User Guide

Linksys EA-Series

Contents

Product Overview

EA2700 1
EA3500 3
EA4500 6

Setting Up: Basics

How to create a home network. 9
What is a network? 9
How to set up a home network 9
Where to find more help 9
How to install your router 10
How to configure your router. 11
How to connect to Cisco Connect Cloud 11
How to connect directly to your router 12
How to improve your wireless connection speed 12
How to change your network's name and password 13
How to change your router's local access password 13
How to change your router's time zone 14
How to test your Internet connection speed 14
How to connect devices to your network 15
How to connect a computer to your network 15
How to connect a USB printer 15
How to connect other devices 16
How to view device details 17
How to set up parental controls 18
How to set parental controls 18
How to configure your guest network 19
How to back up your router configuration 20
How to customize Cisco Connect Cloud 21
Using widgets 21
Customizing the Device List 21

Setting Up: Advanced

How to manually set up your router. 22
How to manually set up your Internet connection 22
How to associate a router with your Cisco Connect Cloud account. .23
How to get the most out of your dual-band router 24
How to control access to your network. 25
How to improve security using the built-in firewall 27
How to set up the DHCP server on your router 28
How to set up DHCP reservation 29
How to access your network on the Internet 30
How to clone a MAC address 31
How to connect to your corporate office using a VPN 31
How to optimize your router for gaming and voice 32
How to enable Voice over IP on your network 33
How to configure UPnP 34
How to use a router as an access point 35
How to put your new router behind an existing router. 36
To add your router to an existing router or gateway 36
To share an Internet connection 37
To extend your network 39
How to expose a device to the Internet 39

Using an External Drive

Overview. 41

How to attach a USB drive 41

How to use secured folder access .42

How to set up authorized users and shared folders 42

How to access shared folders 43

How to set up your router as a media server 44

How to connect your UPnP device to the media server 45

How to remotely access storage 46

Port Forwarding and Port Triggering

How to set up port forwarding 48

How to set up port forwarding for a single port 48

How to set up port forwarding for multiple ports 49

How to set up port forwarding for a range of ports 49

How to set up port range triggering for online gaming 50

Maintaining and Monitoring

How to back up and restore your router configuration. 52

How to upgrade the router's firmware 53

How to restore factory defaults .53

How to check the status of your router. 54

How to disable the Ethernet port status lights 55

How to test your Internet connection 55

How to configure and use logs 56

Troubleshooting

During setup 57

Your router was not successfully set up 57

Windows XP Service Pack update 57

Your Internet cable is not plugged in message 58

Cannot access your router message 58

After setup. 60

The Internet appears to be unavailable 60

Cisco Connect Cloud does not open in your web browser 61

You cannot access Cisco Connect Cloud 61

All other troubleshooting has been unsuccessful 61

Specifications

Linksys EA2700 62

Linksys EA3500 63

Linksys EA4500 64

Product Overview

EA2700

Package contents

In addition to your router, your router package includes:

- Network (Ethernet) cable
- AC power adapter
- Setup CD containing router setup software and documentation

Features

Wireless-N technology

Built with leading 802.11n technology, create a powerful home wireless network with double the capacity for surfing the Internet, streaming multimedia, and running applications simultaneously. Connect your computers, Internet-ready TVs, game consoles, smartphones, and other Wi-Fi devices at fast transfer rates for an unrivaled experience.

The power of dual band

Double your network bandwidth with simultaneous dual-band N (2.4 and 5 GHz). The dual-band feature is designed to avoid interference and optimize throughput for smoother and faster HD video streaming, file transfers, and wireless gaming.

Advanced security

Keep Wi-Fi freeloaders and Internet threats at bay with WPA2 encryption and SPI firewall to help keep your network protected.

Benefits of gigabit

Use the four Gigabit Ethernet (10/100/1000) ports for quick file sharing (up to 10× faster than standard Ethernet) between other Gigabit-enabled devices like computers and servers.

