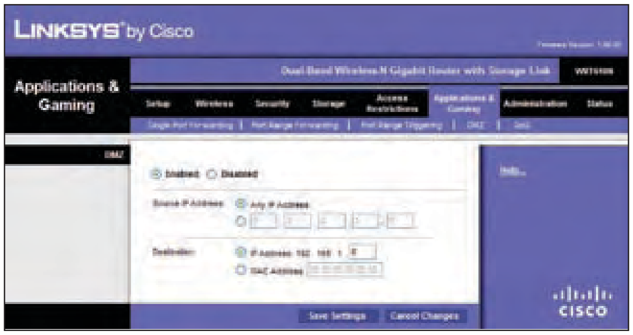
End Port Enter the ending port number of the Forwarded Range.

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

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

Applications and Gaming > DMZ

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



DMZ

● Enabled ○ Disabled

Source IP Address: ● Any IP Address ○ [illegible]

Destination: ● IP Address: 192 . 168 . 1 . [illegible] ○ MAC Address: [illegible]

Applications and Gaming > DMZ

DMZ

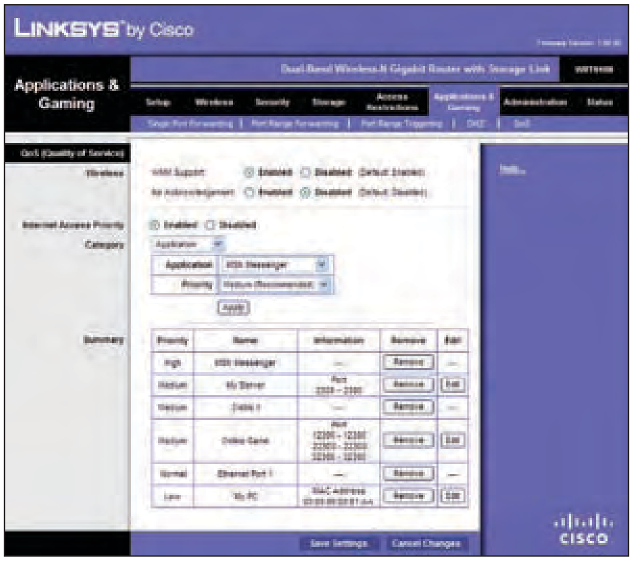
Any PC whose port is being forwarded should have its DHCP client function disabled and have a new static IP address assigned to it because its IP address may change when using the DHCP function.

To allow PCs on the Internet to access a local PC, select **Enabled**. Then, select **Any IP Address** or manually enter a specific source IP address of the computer you want to allow access from the Internet. Then, enter your local PC's IP address or MAC address that you want to allow access to. This feature is disabled by default.

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

Applications and Gaming > QoS

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



Wireless: WMM Support: ● Enabled ○ Disabled (Default: Enabled)

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

Internet Access Priority: ● Enabled ○ Disabled

Category: Application

Application: MSN Messenger

Priority: Medium (Recommended)

Summary

Priority	Name	Information	Remove	Edit
High	MSN Messenger	—	Remove	—
Medium	My Server	Port [illegible]	Remove	Edit
Medium	Cable 1	—	Remove	—
Medium	Online Game	Port [illegible]	Remove	Edit
Normal	Ethernet Port 1	—	Remove	—
Low	My PC	MAC Address [illegible]	Remove	Edit

Applications and Gaming > QoS

QoS (Quality of Service)

Wireless

Wireless WMM (Wi-Fi Multimedia) WMM is a wireless Quality of Service feature that improves quality for audio, video, and voice applications by prioritizing wireless traffic. To use this feature, your wireless client devices in your network must support Wireless WMM. If you would like to disable this feature, select **Disabled**. Otherwise, keep the default, **Enabled**.

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

Internet Access Priority

In this section, you can set the bandwidth priority for a variety of applications and devices. There are four levels of 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 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.

