User Guide

Linksys E4200 | Maximum Performance Wireless-N Router

Contents

Chapter 1: Product Overview

Thank you for choosing the Linksys E4200 Maximum Performance Wireless-N Router. The router lets you access the Internet via a wireless connection or through one of its four switched ports. You can also use the router to share resources such as computers, printers and files. The router's USB port connects to a USB storage device, so you can add storage space to your network using a USB hard drive or access your portable files using a USB flash disk. The router's media server streams music, video, and photos from an attached storage device to any UPnP-compatible media adapter or player.

Various security features help protect your data and your privacy while you are online. Security features include Wi-Fi Protected Access 2 (WPA2) security, which encrypts data on your wireless network; a Stateful Packet Inspection (SPI) firewall to help block unauthorized access to your router; and Network Address Translation (NAT) technology, which enhances network protection by allowing your computers to share Internet access through a single, public Internet IP address. (IP stands for Internet Protocol.)

Setup and use of the router is easy using Cisco Connect, the software that is installed when you run the included CD. Advanced configuration of the router is available through the provided browser-based utility.

For more wireless bandwidth, the router can create two simultaneous yet separate Wireless-N networks, one using the 5 GHz radio frequency band and one using the 2.4 GHz band. For example, use the Wireless-N 2.4 GHz network to surf, email, and print while keeping the less crowded, Wireless-N 5 GHz network free for time-sensitive traffic like Voice over IP (VoIP) calls, online gaming, and high-definition video. For more information, refer to "**Simultaneous Networks**" on page 10. The Guest Access feature allows you to provide Internet access to guests visiting your home without granting them access to your local network.

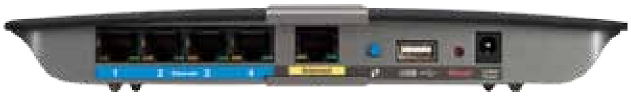
Top

This light indicates power or Wi-Fi Protected Setup status. If you have client devices, such as wireless printers, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup to automatically configure wireless security for your wireless network. To use Wi-Fi Protected Setup, refer to "**Wi-Fi Protected Setup**" on page 12.

Power (white) When the router is powered on, resets to factory defaults, or upgrades its firmware, the light flashes slowly (every three seconds). When the router is ready for use, the light is continuously lit. If there is an error, the light flashes quickly (every second); disconnect the power adapter from your router, wait two seconds, and then reconnect the power adapter to your router.

Wi-Fi Protected Setup (white) When the Wi-Fi Protected Setup process is active, the light flashes slowly (every two seconds) for two minutes. When the Wi-Fi Protected Setup is successful, the light is continuously lit. If there is an error, the light flashes quickly (every second) for two minutes; please wait and try again.

Back



Ethernet 1-4 (yellow and green) Using Ethernet cables (also called network cables), these Ethernet ports connect the router to computers and other Ethernet network devices on your wired network.

The yellow light flashes to indicate network activity over that port. The green light turns on when the local network port is connected to a 10/100/1000 Gigabit port.

Internet (yellow and green) Using an Ethernet cable (also called a network or Internet cable), the Internet port connects the router to your Internet connection, which is typically a cable or Digital Subscriber Line (DSL) modem.

The yellow light flashes to indicate network activity over that port. The green light turns on when the Internet port is connected to a 10/100/1000 Gigabit port.

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

To use Wi-Fi Protected Setup, refer to "**Wi-Fi Protected Setup**" on page 12.

USB Port The USB port connects to a USB storage device.

Reset This button allows you to reset the router to its factory defaults. Press and hold the Reset button for approximately five seconds.

As an alternative, you can restore the defaults from the *Administration > Factory Defaults* screen in the router's browser-based utility (refer to "**Administration > Factory Defaults**" on page 42).

Power The Power port connects to the included power adapter.

Chapter 2: Advanced Configuration

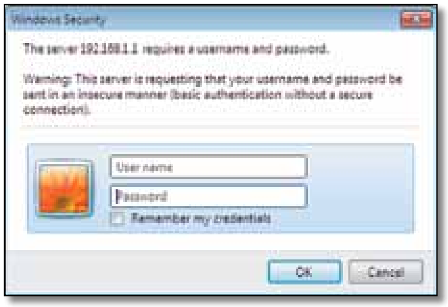
After setting up the router with the setup software (located on the CD-ROM), the router will be ready for use. If you would like to change its advanced settings, use the router's browser-based utility. This chapter describes each web page of the utility and each page's key functions. You can access the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

How to Access the Browser-Based Utility

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

NOTE: You can also access the browser-based utility on Windows computers by entering the device name in the *Address* field. Refer to *Device Name* under "**Router Address**" on page 6.

A login screen appears. (A similar screen appears for non-Windows 7 users.)



The server 192.168.1.1 requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

Login Screen

1. In the *User name* field, enter **admin**.
2. In the *Password* field, enter the password created by the setup software. If you did not run the setup software, then enter the default, **admin**.

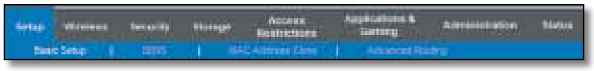
NOTE: You can set a new password on the *Administration > Management* screen. Refer to "**Administration > Management**" on page 41.

3. Click **OK** to continue.

NOTE: You can also access the browser-based utility through Cisco Connect.

How to Use the Browser-Based Utility

Use the tabs at the top of each screen to navigate within the utility. The tabs are arranged in two levels, top-level tabs for general functions and lower-level tabs for the corresponding specific functions.



Top- and Lower-Level Tabs

The top-level tabs are: *Setup*, *Wireless*, *Security*, *Storage*, *Access Restrictions*, *Applications & Gaming*, *Administration*, and *Status*. Each of these has its own unique, lower-level tabs.

NOTE: Within this User Guide, each screen is identified by its top- and lower-level tab names. For example, "Setup > Basic Setup" is the screen accessed via the Setup top-level tab, and its Basic Setup lower-level tab.

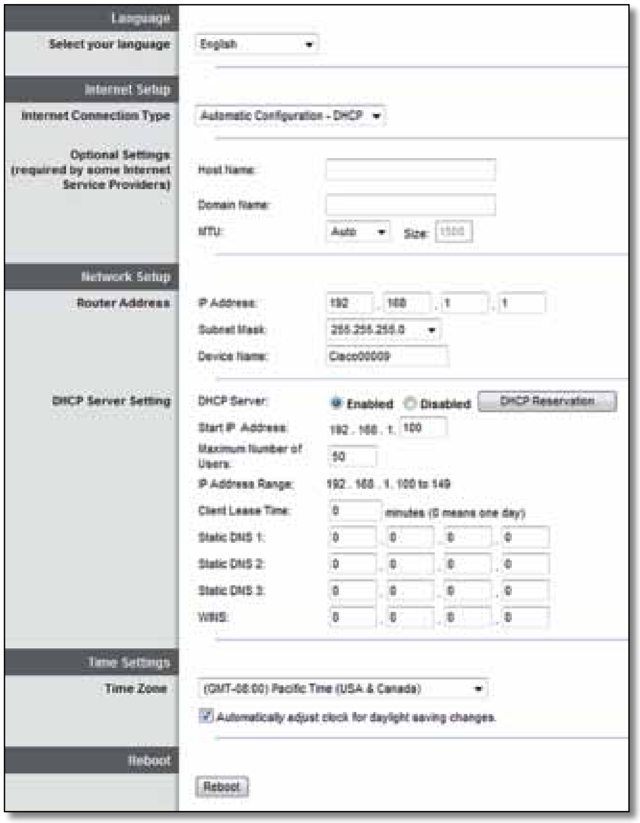
If you change any settings on a screen, you must click **Save Settings** to apply your changes, or click **Cancel Changes** to clear your changes. These controls are located at the bottom of each screen.

Save Settings or Cancel Settings

Click **Help** on the right side of a screen for additional information on the screen's options.

Setup > Basic Setup

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



Select your language: English

Internet Connection Type: Automatic Configuration - DHCP

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

Router Address
IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255.255.255.0
Device Name: Cisco00009

DHCP Server Setting
DHCP Server: ● Enabled ○ Disabled
Start IP Address: 192 . 168 . 1. 100
Maximum Number of Users: 50
IP Address Range: 192 . 168 . 1. 100 to 149
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0 . 0 . 0 . 0
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0
WINS: 0 . 0 . 0 . 0

Time Zone: (GMT-08:00) Pacific Time (USA & Canada)
☑ Automatically adjust clock for daylight saving changes.

Setup > Basic Setup

Language

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

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).

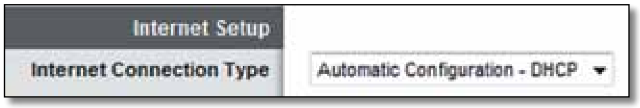
Internet Connection Type

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

The default Internet Connection Type is **Automatic Configuration - DHCP** (Dynamic Host Configuration Protocol). Keep the default only if your ISP supports DHCP or if you connect using a dynamic IP address. (This option usually applies to cable connections.)

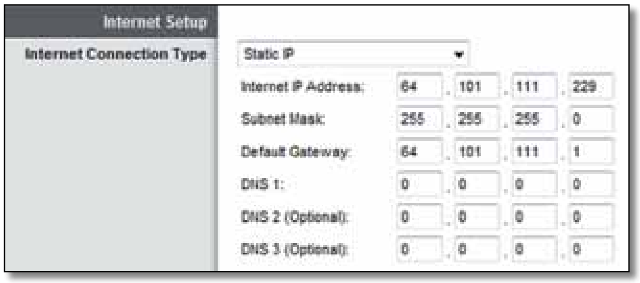


Internet Connection Type: Automatic Configuration - DHCP

Internet Connection Type > Automatic Configuration - DHCP

Static IP

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



Internet Connection Type: Static IP
Internet IP Address: 64 . 101 . 111 . 229
Subnet Mask: 255 . 255 . 255 . 0
Default Gateway: 64 . 101 . 111 . 1
DNS 1: 0 . 0 . 0 . 0
DNS 2 (Optional): 0 . 0 . 0 . 0
DNS 3 (Optional): 0 . 0 . 0 . 0

Internet Connection Type > Static IP

Internet IP Address This is the router's IP address as seen from the Internet. Enter the IP address provided by your ISP.

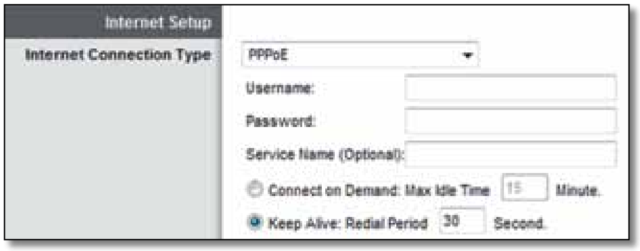
Subnet Mask This is the router's subnet mask as seen from the Internet. Enter the subnet mask provided by your ISP.

Default Gateway This is the IP address of your ISP's gateway server. Enter the gateway IP address provided by your ISP.

DNS 1-3 This is the IP address of your ISP's Domain Name System (DNS) server. Enter the DNS server IP address(es) provided by your ISP.

PPPoE

If you have a DSL connection, check whether your ISP uses Point-to-Point Protocol over Ethernet (PPPoE). If so, select PPPoE.



Internet Setup

Internet Connection Type: PPPoE ▾

Username:

Password:

Service Name (Optional):

○ Connect on Demand: Max Idle Time 15 Minute.

● Keep Alive: Redial Period 30 Second.

Internet Connection Type > PPPoE

Username Enter the username provided by your ISP.

Password Enter the password provided by your ISP.

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

Connect on Demand or Keep Alive

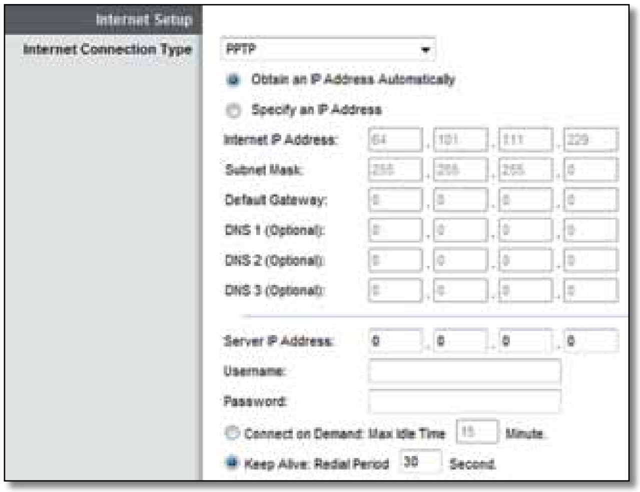
The Connect on Demand and Keep Alive options let you choose whether the router connects to the Internet only as needed (useful if your ISP charges for connect time), or if the router should always be connected. Select the appropriate option.

Connect on Demand: Max Idle Time This option causes the router to drop the Internet connection if the router is inactive for a specified period, and to reconnect only when you try to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the duration of inactivity allowed before your Internet connection terminates. The default is **5** minutes.

Keep Alive: Redial Period This option causes the router to periodically check its Internet connection and automatically reconnect if the connection is down. To use this option, keep the default, **Keep Alive**. In the *Redial Period* field, specify how often the router should check the Internet connection. The default is **30** seconds.

PPTP

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



Internet Setup

Internet Connection Type: PPTP ▾

● Obtain an IP Address Automatically

○ Specify an IP Address

Internet IP Address: 64 . 101 . 111 . 229

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

DNS 1 (Optional): 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

Username:

Password:

○ Connect on Demand: Max Idle Time 15 Minute.

● Keep Alive: Redial Period 30 Second.

Internet Connection Type > PPTP

If your PPTP connection supports DHCP or a dynamic IP address, then select **Obtain an IP Address Automatically**. If you are required to use a fixed IP address to connect to the Internet, then select **Specify an IP Address** and configure the options below.

Internet IP Address This is the router's IP address as seen from the Internet. Enter the IP address provided by your ISP.

Subnet Mask This is the router's subnet mask as seen from the Internet. Enter the subnet mask provided by your ISP.

Default Gateway This is the IP address of your ISP's gateway server. Enter the gateway IP address provided by your ISP.

DNS 1-3 This is the IP address of your ISP's DNS server. Enter the DNS server IP address(es) provided by your ISP.

Server IP Address This is the IP address of the PPTP server. Enter the IP address provided by your ISP.

Username Enter the username provided by your ISP.

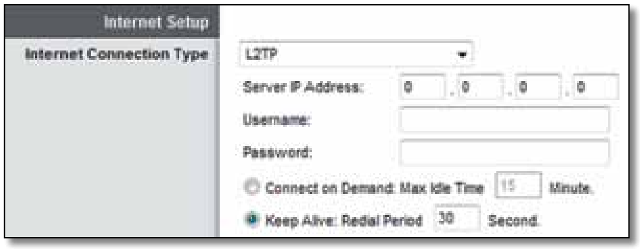
Password Enter the password provided by your ISP.

Connect on Demand: Max Idle Time For details, refer to "**Connect on Demand or Keep Alive**" on page 5.

Keep Alive: Redial Period For details, refer to "**Connect on Demand or Keep Alive**" on page 5.

L2TP

Layer 2 Tunneling Protocol (L2TP) is a service that generally applies to connections in Israel.


Internet Setup

Internet Connection Type: L2TP

Server IP Address: 0 . 0 . 0 . 0

Username:

Password:

○ Connect on Demand: Max Idle Time 15 Minute.

● Keep Alive: Redial Period 30 Second.

Internet Connection Type > L2TP

Server IP Address This is the IP address of the L2TP server. Enter the IP address provided by your ISP.

Username Enter the username provided by your ISP.

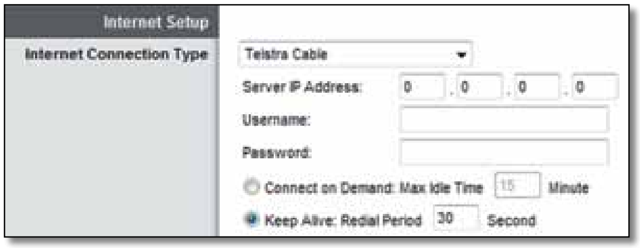
Password Enter the password provided by your ISP.

Connect on Demand: Max Idle Time For details, refer to "**Connect on Demand or Keep Alive**" on page 5.

Keep Alive: Redial Period For details, refer to "**Connect on Demand or Keep Alive**" on page 5.

Telstra Cable

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


Internet Setup

Internet Connection Type: Telstra Cable

Server IP Address: 0 . 0 . 0 . 0

Username:

Password:

○ Connect on Demand: Max Idle Time 15 Minute

● Keep Alive: Redial Period 30 Second

Internet Connection Type > Telstra Cable

Server IP Address This is the IP address of the Telstra Cable server. Enter the IP address provided by your ISP.

Username Enter the username provided by your ISP.

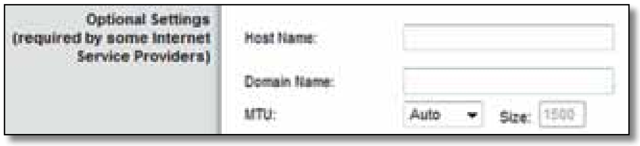
Password Enter the password provided by your ISP.

Connect on Demand: Max Idle Time For details, refer to "**Connect on Demand or Keep Alive**" on page 5.

Keep Alive: Redial Period For details, refer to "**Connect on Demand or Keep Alive**" on page 5.

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

Basic Setup > Optional Settings

Host Name Some ISPs, usually cable ISPs, require a host name as identification. You may have to check with your ISP to see if your service has been configured with a host name. Enter a host name for the router, if required. In most cases, you can leave this field blank.

Domain Name Some ISPs, usually cable ISPs, require a domain name as identification. You may have to check with your ISP to see if your service has been configured with a domain name. Enter a domain name for the router, if required. In most cases, you can leave this field blank.

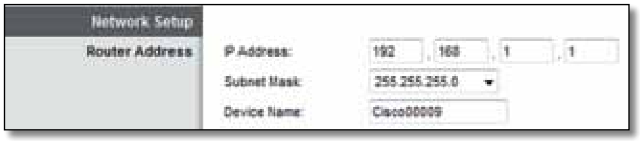
MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select **Manual** if you want to manually enter the largest packet size that is transmitted. To have the router select the best MTU for your Internet connection, keep the default, **Auto**.

Size When Manual is selected in the *MTU* field, this option is available. 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 configures the IP settings for your local network.


Network Setup

Router Address

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

Device Name: Cisco00009

Basic Setup > Router Address

Router Address

IP Address The router's local IP address is displayed. The default is **192.168.1.1**.

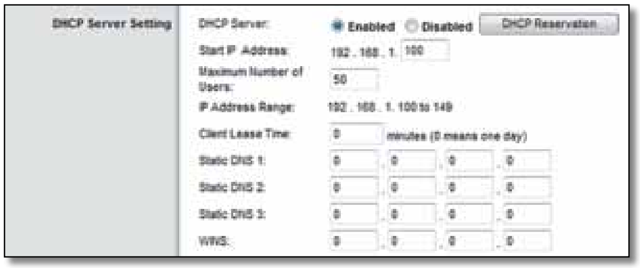
Subnet Mask The router's local subnet mask is displayed. The default is **255.255.255.0**.

Device Name The default is **Cisco** followed by the last 5 digits of the router's serial number, which is found on the bottom of the router. (The Device Name is also the router's NetBIOS name.) If you used the setup software for installation, then the Device Name is the name of your wireless network (up to 15 characters).

DHCP Server Settings

The settings allow you to configure the router's 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 or device on your network.

> **NOTE:** If you choose to enable the 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 to 149
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0 . 0 . 0 . 0
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0
WINS: 0 . 0 . 0 . 0

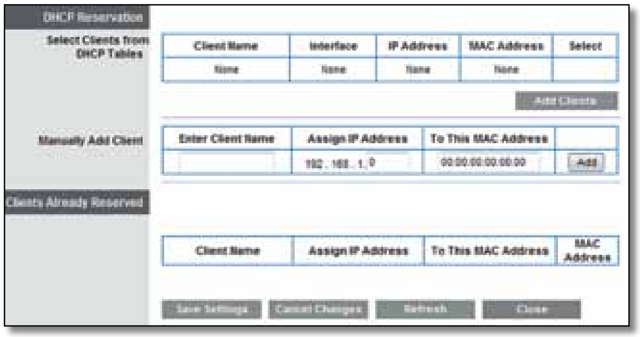
Basic Setup > DHCP Server Settings

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

DHCP Reservation Click **DHCP Reservation** if you want to assign a fixed local IP address to a specific device on your network. This is helpful if you have a device whose IP address must always remain the same, such as a media server or print server. To reserve an IP address for a specific device, select it from the list of devices or manually enter the Media Access Control (MAC) address of the device.

DHCP Reservation

The *DHCP Reservation* screen appears and displays a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address.


DHCP Reservation

Select Clients from DHCP Tables

Client Name	Interface	IP Address	MAC Address	Select
None	None	None	None	

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	MAC Address

Basic Setup > DHCP Reservation

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

Clients Already Reserved

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

Click **Save Settings** to apply your changes, or click **Cancel Changes** to clear your changes. To update the on-screen information, click **Refresh**. To exit this screen and return to the *Basic Setup* screen, click **Close**.

Start IP Address The Start IP Address specifies the starting IP address for the range of addresses assigned by your router when it functions as a DHCP server. (The first IP address assigned by the router will be randomly selected within the range you specify.)

Because the router's default IP address is 192.168.1.1, the Start IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.254. The default Start IP Address is **192.168.1.100**.

Maximum Number of Users The Maximum Number of Users specifies the number of IP addresses that can be assigned by your router when it functions as a DHCP server. This number cannot be greater than 253. The default is **50**.

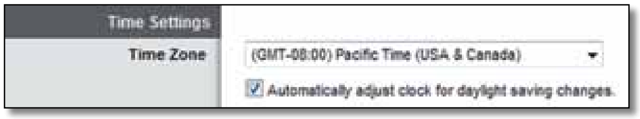
IP Address Range The range of available IP addresses is displayed.

Client Lease Time The Client Lease Time is the length of time that a dynamically assigned IP address will remain in effect. After this time is up, the device will be automatically assigned a new dynamic IP address, or the lease will be renewed. Enter the length of time, in minutes, that a user will be "leased" a 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, however, you wish to use a different DNS server, enter its IP address (you can enter up to three DNS server IP addresses). These static DNS server(s) will have higher priority than the ISP's DNS servers. The router will assign these DNS servers to the computers and other devices in your local network.

WINS The Windows Internet Naming Service (WINS) manages each computer's interaction with the Internet. If you use a WINS server, enter its IP address. Otherwise, leave this field blank.

Time Settings



Time Settings

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

☑ Automatically adjust clock for daylight saving changes.

Basic Setup > Time Settings

Time Zone Select your network's time zone from this drop-down menu.

Automatically adjust clock for daylight saving changes Select this option to have the router automatically adjust for daylight saving time.

Reboot

Reboot

Basic Setup > Reboot

Reboot Click this option to restart the router.

NOTE: If you have changed any settings on this screen, click **Save Settings** before you use the Reboot option; otherwise you will lose your new settings.

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, File Transfer Protocol (FTP) server, or other server behind the router.

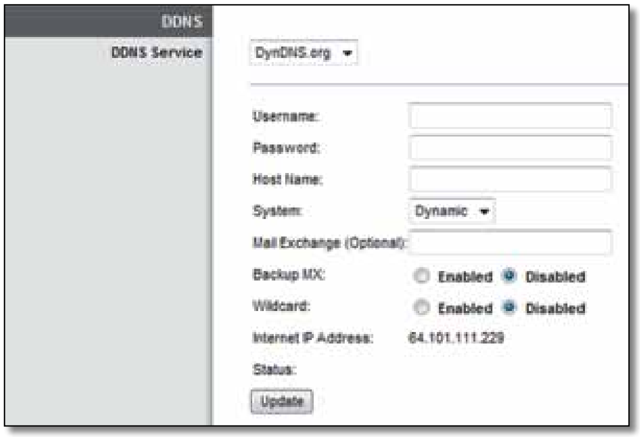
Before you can use this option, you need to sign up for DDNS service with a DDNS service provider, **www.dyndns.org** or **www.tzo.com**. If you do not want to use this option, keep the default, **Disabled**.

DDNS

DDNS Service

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

DynDNS.org



DDNS

DDNS Service DynDNS.org

Username:

Password:

Host Name:

System: Dynamic

Mail Exchange (Optional):

Backup MX: ○ Enabled ● Disabled

Wildcard: ○ Enabled ● Disabled

Internet IP Address: 64.101.111.229

Status:

Setup > DDNS > DynDNS

Username Enter the username for your DynDNS account.

Password Enter the password for your DynDNS account.

Host Name Enter the host name for your DynDNS account.

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

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

Backup MX This option allows the Mail eXchange (MX) server to be a backup. To disable this option, keep the default, **Disabled**. To enable the option, select **Enabled**. If you are not sure which setting to select, keep the default, **Disabled**.

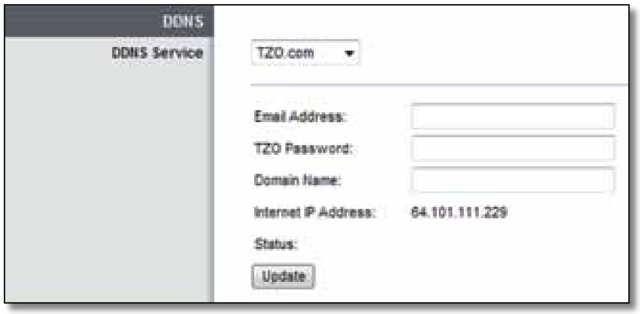
Wildcard This setting enables or disables wildcards for your host. For example, if your DDNS address is *myplace.dyndns.org* and you enable wildcards, then *x.myplace.dyndns.org* will work as well (x is the wildcard). To disable wildcards, keep the default, **Disabled**. To enable wildcards, select **Enabled**.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

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

Status The status of the DDNS service connection is displayed.

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

TZO.com



DDNS Service: TZO.com

Email Address:

TZO Password:

Domain Name:

Internet IP Address: 64.101.111.229

Status:

Setup > DDNS > TZO

Email Address Enter the email account for your TZO account.

TZO Password Enter the password for your TZO account.

Domain Name Enter the domain name for your TZO account.

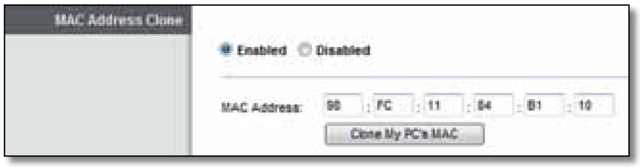
Internet IP Address The router's Internet IP address is displayed. Because it is dynamic, it will change periodically.

Status The status of the DDNS service connection is displayed.

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

Setup > MAC Address Clone

A Media Access Control (MAC) address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs require you to register a MAC address for Internet access. If your computer's MAC address is registered with your ISP and you do not wish to re-register the MAC address, then you may assign the registered MAC address to the router with the MAC Address Clone feature.



● Enabled ○ Disabled

MAC Address: 90 : FC : 11 : 84 : B1 : 10

Setup > MAC Address Clone

MAC Address Clone

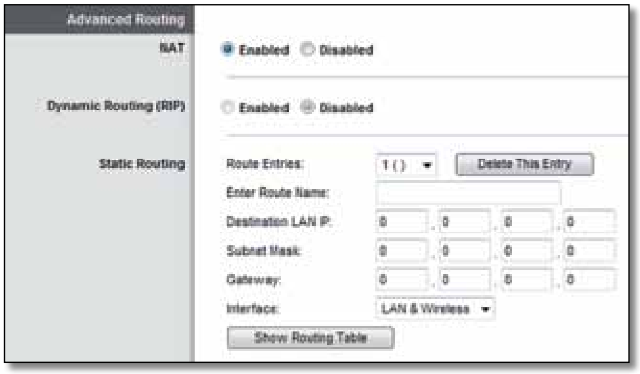
Enabled/Disabled To have the router clone the MAC address you specify below, select **Enabled**.

MAC Address Enter the MAC address registered with your ISP.

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

Setup > Advanced Routing

This screen is used to set up the router's advanced functions. Dynamic Routing automatically adjusts how packets travel on your network. Static Routing sets up a fixed route to another network destination.



NAT: ● Enabled ○ Disabled

Dynamic Routing (RIP): ○ Enabled ● Disabled

Static Routing

Route Entries: 1 ( )

Enter Route Name:

Destination LAN IP: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Gateway: 0 . 0 . 0 . 0

Interface: LAN & Wireless

Setup > Advanced Routing

Advanced Routing

NAT

Enabled/Disabled If this Router shares your Internet connection for your local network, keep the default, **Enabled**. When Network Address Translation (NAT) is disabled, dynamic routing is available.

Dynamic Routing (RIP)

Dynamic routing uses the Routing Information Protocol (RIP). This option enables the router to automatically 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.

Enabled/Disabled When NAT is disabled, the Dynamic Routing option is available. To use the Dynamic Routing option, select **Enabled**.

Static Routing

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

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

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

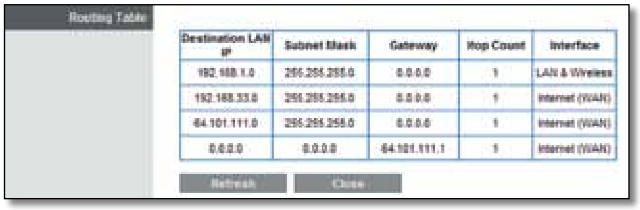
Destination LAN IP Enter the IP address of the remote network or host to which you want to assign a static route. (LAN stands for Local Area Network.)

Subnet Mask Enter the subnet mask for the Destination LAN IP address.

Gateway Enter the IP address of the gateway server that enables communication between the router and the remote network or host.

Interface Select the location of the Destination LAN IP address, the **LAN & Wireless** (Ethernet and wireless networks) or the **Internet (WAN)**. (WAN stands for Wide Area Network.)