Network ready

Connect computers, printers, scanners, and more to your wireless network and the Internet. QoS traffic prioritization technology delivers maximum speed and performance so you can enjoy fast downloads and reliable VoIP.

Easy to manage

Cisco Connect software helps you customize your settings and quickly add multiple devices to your network:

Separate guest network

Create a separate, password-protected network for guests.

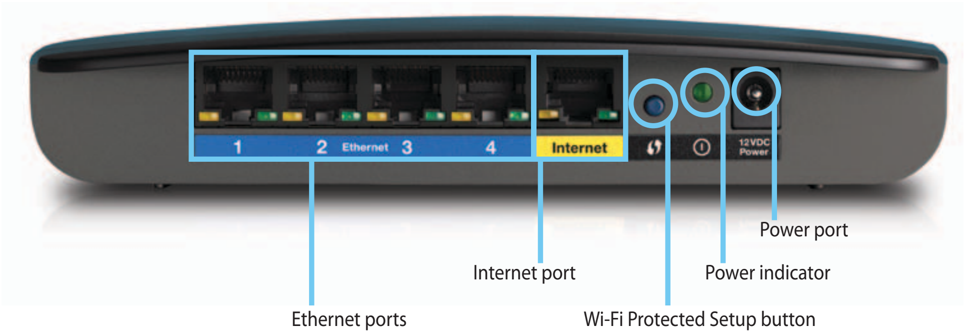
Parental controls

Limit access time and websites with parental controls.

IPv6 enabled

Supports the latest Internet protocol technology to future-proof your network.

Back view



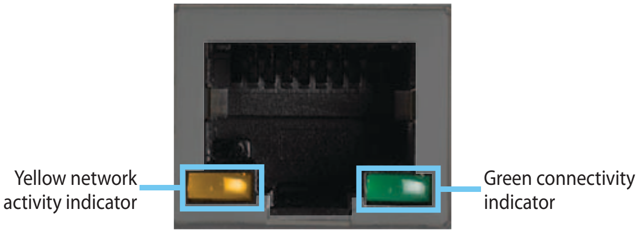
- **Ethernet ports**—Connect Ethernet cables (also called network cables) to these Gigabit Ethernet (10/100/1000) ports, color coded blue, and to wired Ethernet network devices on your network.

> **NOTE**
> For best performance, use CAT5E or higher rated cables on the Ethernet ports.

- **Internet port**—Connect an Ethernet cable (also called a network or Internet cable) to this port, color coded yellow, and to your modem.
- **Wi-Fi Protected Setup™ button**—Press this button to easily configure wireless security on Wi-Fi Protected Setup-enabled network devices. For more information, see "How to connect a network device using Wi-Fi Protected Setup" on page 16.
- **Power indicator**—Stays on steadily while power is connected and following a successful Wi-Fi Protected Setup connection. Flashes slowly during bootup, firmware upgrades, factory reset, and Wi-Fi Protected Setup. Flashes quickly when there is a Wi-Fi Protected Setup error.
- **Power port**—Connect the included AC power adapter to this port.

> **CAUTION**
> Use only the adapter that came with your router.

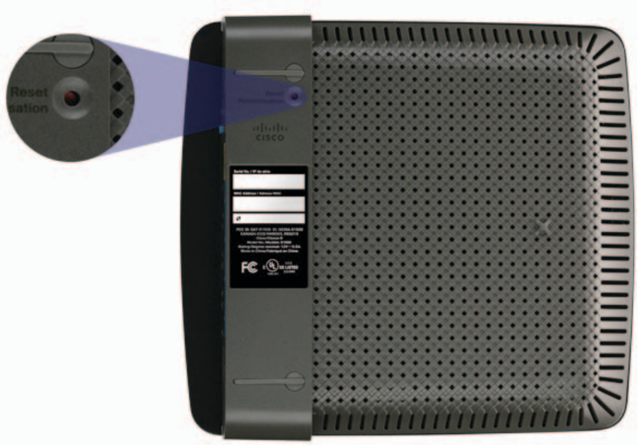
Port activity indicator


Yellow network activity indicator
Green connectivity indicator

Network or Internet port

- **Green connectivity indicator**—On Ethernet ports, turns on when a cable connects the port to another Gigabit Ethernet port. On the Internet port, turns on while connected to a modem.
- **Yellow activity indicator**—Flashes to indicate network activity over that port.