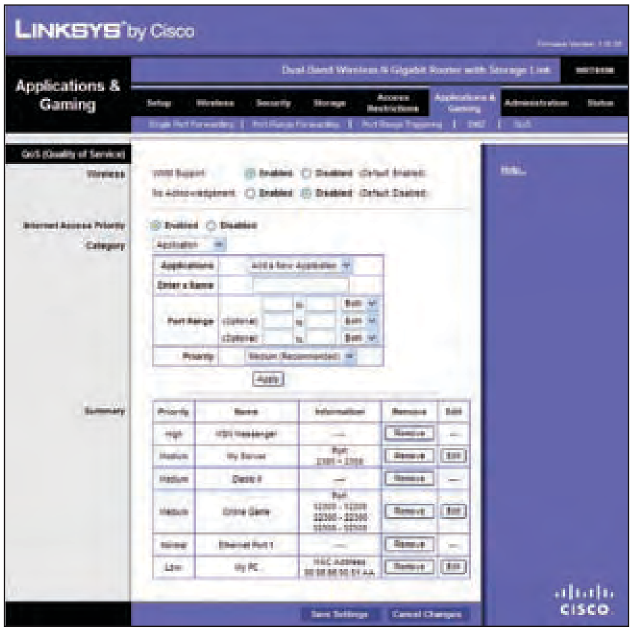
Applications

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

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

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

Add a New Application



Wireless: WMM Support ● Enabled ○ Disabled (Default: Enabled)
No Acknowledgement ○ Enabled ● Disabled (Default: Disabled)

Internet Access Priority: ● Enabled ○ Disabled

Category: Application

Applications: Add a New Application
Enter a Name:
Port Range: to Both; (Optional) to Both; (Optional) to Both
Priority: Medium (Recommended)

Summary

Priority	Name	Information	Remove	Edit
High	MSN Messenger	---	Remove	---
Medium	My Server	Port 2301 - 2306	Remove	Edit
Medium	Diablo II	---	Remove	---
Medium	Online Game	Port 12000 - 12200 22300 - 22300 32000 - 32000	Remove	Edit
Normal	Ethernet Port 1	---	Remove	---
Low	My PC	MAC Address 00:00:00:00:01:AA	Remove	Edit

Add a New Application

Enter a Name Enter a name for this application.

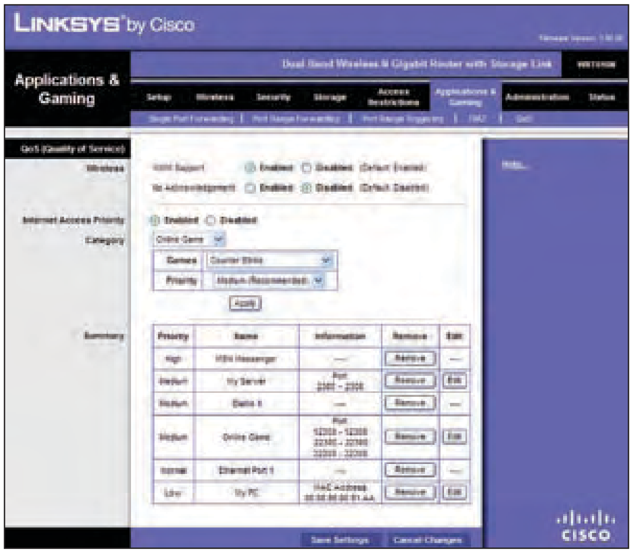
Port Range Enter the port range that the application will be using. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an application that uses from 1000 to 1250, you enter 1000-1250 as your settings. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.

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

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

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

Online Games



Wireless: WMM Support ● Enabled ○ Disabled (Default: Enabled)
No Acknowledgement ○ Enabled ● Disabled (Default: Disabled)

Internet Access Priority: ● Enabled ○ Disabled

Category: Online Game

Games: Counter Strike
Priority: Medium (Recommended)

Summary

Priority	Name	Information	Remove	Edit
High	MSN Messenger	---	Remove	---
Medium	My Server	Port 2301 - 2306	Remove	Edit
Medium	Diablo II	---	Remove	---
Medium	Online Game	Port 12000 - 12200 22300 - 22300 32000 - 32000	Remove	Edit
Normal	Ethernet Port 1	---	Remove	---
Low	My PC	MAC Address 00:00:00:00:01:AA	Remove	Edit

Online Games

Games

Games Select the appropriate game. If you select *Add a New Game*, follow the instructions in the "Add a New Game section".