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



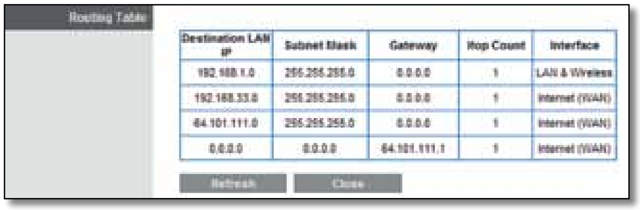
Routing Table

Destination LAN IP	Subnet Mask	Gateway	Hop Count	Interface
192.168.1.0	255.255.255.0	0.0.0.0	1	LAN & Wireless
192.168.33.0	255.255.255.0	0.0.0.0	1	Internet (WAN)
64.101.111.0	255.255.255.0	0.0.0.0	1	Internet (WAN)
0.0.0.0	0.0.0.0	64.101.111.1	1	Internet (WAN)

Advanced Routing > Routing Table

Routing Table

The *Routing Table* screen appears. For each route, the Destination LAN IP address, Subnet Mask, Gateway, Hop Count, and Interface are displayed.



Routing Table

Destination LAN IP	Subnet Mask	Gateway	Hop Count	Interface
192.168.1.0	255.255.255.0	0.0.0.0	1	LAN & Wireless
192.168.33.0	255.255.255.0	0.0.0.0	1	Internet (WAN)
64.101.111.0	255.255.255.0	0.0.0.0	1	Internet (WAN)
0.0.0.0	0.0.0.0	64.101.111.1	1	Internet (WAN)

Advanced Routing > Routing Table

Click **Refresh** to update the information. Click **Close** to exit this screen and return to the *Advanced Routing* screen.

Wireless > Basic Wireless Settings

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

Simultaneous Networks

For more wireless bandwidth, the router can create two simultaneous yet separate Wireless-N networks, one using the 5 GHz radio frequency band and one using the 2.4 GHz band. This allows you to isolate higher-priority traffic, such as online gaming, Voice over Internet Protocol (VoIP) calls, and video streaming.

For example, in this diagram ("**Simultaneous Networks Diagram**" on page 11), the 2.4 GHz wireless network is represented by green waves between the router and the office devices, the wireless printer and notebook. The 5 GHz wireless network is represented by the blue waves between the router and the living room devices, the gaming console and media player.

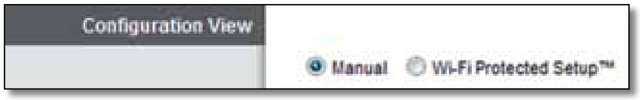
Choose which computers and other wireless devices should join which network. Wireless-N devices support both the 5 GHz and 2.4 GHz bands, so they can join either network. Wireless-G and Wireless-B devices support only the 2.4 GHz band, so they should join the 2.4 GHz network. Wireless-A devices support only the 5 GHz band, so they should join the 5 GHz network.

For the 5 GHz network, configure all computers and other wireless devices with the same 5 GHz Network Name and wireless security settings. For the 2.4 GHz network, configure all computers and other wireless devices with the same 2.4 GHz Network Name and wireless security settings.

NOTE: You should use the same Network Name for both your 5 GHz and 2.4 GHz wireless networks; this allows seamless roaming by dual-band Wireless-N client devices.

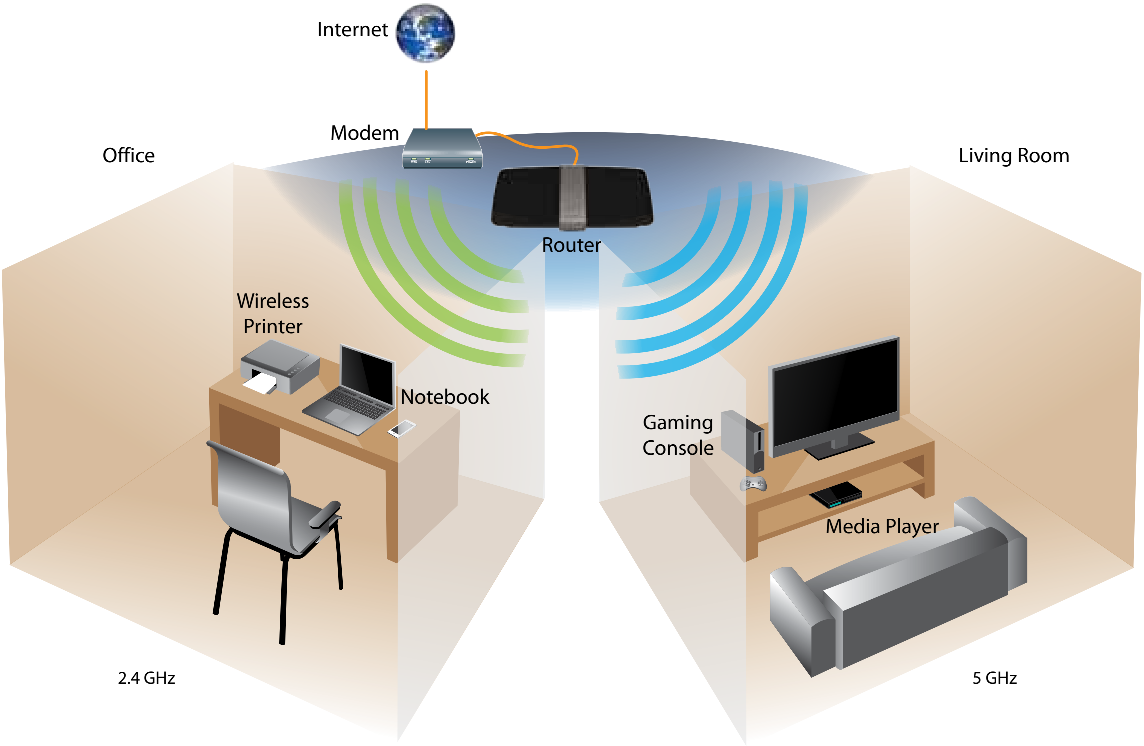
You can use Wi-Fi Protected Setup to set up both networks, or you can manually configure the router. Wi-Fi Protected Setup is a feature that makes it easy to set up your wireless network. If you have client devices, such as wireless printers, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup.

Configuration View To manually configure your wireless networks, select **Manual**. Go to "**Manual Setup**" on page 12. To use Wi-Fi Protected Setup, select **Wi-Fi Protected Setup**. Go to "**Wi-Fi Protected Setup**" on page 13.


Configuration View

● Manual ○ Wi-Fi Protected Setup™

Basic Wireless Settings (Manual) > Configuration View

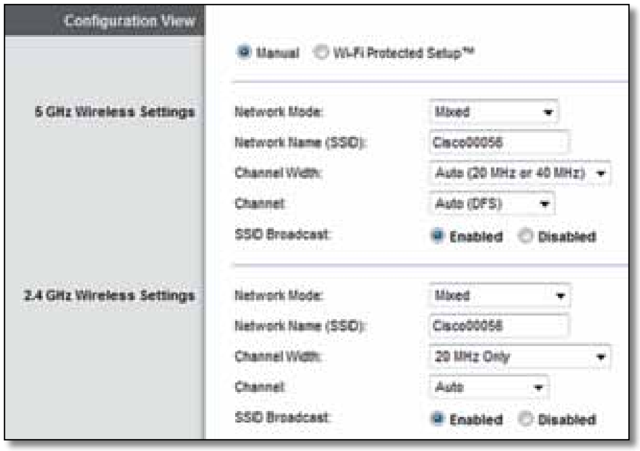


Simultaneous Networks Diagram

Manual Setup

Set up the 5 GHz and 2.4 GHz wireless networks on this screen.

NOTE: After you set up the wireless network(s), set up the wireless security settings. Go to "**Wireless > Wireless Security**" on page 14.


Configuration View

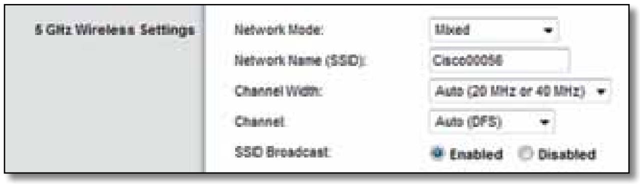
● Manual ○ Wi-Fi Protected Setup™

5 GHz Wireless Settings
Network Mode: Mixed
Network Name (SSID): Cisco00056
Channel Width: Auto (20 MHz or 40 MHz)
Channel: Auto (DFS)
SSID Broadcast: ● Enabled ○ Disabled

2.4 GHz Wireless Settings
Network Mode: Mixed
Network Name (SSID): Cisco00056
Channel Width: 20 MHz Only
Channel: Auto
SSID Broadcast: ● Enabled ○ Disabled

Wireless > Basic Wireless Settings (Manual)

5 GHz Wireless Settings


5 GHz Wireless Settings
Network Mode: Mixed
Network Name (SSID): Cisco00056
Channel Width: Auto (20 MHz or 40 MHz)
Channel: Auto (DFS)
SSID Broadcast: ● Enabled ○ Disabled

Basic Wireless Settings (Manual) > 5 GHz Wireless Settings

Network Mode Select the wireless standards your network will support.

- **Mixed** If you have Wireless-A and Wireless-N (5 GHz) devices in your network, keep the default, **Mixed**.
- **Wireless-A Only** If you have only Wireless-A devices, select **Wireless-A Only**.
- **Wireless-N Only** If you have only Wireless-N (5 GHz) devices, select **Wireless-N Only**.
- **Disabled** If you do not have any Wireless-A and Wireless-N (5 GHz) devices in your 5 GHz network, select **Disabled**.

NOTE: If you are not sure which mode to use, keep the default, **Mixed**.

Network Name (SSID) The Service Set Identifier (SSID) is the network name shared by all devices in a wireless network. It is case-sensitive and must not exceed 32 keyboard characters. The default is **Cisco** followed by the last 5 digits of the router's serial number, which is found on the bottom of the router. If you used the setup software for installation, then the default Network Name is changed to an easy-to-remember name.

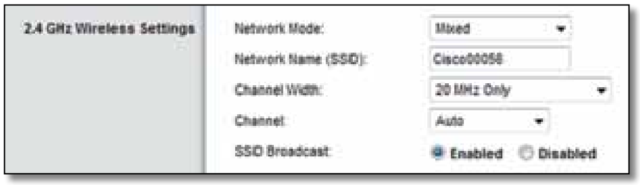
NOTE: If you restore the router's factory default settings (by pressing the Reset button or using the *Administration > Factory Defaults* screen), the Network Name will return to its default value, and all devices on your wireless network will need to be reconnected.

Channel Width For best performance in a network using Wireless-A and Wireless-N (5 GHz) devices, keep the default, **Auto (20 MHz or 40 MHz)**. For a channel width of 40 MHz, select **40 MHz Only**. For a channel width of 20 MHz, select **20 MHz Only**.

Channel Select the channel from the drop-down list for Wireless-A and Wireless-N (5 GHz) networking. If you are not sure which channel to select, then keep the default, **Auto (DFS)**.

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

2.4 GHz Wireless Settings


2.4 GHz Wireless Settings
Network Mode: Mixed
Network Name (SSID): Cisco00056
Channel Width: 20 MHz Only
Channel: Auto
SSID Broadcast: ● Enabled ○ Disabled

Basic Wireless Settings (Manual) > 2.4 GHz Wireless Settings

Network Mode Select the wireless standards your network will support.

- **Mixed** If you have Wireless-N (2.4 GHz), Wireless-G, and Wireless-B devices in your network, keep the default, **Mixed**.
- **Wireless-B/G Only** If you have both Wireless-B and Wireless-G (2.4 GHz) devices in your network, select **Wireless-B/G Only**.
- **Wireless-B Only** If you have only Wireless-B devices, select **Wireless-B Only**.
- **Wireless-G Only** If you have only Wireless-G devices, select **Wireless-G Only**.
- **Wireless-N Only** If you have only Wireless-N (2.4 GHz) devices, select **Wireless-N Only**.
- **Disabled** If you have no Wireless-B, Wireless-G, and Wireless-N (2.4 GHz) devices in your network, select **Disabled**.

NOTE: If you are not sure which mode to use, keep the default, **Mixed**.

Network Name (SSID) The Service Set Identifier (SSID) is the network name shared by all devices in a wireless network. It is case-sensitive and must not exceed 32 keyboard characters. The default is **Cisco** followed by the last 5 digits of the router's serial number, which is found on the bottom of the router. If you used the setup software for installation, then the default Network Name is changed to an easy-to-remember name.

NOTE: If you restore the router's factory default settings (by pressing the Reset button or using the *Administration* > *Factory Defaults* screen), the Network Name will return to its default value, and all devices on your wireless network will need to be reconnected.

Channel Width For best performance in a network using Wireless-B, Wireless-G and Wireless-N (2.4 GHz) devices, select **Auto (20 MHz or 40 MHz)**. For a channel width of 20 MHz, keep the default, **20 MHz only**.

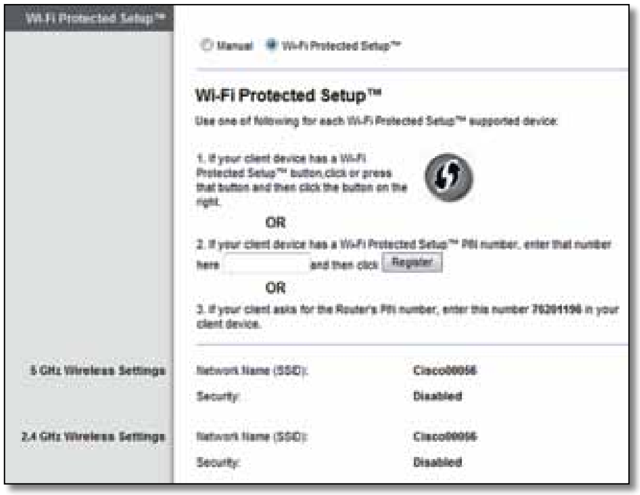
Channel Select the channel from the drop-down list for Wireless-B, Wireless-G, and Wireless-N (2.4 GHz) networking. If you are not sure which channel to select, then keep the default, **Auto**.

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

Wi-Fi Protected Setup

Wi-Fi Protected Setup is a feature that makes it easy to set up your wireless network. If you have client devices, such as wireless printers, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup.

Three methods of Wi-Fi Protected Setup are available. Use the method that applies to the client device you are configuring.



Wi-Fi Protected Setup™

○ Manual ● Wi-Fi Protected Setup™

Wi-Fi Protected Setup™

Use one of following for each Wi-Fi Protected Setup™ supported device:

1. If your client device has a Wi-Fi Protected Setup™ button,click or press that button and then click the button on the right.

OR

2. If your client device has a Wi-Fi Protected Setup™ PIN number, enter that number here [ ] and then click [Register]

OR

3. If your client asks for the Router's PIN number, enter this number 76201196 in your client device.

5 GHz Wireless Settings	Network Name (SSID):	Cisco00056
	Security:	Disabled
2.4 GHz Wireless Settings	Network Name (SSID):	Cisco00056
	Security:	Disabled

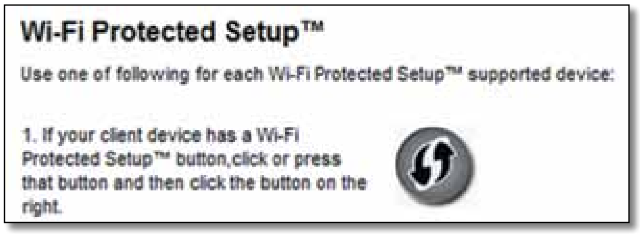
Wireless > Basic Wireless Settings (Wi-Fi Protected Setup)

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.

Wi-Fi Protected Setup Light Activity

- The Cisco logo on the top panel of the router functions as the Wi-Fi Protected Setup light.
- When the Wi-Fi Protected Setup process is active, the light flashes slowly. When the Wi-Fi Protected Setup is successful, the light is continuously lit.
- If there is an error, the light flashes quickly for two minutes; please wait and try again.
- Wait until the light is continuously lit, before starting the next Wi-Fi Protected Setup session.
- **Wi-Fi Protected Setup Button** Use this method if your client device has a Wi-Fi Protected Setup button.

NOTE: Make sure you configure one client device at a time.



Wi-Fi Protected Setup™

Use one of following for each Wi-Fi Protected Setup™ supported device:

1. If your client device has a Wi-Fi Protected Setup™ button,click or press that button and then click the button on the right.

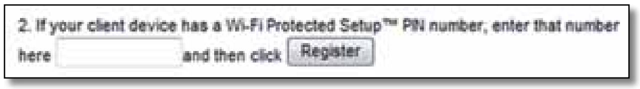
Wi-Fi Protected Setup > Wi-Fi Protected Setup Button

a. Click or press the **Wi-Fi Protected Setup** button on the client device.

b. Click the **Wi-Fi Protected Setup** button on the router's *Wi-Fi Protected Setup* screen, OR press and hold the Wi-Fi Protected Setup button on the back panel of the router for one second.

c. After the client device has been configured, click **OK** on the router's *Wi-Fi Protected Setup* screen within two minutes.

- **Enter Client Device PIN on Router** Use this method if your client device has a Wi-Fi Protected Setup PIN (Personal Identification Number).



2. If your client device has a Wi-Fi Protected Setup™ PIN number, enter that number here and then click Register

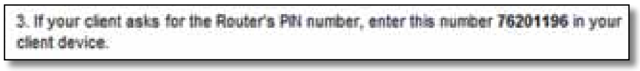
Wi-Fi Protected Setup > Enter Client Device PIN on Router

a. Enter the PIN from the client device in the field on the router's *Wi-Fi Protected Setup* screen.

b. Click the **Register** button on the router's *Wi-Fi Protected Setup* screen.

c. After the client device has been configured, click **OK** on the router's *Wi-Fi Protected Setup* screen within two minutes.

- **Enter Router PIN on Client Device** Use this method if your client device asks for the router's PIN.



3. If your client asks for the Router's PIN number, enter this number 76201196 in your client device.

Wi-Fi Protected Setup > Enter Router PIN on Client Device

a. On the client device, enter the PIN listed on the router's *Wi-Fi Protected Setup* screen. (It is also listed on the bottom of the router.)

b. After the client device has been configured, click **OK** on the router's *Wi-Fi Protected Setup* screen within two minutes.

For each wireless network, the Network Name (SSID), Security, 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(s). The router supports the following wireless security options: WPA2/WPA Mixed Mode, WPA2 Personal, WPA Personal, WPA2/WPA Enterprise Mixed Mode, WPA2 Enterprise, WPA Enterprise, WEP, and RADIUS. (WPA stands for Wi-Fi Protected Access. WEP stands for Wireless Equivalent Privacy. RADIUS stands for Remote Authentication Dial-In User Service.)

Personal Options

Security Option	Strength
WPA2 Personal	Strongest
WPA2/WPA Mixed Mode	WPA2: Strongest WPA: Strong
WPA Personal	Strong
WEP	Basic

Office Options

The office options are available for networks that use a RADIUS server for authentication. The office options are stronger than the personal options because WPA2 or WPA provides encryption while RADIUS provides authentication.

Security Option	Strength
WPA2 Enterprise	Strongest
WPA2/WPA Enterprise Mixed Mode	WPA2: Strongest WPA: Strong
WPA Enterprise	Strong
RADIUS	Basic

5 GHz Wireless Security or 2.4 GHz Wireless Security

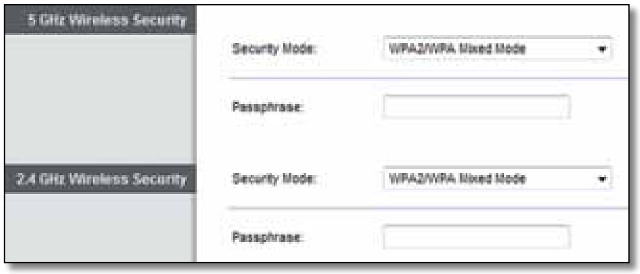
Wireless security is strongly recommended, and WPA2 is the strongest method available. Use WPA2 if it is supported by all of your wireless devices.

Security Mode

The 5 GHz and 2.4 GHz networks can use different security options. Select the security option for each wireless network. Then go to the instructions for your selection.

WPA2/WPA Mixed Mode

NOTE: If you select WPA2/WPA Mixed Mode as your Security Mode, each device in your wireless network MUST use WPA2/WPA and the same passphrase.


5 GHz Wireless Security

Security Mode: WPA2/WPA Mixed Mode

Passphrase:

2.4 GHz Wireless Security

Security Mode: WPA2/WPA Mixed Mode

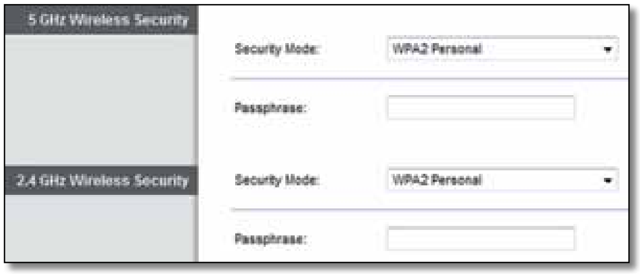
Passphrase:

Wireless Security > WPA2/WPA Mixed Mode

Passphrase Enter a passphrase of 8-63 characters. The default is **password**. If you used the setup software for installation, then the default is changed to a unique passphrase.

WPA2 Personal

NOTE: If you select WPA2 Personal as your Security Mode, each device in your wireless network MUST use WPA2 Personal and the same passphrase.


5 GHz Wireless Security

Security Mode: WPA2 Personal

Passphrase:

2.4 GHz Wireless Security

Security Mode: WPA2 Personal

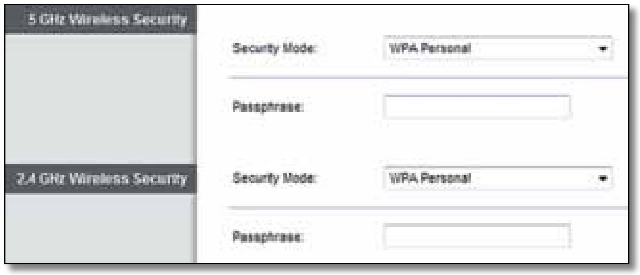
Passphrase:

Wireless Security > WPA2 Personal

Passphrase Enter a passphrase of 8-63 characters. The default is **password**. If you used the setup software for installation, then the default is changed to a unique passphrase.

WPA Personal

NOTE: If you select WPA Personal as your Security Mode, each device in your wireless network MUST use WPA Personal and the same passphrase.


5 GHz Wireless Security

Security Mode: WPA Personal

Passphrase:

2.4 GHz Wireless Security

Security Mode: WPA Personal

Passphrase:

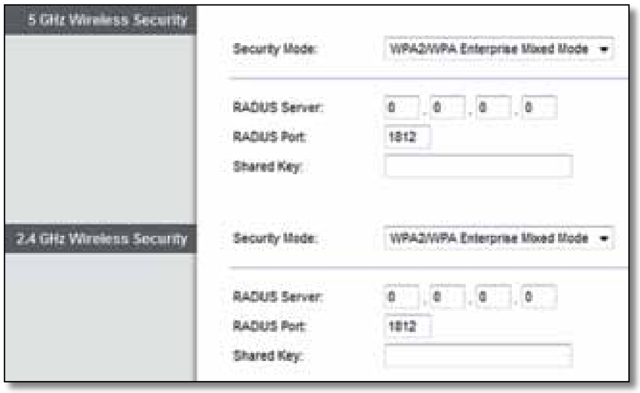
Wireless Security > WPA Personal

Passphrase Enter a passphrase of 8-63 characters. The default is **password**. If you used the setup software for installation, then the default is changed to a unique passphrase.

WPA2/WPA Enterprise Mixed Mode

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

NOTE: If you select WPA2/WPA Enterprise Mixed Mode as your Security Mode, each device in your wireless network MUST use WPA2/WPA Enterprise and the same shared key.


5 GHz Wireless Security

Security Mode: WPA2/WPA Enterprise Mixed Mode

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Key:

2.4 GHz Wireless Security

Security Mode: WPA2/WPA Enterprise Mixed Mode

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Key:

Wireless Security > WPA2/WPA Enterprise Mixed Mode

RADIUS Server Enter the IP address of the RADIUS server.

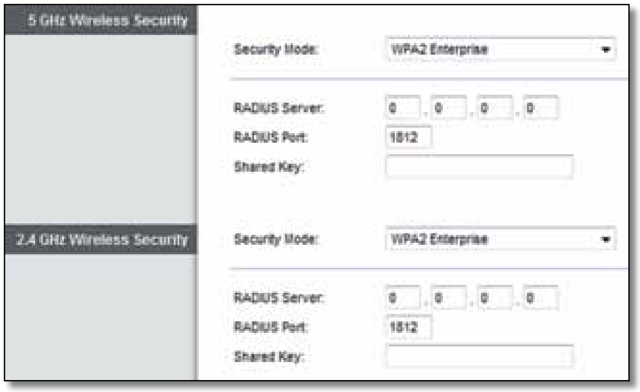
RADIUS Port Enter the port number of the RADIUS server. The default is **1812**.

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

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.)

NOTE: If you select WPA2 Enterprise as your Security Mode, each device in your wireless network MUST use WPA2 Enterprise and the same shared key.



5 GHz Wireless Security

Security Mode: WPA2 Enterprise

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Key:

2.4 GHz Wireless Security

Security Mode: WPA2 Enterprise

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Key:

Wireless Security > WPA2 Enterprise

RADIUS Server Enter the IP address of the RADIUS server.

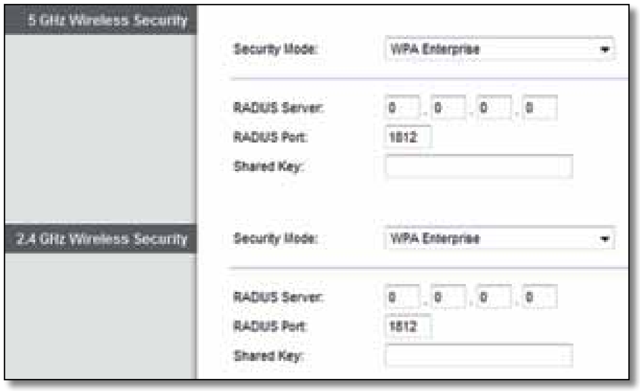
RADIUS Port Enter the port number of the RADIUS server. The default is **1812**.

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

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.)

NOTE: If you select WPA Enterprise as your Security Mode, each device in your wireless network MUST use WPA Enterprise and the same shared key.



5 GHz Wireless Security

Security Mode: WPA Enterprise

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Key:

2.4 GHz Wireless Security

Security Mode: WPA Enterprise

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Key:

Wireless Security > WPA Enterprise

RADIUS Server Enter the IP address of the RADIUS server.

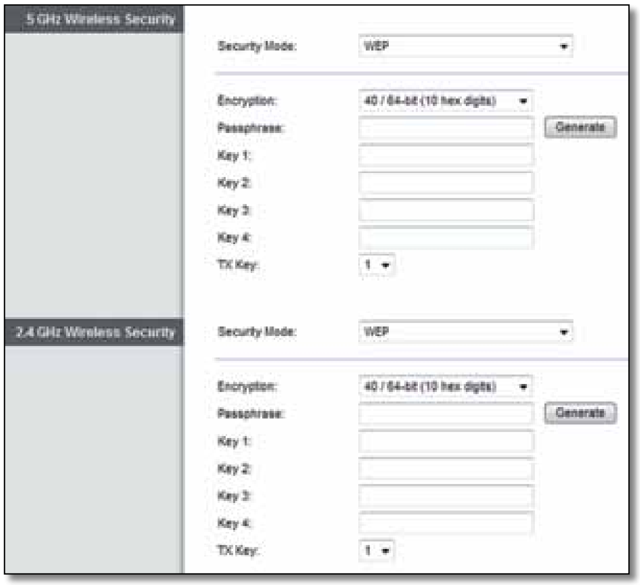
RADIUS Port Enter the port number of the RADIUS server. The default is **1812**.

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

WEP

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

NOTE: If you select WEP as your Security Mode, each device in your wireless network MUST use WEP and the same encryption and shared key.



5 GHz Wireless Security

Security Mode: WEP

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

Passphrase: Generate

Key 1:

Key 2:

Key 3:

Key 4:

TX Key: 1

2.4 GHz Wireless Security

Security Mode: WEP

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

Passphrase: Generate

Key 1:

Key 2:

Key 3:

Key 4:

TX Key: 1

Wireless Security > WEP

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

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

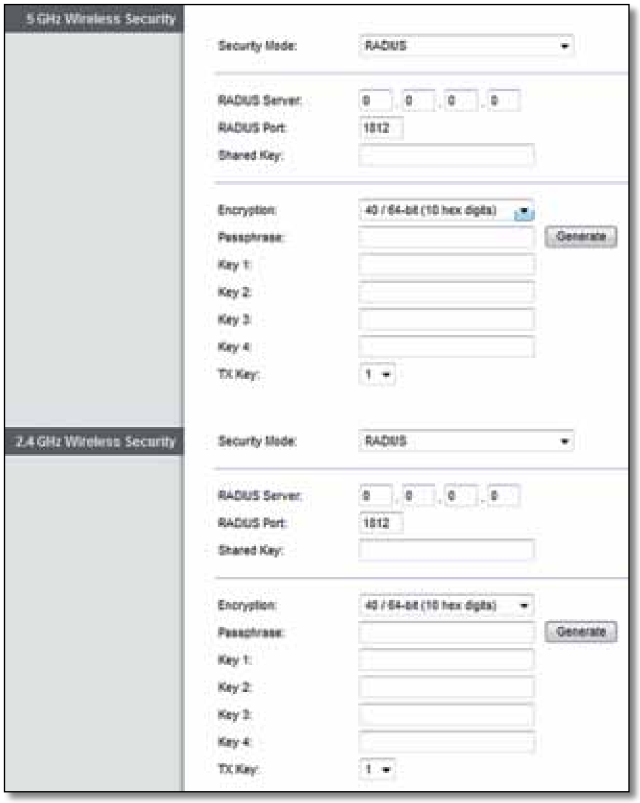
Key 1-4 If you did not enter a passphrase, enter the WEP key(s) manually.

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

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.)

> **NOTE:** If you select RADIUS as your Security Mode, each device in your wireless network MUST use RADIUS and the same encryption and shared key.



5 GHz 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

2.4 GHz 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

Wireless Security > RADIUS

RADIUS Server Enter the IP address of the RADIUS server.

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

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

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

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

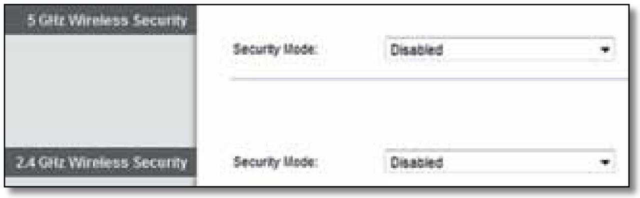
Key 1-4 If you did not enter a passphrase, enter the WEP key(s) manually.