Bottom view



- **Reset button**—Press and hold this button for 15 seconds (until the port lights flash at the same time) to reset the router to its factory defaults. You can also restore the defaults using the browser-based utility. For more information, see "How to restore factory defaults" on page 53.

EA3500

Package contents

In addition to your router, your router package includes:

- Network (Ethernet) cable
- AC power adapter
- Setup CD containing router setup software and documentation

Features

Wireless-N technology

Built with leading 802.11n technology, create a powerful home wireless network optimized for video, music, and multi-player gaming. Connect your computers, Internet-ready TVs, game consoles, smartphones, and other Wi-Fi devices at blazingly fast transfer rates for an unrivaled experience.

The power of dual band

Double your network bandwidth with simultaneous dual-band N (2.4 and 5 GHz). The dual-band feature is designed to avoid interference and optimize throughput for smoother and faster HD video streaming, file transfers, and wireless gaming.

SpeedBoost

Higher quality antenna technology helps maintain high speeds across greater distances throughout your home.

Advanced security

Keep Wi-Fi freeloaders and Internet threats at bay with WPA2 encryption and SPI firewall to help keep your network protected.

Benefits of gigabit

Use the four Gigabit Ethernet (10/100/1000) ports for quick file sharing (up to 10× faster than standard Ethernet) between other Gigabit-enabled devices like computers and servers.

Built-in USB port

The USB port lets you add an external USB drive to your network and share files at home or over the Internet. You can also connect a USB printer and share it across your network.

Home theater ready

Bring the ultimate entertainment experience to your home by connecting computers, Internet-ready TVs, game consoles, media players, and more to your wireless network and the Internet. Simultaneous dual-band N and QoS traffic prioritization technology delivers maximum speed and performance so you can enjoy fast downloads, smooth video and music streaming, and reliable gaming and VoIP.

Easy to manage

Cisco Connect software helps you customize your settings and quickly add multiple devices to your network:

Separate guest network

Create a separate, password-protected network for guests.

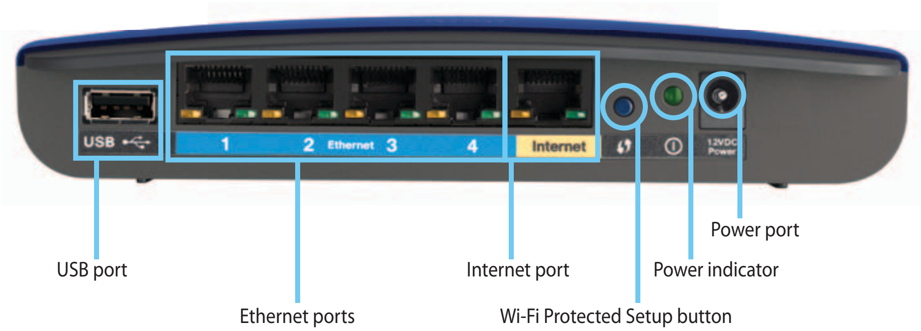
Parental controls

Limit access time and websites with parental controls.

IPv6 enabled

Supports the latest Internet protocol technology to future-proof your network.

Back view



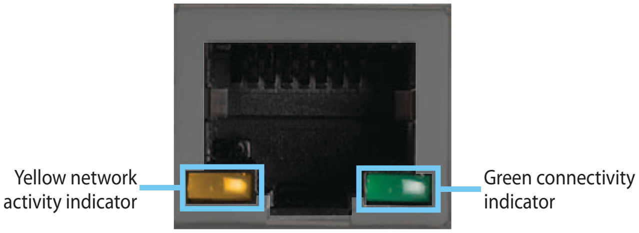
- **USB port**—To easily share disk storage with other users on your network or on the Internet, connect a USB drive to this port. For more information, see "Using an External Drive" on page 41. You can also connect a USB printer and share it across your network. For more information, see "How to connect a USB printer" on page 15.
- **Ethernet ports**—Connect Ethernet cables (also called network cables) to these Gigabit (10/100/1000) ports, color coded blue, and to wired Ethernet network devices on your network.