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

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

Add a New Game

Enter a Name Enter any name to indicate the name of the entry.

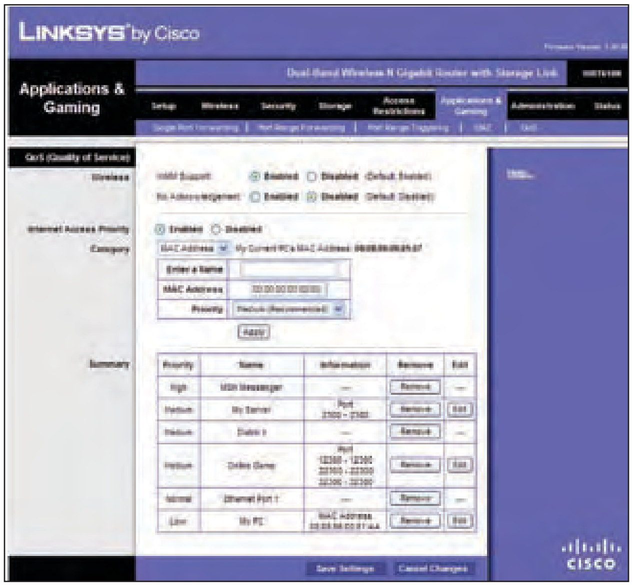
Port Range Enter the port range that the application will be using. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an application that uses from 1000 to 1250, you enter 1000-1250 as your settings. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.

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

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

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

MAC Address



QoS (Quality of Service)

Wireless: WMM Support ● Enabled ○ Disabled (Default: Enabled)
No Acknowledgement ○ Enabled ● Disabled (Default: Disabled)

Internet Access Priority: ● Enabled ○ Disabled
Category: MAC Address — My Current PC's MAC Address: 00:00:00:00:00:07

Enter a Name:
MAC Address: 00:00:00:00:00:00
Priority: Medium (Recommended)
Apply

Summary

Priority	Name	Information	Remove	Edit
High	MSN Messenger	—	Remove	—
Medium	My Server	Port 2300 - 2300	Remove	Edit
Medium	Diablo II	—	Remove	—
Medium	Online Game	Port 12300 - 12300 22300 - 22300 32300 - 32300	Remove	Edit
Normal	Ethernet Port 1	—	Remove	—
Low	My PC	MAC Address 00:00:00:00:01:AA	Remove	Edit

MAC Address

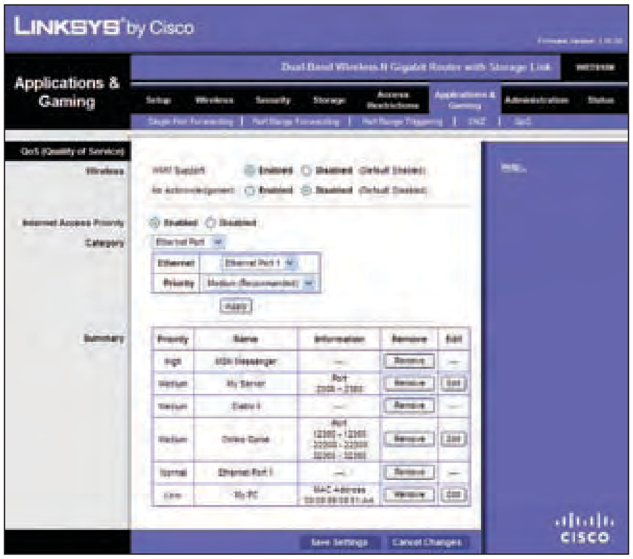
Enter a Name Enter a name for your device.

MAC Address Enter the MAC address of your device.