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

Disabled

If you choose to disable wireless security, you will be informed that wireless security is disabled when you first attempt to access the Internet. You will given the option to enable wireless security, or confirm that you understand the risks but still wish to proceed without wireless security.

> **NOTE:** When wireless security is disabled, anyone can access your wireless network at any time.



5 GHz Wireless Security

Security Mode: Disabled

2.4 GHz Wireless Security

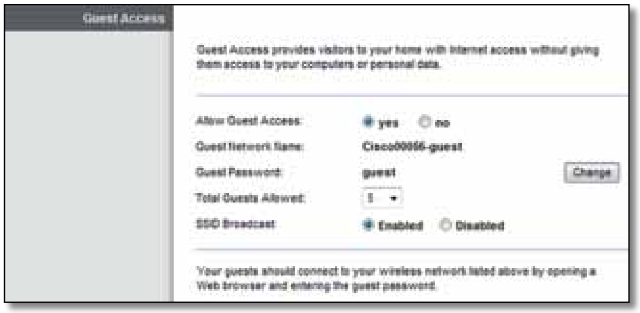
Security Mode: Disabled

Wireless Security > Disabled

Wireless > Guest Access

The Guest Access feature allows you to provide guests visiting your home with Internet access via wireless. The guest network is a wireless network separate from your local network. The Guest Access feature does not provide access to the local network and its resources, so your guests will not have access to your computers or personal data. For example, the guest computer cannot print to a printer on the local network or copy files to a computer on the local network. This helps minimize exposure of your local network.

For example, in the diagram ("**Local Access and Guest Access Diagram**" on page 18), the local network includes the wired network and the local wireless network, which is represented by yellow waves between the router and the wireless printer in the office and the notebook in the bedroom. The Guest Access feature is represented by the purple waves between the router and the notebook in the living room.



Guest Access provides visitors to your home with Internet access without giving them access to your computers or personal data.

Allow Guest Access: ● yes ○ no

Guest Network Name: Cisco00056-guest

Guest Password: guest

Total Guests Allowed: 5

SSID Broadcast: ● Enabled ○ Disabled

Your guests should connect to your wireless network listed above by opening a Web browser and entering the guest password.

Wireless > Guest Access

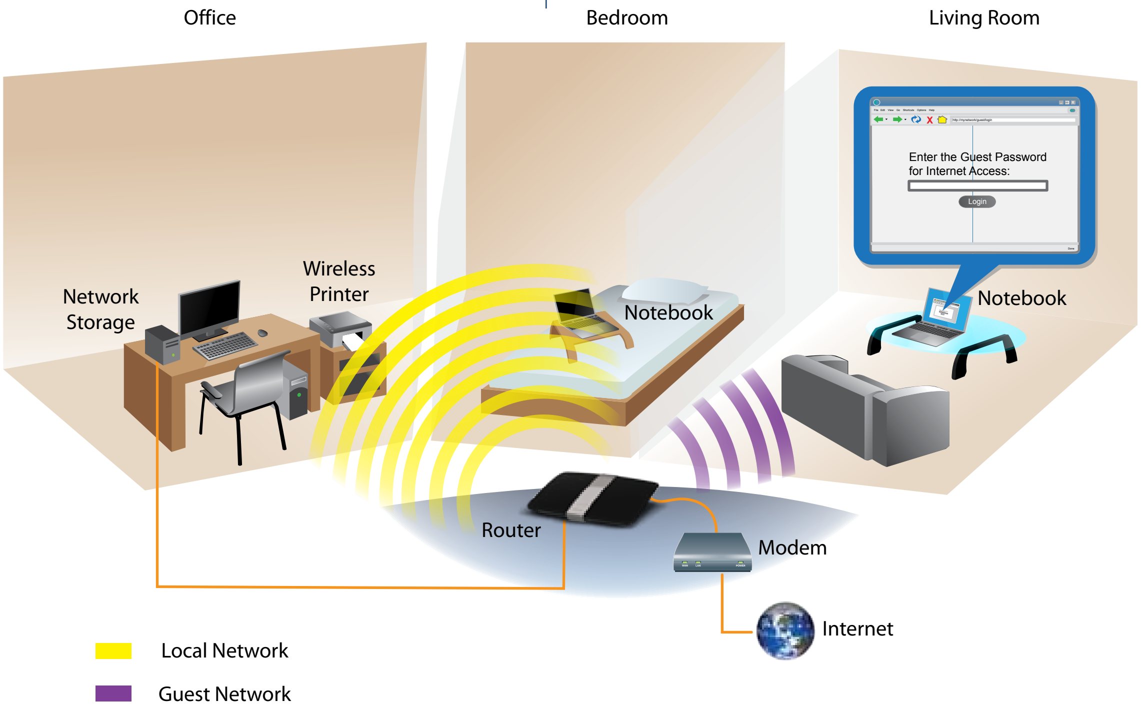
Guest Access

Allow Guest Access To allow Internet access through a guest network, keep the default, **yes**. Otherwise, select **no**.

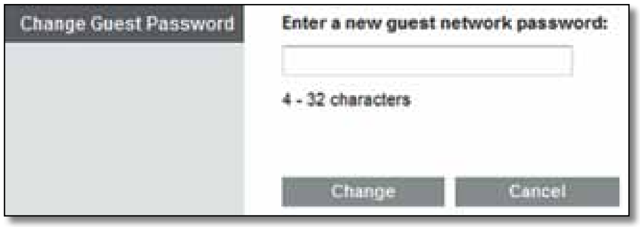
Guest Network Name The default is the name of your wireless network, followed by **-guest**.

Guest Password The default is **guest**. If you used the setup software for installation, then the default is changed to a unique password.

Change Click this option to change the Guest Password. The *Change Guest Password* screen appears.



Local Access and Guest Access Diagram



Change Guest Password

Enter a new guest network password:

4 - 32 characters

Guest Access > Change Guest Password

Change Guest Password

- **Enter a new guest network password** Enter a password of 4-32 characters.

  Then click **Change** to save the new password and return to the *Guest Access* screen.

Total Guests Allowed By default, **5** guests are allowed Internet access through the guest network. Select the number of guests you want to allow on your guest network.

SSID Broadcast When wireless devices survey the local area for wireless networks to associate with, they will detect the SSID (wireless network name) broadcast by the router. To broadcast the SSID of the guest network, keep the default, **Enabled**. If you do not want to broadcast the SSID of the guest network, then select **Disabled**.

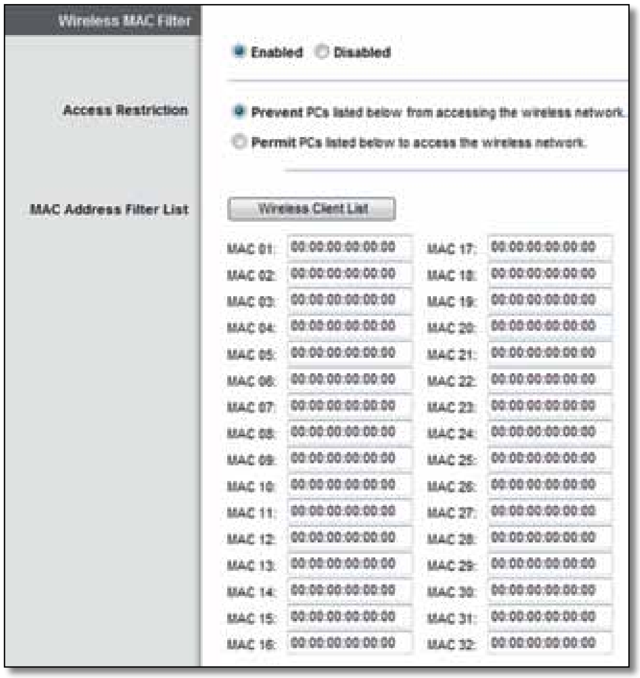
Guest Instructions

When a guest wants Internet access in your home, provide these instructions:

1. On the guest computer, connect to the wireless guest network named on the *Guest Access* screen.
2. Open a web browser.
3. On the login screen, enter the password displayed on the *Guest Access* screen.
4. Click **Login**.

Wireless > Wireless MAC Filter

Wireless access can be filtered (restricted) by specifying the MAC addresses of the devices in your wireless network(s).



Wireless MAC Filter

● Enabled ○ Disabled

Access Restriction

● Prevent PCs listed below from accessing the wireless network.

○ Permit PCs listed below to access the wireless network.

MAC Address Filter List

MAC 01:	00:00:00:00:00:00	MAC 17:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 18:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 19:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 20:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 21:	00:00:00:00:00:00
MAC 06:	00:00:00:00:00:00	MAC 22:	00:00:00:00:00:00
MAC 07:	00:00:00:00:00:00	MAC 23:	00:00:00:00:00:00
MAC 08:	00:00:00:00:00:00	MAC 24:	00:00:00:00:00:00
MAC 09:	00:00:00:00:00:00	MAC 25:	00:00:00:00:00:00
MAC 10:	00:00:00:00:00:00	MAC 26:	00:00:00:00:00:00
MAC 11:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00
MAC 12:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 13:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 14:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 15:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00
MAC 16:	00:00:00:00:00:00	MAC 32:	00:00:00:00:00:00

Wireless > Wireless MAC Filter

Wireless MAC Filter

Enabled/Disabled To filter wireless users by the MAC addresses of their computers or devices, select **Enabled**. Otherwise, keep the default, **Disabled**.

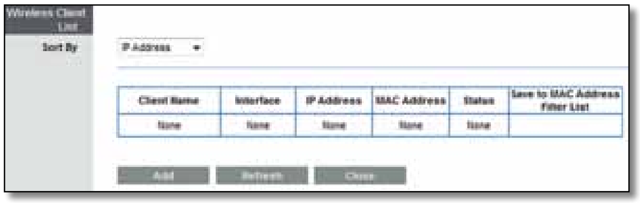
Access Restriction

Prevent PCs listed below from accessing the wireless network When the Wireless Mac Filter is enabled and this option is selected, computers on the MAC Address filter list will not have access to the wireless network.

Permit PCs listed below to access to the wireless network When the Wireless Mac Filter is enabled and this option is selected, only computers on the MAC Address filter list will have access to the wireless network.

MAC Address Filter List

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



Wireless Client List

Sort By: IP Address

Client Name	Interface	IP Address	MAC Address	Status	Save to MAC Address Filter List
None	None	None	None	None	

Wireless MAC Filter > Wireless Client List

Wireless Client List

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

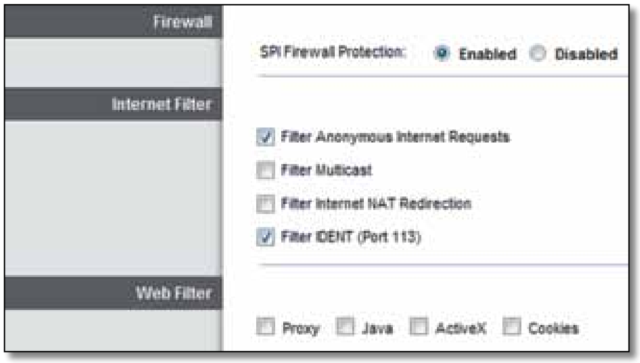
Select **Save to MAC Address Filter List** for any device you want to add to the MAC Address Filter List. Then click **Add**.

To update the on-screen information, click **Refresh**. To exit this screen and return to the *Wireless MAC Filter* screen, click **Close**.

MAC 01-32 Enter the MAC addresses of the devices whose wireless access you want to control.

Security > Firewall

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



SPI Firewall Protection: ● Enabled ○ Disabled

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

□ Proxy □ Java □ ActiveX □ Cookies

Security > Firewall

Firewall

SPI Firewall Protection SPI firewall protection helps protect your local network from the Internet. This option is enabled by default.

WARNING: To help protect your local network, you should keep the SPI Firewall Protection option enabled.

Internet Filters

Filter Anonymous Internet Requests This filter blocks Internet requests from unknown sources, such as ping requests. This option is enabled by default.

Filter Multicast Multicasting allows a single transmission to simultaneously reach specific recipients within your local network. Select this option to enable the filter that blocks multicasting. This option is disabled by default.

Filter Internet NAT Redirection This filter prevents a local computer from using a URL or Internet IP address to access the local server. Select this option to enable the filter. This option is disabled by default.

Filter IDENT (Port 113) This filter keeps port 113 from being scanned by devices from the Internet. This option is enabled by default.

Web Filters

Proxy This filter blocks the use of Internet proxy servers. To deny proxy requests, select this option. Proxy access is allowed by default.

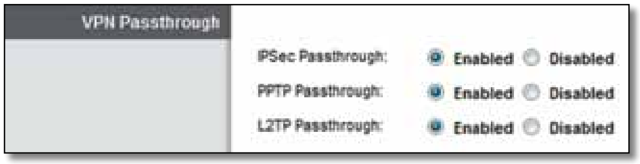
Java This filter blocks Java, so you may not be able to access Java content on websites. To deny Java requests, select this option. Java content is allowed by default.

ActiveX This filter blocks ActiveX, so you may not be able to access ActiveX content on websites. To deny ActiveX requests, select this option. ActiveX content is allowed by default.

Cookies This filter blocks cookies, which are data stored on your computer and used by websites when you interact with them. To deny cookie requests, select this option. Cookie usage is allowed by default.

Security > VPN Passthrough

The *VPN Passthrough* screen allows you to enable Virtual Private Network (VPN) tunnels using IPSec, PPTP, or L2TP protocols to pass through the router's firewall.



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

Security > VPN Passthrough

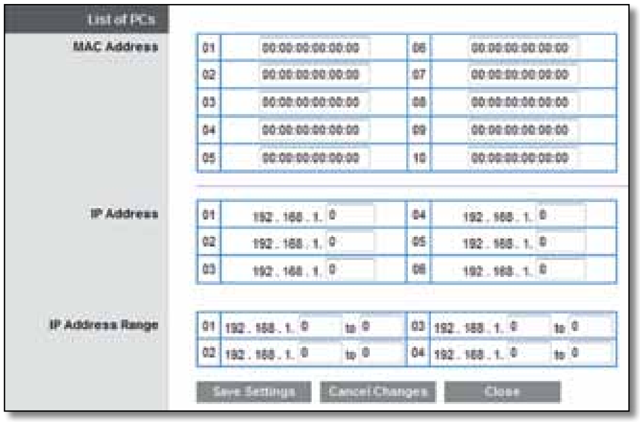
VPN Passthrough

IPSec Passthrough Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. The VPN client(s) on the local network can establish an IPSec VPN tunnel through the router. This option is enabled by default.

PPTP Passthrough Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. The VPN client(s) on the local network can establish a PPTP VPN tunnel through the router. This option is enabled by default.

L2TP Passthrough Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. The VPN client(s) on the local network can establish an L2TP VPN tunnel through the router. This option is enabled by default.

byour changes. Then click **Close** to exit this screen and return to the *Internet Access Policy* screen.



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

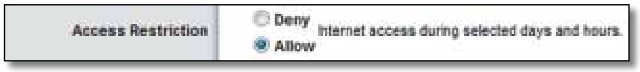
01	192 . 168 . 1. 0	04	192 . 168 . 1. 0
02	192 . 168 . 1. 0	05	192 . 168 . 1. 0
03	192 . 168 . 1. 0	06	192 . 168 . 1. 0

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

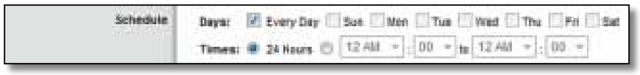
6. To block Internet access for the computers on the *List of PCs* screen, select **Deny**. To allow Internet access for the computers on the *List of PCs* screen, select **Allow**.



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

Deny or Allow

7. 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 **Every Day**. Then enter a time span during which the policy will be in effect, or select **24 Hours**.



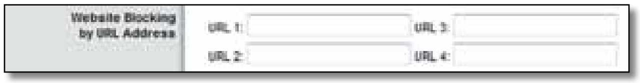
Schedule

Days: ☑ Every Day □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

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

Schedule

7. To block websites with specific URL addresses, enter each URL in a separate *Website Blocking by URL Address* field.



Website Blocking by URL Address

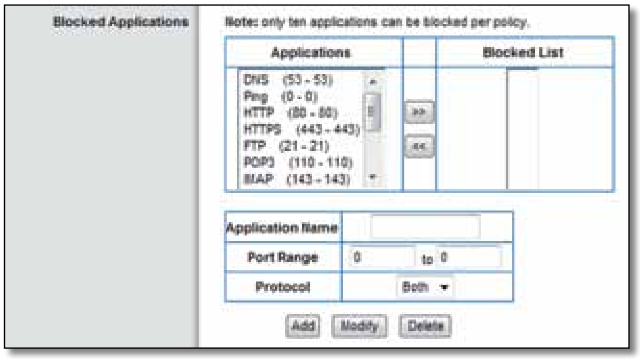
URL 1: URL 3:

URL 2: URL 4:

Website Blocking by URL Address

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

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



Blocked Applications

Note: only ten applications can be blocked per policy.

Applications		Blocked List
DNS (53 - 53) Ping (0 - 0) HTTP (80 - 80) HTTPS (443 - 443) FTP (21 - 21) POP3 (110 - 110) IMAP (143 - 143)	>> <<	

Application Name	
Port Range	0 to 0
Protocol	Both

Blocked Applications

9. If the application you want to block is not listed or you want to edit a service's settings, enter the application's name in the *Application Name* field. Enter its range in the *Port Range* fields. Select **TCP** (Transmission Control Protocol), **UDP** (User Datagram Protocol), or **Both** from the *Protocol* drop-down menu. Then click **Add**.

   To modify a service, select it from the *Applications* column. Change its Application Name, Port Range, and/or Protocol setting. Then click **Modify**.

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

10. Click **Save Settings** to save the policy's settings, or click **Cancel Changes** to clear the changes.

NOTE: If you have already set up Parental Controls and now want to use Internet Access Policy, then you will be asked to enter the password for Parental Controls before you can click Save Settings.

Storage > Disk

The router’s USB port lets you connect USB storage that can be accessed over your network.

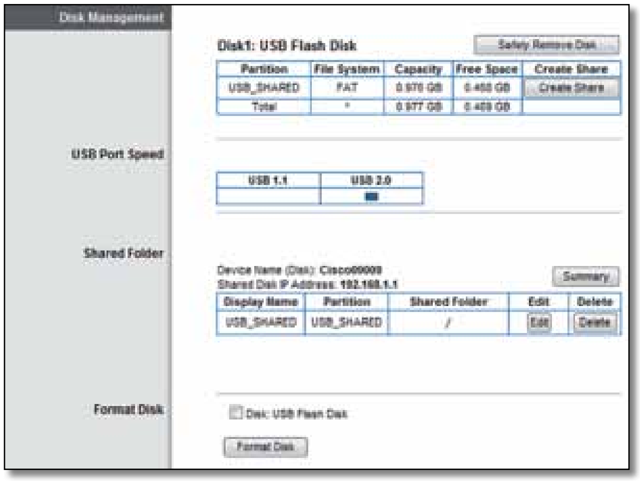
When you connect a USB storage device to the router’s USB port, you can access its content without a password via Windows Explorer or the Mac Finder. For more information, go to Appendix B: How to Install and Access USB Storage, “**Overview**” on page 49.

The options on the various *Storage* screens are available when a USB storage device is connected to the USB port of the router. The *Disk* screen describes the USB disk currently attached to the router. Use this screen to create shared folders, safely remove a disk, or format a disk (any data on the disk will be deleted during formatting).

You can use shared folders to manage network access to the contents on the disk. You can specify individual folders that you want to share, or you can share the entire partition. Each shared folder created on the *Disk* screen has a unique name (Display Name), is mapped to a physical folder on the disk, and specifies access rights to that folder.

Access rights are managed by group and user accounts that you can create on the *Storage > Administration* screen (go to “**Storage > Administration**” on page 29). Each user has his or her own login and belongs to a group. Each group has either read-and-write or read-only access rights.

NOTE: By default, all content on the disk can be accessed without a password. If you want to specify which groups can access the shared folders, select **Disabled** for the *Anonymous Disk Access* option. Go to “**Storage > Administration**” on page 29.



Disk1: USB Flash Disk

Partition	File System	Capacity	Free Space	Create Share
USB_SHARED	FAT	0.976 GB	0.455 GB	Create Share
Total	*	0.977 GB	0.459 GB	

USB 1.1	USB 2.0
	■

Device Name (Disk): Cisco00009
Shared Disk IP Address: 192.168.1.1

Display Name	Partition	Shared Folder	Edit	Delete
USB_SHARED	USB_SHARED	/	Edit	Delete

□ Disk: USB Flash Disk

Storage > Disk

Disk Management

If a formatted disk is connected to the router, then its name is displayed. For each partition of the disk, the Partition, File System, Capacity, and Free Space information are displayed.

Safely Remove Disk Before you physically disconnect a USB disk from the router, click **Safely Remove Disk** first.

NOTE: Use the *Safely Remove Disk* option to prevent the possible loss or corruption of data, which may occur if you remove the disk while it is transferring data.

Create Share To create a shared folder, click this option for the appropriate partition. Go to “**Create a Shared Folder**” on page 24.

USB Port Speed

USB 1.1 or USB 2.0 The USB type of the connected disk is displayed. The USB 1.1 standard supports speeds up to 12 Mbps. The USB 2.0 standard supports speeds up to 480 Mbps.

Shared Folder

Device Name (Disk) The Device Name (or NetBIOS name) of the router is displayed. The default is **Cisco** followed by the last 5 digits of the router’s serial number, which is found on the bottom of the router. If you used the setup software for installation, then the Device Name is the name of your wireless network (up to 15 characters).

Shared Disk IP Address The IP address of the disk is displayed.

Summary To view a list of shared folders, click this option. Go to “**Shared Folders Summary**” on page 24.

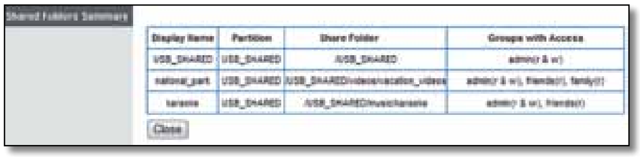
The Shared Folder table lists the shared folders with the following information: Display Name, Partition, and Shared Folder location.

Edit To change the access settings of a shared folder, click this option. Go to "**Edit a Shared Folder**" on page 25.

Delete To delete a shared folder, click this option.

Shared Folders Summary

For each folder, the Display Name, Partition, Shared Folder location, and Groups with Access are displayed.



Shared Folders Summary

Display Name	Partition	Share Folder	Groups with Access
USB_SHARED	USB_SHARED	/USB_SHARED	admin(r & w)
national_park	USB_SHARED	/USB_SHARED/videos/vacation_videos	admin(r & w), friends(r), family(r)
karaoke	USB_SHARED	/USB_SHARED/music/karaoke	admin(r & w), friends(r)

Disk > Shared Folders Summary

Click **Close** to exit this screen and return to the *Disk* screen.

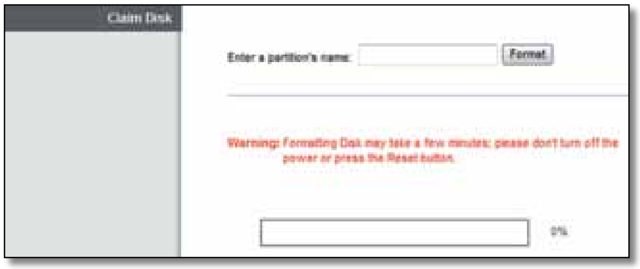
Format Disk

Disk To format the disk as FAT32, select the disk you want to format, and then click **Format Disk**. (If your disk was formatted with multiple partitions, then the formatting will delete them and create a single partition.) The *Claim Disk* screen appears.

Claim Disk

Enter a partition's name Enter a name for the partition.

Click **Format** and follow the on-screen instructions.



Claim Disk

Enter a partition's name:

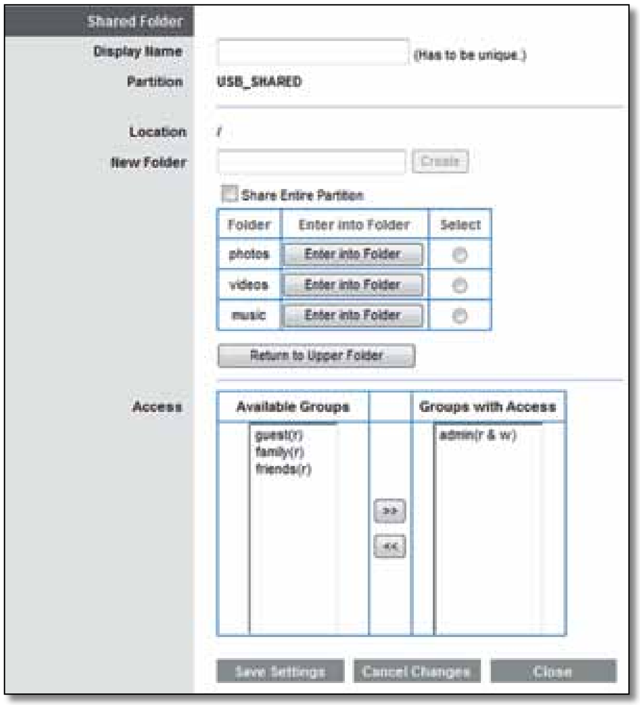
Warning: Formatting Disk may take a few minutes; please don't turn off the power or press the Reset button.

0%

Disk > Claim Disk

On the *Disk* screen, click **Refresh** to update the on-screen information.

Create a Shared Folder



Shared Folder

Display Name (Has to be unique.)

Partition USB_SHARED

Location /

New Folder

□ Share Entire Partition

Folder	Enter into Folder	Select
photos	Enter into Folder	○
videos	Enter into Folder	○
music	Enter into Folder	○

Access

Available Groups		Groups with Access

guest(r)
family(r)
friends(r)
	>>
	<<
		admin(r & w)

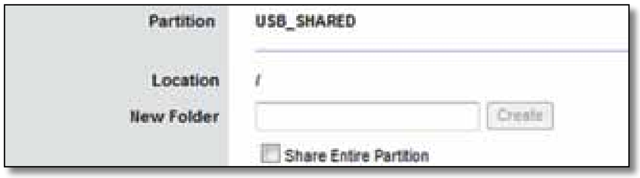
Disk > Shared Folder

1. In the *Display Name* field, enter a name for the shared folder.

Display Name (Has to be unique.)

Shared Folder > Enter Display Name

2. The Partition name is displayed. If the shared folder should include the entire partition, select **Share Entire Partition** and go to step 4.



Partition USB_SHARED

Location /

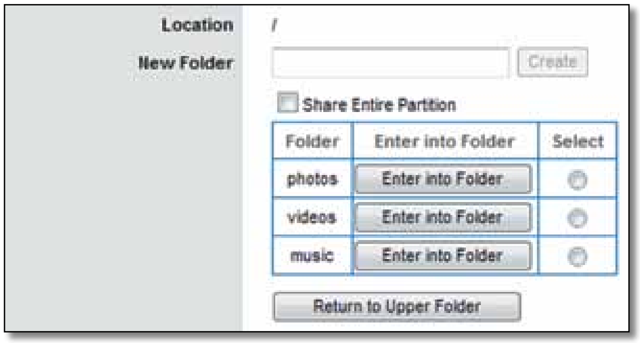
New Folder

□ Share Entire Partition

Shared Folder > Share Entire Partition

NOTE: If you select **Share Entire Partition**, then all of the Groups with Access (see step 4) can access any folder in the partition.

3. To specify a folder to share, click **Select**. To display subfolders, click **Enter into Folder**. To return to the previous folder, click **Return to Upper Folder**.



Location: /

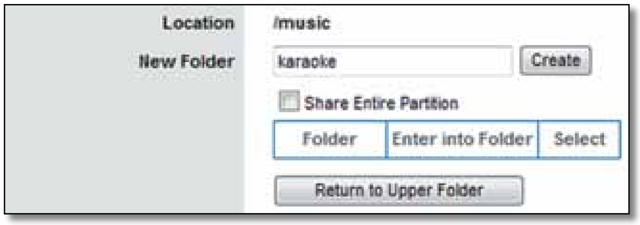
New Folder:

☐ Share Entire Partition

Folder	Enter into Folder	Select
photos	Enter into Folder	○
videos	Enter into Folder	○
music	Enter into Folder	○

Shared Folder > Select Folder or Enter into Folder

To create a new folder, enter its name in the *New Folder* field. Then click **Create**.



Location: /music

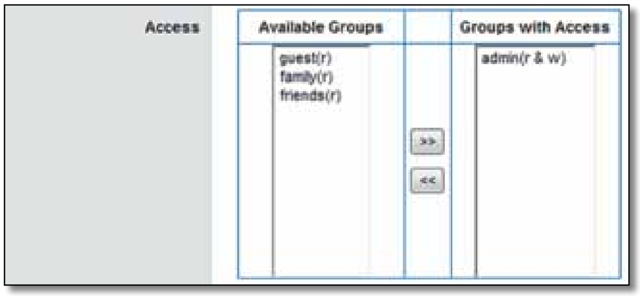
New Folder: karaoke

☐ Share Entire Partition

Folder	Enter into Folder	Select

Shared Folder > Create New Folder

4. To allow a group to access the shared folder, select it from the *Available Groups* column, and then click the **>>** button. (To create groups, go to "**Create or Edit a Group Account**" on page 31.)



Access

Available Groups		Groups with Access

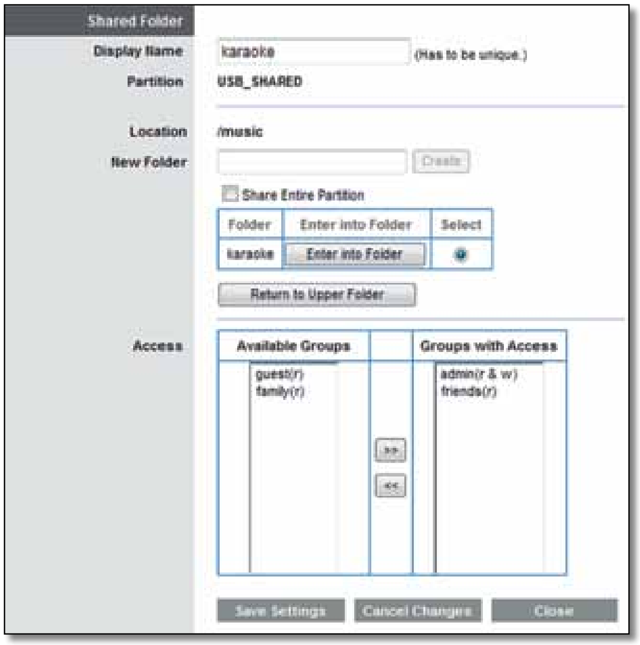
guest(r)
family(r)
friends(r)
	>>
	<<
		admin(r & w)

Shared Folder > Groups with Access

NOTE: By default, no password is needed for read-and-write access to the disk. If you want to specify which groups can access the shared folder, select **Disabled** for the *Anonymous Disk Access* option. Go to "**Storage > Administration**" on page 29.