  NOTE
  For best performance, use CAT5E or higher rated cables on the Ethernet ports.

- **Internet port**—Connect an Ethernet cable (also called a network or Internet cable) to this port, color coded yellow, and to your modem.
- **Wi-Fi Protected Setup™ button**—Press this button to easily configure wireless security on Wi-Fi Protected Setup-enabled network devices. For more information, see "How to connect a network device using Wi-Fi Protected Setup" on page 16.
- **Power indicator**—Stays on steadily while power is connected and following a Wi-Fi Protected Setup connection. Flashes slowly during bootup, firmware upgrades, factory reset, and Wi-Fi Protected Setup. Flashes quickly when there is a Wi-Fi Protected Setup error.
- **Power port**—Connect the included AC power adapter to this port.

  CAUTION
  Use only the adapter that came with your router.

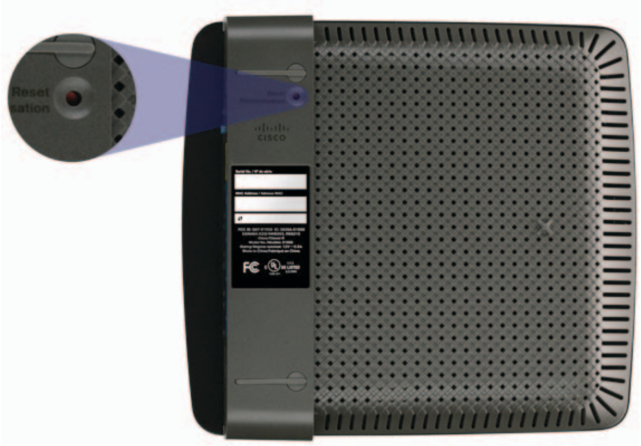
Port activity indicators


Yellow network activity indicator
Green connectivity indicator

Network or Internet port

- **Green connectivity indicator**—On Ethernet ports, turns on when a cable connects the port to another Gigabit Ethernet port. On the Internet port, turns on while connected to a modem.
- **Yellow activity indicator**—Flashes to indicate network activity over that port.

Bottom view



- **Reset button**—Press and hold this button for 15 seconds (until the port lights flash at the same time) to reset the router to its factory defaults. You can also restore the defaults using the browser-based utility. For more information, see "How to restore factory defaults" on page 53.

EA4500

Package contents

In addition to your router, your router package includes:

- Network (Ethernet) cable
- AC power adapter
- Setup CD containing router setup software and documentation

Features

Wireless-N technology

Built with leading 802.11n wireless technology, your router offers maximum speed and range to create an ultra-powerful network designed for home theater performance. Connect your computers, Internet-ready TVs, game consoles, smartphones and other Wi-Fi devices at blazingly fast transfer rates for an unrivaled experience.

The power of dual band

Double your network bandwidth with simultaneous dual-band N (2.4 and 5 GHz). The dual-band feature is designed to avoid interference and optimize throughput for smoother and faster HD video streaming, file transfers, and wireless gaming.

SpeedBoost

Higher quality antenna technology helps maintain high speeds across greater distances throughout your home.

Advanced security

Keep Wi-Fi freeloaders and Internet threats at bay with WPA2 encryption and SPI firewall to help keep your network protected.

Benefits of gigabit

Use the four Gigabit Ethernet (10/100/1000) ports for quick file sharing (up to 10× faster than standard Ethernet) between other Gigabit-enabled devices like computers and servers.