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

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

Ethernet Port



QoS (Quality of Service)

Wireless: WMM Support ● Enabled ○ Disabled (Default: Enabled)
No Acknowledgement ○ Enabled ● Disabled (Default: Disabled)

Internet Access Priority: ● Enabled ○ Disabled
Category: Ethernet Port

Ethernet: Ethernet Port 1
Priority: Medium (Recommended)
Apply

Summary

Priority	Name	Information	Remove	Edit
High	MSN Messenger	—	Remove	—
Medium	My Server	Port 2300 - 2300	Remove	Edit
Medium	Diablo II	—	Remove	—
Medium	Online Game	Port 12300 - 12300 22300 - 22300 32300 - 32300	Remove	Edit
Normal	Ethernet Port 1	—	Remove	—
Low	My PC	MAC Address 00:00:00:00:01:AA	Remove	Edit

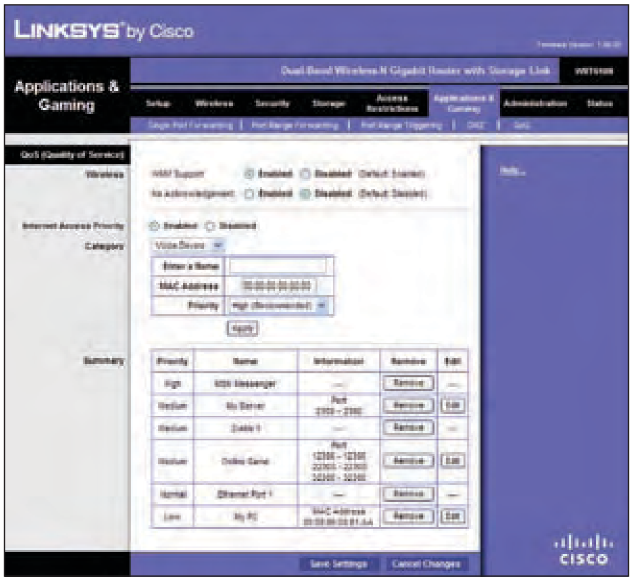
Ethernet Port

Ethernet Select the Ethernet port that you want to use.

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

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

Voice Device



QoS (Quality of Service)

Wireless: WMM Support ● Enabled ○ Disabled (Default: Enabled)
No Acknowledgement ○ Enabled ● Disabled (Default: Disabled)

Internet Access Priority: ● Enabled ○ Disabled
Category: Voice Device

Enter a Name:
MAC Address: 00:00:00:00:00:00
Priority: High (Recommended)
Apply

Summary

Priority	Name	Information	Remove	Edit
High	MSN Messenger	—	Remove	—
Medium	My Server	Port 2300 - 2300	Remove	Edit
Medium	Diablo II	—	Remove	—
Medium	Online Game	Port 12300 - 12300 22300 - 22300 32300 - 32300	Remove	Edit
Normal	Ethernet Port 1	—	Remove	—
Low	My PC	MAC Address 00:00:00:00:01:AA	Remove	Edit

Voice Device

Enter a Name Enter a name for your voice device.

MAC Address. Enter the MAC address of your voice device.

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

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

Summary

This lists the QoS entries you have created for your applications and devices.

Priority This displays the bandwidth priority of High, Medium, Normal, or Low.

Name This displays the application, device, or port name.

Information This displays the port range or MAC address entered for your entry. If a pre-configured application or game was selected, there will be no valid entry shown in this section.