5. Click **Save Settings** to apply your changes, or click **Cancel Changes** to clear your changes. Click **Close** to exit this screen and return to the *Disk* screen.

Edit a Shared Folder



Shared Folder

Display Name: karaoke (Has to be unique.)

Partition: USB_SHARED

Location: /music

New Folder:

☐ Share Entire Partition

Folder	Enter into Folder	Select
karaoke	Enter into Folder	●

Access

Available Groups		Groups with Access

guest(r)
family(r)
	>>
	<<
		admin(r & w)
		friends(r)

Disk > Shared Folder

Make the appropriate changes to the following options:

Display Name The current Display Name is shown. To change the name, enter a new name.

Partition The name of the partition is displayed.

Location The path to the displayed folder is displayed.

New Folder To create a new folder, enter its name and then click **Create**.

Share Entire Partition If the shared folder should include the entire partition, select this option. If you do not want to share the entire partition, then select the folder you do want to share.

Folder The available folders are listed by Folder name.

- **Enter into Folder** To display subfolders, click this option.
- **Select** To specify a folder, click **Select**.
- **Return to Upper Folder** To return to the previous folder, click this option.

Access Specify which groups have read-and-write or read-only access to the folder. (To create groups, go to "**Create or Edit a Group Account**" on page 31.)

- **Available Groups** To allow a group to access the folder, select it, and then click the **>>** button.
- **Groups with Access** To block a group from accessing the folder, select it, and then click the **<<** button.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to clear your changes. Click **Close** to exit this screen and return to the *Disk* screen.

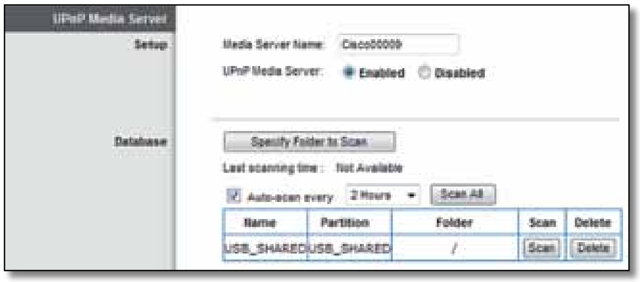
Storage > Media Server

The options on the various *Storage* screens are available when a USB storage device is connected to the USB port of the router.

The Media Server feature allows you to share stored content with other computers and devices on your home network and on the Internet.

If you have UPnP AV (Audio and Video)-enabled or Digital Living Network Alliance (DLNA)-certified devices in your home, then you can use the router as a media server. Examples of UPnP AV-enabled devices include a digital media player, a gaming console with a built-in media player, or a digital picture frame.

For example, if you have a digital media adapter that sends content to your entertainment system, then the digital media adapter can locate the router using the UPnP AV standard. The folders you specify can then be accessed and played by the digital media adapter.



Media Server Name: Cisco00009

UPnP Media Server: ● Enabled ○ Disabled

Last scanning time : Not Available

☑ Auto-scan every 2 Hours

Name	Partition	Folder	Scan	Delete
USB_SHARED	USB_SHARED	/	Scan	Delete

Storage > Media Server

UPnP Media Server

Setup

Media Server Name Enter the display name of the UPnP media server. Use only alphanumeric characters (letters A to Z and numbers 0 to 9). The default is **Cisco** followed by the last 5 digits of the router's serial number, which is found on the bottom of the router.

NOTE: If you used the setup software for installation, then the UPnP Media Server Name is the name of your wireless network (up to 15 characters).

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

Database Setup

This section lets you select content to add to the database of the router's media server.

NOTE: Scanning media files may take up to 40 minutes, depending on the number and size of the files.

Specify Folder to Scan To add a media folder to the database of the router's media server, click this option. Go to "**Add a Media Folder**" on page 26.

Last scanning time The last time the media server scanned for content is displayed.

Auto-scan every __ To automatically scan the media folders, select this option. Then select the appropriate interval: **2 Hours** (default), **6 Hours**, **12 Hours**, **24 Hours**, or **48 Hours**.

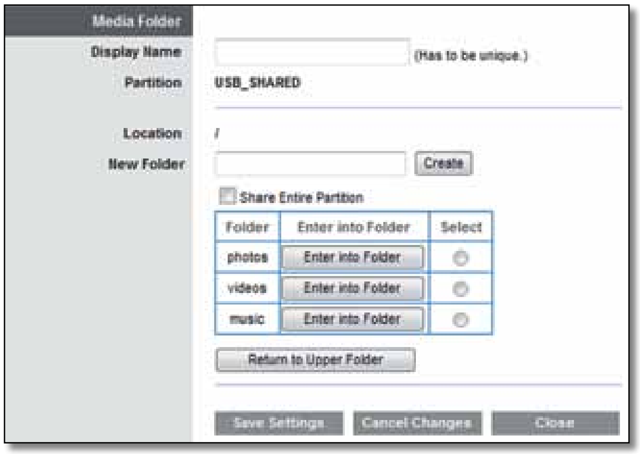
Scan All To scan all media files now, click this option.

For each media folder, the Name, Partition, and Folder location are displayed.

Scan To scan a folder now, click **Scan**.

Delete To delete a folder, click **Delete**.

Add a Media Folder



Display Name (Has to be unique.)

Partition USB_SHARED

Location /

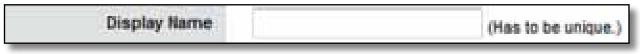
New Folder

□ Share Entire Partition

Folder	Enter into Folder	Select
photos	Enter into Folder	○
videos	Enter into Folder	○
music	Enter into Folder	○

Media Server > Media Folder

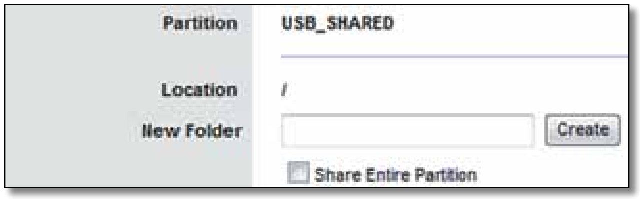
1. In the *Display Name* field, enter a name for the media folder.



Display Name (Has to be unique.)

Media Folder > Enter Display Name

2. The Partition name is displayed. If the media folder should include the entire partition, select **Share Entire Partition** and go to step 4.



Partition USB_SHARED

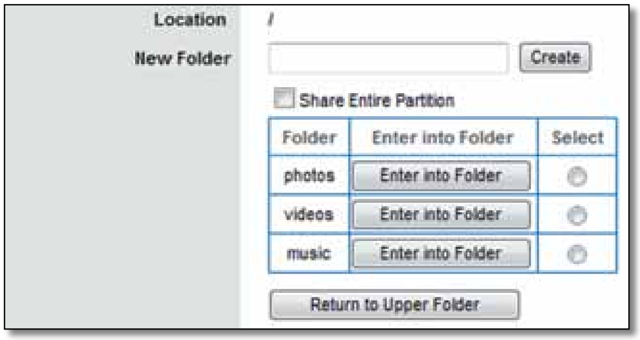
Location /

New Folder

□ Share Entire Partition

Media Folder > Share Entire Partition

3. To specify a folder to scan, click **Select**. To display subfolders, click **Enter into Folder**. To return to the previous folder, click **Return to Upper Folder**.



Location /

New Folder [ ] Create

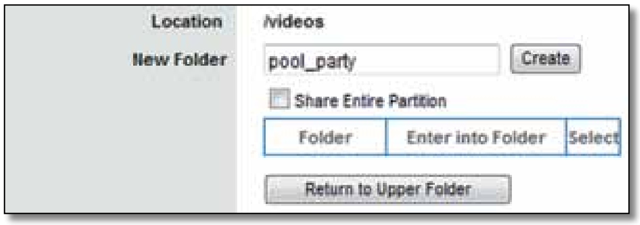
□ Share Entire Partition

Folder	Enter into Folder	Select
photos	Enter into Folder	○
videos	Enter into Folder	○
music	Enter into Folder	○

Return to Upper Folder

Media Folder > Select Folder or Enter into Folder

To create a new folder, enter its name in the *New Folder* field. Then click **Create**.



Location /videos

New Folder pool_party Create

□ Share Entire Partition

Folder	Enter into Folder	Select

Return to Upper Folder

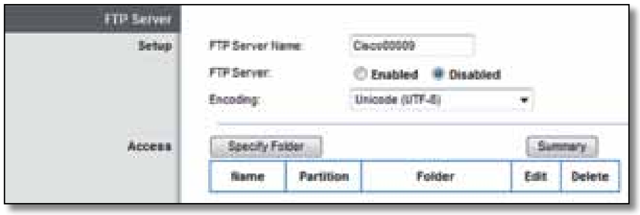
Media Folder > Create New Folder

4. Click **Save Settings** to apply your changes, or click **Cancel Changes** to clear your changes. Click **Close** to exit this screen and return to the *Media Server* screen.

Storage > FTP Server

The options on the various *Storage* screens are available when a USB storage device is connected to the USB port of the router.

Use the *FTP Server* screen to create an FTP server that can be accessed from the Internet or your local network. You can also create FTP folders, which are folders you create to manage FTP client access to the folders on the disk.



FTP Server

Setup

FTP Server Name: Cisco00009

FTP Server: ○ Enabled ● Disabled

Encoding: Unicode (UTF-8)

Access

Specify Folder Summary

Name	Partition	Folder	Edit	Delete

Storage> FTP Server

FTP Server

Setup

FTP Server Name Enter the display name of the FTP server. Use only alphanumeric characters (letters A to Z and numbers 0 to 9). The default is **Cisco** followed by the last 5 digits of the router’s serial number, which is found on the bottom of the router. If you used the setup software for installation, then the FTP Server Name is the name of your wireless network (up to 15 characters).

FTP Server Select **Enabled** to use the router as an FTP server. Otherwise, select **Disabled**. An external USB hard drive or USB disk must be connected to the USB port to use this service.

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

Encoding The router supports different character sets for the transfer of files in different languages. Select the appropriate character encoding set: **Unicode (UTF-8)**, **Chinese Simplified (GB18030)**, **Vietnamese (CP1258)**, or **ISO 8859_1**. The default is **Unicode (UTF-8)**.

Access

This section lets you add FTP folders that can be accessed through the FTP client.

Specify Folder To add an FTP folder, click this option. Go to “**Create an FTP Folder**” on page 28.

Summary To view a list of FTP folders, click this option. Go to “**FTP Summary**” on page 27.

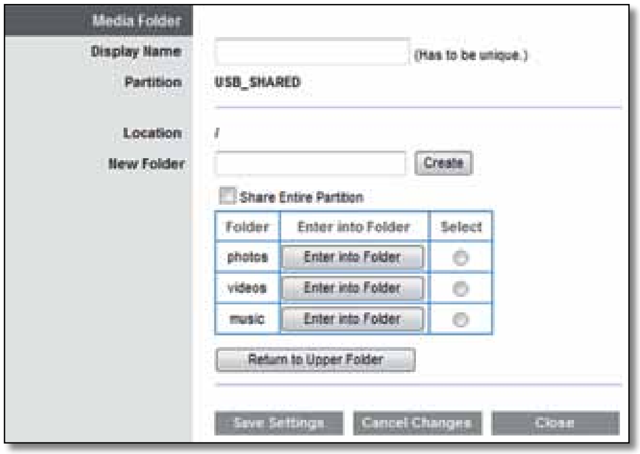
The Access table lists the FTP folders with the following information: Display Name, Partition, and Folder location.

Edit To change the access settings of an FTP folder, click this option. Go to “**Edit an FTP Folder**” on page 29.

Delete To delete an FTP folder, click this option.

FTP Summary

For each folder, the Display Name, Partition, Shared Folder location, and Groups with Access are displayed.



Media Folder

Display Name [ ] (Has to be unique.)

Partition USB_SHARED

Location /

New Folder [ ] Create

□ Share Entire Partition

Folder	Enter into Folder	Select
photos	Enter into Folder	○
videos	Enter into Folder	○
music	Enter into Folder	○

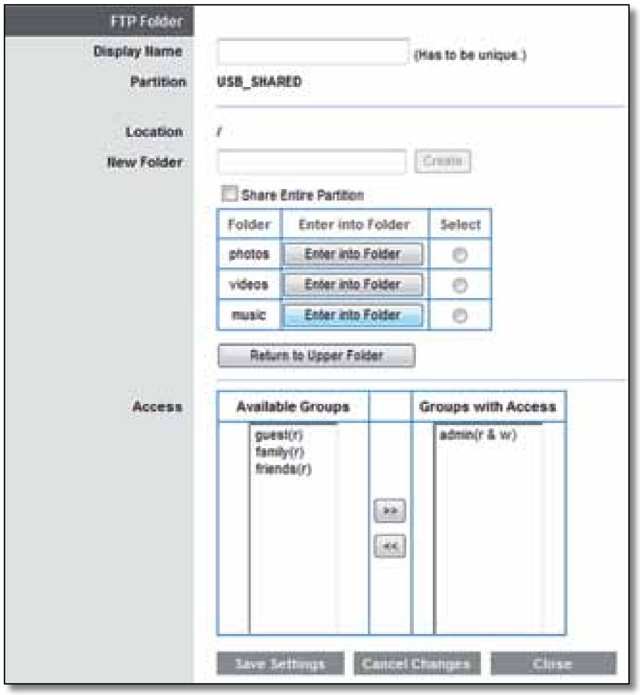
Return to Upper Folder

Save Settings Cancel Changes Close

FTP Server > FTP Summary

Click **Close** to exit this screen and return to the *FTP Server* screen.

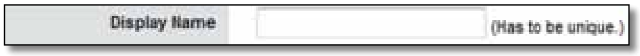
Create an FTP Folder



Folder	Enter into Folder	Select
photos	Enter into Folder	○
videos	Enter into Folder	○
music	Enter into Folder	○

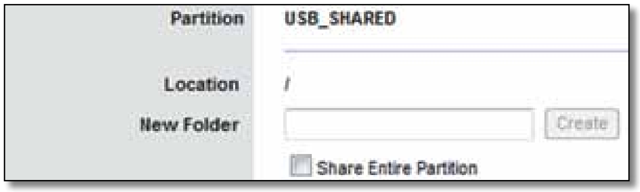
FTP Server > FTP Folder

1. In the *Display Name* field, enter a name for the FTP folder.



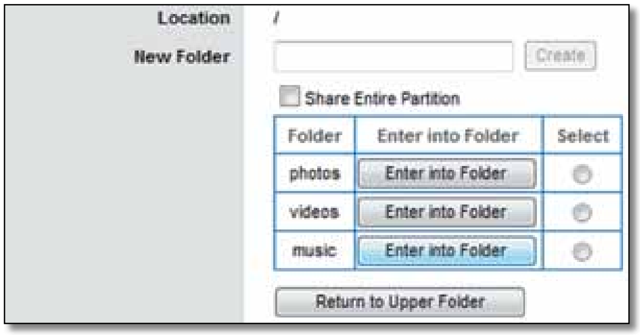
FTP Folder > Enter Display Name

2. The Partition name is displayed. If the FTP folder should include the entire partition, select **Share Entire Partition** and go to step 4.



FTP Folder > Share Entire Partition

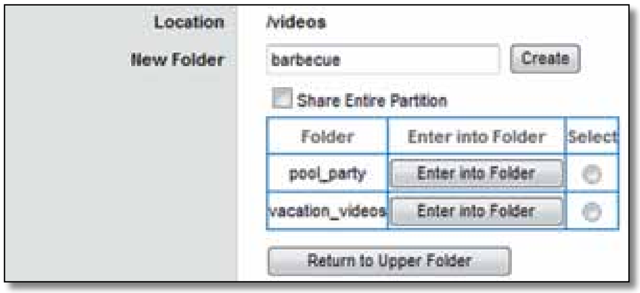
3. To specify a folder for FTP client access, click **Select**. To display subfolders, click **Enter into Folder**. To return to the previous folder, click **Return to Upper Folder**.



Folder	Enter into Folder	Select
photos	Enter into Folder	○
videos	Enter into Folder	○
music	Enter into Folder	○

FTP Folder > Select Folder or Enter into Folder

To create a new folder, enter its name in the *New Folder* field. Then click **Create**.

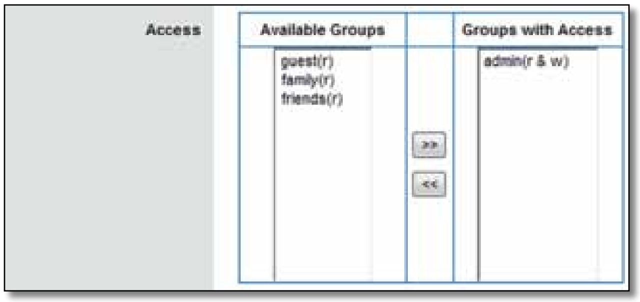


New Folder: barbecue

Folder	Enter into Folder	Select
pool_party	Enter into Folder	○
vacation_videos	Enter into Folder	○

FTP Folder > Create New Folder

4. To allow a group to access the FTP folder, select it from the *Available Groups* column, and then click the **>>** button. (To create groups, go to "**Create or Edit a Group Account**" on page 31.)

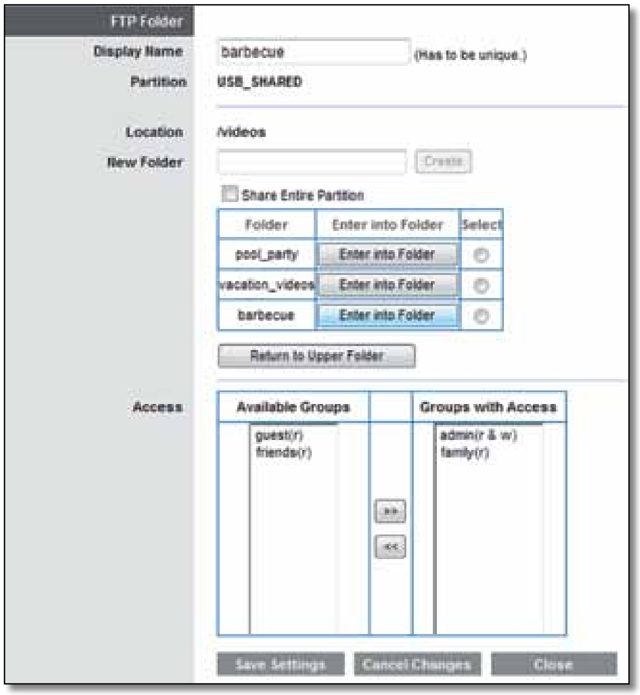


FTP Folder > Groups with Access

NOTE: By default, the disk can be accessed without a password. If you want to specify which groups can access the FTP folder, select **Disabled** for the *Anonymous Disk Access* option. Go to "**Storage > Administration**" on page 29.

5. Click **Save Settings** to apply your changes, or click **Cancel Changes** to clear your changes. Click **Close** to exit this screen and return to the *FTP Server* screen.

Edit an FTP Folder



FTP Folder

Display Name: barbecue (Has to be unique.)

Partition: USB_SHARED

Location: /videos

New Folder: [ ] Create

□ Share Entire Partition

Folder	Enter into Folder	Select
pool_party	Enter into Folder	○
vacation_videos	Enter into Folder	○
barbecue	Enter into Folder	○

Return to Upper Folder

Access

Available Groups		Groups with Access

guest(r)
friends(r)
	>>
	<<
		admin(r & w)
		family(r)

Save Settings | Cancel Changes | Close

FTP Server > FTP Folder

Make the appropriate changes to the following options:

Display Name The current Display Name is shown. To change the name, enter a new name.

Partition The name of the partition is displayed.

Location The path to the displayed folder is displayed.

New Folder To create a new folder, enter its name and then click **Create**.

Share Entire Partition If the FTP folder should include the entire partition, select this option. If you do not want to share the entire partition, then select the folder you do want to share.

Folder The available folders are listed by Folder name.

- **Enter into Folder** To display subfolders, click this option.
- **Select** To specify a folder for FTP client access, click **Select**.
- **Return to Upper Folder** To return to the previous folder, click this option.

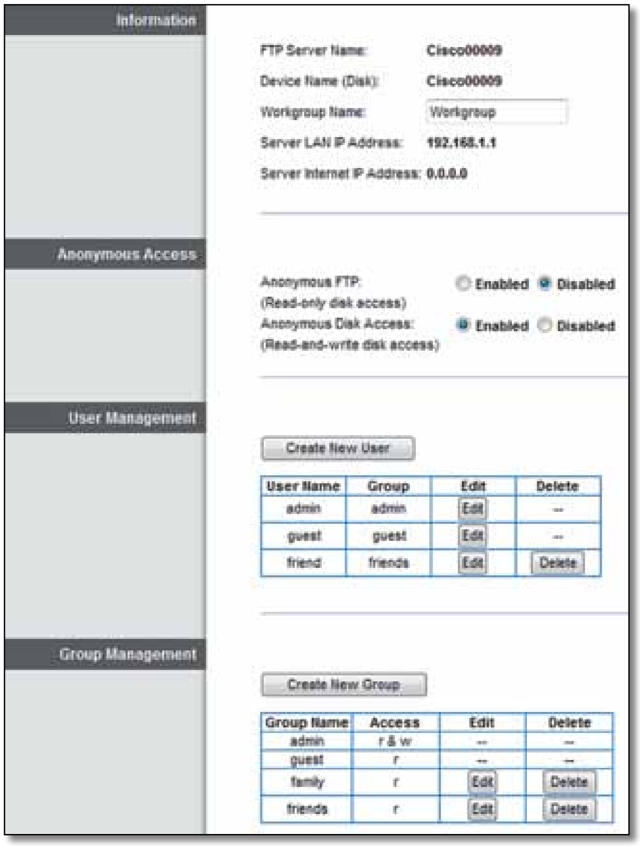
Access Specify which groups have read-and-write or read-only access to the FTP folders. (To create groups, go to "**Create or Edit a Group Account**" on page 31.)

- **Available Groups** To allow a group to access the folder, select it, and then click the >> button.
- **Groups with Access** To block a group from accessing the folder, select it, and then click the << button.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to clear your changes. Click **Close** to exit this screen and return to the *FTP Server* screen.

Storage > Administration

The *Administration* screen allows you to manage the groups and individual users who can access the shared folders.



Information

FTP Server Name: Cisco00009

Device Name (Disk): Cisco00009

Workgroup Name: Workgroup

Server LAN IP Address: 192.168.1.1

Server Internet IP Address: 0.0.0.0

Anonymous Access

Anonymous FTP: (Read-only disk access) ○ Enabled ● Disabled

Anonymous Disk Access: (Read-and-write disk access) ● Enabled ○ Disabled

User Management

Create New User

User Name	Group	Edit	Delete
admin	admin	Edit	--
guest	guest	Edit	--
friend	friends	Edit	Delete

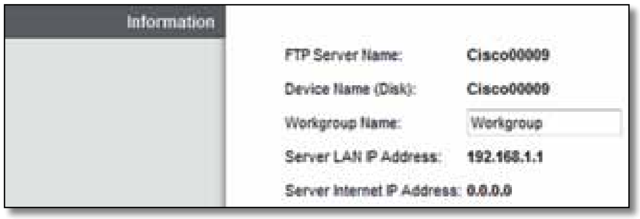
Group Management

Create New Group

Group Name	Access	Edit	Delete
admin	r & w	--	--
guest	r	--	--
family	r	Edit	Delete
friends	r	Edit	Delete

Storage > Administration

Information



Information

FTP Server Name: Cisco00009

Device Name (Disk): Cisco00009

Workgroup Name: Workgroup

Server LAN IP Address: 192.168.1.1

Server Internet IP Address: 0.0.0.0

Administration > Information

FTP Server Name The display name of the FTP server is displayed. The default is **Cisco** followed by the last 5 digits of the router's serial number, which is found on the bottom of the router. If you used the setup software for installation, then the FTP Server Name is the name of your wireless network (up to 15 characters).

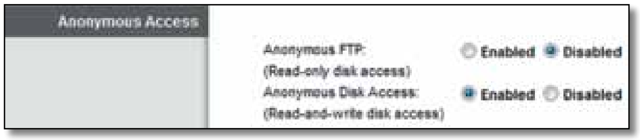
Device Name (Disk) The Device Name (or NetBIOS name) of the router is displayed. The default is **Cisco** followed by the last 5 digits of the router's serial number, which is found on the bottom of the router. If you used the setup software for installation, then the Device Name is the name of your wireless network (up to 15 characters).

Workgroup Name Enter the workgroup name for the router; it should match the workgroup name of the computers on your local network. The router's default is **workgroup**.

Server LAN IP Address The local IP address of the router's media and FTP server is displayed.

Server Internet IP Address The Internet IP address of the router's FTP server is displayed.

Anonymous Access



Anonymous FTP: (Read-only disk access) ○ Enabled ● Disabled

Anonymous Disk Access: (Read-and-write disk access) ● Enabled ○ Disabled

Administration > Anonymous Access

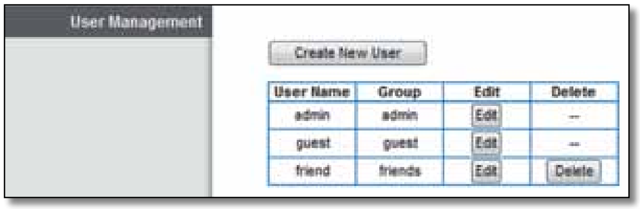
Anonymous FTP By default, this option is disabled. To allow read-only, anonymous FTP user access, select **Enabled**.

Anonymous Disk Access By default, no password is needed for read-and-write access to the disk. To manage group and user access to specific shared folders, select **Disabled**.

User Management

By default the router creates two users, **admin** and **guest**.

The users are listed by User Name and Group.



User Name	Group	Edit	Delete
admin	admin	Edit	--
guest	guest	Edit	--
friend	friends	Edit	Delete

Administration > User Management

Create New User To create a new user, click this option. Go to "**Create or Edit a User Account**" on page 30.

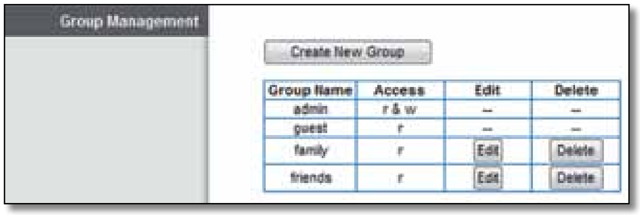
Edit To change the settings of a user account, click **Modify**. Go to "**Create or Edit a User Account**" on page 30.

Delete To delete a user, click this option.

Group Management

By default the router creates two groups, **admin** (read-and-write access) and **guest** (read-only access).

The groups are listed by Group Name and Access level. There are two levels of access, r & w (read-and-write) and r (read-only).



Group Name	Access	Edit	Delete
admin	r & w	--	--
guest	r	--	--
family	r	Edit	Delete
friends	r	Edit	Delete

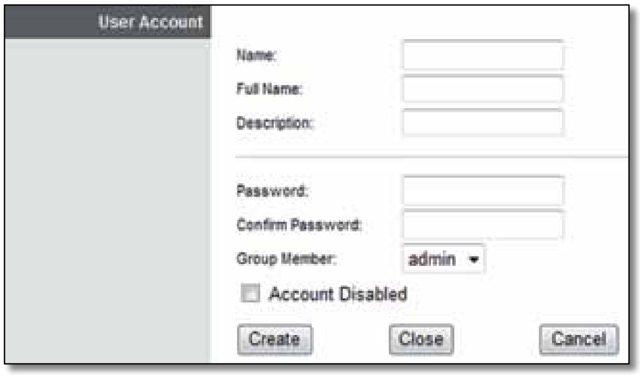
Administration > Group Management

Create New Group To create a new group of users, click this option. Go to "**Create or Edit a Group Account**" on page 31.

Edit To change the description or access rights of a group, click **Modify**. Go to "**Create or Edit a Group Account**" on page 31.

Delete To delete a group, click this option.

Create or Edit a User Account



Name:

Full Name:

Description:

Password:

Confirm Password:

Group Member: admin ▾

□ Account Disabled

Administration > User Account

To create a user account, complete the options. To edit a user account, make the appropriate changes.

Name Enter a name for the user.

Full Name Enter the actual name of the user.

Description Enter keywords to describe the user.

Password Enter the login password.

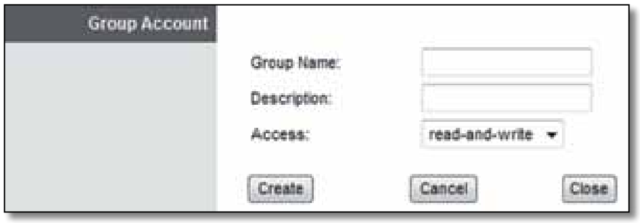
Confirm Password Enter the password again to confirm.

Group Member Select the appropriate group.

Account Disabled To temporarily disable an account, select this option.

Click **Create**/**Modify** to apply your changes, or click **Cancel** to clear your changes. Click **Close** to exit this screen and return to the *Administration* screen.

Create or Edit a Group Account



Administration > Group Account

To create a group account, complete the options. To edit a group account, make the appropriate changes.

Group Name Enter a name for the group.

Description Enter keywords to describe the group.

Access Select the appropriate level of access, **read-and-write** or **read-only**.

Click **Create**/**Modify** to apply your changes, or click **Cancel** to clear your changes. Click **Close** to exit this screen and return to the *Administration* screen.

6. Click **Save Settings** to save the policy's settings, or click **Cancel Changes** to clear the changes.

> ✓ **NOTE:** If you have already set up Parental Controls and now want to use Internet Access Policy, then you will be asked to enter the password for Parental Controls before you can click Save Settings.