Built-in USB port and DLNA media server

The USB storage port lets you add an external USB drive to your network and share files at home or over the Internet. It also features a built-in DLNA media server for seamless streaming of your video and media files to an Xbox 360, PS3, or other DLNA-compatible device. You can also connect a USB printer and share it across your network.

Home theater ready

Bring the ultimate entertainment experience to your home by connecting computers, Internet-ready TVs, game consoles, media players, and more to your wireless network and the Internet. Simultaneous dual-band N and QoS traffic prioritization technology delivers maximum speed and performance so you can enjoy fast downloads, smooth video and music streaming, and reliable gaming and VoIP.

Quick to install

Cisco Connect software helps you easily set up your router.

IPv6 enabled

Supports the latest Internet protocol technology to future-proof your network.

Easy to manage

Cisco Connect software helps you customize your settings and quickly add multiple devices to your network:

Separate guest network

Create a separate, password-protected network for guests.

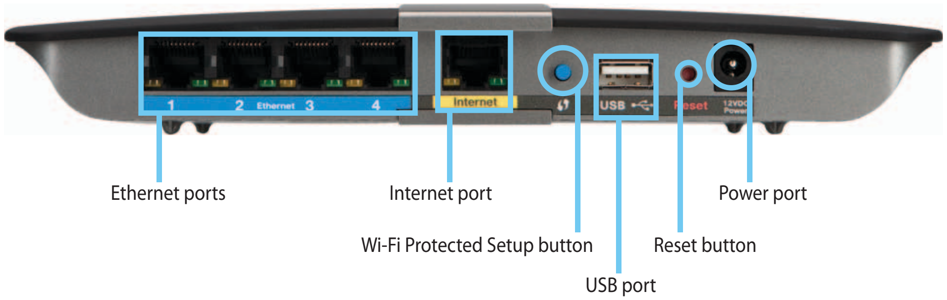
Parental controls

Limit access time and websites with parental controls.

Top view

- **Indicator light**—Stays on steadily while power is connected and following a successful Wi-Fi Protected Setup connection. Pulses slowly during bootup, firmware upgrades, factory reset, and Wi-Fi Protected Setup. Flashes quickly when there is a Wi-Fi Protected Setup error.

Back view



- **Ethernet ports**—Connect Ethernet cables (also called network cables) to these Gigabit (10/100/1000) ports, color coded blue, and to wired Ethernet network devices on your network.

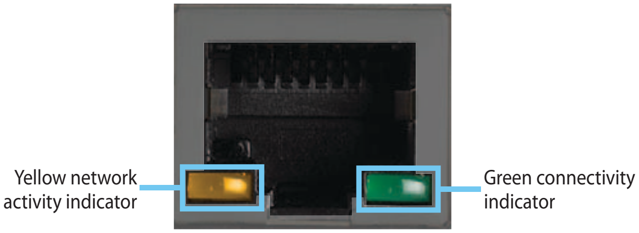
> **NOTE**
> For best performance, use CAT5E or higher rated cables on the Ethernet ports.

- **Internet port**—Connect an Ethernet cable (also called a network or Internet cable) to this port, color coded yellow, and to your modem.
- **Wi-Fi Protected Setup™ button**—Press this button to add Wi-Fi Protected Setup-enabled devices automatically. For more information, see “How to connect a network device using Wi-Fi Protected Setup” on page 16.
- **USB port**—To easily share disk storage with other users on your network or on the Internet, connect a USB drive to this port. For more information, see “Using an External Drive” on page 41. You can also connect a USB printer and share it across your network. For more information, see “How to connect a USB printer” on page 15.

- **Reset button**—Press and hold this button for 15 seconds (until the port lights flash at the same time) to reset the router to its factory defaults. You can also restore the defaults using the browser-based utility. For more information, see "How to restore factory defaults" on page 53.
- **Power port**—Connect the included AC power adapter to this port.

> **CAUTION**
> Use only the adapter that came with your router.