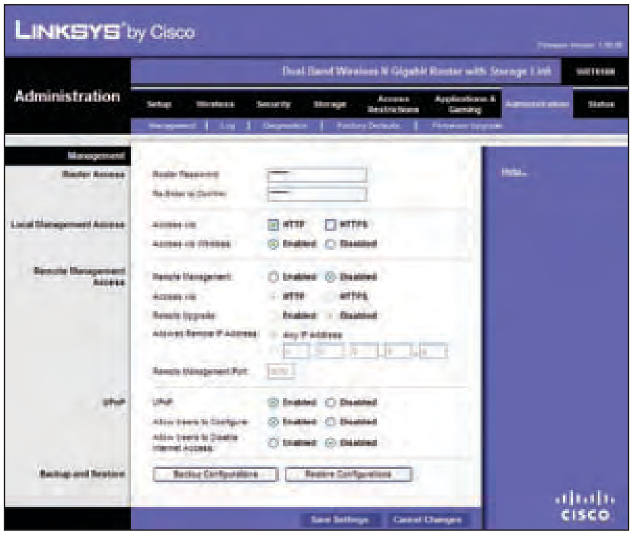
Remove Click this button to remove an entry.

Edit Click this button to make changes.

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

Administration > Management

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



Administration > Management

Router Password

Router Access

Router Password Enter a new Password for the Router.

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

Local Management Access

Access via HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. Select the **HTTP** or **HTTPS** check box. The default selection is **HTTP**.

Access via Wireless If you are using the Router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Router's web-based utility. You will only be able to access the web-based utility via a wired connection if you disable the setting. Keep the default, **Enabled**, to enable wireless access to the Router's web-based utility, or select **Disabled** to disable wireless access to the utility.

Remote Management Access

Remote Management To access the Router remotely from the Internet, select **Enabled**.

Access via Select **HTTP** or **HTTPS** communications protocols for remote access from the Internet.

Remote Upgrade Select **Enabled** to be able to upgrade the firmware remotely from the Internet.

Allowed Remote IP Address Select **Any IP Address** or manually enter an Internet IP address to allow remote access to the web-based utility from the Internet.

Remote Management Port Enter the port number that will provide outside access to the Router's web-based utility. You will need to enter the Router's password when accessing the Router this way, as usual.

UPnP

UPnP Keep the default, **Enabled**, to enable the UPnP feature; otherwise, select **Disabled**.

Allow Users to Configure To use the Allow Users to Configure UPnP options from the Windows operating system, select **Enabled**.

Allow Users to Disabled Internet Access To use the Allow Users to Disabled Internet Access options from the Windows operating system, click **Disabled**.

Backup and Restore

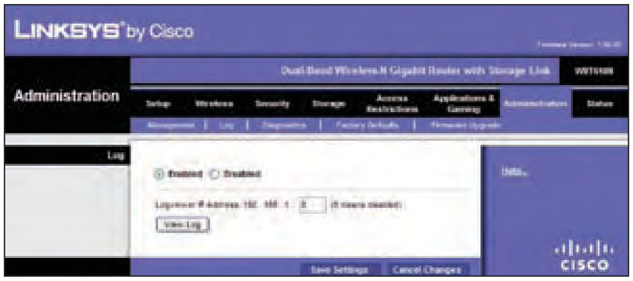
Backup Configurations To back up the Router's configuration file, click this button. Then, follow the on-screen instructions.

Restore Configurations To restore the Router's configuration file, click this button. Then, follow the on-screen instructions.

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

Administration > Log

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



Administration > Log

Log

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

Logviewer IP Address If your computer uses Logviewer software you can enter enter the fixed IP address of the PC running the software in the Logviewer IP Address field.s The Router will now send updated logs to that PC.

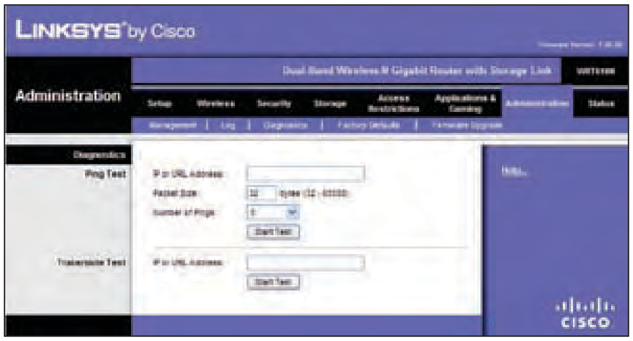
When you wish to view the logs, click **View Log**.

Click **Save the Log** to save your log, click **Refresh** to refresh the screen, or click **Clear** to clear the screen.