Access Restrictions > Parental Controls + Internet Access Policy

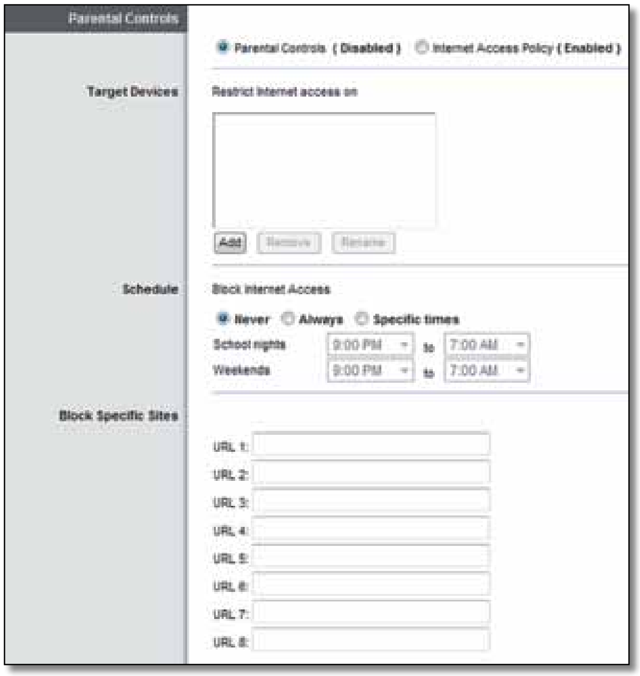
To manage Internet access, you have two methods available, Parental Controls and Internet Access Policy. Only one method can be used at a time.

As part of Cisco Connect, Parental Controls can restrict Internet access for up to five computers or devices. You can block Internet access or limit it to specific times, and you can also block specific websites.

Up to five Internet Access Policies manage Internet access for multiple computers or devices. You can block Internet access or limit it to specific times, block specific websites, and block specific applications.

Parental Controls or Internet Access Policy

Parental Controls/Internet Access Policy Select the method you want to use. If you select Parental Controls, go to "**Parental Controls**" on page 32. If you select Internet Access Policy, go to "**Internet Access Policy**" on page 33.



● Parental Controls (Disabled) ○ Internet Access Policy (Enabled)

● Never ○ Always ○ Specific times

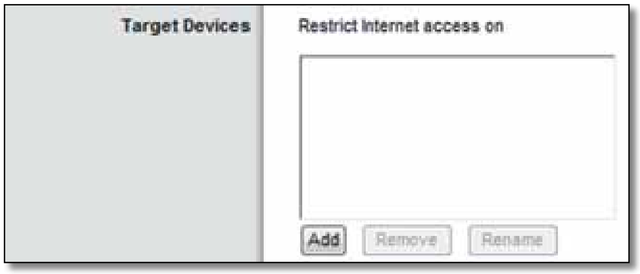
School nights 9:00 PM to 7:00 AM

Weekends 9:00 PM to 7:00 AM

Access Restrictions > Parental Controls

Parental Controls

Target Devices



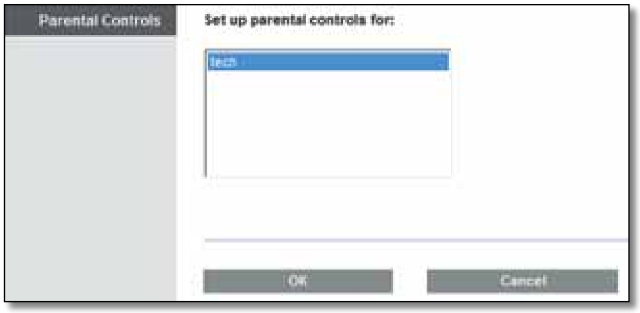
Parental Controls > Target Devices

Restrict Internet access on Parental Controls manages the computers or other devices on this list.

Add If you want to apply Parental Controls to more computers or other devices, click **Add**, and a new *Parental Controls* screen appears.

Parental Controls

- **Set up parental controls for:** Select the appropriate computer. Then click **OK** to exit this screen and return to the main *Parental Controls* screen.



tech

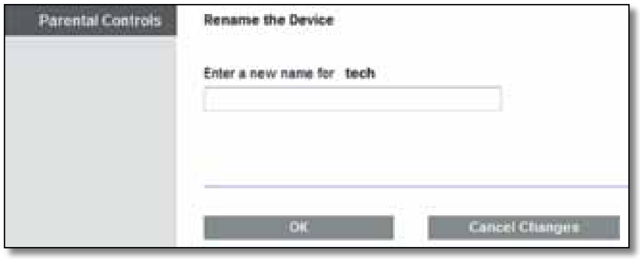
Parental Controls > Set Up Parental Controls

Remove If you no longer want to apply Parental Controls to a device, select it and click **Remove**.

Rename To change the name of a device, select it and click **Rename**. A new *Parental Controls* screen appears.

Rename the Device

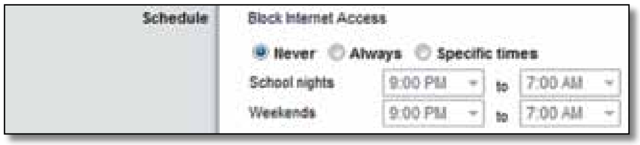
- **Enter a new name for (current name of device)** Enter the new name. Then click **OK** to save the new name and return to the main *Parental Controls* screen.



Enter a new name for tech

Parental Controls > Rename Device

Schedule



Schedule

Block Internet Access

● Never ○ Always ○ Specific times

School nights 9:00 PM to 7:00 AM

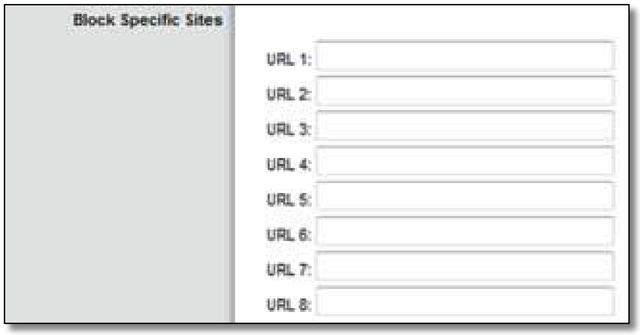
Weekends 9:00 PM to 7:00 AM

Parental Controls > Schedule

Never/Always/Specific times Specify when Internet access is blocked. To never block Internet access, keep the default, **Never**. To always block Internet access, select **Always**. To specify days and times when Internet access is blocked, select **Specific times**. Then set the schedule:

- **School nights** Select the appropriate start and end times.
- **Weekends** Select the appropriate start and end times.

Block Specific Sites



Block Specific Sites

URL 1:

URL 2:

URL 3:

URL 4:

URL 5:

URL 6:

URL 7:

URL 8:

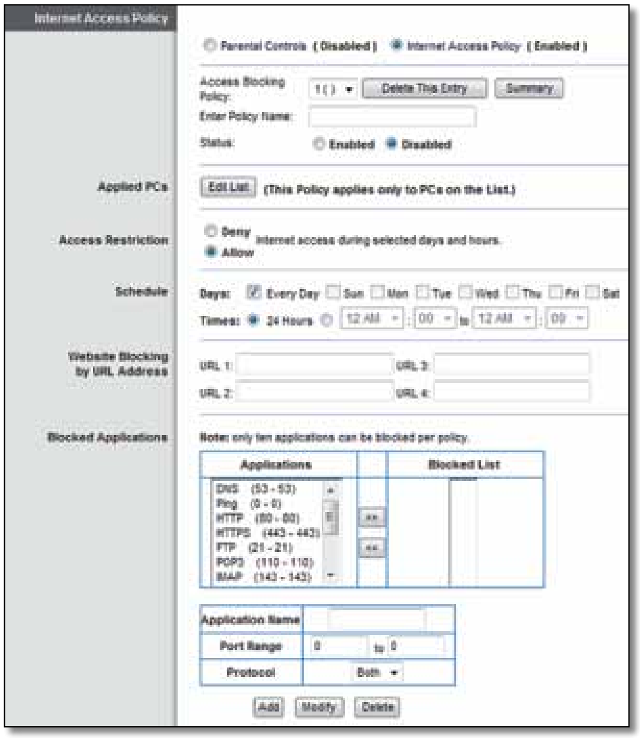
Parental Controls > Block Specific Sites

URL 1-8 In each field, enter a website address that you want to block.

For example, to block **http://www.example.com**, enter **example.com** in a field.

NOTE: When you set up Parental Controls for the first time and click Save Settings, you will be asked to set up a password that protects access to Parental Controls. Follow the on-screen instructions.

Internet Access Policy



Internet Access Policy

○ Parental Controls (Disabled) ● Internet Access Policy (Enabled)

Access Blocking Policy: 1 ( ) Delete This Entry Summary

Enter Policy Name:

Status: ○ Enabled ● Disabled

Applied PCs: Edit List (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 3: URL 2: URL 4:

Blocked Applications: Note: only ten applications can be blocked per policy.

Applications		Blocked List
DNS (53 - 53) Ping (0 - 0) HTTP (80 - 80) HTTPS (443 - 443) FTP (21 - 21) POP3 (110 - 110) IMAP (143 - 143)	>> <<	

Application Name	
Port Range	0 to 0
Protocol	Both

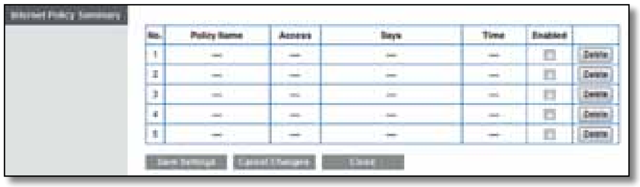
Add Modify Delete

Access Restrictions > Internet Access Policy

Access Blocking Policy To display a policy's settings, select its number from the drop-down menu. To delete a policy, select its number and click **Delete This Policy**. To view all the policies, click **Summary**, and the *Summary* screen appears.

Summary

The policies are listed with the following information: No. (Number), Policy Name, Access, Days, Time, and Enabled/Disabled (status). To enable a policy, select **Enabled**. To delete a policy, click **Delete**. Click **Save Settings** to save your changes, or click **Cancel Changes** to clear your changes. To exit this screen and return to the *Internet Access Policy* screen, click **Close**.



Internet Policy Summary

No.	Policy Name	Access	Days	Time	Enabled	
1	—	—	—	—	☐	Delete
2	—	—	—	—	☐	Delete
3	—	—	—	—	☐	Delete
4	—	—	—	—	☐	Delete
5	—	—	—	—	☐	Delete

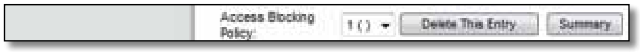
Save Settings Cancel Changes Close

Summary

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

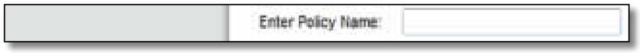
To create or change a policy, follow steps 1-10. Repeat these steps to create additional policies, one at a time.

1. Select a number from the *Access Blocking Policy* drop-down menu.



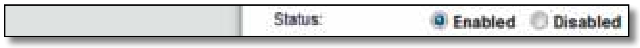
Select Policy Number

2. Enter a Policy Name.



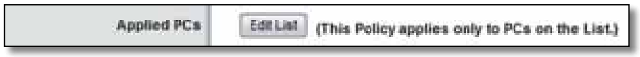
Enter Policy Name

3. To activate this policy, select **Enabled**.



Enable Policy

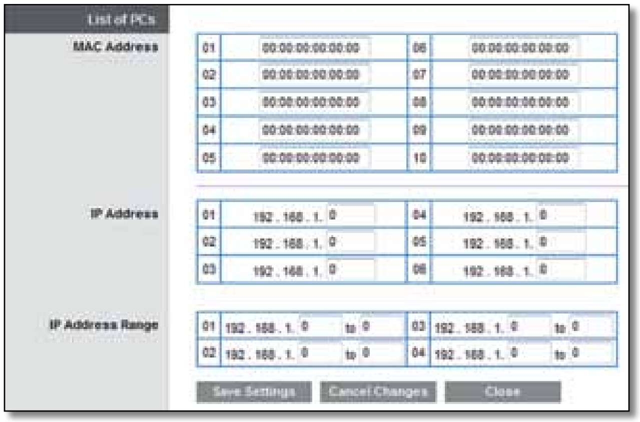
4. Click **Edit List** to select which computers will be affected by the policy.



Edit List

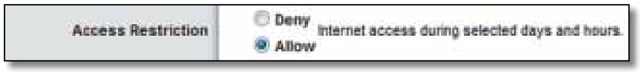
The *List of PCs* screen appears. You can select a computer by MAC address or IP address. You can also enter a range of IP addresses if you want to apply this policy to a group of computers. (To assign a static IP address to a computer, go to "**DHCP Reservation**" on page 7. To look up the MAC address of a computer, go to "**DHCP Client Table**" on page 37.)

After making your changes, click **Save Settings** to apply your changes, or click **Cancel Changes** to clear your changes. Then click **Close** to exit this screen and return to the *Internet Access Policy* screen.



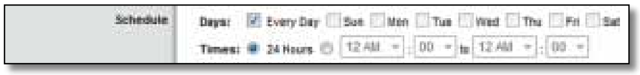
List of PCs

6. To block Internet access for the computers on the *List of PCs* screen, select **Deny**. To allow Internet access for the computers on the *List of PCs* screen, select **Allow**.



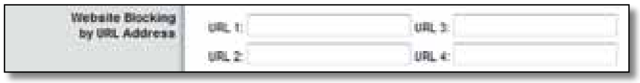
Deny or Allow

7. 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 **Every Day**. Then enter a time span during which the policy will be in effect, or select **24 Hours**.


Schedule
Days: ☑ Every Day □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
Times: ● 24 Hours ○ 12 AM : 00 to 12 AM : 00

Schedule

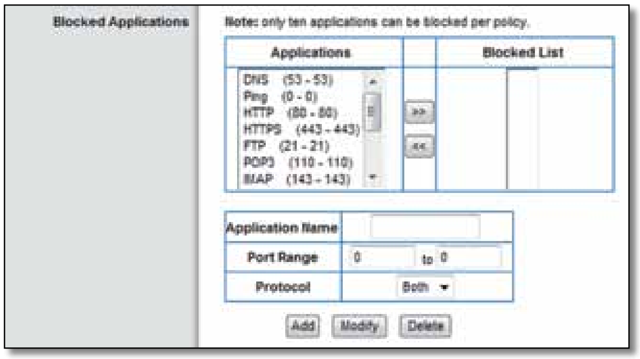
7. To block websites with specific URL addresses, enter each URL in a separate *Website Blocking by URL Address* field.



Website Blocking by URL Address

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

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



Blocked Applications

9. If the application you want to block is not listed or you want to edit a service's settings, enter the application's name in the *Application Name* field. Enter its range in the *Port Range* fields. Select **TCP** (Transmission Control Protocol), **UDP** (User Datagram Protocol), or **Both** from the *Protocol* drop-down menu. Then click **Add**.

To modify a service, select it from the *Applications* column. Change its Application Name, Port Range, and/or Protocol setting. Then click **Modify**.

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

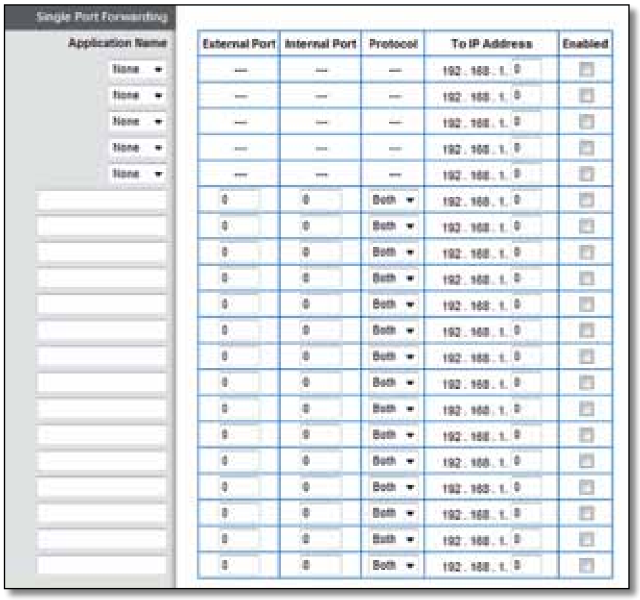
10. Click **Save Settings** to save the policy's settings, or click **Cancel Changes** to clear the changes.

✓ **NOTE:** If you have already set up Parental Controls and now want to use Internet Access Policy, then you will be asked to enter the password for Parental Controls before you can click Save Settings.

Applications and Gaming > Single Port Forwarding

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

When users send these types of requests to your network via the Internet, the router will forward those requests to the appropriate computers (also called servers). Before using forwarding, you should assign static IP addresses to the designated computers. Use the DHCP Reservation option on the *Basic Setup* screen; go to "**DHCP Reservation**" on page 7.



Single Port Forwarding

Application Name	External Port	Internal Port	Protocol	To IP Address	Enabled
None ▾	—	—	—	192 . 168 . 1. 0	□
None ▾	—	—	—	192 . 168 . 1. 0	□
None ▾	—	—	—	192 . 168 . 1. 0	□
None ▾	—	—	—	192 . 168 . 1. 0	□
None ▾	—	—	—	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□
	0	0	Both ▾	192 . 168 . 1. 0	□

Applications and Gaming > Single Port Forwarding

Single Port Forwarding

Pre-defined applications are available for the first five entries. For each entry, complete the following:

Application Name Select the appropriate application.

To IP Address Enter the IP address of the server that should receive the requests. If you need to assign a static IP address to the computer, then go to "**DHCP Reservation**" on page 7.

Enabled Select **Enabled** to activate port forwarding.

For additional applications, complete the following fields:

Application Name Enter the name of the application. Each name can have up to 12 characters.

External Port Enter the external port number that accepts incoming traffic. Check the Internet application's documentation for more information.

Internal Port Enter the internal port number that accepts traffic forwarded by the router. Check the Internet application's documentation for more information.

Protocol Select the protocol(s) used for this application, **TCP**, **UDP**, or **Both**.

To IP Address Enter the IP address of the computer that should receive the traffic. If you need to assign a static IP address to the computer, then go to "**DHCP Reservation**" on page 7.

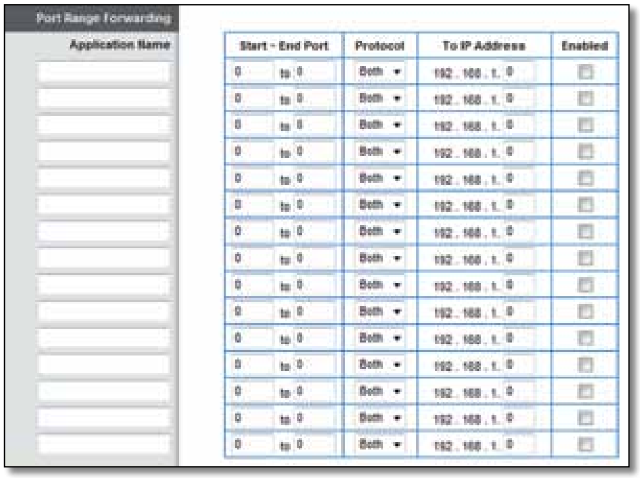
Enabled Select **Enabled** to activate port forwarding.

Applications and Gaming > Port Range Forwarding

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

When users send these types of requests to your network via the Internet, the router will forward those requests to the appropriate computers (also called servers). Before using forwarding, you should assign static IP addresses to the designated computers. Use the DHCP Reservation option on the *Basic Setup* screen; go to "**DHCP Reservation**" on page 7.

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



Port Range Forwarding

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

Applications and Gaming > Port Range Forwarding

Port Range Forwarding

For each entry, complete the following:

Application Name Enter the name of the application. Each name can have up to 12 characters.

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

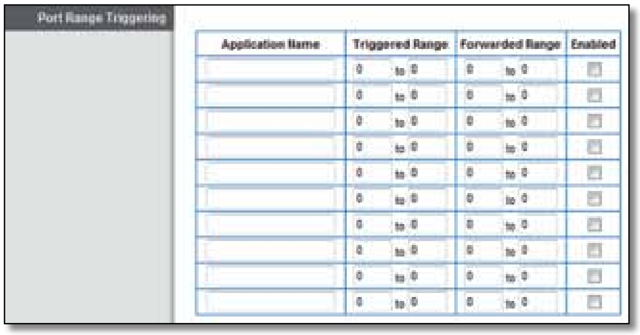
Protocol Select the protocol(s) used for this application, **TCP**, **UDP**, or **Both**.

To IP Address Enter the IP address of the server running the specific application. If you need to assign a static IP address to the computer, then go to "**DHCP Reservation**" on page 7.

Enabled Select **Enabled** to activate port forwarding.

Applications & Gaming > Port Range Triggering

The *Port Range 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.



Port Range Triggering

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

Applications and Gaming > Port Range Triggering

Port Range Triggering

For each entry, complete the following:

Application Name Enter the name of the application. Each name can have up to 12 characters.

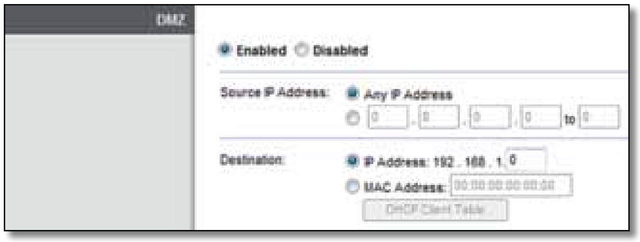
Triggered Range Enter the starting and ending port numbers of the outgoing traffic. Check the Internet application's documentation for more information.

Forwarded Range Enter the starting and ending port numbers of the incoming traffic. Check the Internet application's documentation for more information.

Enabled Select **Enabled** to activate port triggering.

Applications and Gaming > DMZ

The DMZ (DeMilitarized Zone) feature allows one network device to be exposed to the Internet for use of a special-purpose service, such as online gaming or videoconferencing. The router forwards all the ports at the same time to the DMZ device (also called host). The Port Range Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one device, exposing the device to the Internet.



DMZ

● Enabled ○ Disabled

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

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

Applications and Gaming > DMZ

DMZ

Any device 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.

Enabled/Disabled To disable DMZ hosting, keep the default, **Disabled**. To expose one device, select **Enabled**. Then configure the options below.

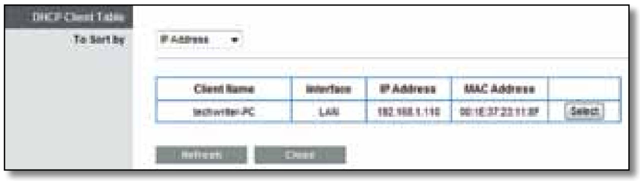
Source IP Address To allow any IP address from the Internet to access the DMZ device, select **Any IP Address**. To specify an IP address or range of IP addresses from the Internet to access the DMZ device, select and complete the IP address range fields.

Destination To specify the DMZ device by IP address, select **IP Address** and enter its IP address. If you need to assign a static IP address to the device, then go to "**DHCP Reservation**" on page 7.

To specify the DMZ device by MAC address, select **MAC Address** and enter its MAC address. To look up its MAC address, click **DHCP Client Table**.

DHCP Client Table

The *DHCP Client Table* screen appears. It lists computers and other devices that have IP addresses assigned by the router. The list can be sorted by Client Name, Interface, IP Address, and MAC Address.



DHCP Client Table

To Sort by: IP Address

Client Name	Interface	IP Address	MAC Address	
techwriter-PC	LAN	192.168.1.110	00:1E:37:23:11:8F	Select

Refresh Close

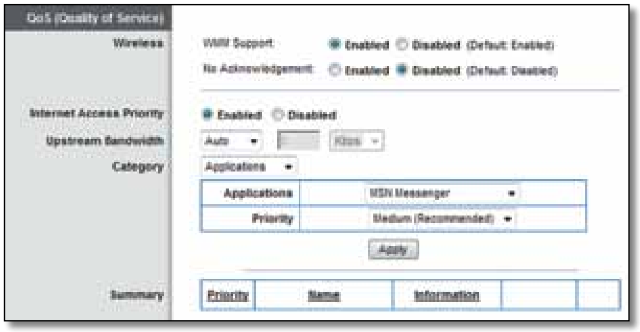
DMZ > DHCP Client Table

To select a DHCP client, click **Select**. To update the on-screen information, click **Refresh**. To exit this screen and return to the *DMZ* screen, click **Close**.

Applications and Gaming > QoS

Quality of Service (QoS) is a method that assigns priority to specific types of network traffic, which often are demanding, real-time applications, such as online gaming, VoIP calls, video streaming, and videoconferencing. QoS can mark packets to designate different levels of priority, so it helps to ensure optimal performance for the most important, real-time applications.

QoS is only applied to traffic streams that are uploaded to the Internet. QoS cannot be guaranteed after the traffic streams reach the Internet.



QoS (Quality of Service)

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

Internet Access Priority: ● Enabled ○ Disabled
Upstream Bandwidth: Auto | Kbps
Category: Applications

Applications	MSN Messenger
Priority	Medium (Recommended)

Apply

Summary

Priority	Name	Information		

Applications and Gaming > QoS

QoS (Quality of Service)

Wireless

WMM Support The Wi-Fi MultiMedia (WMM) feature is a wireless QoS feature based on the IEEE 802.11e standard. WMM improves quality for audio, video, and voice applications by prioritizing wireless traffic. To use this feature, the wireless client devices in your network must support WMM. To disable this option, select **Disabled**. Otherwise, keep the default, **Enabled**.

No Acknowledgement If you want the router to re-send data if an error occurs, keep the default, **Disabled**. If you do not want the router to re-send data if an error occurs, select **Enabled**.

Internet Access Priority

The router is the interface between the local network and the Internet. The user can configure the router to assign higher priority for these categories: Applications, Online Games, MAC Address, and Voice Device.

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, keep the default, **Disabled**.

Upstream Bandwidth

The Upstream Bandwidth feature sets the maximum outgoing bandwidth that applications can use. The default, **Auto**, allows the router to set the maximum. The router sets speeds that are multiples of 512 Kbps. Here are a couple of examples:

- If the router auto-detects an upstream speed between 512 Kbps and 1024 Kbps, it will set the maximum at 512 Kbps.
- If the router auto-detects an upstream speed of 2300 Kbps, it will set the maximum at 2048 Kbps (512 Kbps x 4).

Upstream Bandwidth This option sets the maximum outgoing bandwidth of your Internet connection. To allow the router to detect the maximum, keep the default, **Auto**. To specify the maximum, select **Manual**. Then enter the appropriate bandwidth and select **Kbps** or **Mbps**.

> **NOTE:** If the maximum bandwidth is too high, then the router cannot apply QoS properly, and there will be adverse QoS issues.

Category

You can define the Internet access priority level for as many selections as you want. The *Summary* section will display all of the priority selections that you enter. Select from the following categories:

- **Applications** Allows you to assign a priority level for a predefined application or one that you add.
- **Online Games** Allows you to assign a priority level for a preset game or one that you add.
- **MAC Address** This option lets you prioritize network traffic based on the device that is accessing the network. For example, if you want your gaming console to have higher priority accessing the Internet than your computer, you can assign their priority levels using their respective MAC addresses.
- **Voice Device** Voice devices require a higher priority level. You can assign a higher priority level to voice devices using their respective MAC addresses.

Summary

This lists the QoS entries you have created for your applications and devices. Go to "**Summary**" on page 40 for more information.

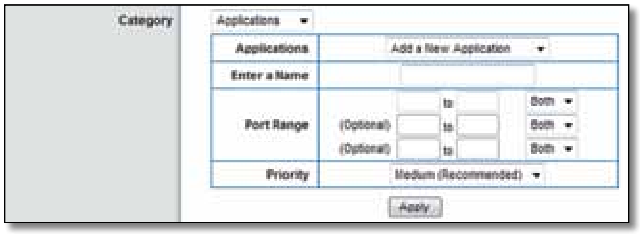
Applications

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 level: **High**, **Medium (Recommended)**, **Normal**, or **Low**.

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

Add a New Application



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

QoS > Add a New Application

Enter a Name Enter a name for this application.

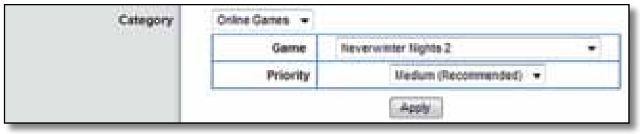
Port Range Enter the port range that the application will use. For example, to allocate a single port for FTP, enter 21 to 21 as the port range. If you need services for an application that uses ports 1000 to 1250, then enter 1000 to 1250 as the port range. You can define up to three ranges for this 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 level: **High**, **Medium (Recommended)**, **Normal**, or **Low**.

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

Online Games



Category: Online Games
Game: Neverwinter Nights 2
Priority: Medium (Recommended)

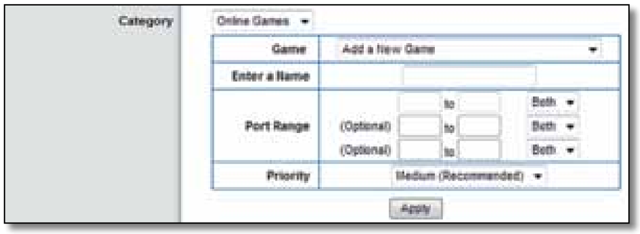
QoS > Online Games

Game 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 level: **High**, **Medium (Recommended)**, **Normal**, or **Low**.

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

Add a New Game



Category: Online Games
Game: Add a New Game
Enter a Name:
Port Range: to Both; (Optional) to Both; (Optional) to Both
Priority: Medium (Recommended)

QoS > Add a New Game

Enter a Name Enter a name for this game.

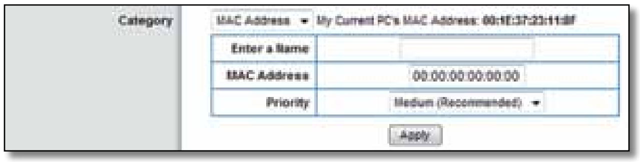
Port Range Enter the port range that the game will use. For example, if your game uses a single port (4000), then enter 4000 to 4000 as the port range. If you need services for a game that uses ports 4000 to 5000, then enter 4000 to 5000 as the port range. You can define up to three ranges for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your game's documentation for details on the service ports used.

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

Priority Select the appropriate priority level: **High**, **Medium (Recommended)**, **Normal**, or **Low**.