Port activity indicators


Yellow network activity indicator
Green connectivity indicator

Network or Internet port

- **Green connectivity indicator**—On Ethernet ports, turns on when a cable connects the port to another Gigabit Ethernet port. On the Internet port, turns on while connected to a modem.
- **Yellow network activity indicator**—Flashes to indicate network activity over that port.

Setting Up: Basics

How to create a home network

What is a network?

A network is any group of devices that can communicate with each other. A home network can also include Internet access, which requires a router like this one.

A typical home network may include multiple computers, a printer, a modem, and a router. A large home network may also have a switch, additional routers, access points, and many Internet-capable media devices such as TVs, game consoles, and web cameras.

- **Modem**—Connects a computer or a router to your ISP (Internet Service Provider). Your ISP may have provided one. The modem is a device that connects to a phone jack or your cable TV outlet.
- **Router**—Connects your wireless and wired network devices to each other and to the modem (and to your ISP).
- **Switch**—Allows you to connect several wired network devices to your home network. Your router has a built-in network switch (the Ethernet ports). If you have more wired network devices than available Ethernet ports on your router, you will need an additional switch to consolidate the wired connections.

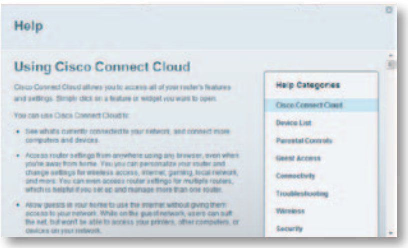
How to set up a home network

1. Purchase the proper equipment. For a network that includes Internet access, you'll need:
   - Computers with an Ethernet port or wireless networking capabilities
   - A modem for connecting to your ISP (typically supplied by your ISP)
   - A router to connect your computers with each other and to the modem
   - Internet service to your home, provided by an ISP (Internet Service Provider)
2. Make sure that your modem is working. Your ISP can help you set up your modem and verify that it's working correctly.
3. Set up your router. See "How to install your router" on page 10.
4. To connect a computer or other network device to the network, see "How to connect a computer to your network" on page 15 and "How to connect other devices" on page 16.

Where to find more help

In addition to this User Guide, you can find help at these locations:

- **Linksys.com/support** (documentation, downloads, FAQs, technical support, live chat, forums)
- Cisco Connect Cloud help (connect to **Cisco Connect Cloud**, then click **Help** at the top of the screen)



Help

Using Cisco Connect Cloud

Cisco Connect Cloud allows you to access all of your router's features and settings. Simple click on a feature or widget you want to open.

You can use Cisco Connect Cloud to:

- See what's currently connected to your network, and connect more computers and devices.
- Access router settings from anywhere using any browser, even when you're away from home. You you can personalize your router and change settings for wireless access, internet, gaming, local network, and more. You can even access router settings for multiple routers, which is helpful if you set up and manage more than one router.
- Allow guests in your home to use the internet without giving them access to your network. While on the guest network, users can surf the net, but won't be able to access your printers, other computers, or devices on your network.

How to install your router

The easiest and fastest way to install your router is to run the Setup software on the CD that came with your router or download it from the router's support site at **Linksys.com/support**. Setup shows you how to connect your router to your home network, step by step.

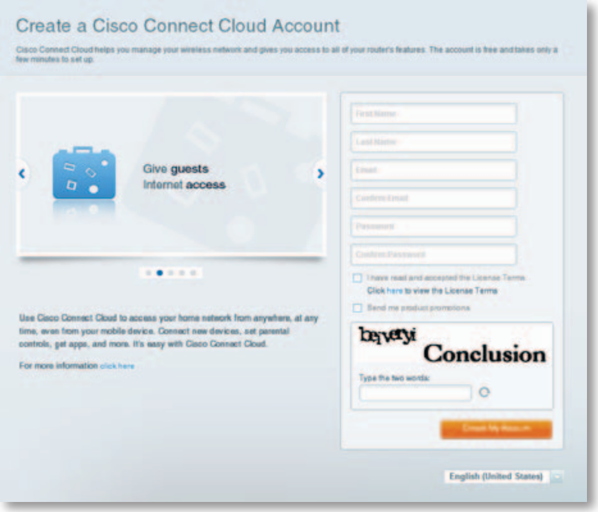
> **NOTE:**
> If you lose your setup CD, you can download the software from **Linksys.com/support**.