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

Administration > Diagnostics

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



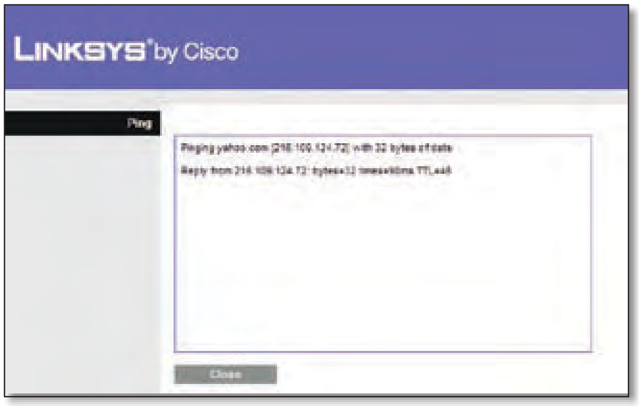
Ping Test
IP or URL Address:
Packet Size: 32 bytes (32 - 65500)
Number of Pings: 5
Start Test

Traceroute Test
IP or URL Address:
Start Test

Administration > Diagnostics

Ping Test

Ping The Ping test checks the status of a connection. Enter the address of the PC whose connection you wish to test and how many times you wish to test it. Then, click **Start to Ping**. The *Ping Test* screen will show if the test was successful. Click **Close** to return to the *Diagnostics* screen.

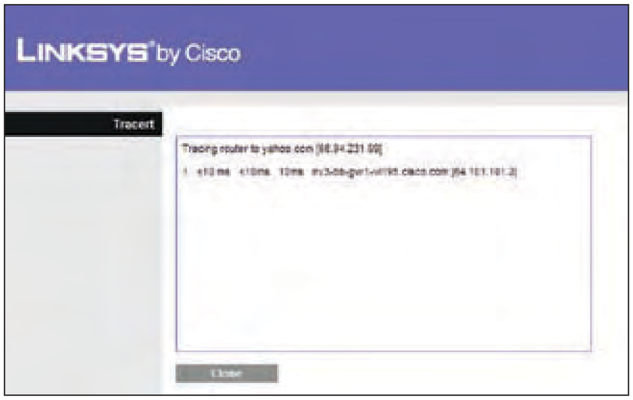


```
Pinging yahoo.com [216.109.124.72] with 32 bytes of data:
Reply from 216.109.124.72: bytes=32 time=40ms TTL=48
```

Ping Test

Traceroute Test

Traceroute To test the performance of a connection, click **Traceroute** to open the *Traceroute Test* screen. Enter the address of the PC whose connection you wish to test and click **Traceroute**. The *Traceroute Test* screen will show if the test was successful. Click **Close** to return to the *Diagnostics* screen.



```
Tracing router to yahoo.com [66.94.231.99]
1   <10 ms   <10ms   10ms   rtr3-bb-gw1-vl195.cisco.com [64.101.101.2]
```

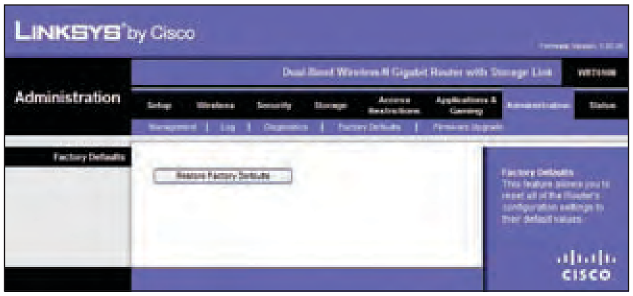
Traceroute Test

Administration > Factory Defaults

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

Factory Defaults

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



Factory Defaults
This feature allows you to reset all of the Router's configuration settings to their default values.

Administration > Factory Defaults

Administration > Firmware Upgrade

The *Administration > Firmware Upgrade* screen allows you to upgrade the Router's firmware. Do not upgrade the firmware unless you are experiencing problems with the Router or the new firmware has a feature you want to use.