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

MAC Address



Category: MAC Address My Current PC's MAC Address: 00:1E:37:23:11:8F
Enter a Name:
MAC Address: 00:00:00:00:00:00
Priority: Medium (Recommended)

QoS > MAC Address

The MAC address of the computer you are using is displayed.

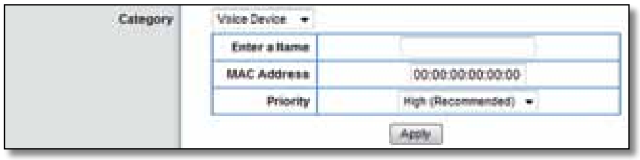
Enter a Name Enter a name for your device.

MAC Address Enter the MAC address of your device.

Priority Select the appropriate priority level: **High**, **Medium (Recommended)**, **Normal**, or **Low**.

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

Voice Device



Category: Voice Device

Enter a Name:

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

Priority: High (Recommended)

QoS > 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 level: **High (Recommended)**, **Medium**, **Normal**, or **Low**.

Click **Apply** 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 column displays the bandwidth priority of High, Medium, Normal, or Low.

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

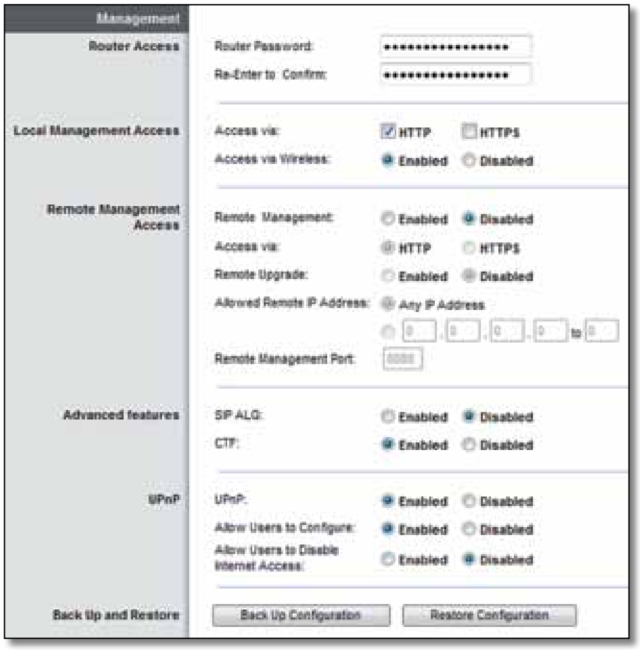
Information This column displays the port range or MAC address entered for your entry. If a predefined application or game was selected, there will be no valid entry shown in this section.

Remove Click this option to remove an entry.

Edit Click this option to make changes.

Administration > Management

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



Management

Router Access
Router Password: ****************
Re-Enter to Confirm: ****************

Local Management Access
Access via: ☑ HTTP ☐ HTTPS
Access via Wireless: ● Enabled ○ Disabled

Remote Management Access
Remote Management: ○ Enabled ● Disabled
Access via: ● HTTP ○ HTTPS
Remote Upgrade: ○ Enabled ● Disabled
Allowed Remote IP Address: ● Any IP Address
○ 0 . 0 . 0 . 0 to 0
Remote Management Port: 8080

Advanced features
SIP ALG: ○ Enabled ● Disabled
CTF: ● Enabled ○ Disabled

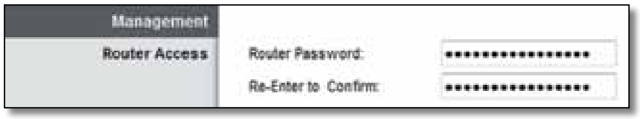
UPnP
UPnP: ● Enabled ○ Disabled
Allow Users to Configure: ● Enabled ○ Disabled
Allow Users to Disable Internet Access: ○ Enabled ● Disabled

Back Up and Restore

Administration > Management

Management

Router Access



Management

Router Access
Router Password: ****************
Re-Enter to Confirm: ****************

Management > Router Access

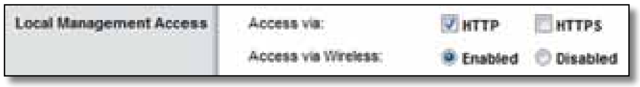
To ensure the router's security, you will be asked for your password when you access the router's browser-based utility. The default is **admin**.

If you used the setup software for installation, the default is changed to a unique password.

Router Password Enter a new password for the router.

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

Local Management Access



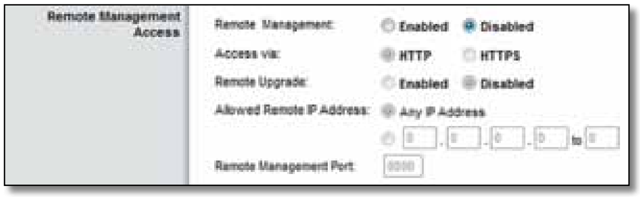
Local Management Access
Access via: ☑ HTTP ☐ HTTPS
Access via Wireless: ● Enabled ○ Disabled

Management > 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 (Secure Socket Layer) to encrypt data transmitted for higher security. Select the protocol for local access, **HTTP** or **HTTPS**. The default is **HTTP**.

Access via Wireless To allow wireless access to the router's browser-based utility, keep the default, **Enabled**.

Remote Access



Remote Management Access
Remote Management: ○ Enabled ● Disabled
Access via: ● HTTP ○ HTTPS
Remote Upgrade: ○ Enabled ● Disabled
Allowed Remote IP Address: ● Any IP Address
○ 0 . 0 . 0 . 0 to 0
Remote Management Port: 8080

Management > Remote Access

Remote Management To manage the router over the Internet, select **Enabled**.

Access via HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the Internet. HTTPS uses SSL (Secure Socket Layer) to encrypt data transmitted for higher security. Select the protocol for remote access, **HTTP** or **HTTPS**. **HTTP** is the default.

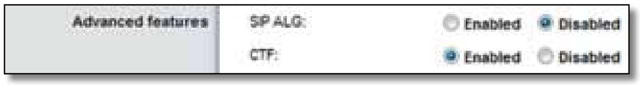
Remote Upgrade To upgrade the router's firmware over the Internet, select **Enabled**. (You must have the Remote Management option enabled as well.)

Allowed Remote IP Address If you want to be able to access the router from any external IP address, select **Any IP Address**. To specify an external IP address or range of IP addresses, select and complete the IP address range fields.

Remote Management Port Enter the port number that will be open to outside access. (To access the router, you will need to enter the router's password.)

✓ **NOTE:** When you are in a remote location and wish to manage the router, enter **http://xxx.xxx.xxx.xxx:yyyy** or **https://xxx.xxx.xxx.xxx:yyyy**, depending on whether you use HTTP or HTTPS. Enter the router's specific Internet IP address in place of xxx.xxx.xxx.xxx, and enter the Remote Management Port number in place of yyyy.

Advanced Features



Advanced features

SIP ALG: ○ Enabled ● Disabled

CTF: ● Enabled ○ Disabled

Management > Advanced Features

SIP ALG The Session Initiation Protocol (SIP) Application Layer Gateway (ALG) feature allows SIP packets, which are used for VoIP, to traverse the NAT firewall. For more information, contact your VoIP service provider.

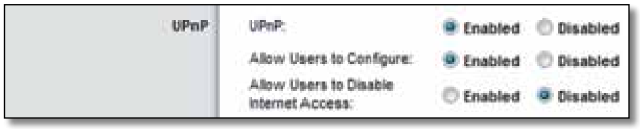
To use the SIP ALG feature for VoIP service, select **Enabled**. If you are not using VoIP service, then keep the default, **Disabled**.

If your VoIP service provider uses other NAT traversal solutions such as Session Traversal Utilities for NAT (STUN), Traversal Using Relay NAT (TURN), or Interactive Connectivity Establishment (ICE), then keep the default, **Disabled**.

CTF The CTF (Cut-Through Forwarding) option improves the efficiency of packet forwarding between the local network and the Internet. Using this option, the router caches route/bridge entries for established connections, so it can expedite the transmission of packets over those connections. To use the CTF option, keep the default, **Enabled**.

UPnP

Universal Plug and Play (UPnP) allows the appropriate operating system to automatically configure the router for various Internet applications, such as online gaming and VoIP calls.



UPnP

UPnP: ● Enabled ○ Disabled

Allow Users to Configure: ● Enabled ○ Disabled

Allow Users to Disable Internet Access: ○ Enabled ● Disabled

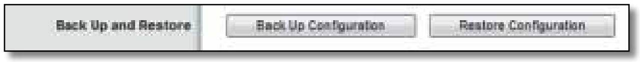
Management > UPnP

UPnP If you want to use UPnP, keep the default, **Enabled**.

Allow Users to Configure If you want to be able to make manual changes to the router while using the UPnP feature, keep the default, **Enabled**.

Allow Users to Disable Internet Access To prevent local network users from disabling your Internet connection through the UPnP feature, keep the default, **Disabled**.

Back Up and Restore



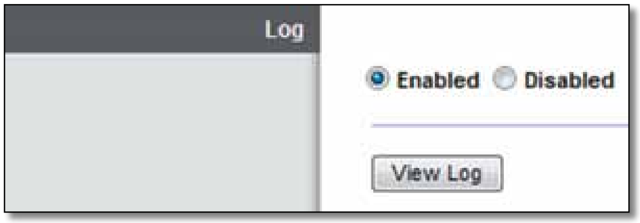
Management > Back Up and Restore

Back Up Configuration To back up the router's configuration settings, click this option and follow the on-screen instructions.

Restore Configuration To restore the router's configuration settings, click this option and follow the on-screen instructions. (You must have previously backed up the router's configuration settings.)

Administration > Log

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



Log

● Enabled ○ Disabled

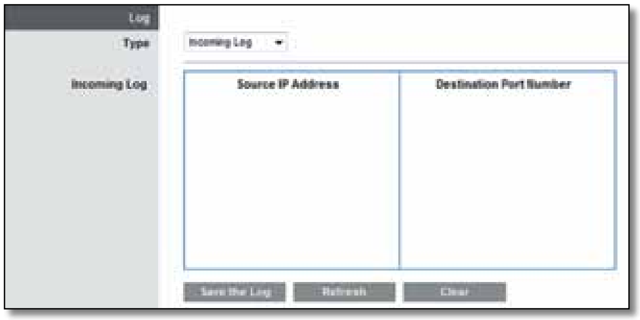
Administration > Log

Log

Enabled/Disabled To disable the Log function, select **Disabled**. To monitor traffic between the local network and the Internet, keep the default, **Enabled**. With logging enabled, you can choose to view temporary logs.

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

Log



Log

Type: Incoming Log

Incoming Log

Source IP Address	Destination Port Number

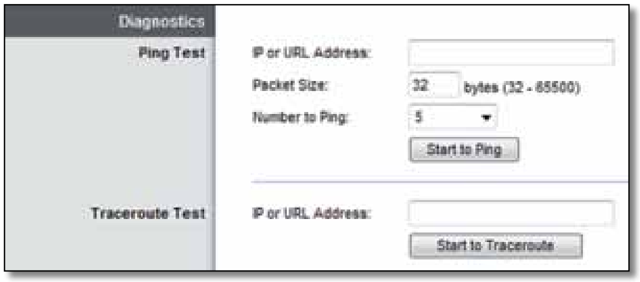
Log > View Log

- **Type** Select **Incoming Log**, **Outgoing Log**, **Security Log**, or **DHCP Client Log**.
- **<Type> Log** The Incoming Log displays a temporary log of the source IP addresses and destination port numbers for the incoming Internet traffic. The Outgoing Log displays a temporary log of the local IP addresses, destination URLs/IP addresses, and service/port numbers for the outgoing Internet traffic. The Security log displays the login information for the browser-based utility. The DHCP Client Log displays the local DHCP server status information.

  Click **Save the Log** to save this information to a file on your computer's hard drive. Click **Refresh** to update the log. Click **Clear** to clear all the information that is displayed.

Administration > Diagnostics

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



IP or URL Address:
Packet Size: 32 bytes (32 - 65500)
Number to Ping: 5
IP or URL Address:

Administration > Diagnostics

Diagnostics

Ping Test

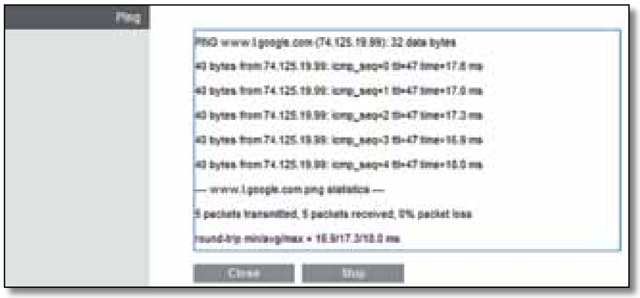
Ping checks whether the IP or URL address is reachable.

IP or URL Address Enter the IP or URL address you want to test.

Packet Size Enter the packet size you want to send. The default is **32** bytes.

Number to Ping Enter the number of times you wish to test the connection. The default is **5**.

Start Test To run the test, click this option. The *Ping* screen shows if the test is successful. Click **Close** to return to the *Diagnostics* screen. Click **Stop** to stop the test.



```
PING www.l.google.com (74.125.19.99): 32 data bytes
40 bytes from 74.125.19.99: icmp_seq=0 ttl=47 time=17.8 ms
40 bytes from 74.125.19.99: icmp_seq=1 ttl=47 time=17.0 ms
40 bytes from 74.125.19.99: icmp_seq=2 ttl=47 time=17.3 ms
40 bytes from 74.125.19.99: icmp_seq=3 ttl=47 time=16.9 ms
40 bytes from 74.125.19.99: icmp_seq=4 ttl=47 time=18.0 ms
--- www.l.google.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 16.9/17.3/18.0 ms
```

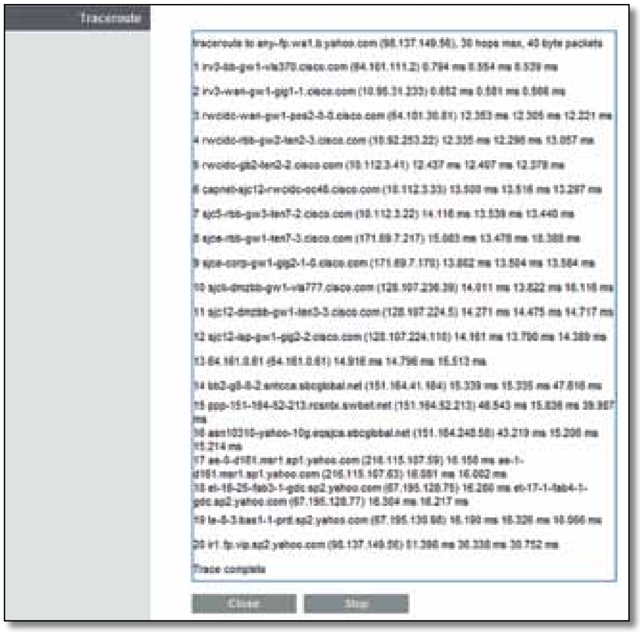
Diagnostics > Ping

Traceroute Test

Traceroute displays the route that packets travel between your computer and the IP or URL address.

IP or URL Address Enter the IP or URL address you want to test.

Start Test To run the test, click this option. The *Traceroute* screen shows if the test is successful. Click **Close** to return to the *Diagnostics* screen. Click **Stop** to stop the test.



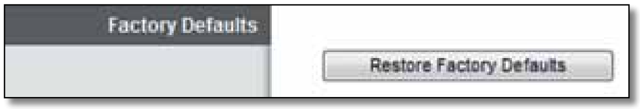
```
traceroute to any-fp.wa1.b.yahoo.com (98.137.149.56), 30 hops max, 40 byte packets
1 rv3-sb-gw1-vla370.cisco.com (64.101.111.2) 0.794 ms 0.554 ms 0.529 ms
2 rv3-wan-gw1-gig1-1.cisco.com (10.96.31.233) 0.652 ms 0.581 ms 0.566 ms
3 rwcidc-wan-gw1-pos2-0-0.cisco.com (64.101.30.81) 12.353 ms 12.305 ms 12.221 ms
4 rwcidc-rbb-gw2-ten2-3.cisco.com (10.92.253.22) 12.335 ms 12.296 ms 13.057 ms
5 rwcidc-gb2-ten2-2.cisco.com (10.112.3.41) 12.437 ms 12.407 ms 12.378 ms
6 capnet-sjc12-rwcidc-cc48.cisco.com (10.112.3.33) 13.500 ms 13.516 ms 13.287 ms
7 sjc5-rbb-gw3-ten7-2.cisco.com (10.112.3.22) 14.116 ms 13.539 ms 13.440 ms
8 sjce-rbb-gw1-ten7-3.cisco.com (171.69.7.217) 15.063 ms 13.478 ms 18.388 ms
9 sjce-corp-gw1-gig2-1-0.cisco.com (171.69.7.170) 13.862 ms 13.504 ms 13.584 ms
10 sjck-dmzbb-gw1-vla777.cisco.com (128.107.236.39) 14.011 ms 13.822 ms 16.116 ms
11 sjc12-dmzbb-gw1-ten3-3.cisco.com (128.107.224.5) 14.271 ms 14.475 ms 14.717 ms
12 sjc12-isp-gw1-gig2-2.cisco.com (128.107.224.110) 14.161 ms 13.790 ms 14.389 ms
13 64.161.0.61 (64.161.0.61) 14.916 ms 14.796 ms 15.513 ms
14 bb2-g8-0-2.snfcca.sbcglobal.net (151.164.41.184) 15.339 ms 15.335 ms 47.616 ms
15 ppp-151-164-52-213.rcsntx.swbell.net (151.164.52.213) 46.543 ms 15.836 ms 39.987
ms
16 asn10310-yahoo-10g.eqsjca.sbcglobal.net (151.164.248.58) 43.219 ms 15.206 ms
15.214 ms
17 ae-0-d161.msr1.sp1.yahoo.com (216.115.107.59) 16.156 ms ae-1-
d161.msr1.sp1.yahoo.com (216.115.107.63) 16.081 ms 16.062 ms
18 et-18-25-fab3-1-gdc.sp2.yahoo.com (67.195.128.75) 16.260 ms et-17-1-fab4-1-
gdc.sp2.yahoo.com (67.195.128.77) 16.304 ms 16.217 ms
19 te-8-3.bas1-1-prd.sp2.yahoo.com (67.195.130.98) 16.190 ms 16.326 ms 16.966 ms
20 ir1.fp.vip.sp2.yahoo.com (98.137.149.56) 31.398 ms 36.338 ms 30.752 ms
Trace complete
```

Diagnostics > Traceroute

Administration > Factory Defaults

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

> **NOTE:** Do not restore the factory defaults unless you are having difficulties with the router and have exhausted all other troubleshooting measures. Once the router is reset, you will have to re-enter all of your configuration settings.



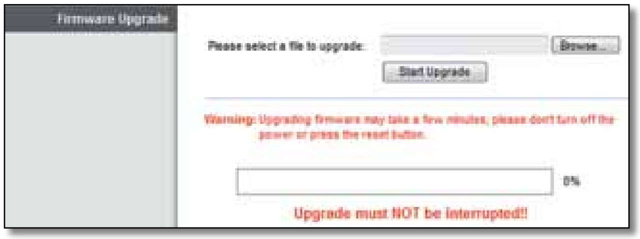
Administration > Factory Defaults

Factory Defaults

Restore Factory Defaults To reset the router's settings to the default values, click this option. Any settings you have saved will be lost when the default values are restored.

Administration > Firmware Upgrade

The *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.



Please select a file to upgrade:

Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.

0%

Upgrade must NOT be interrupted!!

Administration > Firmware Upgrade

NOTE: The router may lose the settings you have customized. Before you upgrade its firmware, write down all of your custom settings. After you upgrade its firmware, you will have to re-enter all of your configuration settings.

Firmware Upgrade

Before upgrading the firmware, download the router's firmware upgrade file from the website, **www.linksys.com/support**.

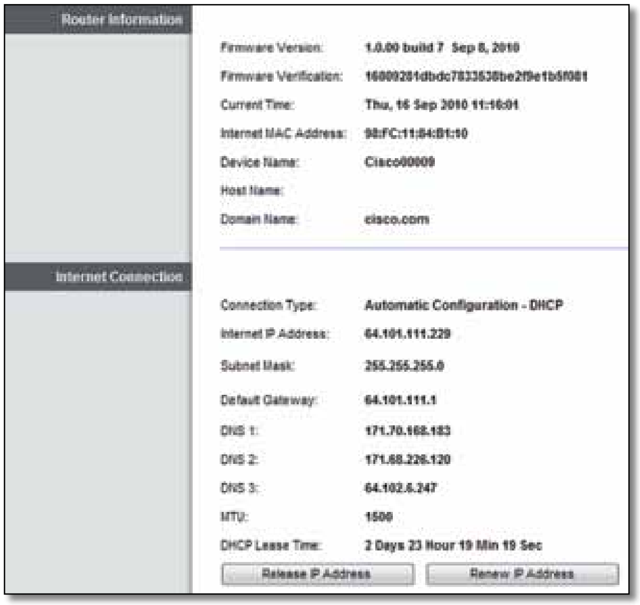
Please select a file to upgrade Click **Browse** and select the firmware upgrade file.

Start Upgrade After you have selected the appropriate file, click this option, and follow the on-screen instructions.

WARNING: Do not interrupt the upgrade process. You should not power off the router or press the Reset button during the upgrade process. Doing so may disable the router.

Status > Router

The *Router* screen displays information about the router and its current settings.



Router Information

Firmware Version: 1.0.00 build 7 Sep 8, 2010

Firmware Verification: 16009281dbdc7833538be2f9e1b5f081

Current Time: Thu, 16 Sep 2010 11:16:01

Internet MAC Address: 98:FC:11:84:B1:10

Device Name: Cisco00009

Host Name:

Domain Name: cisco.com

Internet Connection

Connection Type: Automatic Configuration - DHCP

Internet IP Address: 64.101.111.229

Subnet Mask: 255.255.255.0

Default Gateway: 64.101.111.1

DNS 1: 171.70.168.183

DNS 2: 171.68.226.120

DNS 3: 64.102.6.247

MTU: 1500

DHCP Lease Time: 2 Days 23 Hour 19 Min 19 Sec

Status > Router

Router Information

Firmware Version The version number of the router's current firmware is displayed.

Firmware Verification The unique identifier of the firmware is displayed.

Current Time The local time is displayed.

Internet MAC Address The router's MAC address, as seen from the Internet, is displayed.

Device Name The Device Name is the NetBIOS name of the router. The default is **Cisco** followed by the last 5 digits of the router's serial number, which is found on the bottom of the router. If you used the setup software for installation, then the Device Name is the name of your wireless network (up to 15 characters).

Host Name The Host Name of the router is displayed.

Domain Name The Domain Name of the router is displayed.

Internet Connection

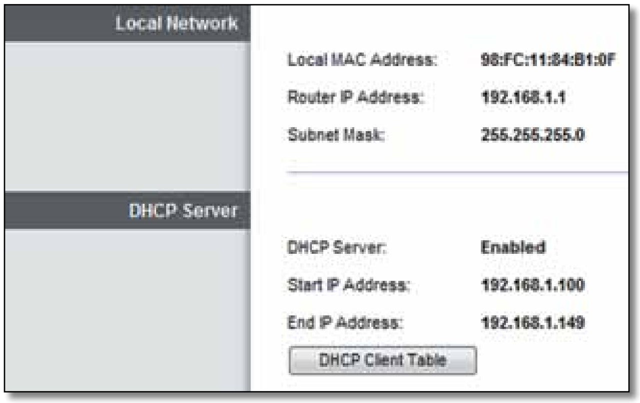
This section shows the current network information. The information varies depending on the Internet connection type selected on the *Setup > Basic Setup* screen.

For a DHCP connection, select **Release IP Address** or **Renew IP Address** as appropriate to release or renew a DHCP lease. For a PPPoE or similar connection, select **Connect** or **Disconnect** as appropriate to connect to or disconnect from the Internet.

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

Status > Local Network

The *Local Network* screen displays information about the local network.



Local Network

Local MAC Address: 98:FC:11:84:B1:0F

Router IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP Server

DHCP Server: Enabled

Start IP Address: 192.168.1.100

End IP Address: 192.168.1.149

Status > Local Network

Local Network

Local MAC Address The MAC address of the router's local, wired interface is displayed.

Router IP Address The router's local IP address is displayed.

Subnet Mask The subnet mask of the router is displayed.

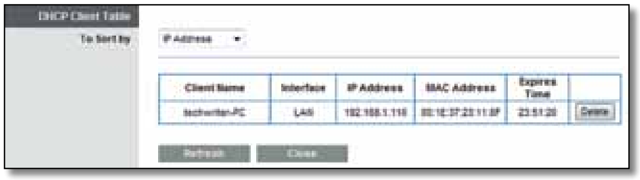
DHCP Server

DHCP Server The status of the router's DHCP server function is displayed.

Start IP Address For the range of available IP addresses, the starting IP address is displayed.

End IP Address For the range of available IP addresses, the ending IP address is displayed.

DHCP Client Table Click this option to view a list of computers or other devices that are using the router as a DHCP server.



DHCP Client Table

To Sort by: IP Address

Client Name	Interface	IP Address	MAC Address	Expires Time	
techwriter-PC	LAN	192.168.1.116	00:1E:37:23:11:8F	23:51:20	Delete

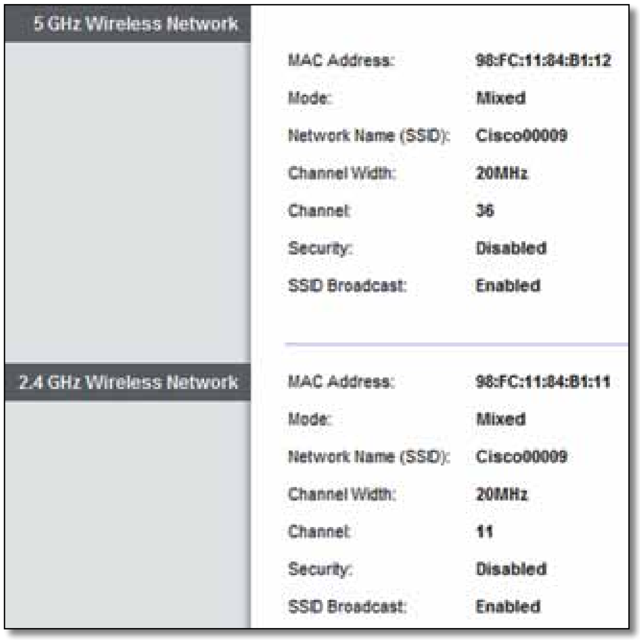
DHCP Client Table

DHCP Client Table

The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the router. The list can be sorted by IP Address, MAC Address, Interface, and Client Name. To remove a DHCP client, click **Delete**. To update the on-screen information, click **Refresh**. To exit this screen and return to the *Local Network* screen, click **Close**.

Status > Wireless Network

The *Wireless Network* screen displays information about your wireless network(s).



5 GHz Wireless Network

MAC Address:	98:FC:11:84:B1:12
Mode:	Mixed
Network Name (SSID):	Cisco00009
Channel Width:	20MHz
Channel:	36
Security:	Disabled
SSID Broadcast:	Enabled

2.4 GHz Wireless Network

MAC Address:	98:FC:11:84:B1:11
Mode:	Mixed
Network Name (SSID):	Cisco00009
Channel Width:	20MHz
Channel:	11
Security:	Disabled
SSID Broadcast:	Enabled

Status > Wireless Network

5 GHz Wireless Network or 2.4 GHz Wireless Network

MAC Address The MAC address of the router's wireless interface is displayed.

Mode The wireless mode used by the network is displayed.

Network Name (SSID) The name of the wireless network, also called the SSID, is displayed

Channel Width The radio channel width used by Wireless-N devices is displayed.

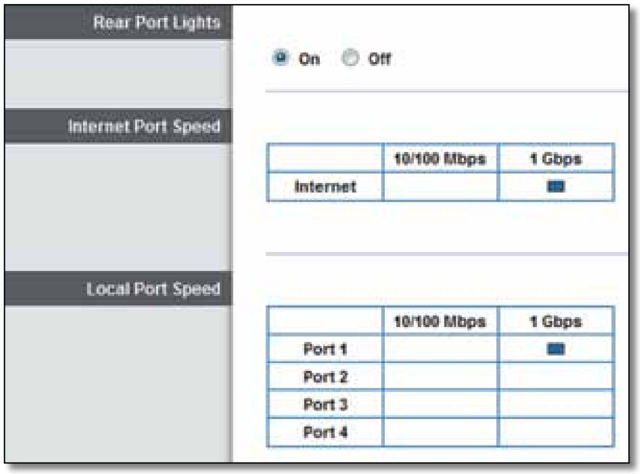
Channel The router's operating radio channel is displayed.

Security The wireless security method used by the wireless network is displayed.

SSID Broadcast The status of the SSID Broadcast option is displayed.

Status > Ports

The *Ports* screen allows you to control the router's port lights and displays information about the router's port speeds.



Rear Port Lights

● On ○ Off

Internet Port Speed

	10/100 Mbps	1 Gbps
Internet		■

Local Port Speed

	10/100 Mbps	1 Gbps
Port 1		■
Port 2		
Port 3		
Port 4		

Status > Ports

Rear Port Lights

On/Off To allow the lights on the router's back panel to turn on, keep the default, **On**.

Internet Port Speed

10/100 Mbps or 1 Gbps The maximum speed of the Internet port is displayed.

Local Port Speed

10/100 Mbps or 1 Gbps The maximum speed of each local port (Ports 1-4) is displayed.

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

Appendix A: Troubleshooting

Your computer cannot connect to the Internet.

Follow these instructions until your computer can connect to the Internet:

- Verify that the power adapter is connected to the router and to a power outlet. If the power adapter is connected to a power strip, make sure the power strip is powered on.
- Make sure that the Power light on the top of the router is lit. If you have any wired computers connected to the router, make sure the appropriate port lights on the back are lit.

> **NOTE:** The Power light flashes after the power adapter is connected to the router. If the light flashes for more than 30 seconds, it may indicate that the router is not working properly. For assistance, use a computer or device with Internet access to refer to the support section on the web, **www.linksys.com/support**

- Make sure that your DSL or cable modem is connected to your router's Internet port using an Ethernet cable.
- Reset all of the devices on your network:
    1. Power off all of your network computers and devices, and then disconnect the power adapter from your router.
    2. Disconnect your modem's power cord (and coaxial cable if you have a cable modem), and wait two minutes.
    3. Reconnect your modem's power cord (and coaxial cable) and wait two more minutes.
    4. Reconnect the power adapter to the router, and then power on all of your network computers and devices.

The modem does not have an Ethernet port.

The modem is a dial-up modem for traditional dial-up service. To use the router, you need a cable/DSL modem and high-speed Internet connection.

You cannot use the DSL service to connect manually to the Internet.

After you have installed the router, it will automatically connect to your Internet Service Provider (ISP), so you no longer need to connect manually.

The DSL telephone line does not fit into the router's Internet port.

The router does not replace your modem. You still need your DSL modem in order to use the router. Connect the telephone line to the DSL modem, and then insert the setup CD into your computer. Click **Set up your Linksys Router** and follow the on-screen instructions.

When you open the web browser, the login screen appears, even though you do not need to log in.

These steps are specific to Internet Explorer but are similar for other browsers.

1. Open the web browser.
2. Go to **Tools** > **Internet Options**.
3. Click the **Connections** tab.
4. Select **Never dial a connection**.
5. Click **OK**.

The router does not have a coaxial port for the cable connection.

The router does not replace your modem. You still need your cable modem in order to use the router. Connect your cable connection to the cable modem, and then insert the setup CD into your computer. Click **Set up your Linksys Router** and follow the on-screen instructions.

The computer cannot connect wirelessly to the network.

Make sure the wireless network name or SSID is the same on both the computer and the router. If you have enabled wireless security, then make sure the same security method and key are used by both the computer and the router.

You need to change the settings on the router.

Wireless network settings can be changed using Cisco Connect. To change the router's advanced settings, refer to "**How to Access the Browser-Based Utility**" on page 3.

You want to access the browser-based utility from Cisco Connect.

To enter the browser-based utility from Cisco Connect, follow these steps:

1. Open Cisco Connect.
2. On the main menu, click **Router settings**.
3. Click **Advanced settings**.
4. Write down the username and password that are displayed. (To help protect your password, you can copy it to the Clipboard by clicking **Copy password**.)
5. Click **OK**.

6. Your web browser automatically opens. Enter the username and password, and then click **OK**. (If you copied the password to the Clipboard in step 4, press **Ctrl-V** to paste it into the *Password* field.)

When you try to log into the browser-based utility, your password does not work.

Your wireless security password also serves as the browser-based utility's login password. To see this password:

1. Open Cisco Connect.
2. On the main menu, click **Router settings**.
3. The *Password* is displayed on the left side of the screen.

The router does not recognize your USB storage device.

Make sure the USB storage device uses the NTFS, FAT, or HSF+ format. To check its format, follow these instructions:

1. Connect the USB storage device directly to your computer.
2. On your desktop, double-click **Computer** or **My Computer** icon.
3. Right-click the USB storage device, and click **Properties**.
4. The format is listed in the File system description. If the format is not NTFS, FAT, or HSF+, then back up the data on the USB storage device.

   After you have backed up the data on the USB storage drive, you can format it.

   Windows: Right-click the USB storage device, and click **Format**. Follow the on-screen instructions. For more information, refer to Windows Help.

   Mac: Use the Disk Utility.

If the router still does not recognize the USB storage device, then remove the power adapter from the router's Power port. Wait five seconds, and then re-connect the power adapter to the router's Power port.

In Windows Vista, you do not see the USB storage device in the* Network *screen.

Make sure the router and your computer use the same workgroup name. (The default workgroup name of the router is **workgroup**. In Windows Vista, right-click the **Computer** icon and select **Properties**. Click **Advanced system settings**. Click the **Computer Name** tab. The workgroup name is displayed.) If they differ, then change the workgroup name of the router. Follow these instructions:

1. Access the web-based utility of the router. (Refer to "**How to Access the Browser-Based Utility**" on page 3.)
2. Click the **Storage** tab.
3. Click the **Administration** tab.
4. In the *Workgroup Name* field, enter the workgroup name of your computer.
5. Click **Save Settings**.

In Windows XP, you do not see the router in the* My Network Places *screen.

In the *Network Tasks* section, click **Show icons for networked UPnP devices**. If the router does not appear, follow these instructions:

1. Go to **Start > Control Panel > Firewall**.
2. Click the **Exceptions** tab.
3. Select **UPnP Framework**.
4. Click **OK**.

In Windows XP, you do not see your USB storage device in the* View workgroup computers *screen.

Make sure the router and your computer use the same workgroup name. (The default workgroup name of the router is **workgroup**. In Windows XP, go to **Start > Control Panel > System**. Click the **Computer Name** tab. The workgroup name is displayed.) If they differ, then change the workgroup name of the router. Follow these instructions:

1. Access the web-based utility of the router. (Refer to "**How to Access the Browser-Based Utility**" on page 3.)
2. Click the **Storage** tab.
3. Click the **Administration** tab.
4. In the *Workgroup Name* field, enter the workgroup name of your computer.
5. Click **Save Settings**.

Your USB storage device includes two USB connectors.

Connect the primary USB connector of the USB storage device to the USB port of the router. If the USB storage device does not work properly (because it requires additional power from the secondary USB connector), then use a different USB storage device with a single USB connector.

WEB: If your questions are not addressed here, refer to our Linksys E4200 section on the web, **www.linksys.com/support**

Appendix B: How to Connect and Access USB Storage

Overview

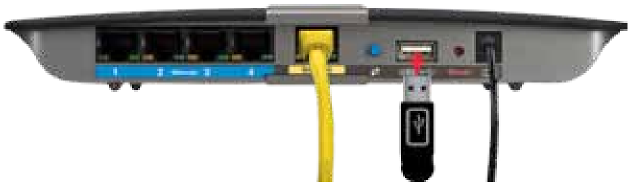
The router's USB port lets you connect USB storage that can be accessed over your network. This appendix covers the following:

- Connect and remove the USB storage device
- Access the USB storage device and create shortcuts
- Map the USB storage device (Windows) or add it to Startup Login Items (Mac)
- Create a shared folder on a USB storage device (advanced users)
- Manage access to shared folders using group and user accounts (advanced users)

Add or Remove USB Storage

Add USB Storage

1. Make sure your computer has a wired or wireless connection to the router.
2. Connect an external USB hard disk drive or USB flash drive to the USB port of the router.



NOTE: If your USB storage device includes two USB connectors, then connect the primary USB connector to the USB port of the router. If the USB storage device does not work properly (because it requires additional power from the secondary USB connector), then use a different USB storage device with a single USB connector.

3. Follow the instructions for your operating system: "**Windows 7**" on page 45, "**Windows Vista**" on page 47, "**Windows XP**" on page 49, or "**Mac OS X**" on page 51.

NOTE: For a quick way to access your USB storage device, go to "**Quick Access**" on page 44.

Remove USB Storage

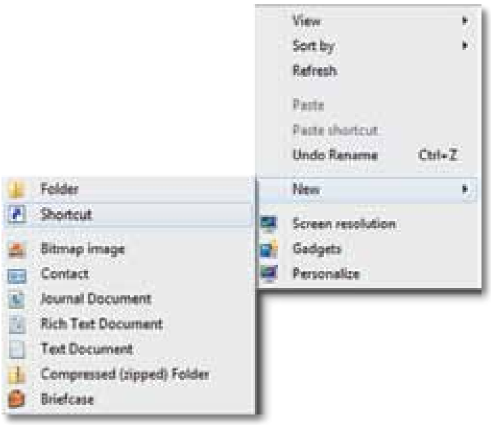
If you need to disconnect a USB storage device from the router, first click **Safely Remove Disk** on the *Storage > Disk* screen (refer to "**Storage > Disk**" on page 22). This prevents the possible loss or corruption of data, which may occur if you remove the disk while it is transferring data.

Quick Access

Windows 7, Vista, or XP

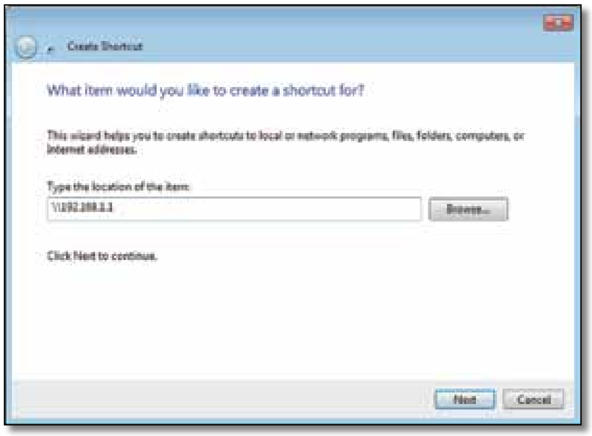
NOTE: The screenshots are shown for Windows 7, and similar screens appear for non-Windows 7 users.

1. Right-click your desktop. Select **New** and click **Shortcut**.



Windows Explorer Icon

2. In the *Type the location of the item* field, enter the default IP address of the router: **\\192.168.1.1** and click **Next**.



Create Shortcut

What item would you like to create a shortcut for?

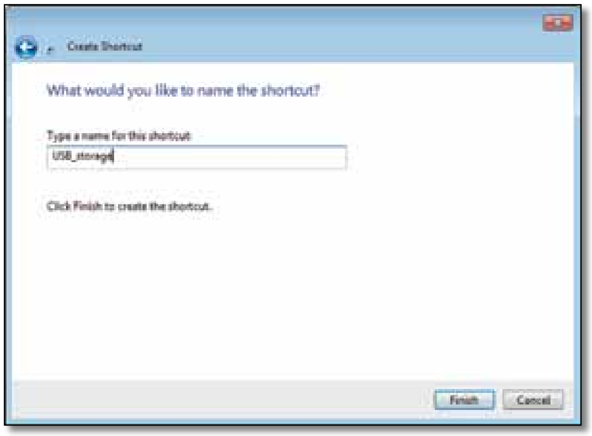
This wizard helps you to create shortcuts to local or network programs, files, folders, computers, or Internet addresses.

Type the location of the item:
\\192.168.1.1

Click Next to continue.

Create Shortcut - Enter IP Address

3. In the *Type a name for this shortcut* field, enter a descriptive name and click **Finish**.


Create Shortcut

What would you like to name the shortcut?

Type a name for this shortcut: USB_storage

Click Finish to create the shortcut.

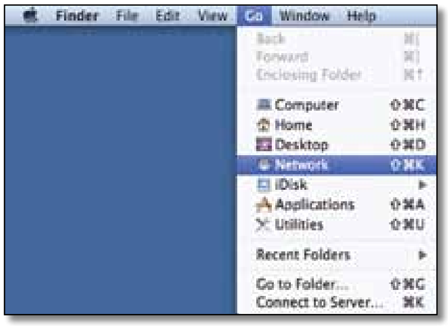
Create Shortcut - Name Shortcut

4. Double-click the shortcut to access the USB storage device.

Shortcut Icon

Mac OS X

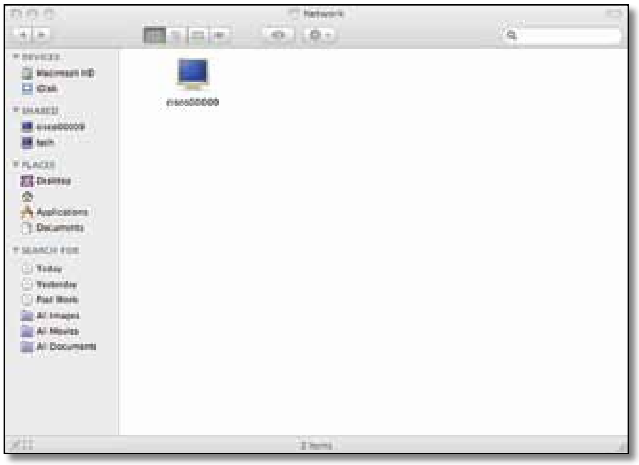
1. From your desktop, go to **Finder** > **Go** > **Network**.



Select Go > Network

2. Double-click the server name.

NOTE: If you used the setup software for installation, then the server name is the name of your wireless network (up to 15 characters). If not, the server name is **Cisco** followed by the last five digits of the router's serial number.



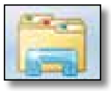
Double-Click Server Name

NOTE: It may take a few moments before the router is detected. Please wait.

Windows 7

Access the USB Storage Device

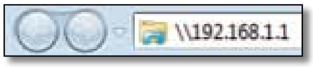
1. On your desktop, click the **Windows Explorer** icon.



Windows Explorer Icon

NOTE: If the Windows Explorer icon is not displayed, then go to **Start** > **All Programs** > **Accessories** > **Windows Explorer**.

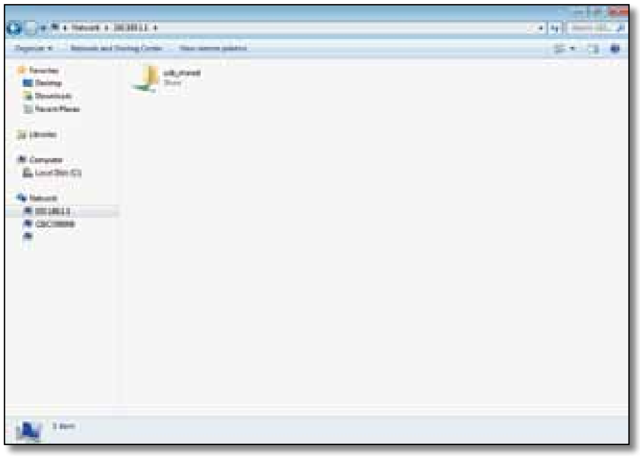
2. In the *Address* field, enter the default IP address of the router: **\\192.168.1.1**


\\192.168.1.1

Enter Local IP Address of Router

NOTE: Another option is to use the Device Name (Disk) of the router. In the *Address* field, enter: **\\Cisco** followed by the last five digits of the router's serial number. If you used the setup software for installation, then enter the name of your wireless network (up to 15 characters) in the *Address* field.

3. Double-click the shared folder.



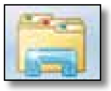
Double-Click Shared Folder

NOTE: If the shared folder is not displayed, right-click **Network**. Click **Properties**. Click **Change advanced sharing settings**. Select **Turn on network discovery**. Select **Turn on file and printer sharing**. Click **Save changes**.

NOTE: If the login screen appears, enter your account username and password. Click **OK**.

Map a Drive

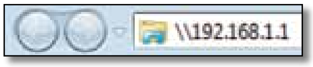
1. On your desktop, click the **Windows Explorer** icon.



Windows Explorer Icon

NOTE: If the Windows Explorer icon is not displayed, then go to **Start > All Programs > Accessories > Windows Explorer**.

2. In the *Address* field, enter the default IP address of the router: **\\192.168.1.1**

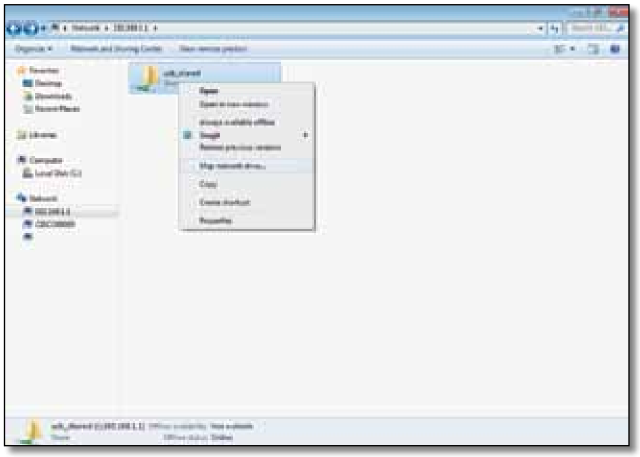


\\192.168.1.1

Enter Local IP Address of Router

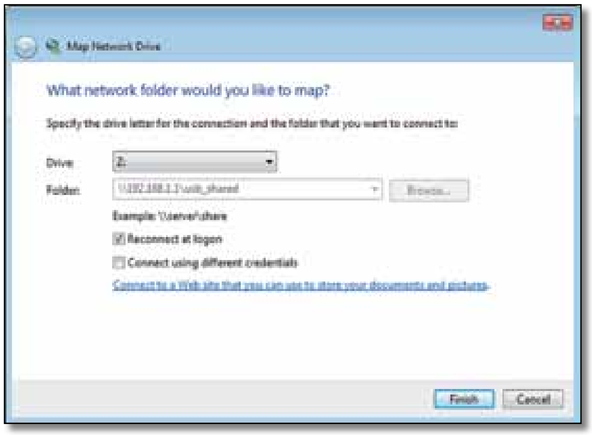
NOTE: Another option is to use the Device Name (Disk) of the router. In the *Address* field, enter: **\\Cisco** followed by the last five digits of the router's serial number. If you used the setup software for installation, then enter the name of your wireless network (up to 15 characters) in the *Address* field.

3. Right-click the folder you want to map, and click **Map network drive**.



Map Network Drive

4. From the *Drive* drop-down menu, select an available drive letter.



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\192.168.1.1\usb_shared

Example: \\server\share

☑ Reconnect at logon

☐ Connect using different credentials

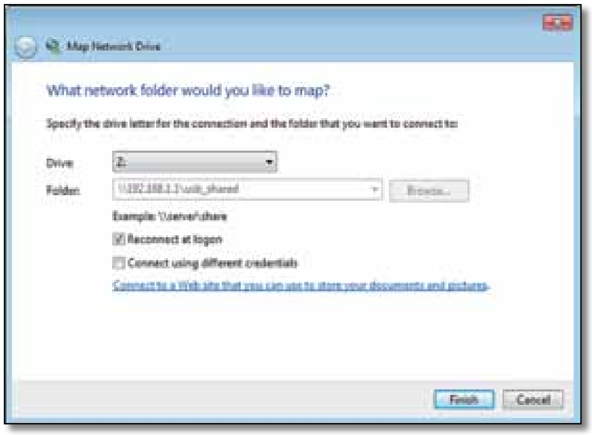
Connect to a Web site that you can use to store your documents and pictures.

Finish Cancel

Select Drive Letter

NOTE: If the login screen appears, enter your account username and password. Click **OK**.

5. Click **Finish**.



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\192.168.1.1\usb_shared

Example: \\server\share

☑ Reconnect at logon

☐ Connect using different credentials

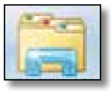
Connect to a Web site that you can use to store your documents and pictures.

Finish Cancel

Click Finish

Access the Mapped Drive

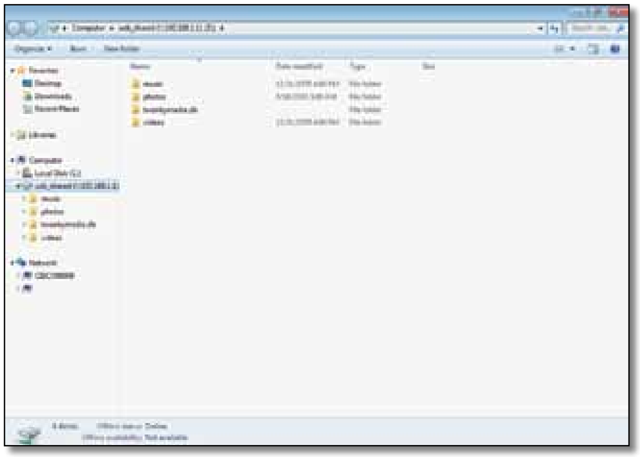
1. On your desktop, click the **Windows Explorer** icon.



Windows Explorer Icon

NOTE: If the Computer icon is not displayed, then go to **Start > All Programs > Accessories > Windows Explorer**.

2. Double-click the mapped drive to access it.



Double-Click Mapped Drive

Windows Vista

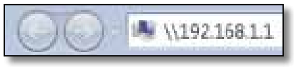
Access the USB Storage Device

1. On your desktop, double-click the **Computer** icon.

Computer Icon

NOTE: If the Computer icon is not displayed, then go to **Start > All Programs > Accessories > Windows Explorer**.

2. In the *Address* field, enter the default IP address of the router: **\\192.168.1.1**

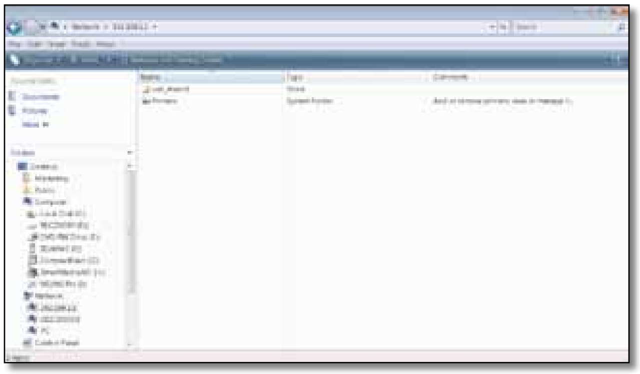


\\192.168.1.1

Enter Local IP Address of Router

NOTE: Another option is to use the Device Name (Disk) of the router. In the *Address* field, enter: **\\Cisco** followed by the last five digits of the router's serial number. If you used the setup software for installation, then enter the name of your wireless network (up to 15 characters) in the *Address* field.

3. Double-click the shared folder.



Double-Click Shared Folder

NOTE: If the login screen appears, enter your account username and password. Click **OK**.

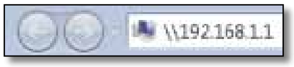
Map a Drive

1. On your desktop, double-click the **Network** icon.

Network Icon

NOTE: If the My Computer icon is not displayed, then go to **Start > All Programs > Accessories > Windows Explorer**.

2. In the *Address* field, enter the default IP address of the router: **\\192.168.1.1**

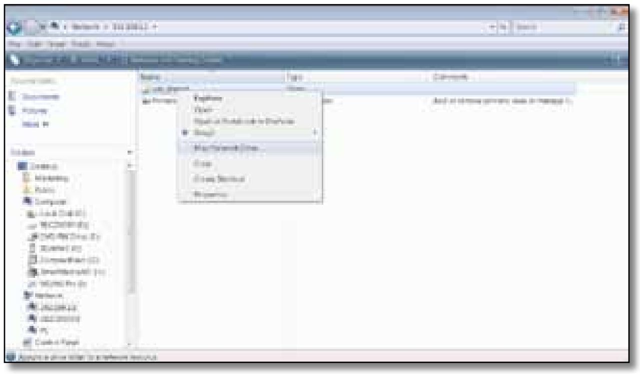


\\192.168.1.1

Enter Local IP Address of Router

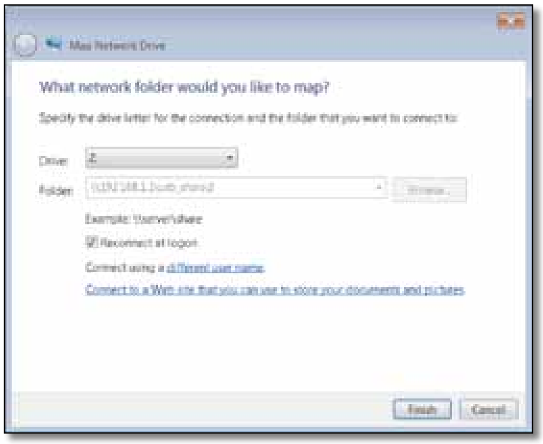
NOTE: Another option is to use the Device Name (Disk) of the router. In the *Address* field, enter: **\\Cisco** followed by the last five digits of the router's serial number. If you used the setup software for installation, then enter the name of your wireless network (up to 15 characters) in the *Address* field.

3. Right-click the folder you want to map, and click **Map Network Drive**.



Map Network Drive

4. From the *Drive* drop-down menu, select an available drive letter.



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\192.168.1.1\usb_share2

Example: \\server\share

☑ Reconnect at logon

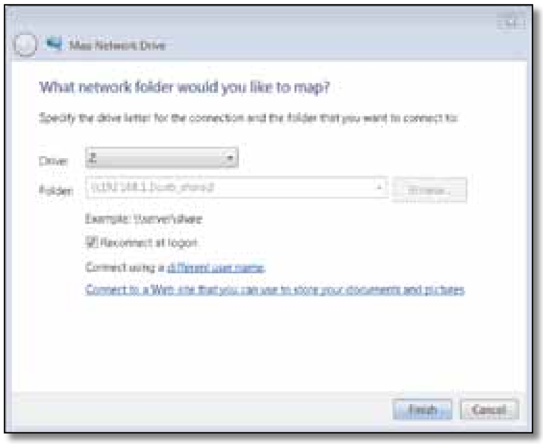
Connect using a different user name.

Connect to a Web site that you can use to store your documents and pictures.

Select Drive Letter

NOTE: If the login screen appears, enter your account username and password. Click **OK**.

5. Click **Finish**.



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\192.168.1.1\usb_share2

Example: \\server\share

☑ Reconnect at logon

Connect using a different user name.

Connect to a Web site that you can use to store your documents and pictures.

Click Finish

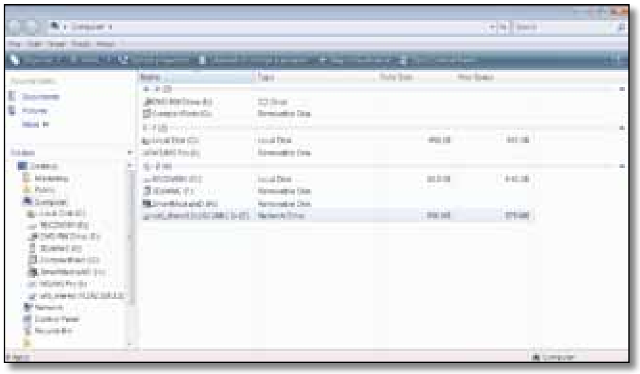
Access the Mapped Drive

1. On your desktop, double-click the **Computer** icon.

Computer Icon

NOTE: If the Computer icon is not displayed, then go to **Start > All Programs > Accessories > Windows Explorer**.

2. Double-click the mapped drive to access it.



Double-Click Mapped Drive

Windows XP

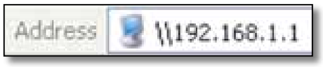
Access the USB Storage Device

1. On your desktop, double-click the **My Computer** icon.

My Computer Icon

NOTE: If the My Computer icon is not displayed, then go to **Start > All Programs > Accessories > Windows Explorer**.

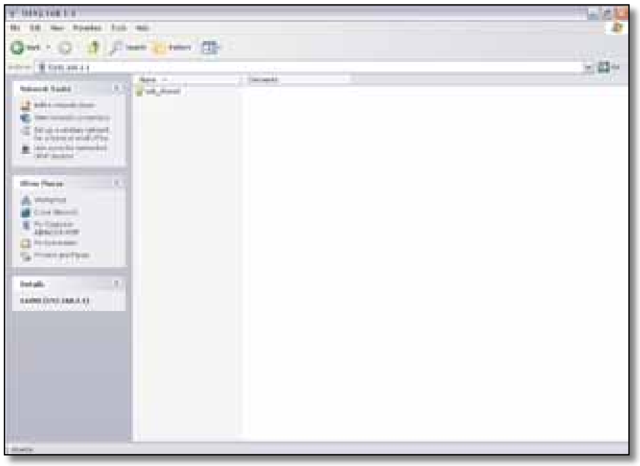
2. In the *Address* field, enter the default IP address of the router: **\\192.168.1.1**



Enter Local IP Address of Router

NOTE: Another option is to use the Device Name (Disk) of the router. In the *Address* field, enter: **\\Cisco** followed by the last five digits of the router's serial number. If you used the setup software for installation, then enter the name of your wireless network (up to 15 characters) in the *Address* field.

3. Double-click the shared folder.



Double-Click Shared Folder

NOTE: If the login screen appears, enter your account username and password. Click **OK**.

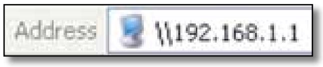
Map a Drive

1. On your desktop, double-click the **My Computer** icon.

My Computer Icon

NOTE: If the My Computer icon is not displayed, then go to **Start** > **All Programs** > **Accessories** > **Windows Explorer**.

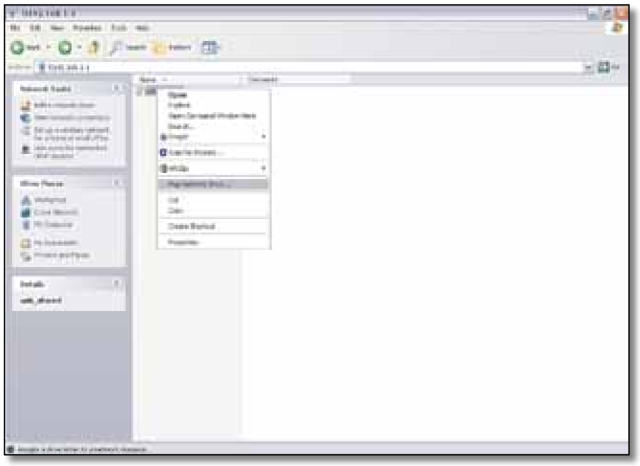
2. In the *Address* field, enter the default IP address of the router: **\\192.168.1.1**



Enter Local IP Address of Router

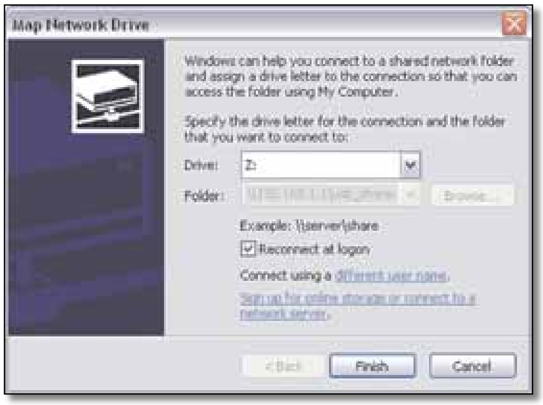
NOTE: Another option is to use the Device Name (Disk) of the router. In the *Address* field, enter: **\\Cisco** followed by the last five digits of the router's serial number. If you used the setup software for installation, then enter the name of your wireless network (up to 15 characters) in the *Address* field.

3. Right-click the folder you want to map, and click **Map Network Drive**.



Map Network Drive

4. From the *Drive* drop-down menu, select an available drive letter.



Map Network Drive

Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder:

Example: \\server\share

☑ Reconnect at logon

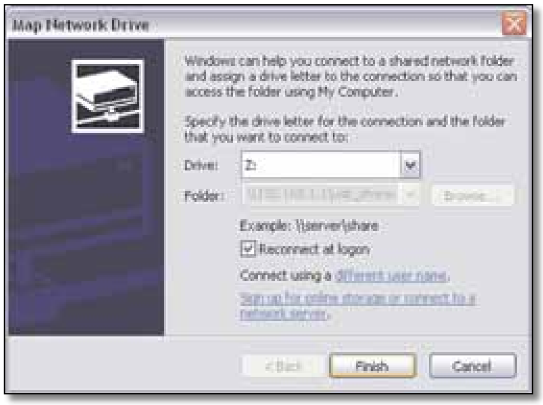
Connect using a different user name.

Sign up for online storage or connect to a network server.

Select Drive Letter

NOTE: If the login screen appears, enter your account username and password. Click **OK**.

5. Click **Finish**.



Map Network Drive

Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: [illegible]

Example: \\server\share

☑ Reconnect at logon

Connect using a different user name.

Sign up for online storage or connect to a network server.

Click Finish

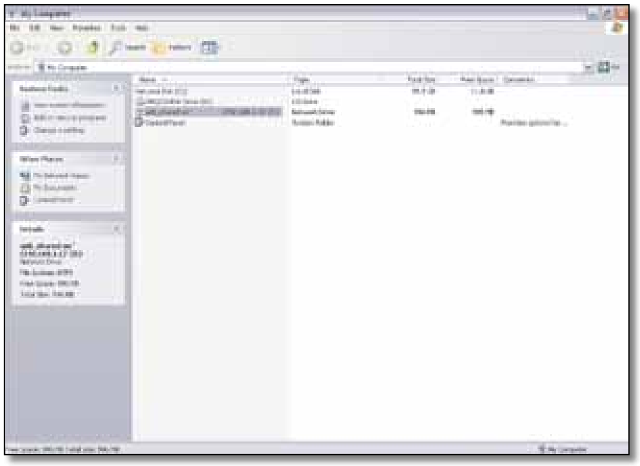
Access the Mapped Drive

1. On your desktop, double-click the **My Computer** icon.

My Computer Icon

NOTE: If the My Computer icon is not displayed, then go to **Start > All Programs > Accessories > Windows Explorer**.

2. Double-click the mapped drive to access it.

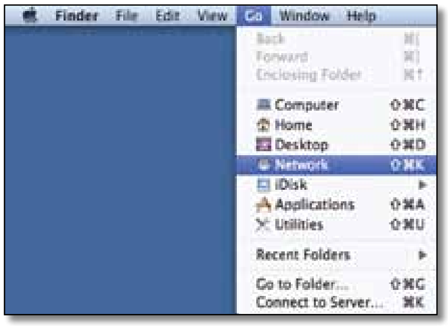


Double-Click Mapped Drive

Mac OS X

Access the USB Storage Device

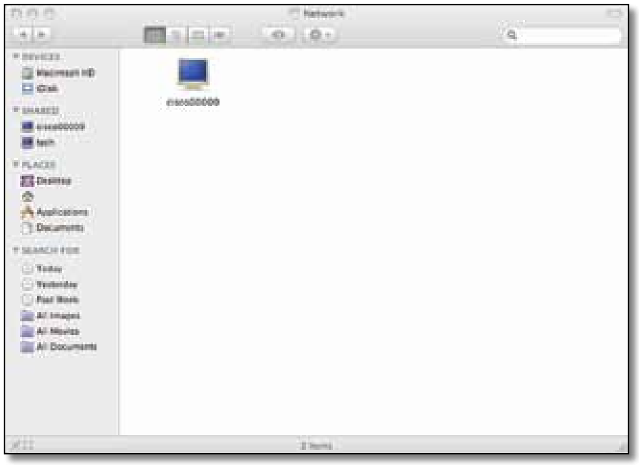
1. From your desktop, go to **Finder > Go > Network**.



Select Go > Network

2. Double-click the server name.

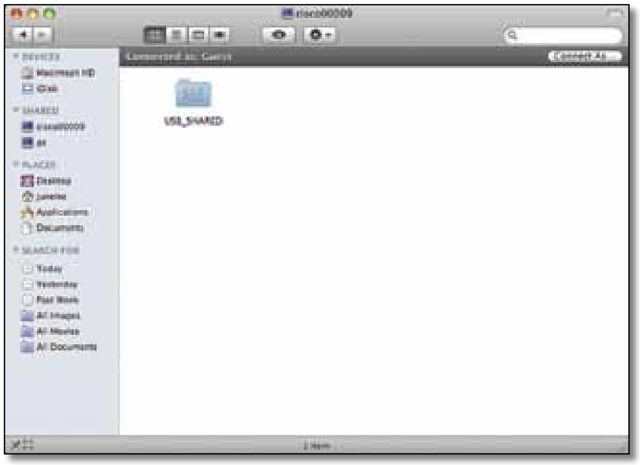
NOTE: If you used the setup software for installation, then the server name is the name of your wireless network (up to 15 characters). If not, the server name is **Cisco** followed by the last five digits of the router's serial number.



Double-Click Server Name

NOTE: It may take a few moments before the router is detected. Please wait.

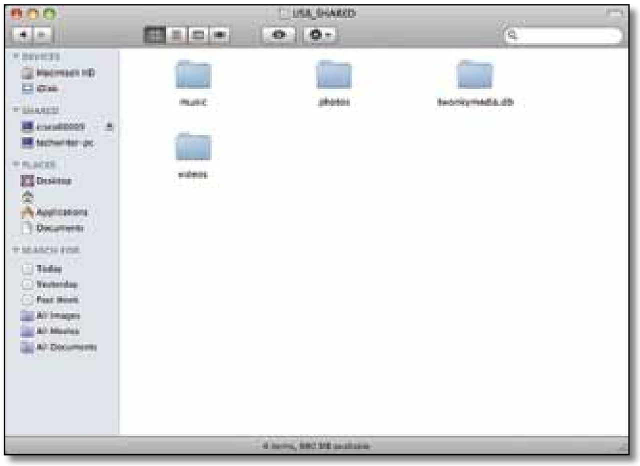
3. By default, the window displays Connected as: Guest. Double-click the shared folder.



Double-Click Shared Folder

NOTE: If you have disabled the *Anonymous Disk Access* option, then click **Connect As**. On the login screen, enter your account username and password. Click **OK**.

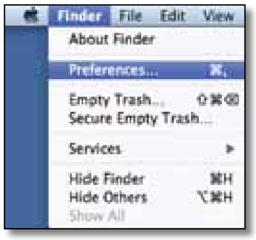
4. The shared folder opens.



Access Shared Folder

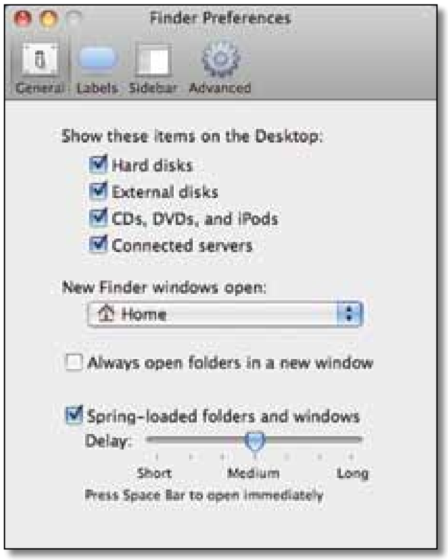
Display the Shared Folder on the Desktop

1. Go to **Finder** > **Preferences**.



Go to Finder > Preferences

2. Select **Connected servers**.



Show these items on the Desktop:

☑ Hard disks

☑ External disks

☑ CDs, DVDs, and iPods

☑ Connected servers

New Finder windows open: Home

□ Always open folders in a new window

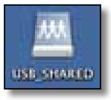
☑ Spring-loaded folders and windows

Delay: Short Medium Long

Press Space Bar to open immediately

Select Connected Servers

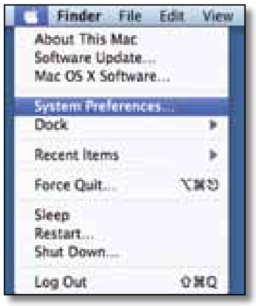
3. The shared folder is displayed on the desktop. To access it, double-click the icon.



Double-Click Shared Folder Icon

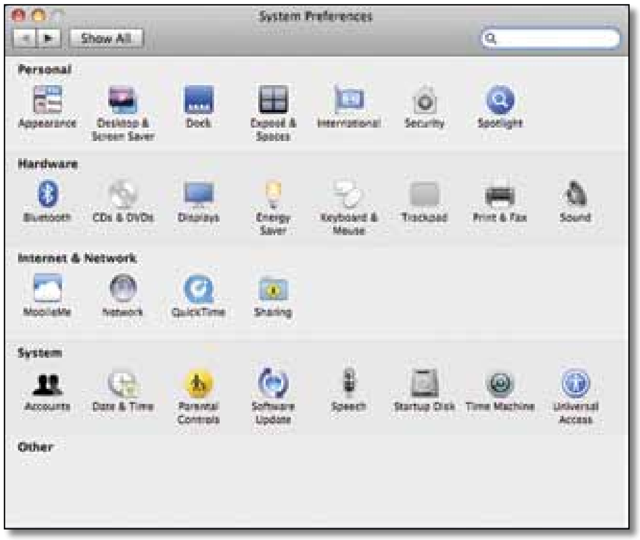
Add to Startup Login Items

1. Go to the **Apple** menu and select **System Preferences**.



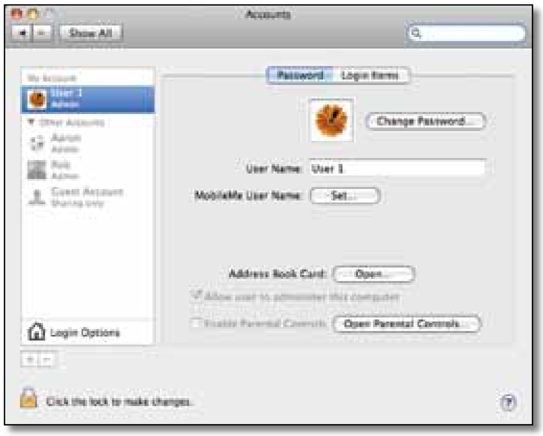
Go to Apple > System Preferences

2. Click **Accounts**.



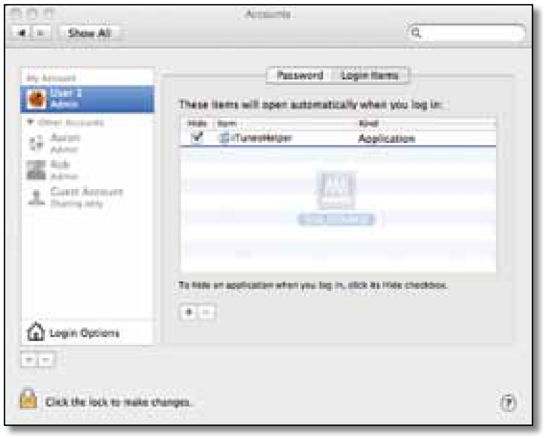
Click Accounts

3. Click **Login Items**.



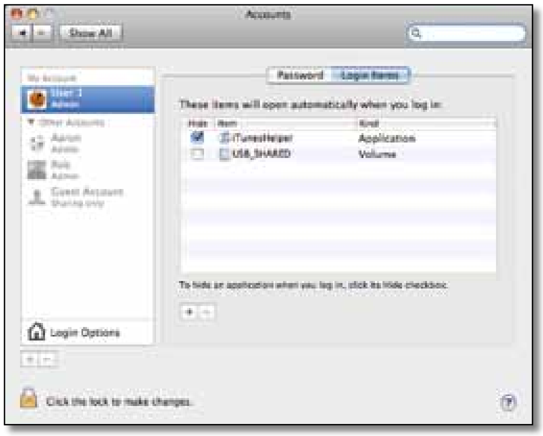
Click Login Items

4. Drag the shared folder to the *Login Items* window.



Drag Shared Folder

5. The folder appears in the list of Login Items. Click the red x to close the window.



Close Window

How to Manage Access to USB Storage

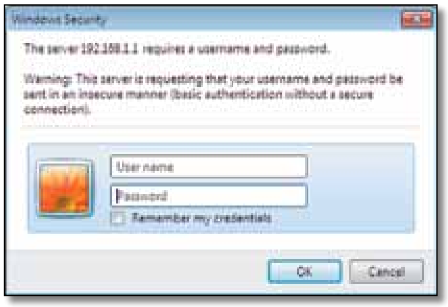
To manage access to the USB storage device, you can create shared folders, groups, and user accounts.

Access the Browser-Based Utility

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

A login screen appears. (A similar screen appears for non-Windows 7 users.)

1. In the *User name* field, enter **admin**.
2. In the *Password* field, enter the password created by the setup software. If you did not run the setup software, then enter the default, **admin**.
3. Click **OK** to continue.



Windows Security

The server 192.168.1.1 requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name

Password

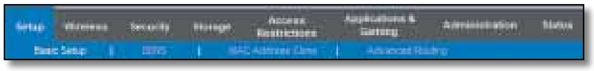
□ Remember my credentials

OK Cancel

Login Screen

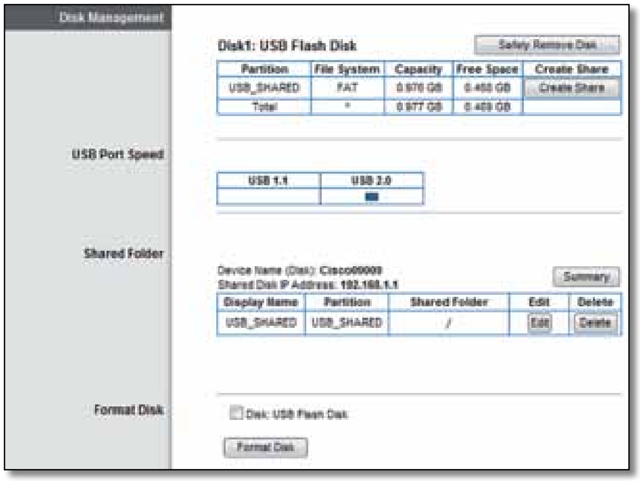
Create a Shared Folder

1. Click the **Storage** tab.



Top- and Lower-Level Tabs

2. Click the **Disk** tab. The *Disk* screen appears.



Disk Management

Disk1: USB Flash Disk (Safely Remove Disk)

Partition	File System	Capacity	Free Space	Create Share
USB_SHARED	FAT	0.976 GB	0.468 GB	Create Share
Total	*	0.977 GB	0.469 GB	

USB Port Speed

USB 1.1	USB 2.0
	■

Shared Folder

Device Name (Disk): Cisco00009 (Summary)
Shared Disk IP Address: 192.168.1.1

Display Name	Partition	Shared Folder	Edit	Delete
USB_SHARED	USB_SHARED	/	Edit	Delete

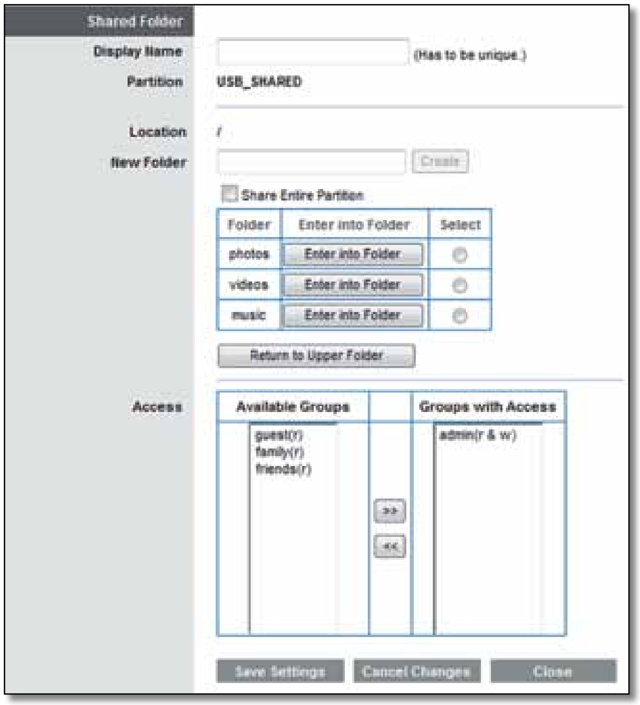
Format Disk

□ Disk: USB Flash Disk

Format Disk

Storage > Disk

3. Click **Create Share** for the appropriate partition. The *Shared Folder* screen appears.



Shared Folder

Display Name (Has to be unique.)

Partition USB_SHARED

Location /

New Folder (Create)

□ Share Entire Partition

Folder	Enter into Folder	Select
photos	Enter into Folder	○
videos	Enter into Folder	○
music	Enter into Folder	○

Return to Upper Folder

Access

Available Groups		Groups with Access

guest(r)
family(r)
friends(r)
	>>
	<<
		admin(r & w)

Save Settings Cancel Changes Close

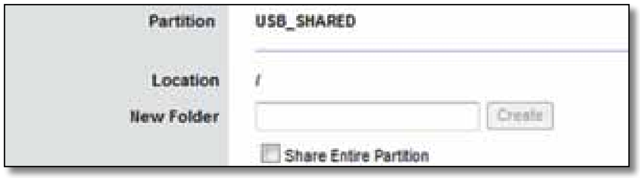
Disk > Shared Folder

4. In the *Display Name* field, enter a name for the shared folder.

Display Name (Has to be unique.)

Shared Folder > Enter Display Name

5. The Partition name is displayed. If the shared folder should include the entire partition, select **Share Entire Partition** and go to step 7.



Partition USB_SHARED

Location /

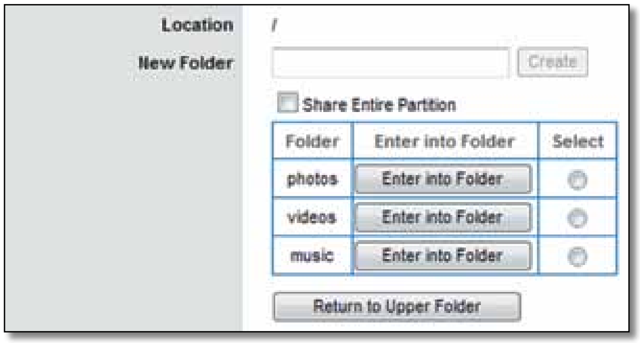
New Folder (Create)

□ Share Entire Partition

Shared Folder > Share Entire Partition

NOTE: If you select **Share Entire Partition**, then all of the Groups with Access (see step 7) can access any folder in the partition.

6. To specify a folder to share, click **Select**. To display subfolders, click **Enter into Folder**. To return to the previous folder, click **Return to Upper Folder**.



Location /

New Folder [ ] Create

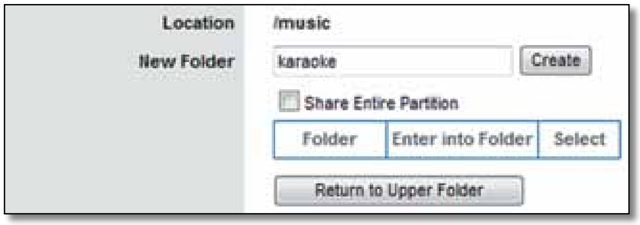
□ Share Entire Partition

Folder	Enter into Folder	Select
photos	Enter into Folder	○
videos	Enter into Folder	○
music	Enter into Folder	○

Return to Upper Folder

Shared Folder > Select Folder or Enter into Folder

To create a new folder, enter its name in the *New Folder* field. Then click **Create**.



Location /music

New Folder karaoke Create

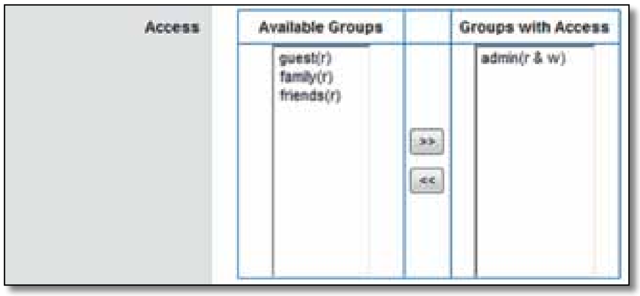
□ Share Entire Partition

Folder	Enter into Folder	Select

Return to Upper Folder

Shared Folder > Create New Folder

7. To allow a group to access the shared folder, select it from the *Available Groups* column, and then click the **>>** button. (To create groups, go to "**Create a Group Account**" on page 53.)



Access

Available Groups		Groups with Access

guest(r)
family(r)
friends(r)
	>>
	<<
		admin(r & w)

Shared Folder > Groups with Access

NOTE: By default, no password is needed for read-and-write access to the disk. If you want to specify which groups can access the shared folder, select **Disabled** for the *Anonymous Disk Access* option on the *Storage > Administration* screen. Go to "**Disable Anonymous Disk Access**" on page 53.

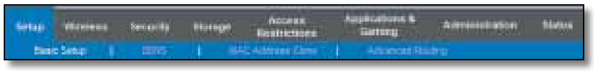
8. Click **Save Settings** to apply your changes, or click **Cancel Changes** to clear your changes. Click **Close** to exit this screen and return to the *Disk* screen.

Manage Group and User Access to Shared Folders

By default, no password is needed for read-and-write access to the disk. Before you can manage group and user access to specific shared folders, you must disable the *Anonymous Disk Access* option.

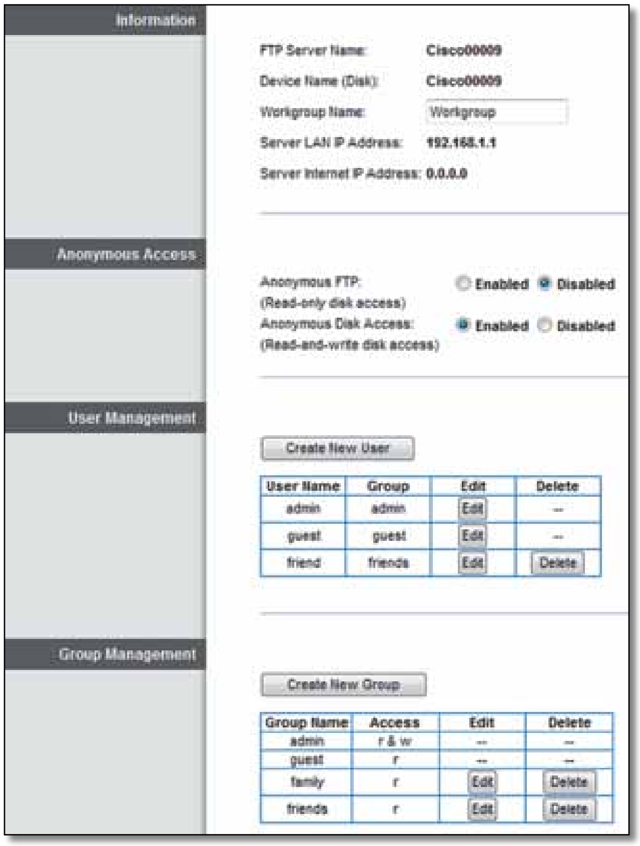
Disable Anonymous Disk Access

1. Click the **Storage** tab.



Top- and Lower-Level Tabs

2. Click the **Administration** tab. The *Administration* screen appears.



Information

FTP Server Name: Cisco00009

Device Name (Disk): Cisco00009

Workgroup Name: Workgroup

Server LAN IP Address: 192.168.1.1

Server Internet IP Address: 0.0.0.0

Anonymous Access

Anonymous FTP: (Read-only disk access) ○ Enabled ● Disabled

Anonymous Disk Access: (Read-and-write disk access) ● Enabled ○ Disabled

User Management

Create New User

User Name	Group	Edit	Delete
admin	admin	Edit	--
guest	guest	Edit	--
friend	friends	Edit	Delete

Group Management

Create New Group

Group Name	Access	Edit	Delete
admin	r & w	--	--
guest	r	--	--
family	r	Edit	Delete
friends	r	Edit	Delete

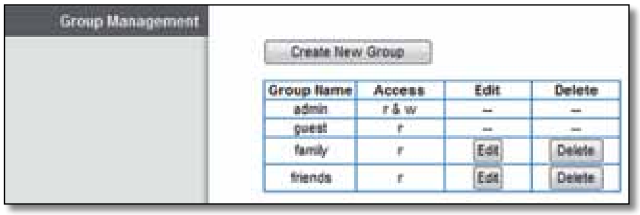
Storage > Administration

3. For the *Anonymous Disk Access* option, select **Disabled**.

4. Click **Save Settings**.

Create a Group Account

1. In the *Group Management* section on the *Storage* > *Administration* screen, click **Create New Group**.

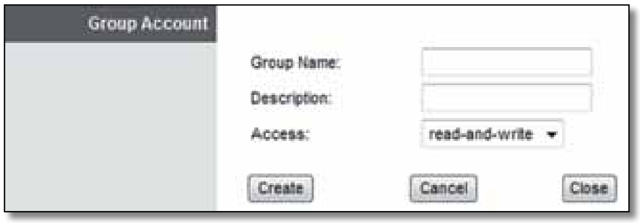


Group Name	Access	Edit	Delete
admin	r & w	--	--
guest	r	--	--
family	r	Edit	Delete
friends	r	Edit	Delete

Administration > Group Management

2. The *Group Account* screen appears.

   In the *Group Name* field, enter a name for the group.



Group Name:

Description:

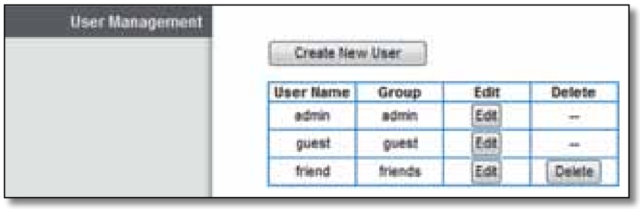
Access: read-and-write

Administration > Group Account

3. In the *Description* field, enter keywords to describe the group.
4. From the *Access* drop-down menu, select the appropriate level of access, **read-and-write** or **read-only**.
5. Click **Create** to apply your changes, or click **Cancel** to clear your changes. Click **Close** to exit the screen and return to the *Administration* screen.

Create a User Account

1. In the *User Management* section on the *Storage* > *Administration* screen, click **Create New User**.

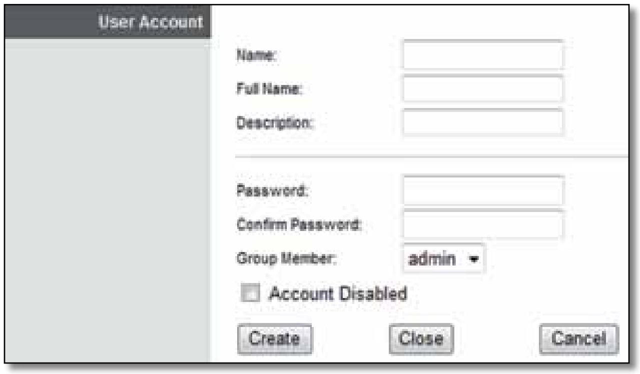


User Name	Group	Edit	Delete
admin	admin	Edit	--
guest	guest	Edit	--
friend	friends	Edit	Delete

Administration > User Management

2. The *User Account* screen appears.

   In the *Name* field, enter a name for the user.



Name:

Full Name:

Description:

Password:

Confirm Password:

Group Member: admin

□ Account Disabled

Administration > User Account

3. In the *Full Name* field, enter the actual name of the user.
4. In the *Description* field, enter keywords to describe the user.
5. In the *Password* and *Confirm Password* fields, enter the password that the user will use for login.
6. From the *Group Member* drop-down menu, select the appropriate group.

NOTE: To temporarily disable an account, select **Account Disabled**.

7. Click **Create** to apply your changes, or click **Cancel** to clear your changes. Click **Close** to exit the screen and return to the *Administration* screen.

Appendix C: Specifications

Model Name	Linksys E4200
Description	Maximum Performance Wireless-N Router
Model Number	E4200
Standards	802.11n, 802.11a, 802.11g, 802.11b, 802.3, 802.3u, 802.3ab
Radio Frequency	2.4 and 5 GHz
Switch Port Speed	10/100/1000 Mbps (Gigabit Ethernet)
Ports	Power, USB, Internet, Ethernet (1-4)
Buttons	Reset, Wi-Fi Protected Setup
LEDs	Top Panel: Power Back Panel: Internet, Ethernet (1-4)
Number of Antennas	6 Total, 3 Internal Antennas per Each 2.4 GHz and 5 GHz Radio Band
Detachable (y/n)	No
Modulations	802.11b: CCK, QPSK, BPSK 802.11g: OFDM 802.11a: OFDM 802.11n: BPSK, QPSK, 16-QAM, 64-QAM
Receive Sensitivity	2.4 GHz 802.11b: -87 dBm @ 11 Mbps (Typical) 802.11g: -77 dBm @ 54 Mbps (Typical) 802.11n: 20 MHz: -71 dBm @ MCS15 (Typical) 802.11n: 40 MHz: -68 dBm @ MCS15 (Typical) 5 GHz 802.11a: -71 dBm @ 54 Mbps (Typical) 802.11n: 20 MHz: -70 dBm @ MCS23 (Typical) 802.11n: 40 MHz: -68 dBm @ MCS23 (Typical)
Antenna Gain in dBi	2.4 GHz (3 internal PIFA antennas) PIFA 1 <= 3.6 dBi (Right) PIFA 2 <= 3.8 dBi (Left) PIFA 3 <= 3.8 dBi (Front) 5 GHz (3 internal PIFA antennas) PIFA 1 <= 4.8 dBi (Right) PIFA 2 <= 5.3 dBi (Left) PIFA 3 <= 5.2 dBi (Front)
Supported File Systems for Storage Device	FAT32, NTFS, and HSF+
UPnP	Supported
Security Features	WEP, WPA, WPA2
Security Key Bits	Up to 128-Bit Encryption

Environmental

Dimensions	8.86" x 0.98" x 6.30" (225 x 25 x 160 mm)
Unit Weight	12.52 oz (355 g)
Power	12V, 2A
Certifications	FCC, IC, CE, Wi-Fi a/b/g/n, Windows 7
Operating Temp.	32 to 104°F (0 to 40°C)
Storage Temp.	-4 to 140°F (-20 to 60°C)
Operating Humidity	10 to 80% Relative Humidity, Noncondensing
Storage Humidity	5 to 90% Noncondensing

Specifications are subject to change without notice.

CISCO™

www.linksys.com/support

Cisco, the Cisco Logo, and Linksys are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

© 2010 Cisco and/or its affiliates. All rights reserved.