To install your router:

1. Insert the CD into your CD or DVD drive. Setup opens. If your Setup CD is not available, download the Setup program from **Linksys.com/support**.
2. Click **Set up your Linksys Router**.

   If you do not see this:

   - For Windows, click **Start**, **Computer**, then double-click the **CD** drive and the **Setup** icon.
   - For Mac, double-click the **CD** icon on your desktop, then double-click the **Setup** icon.
3. Follow the on-screen instructions to complete your router setup.



Create a Cisco Connect Cloud Account

Cisco Connect Cloud helps you manage your wireless network and gives you access to all of your router's features. The account is free and takes only a few minutes to set up.

Use Cisco Connect Cloud to access your home network from anywhere, at any time, even from your mobile device. Connect new devices, set parental controls, get apps, and more. It's easy with Cisco Connect Cloud.

For more information click here

□ I have read and accepted the License Terms
Click here to view the License Terms

□ Send me product promotions

As part of the router setup process, you will be sent a verification e-mail. From your home network, click the link in the e-mail to associate your router with the Cisco Connect Cloud account. Make sure that the link opens in a supported web browser, such as Internet Explorer 8 or higher, Firefox 8 or higher, Google Chrome 10 or higher, and Safari 5 (for Mac) or higher.

If you cannot click the link while behind your new Linksys router, log into Cisco Connect Cloud while behind the router and add your router there. For more information, see "How to associate a router with your Cisco Connect Cloud account" on page 23.

> **TIP:**
> Print this page, then record your router and account settings in the table below as a reference. Store your notes in a safe place. Setup also saves your setup information as a file to your computer desktop.

Network Name (SSID)	
Network Password	
Router Password	
Guest Network Name	
Guest Network Password	
Cisco Connect Cloud Username	
Cisco Connect Cloud Password	

How to configure your router

You can change router settings to make your network more secure or to work better with a device or game. Being able to adjust the settings while you're away from home can help make router administration easier. You can configure your router from anywhere in the world by using Cisco Connect Cloud, but you can also configure your router directly from your home network.

Cisco Connect Cloud may be available for your mobile device, as well. See your device's app store for information.

Use Cisco Connect Cloud to easily manage your router's settings, such as:

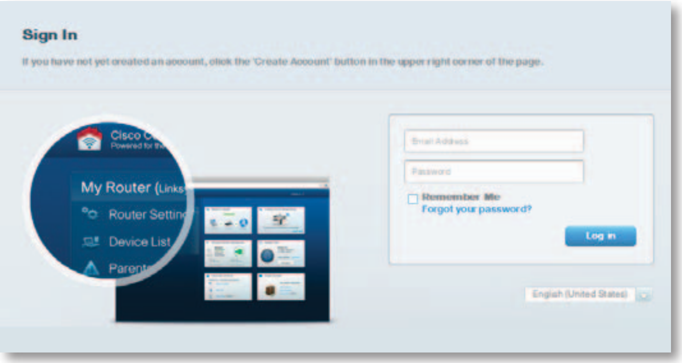
- Change your router's name and password
- Set up guest access
- Configure parental controls
- Connect devices to your network
- Test your Internet connection speed

Your Cisco Connect Cloud account can also be used to manage multiple Linksys routers. For more information, see "How to associate a router with your Cisco Connect Cloud account" on page 23.

How to connect to Cisco Connect Cloud

To connect to Cisco Connect Cloud:

1. Open your computer's web browser.
2. Go to **www.ciscoconnectcloud.com** and log into your account.



Sign In

If you have not yet created an account, click the 'Create Account' button in the upper right corner of the page.

If you can't remember your password, click **Forgot your password?** and follow the on-screen instructions to recover it.

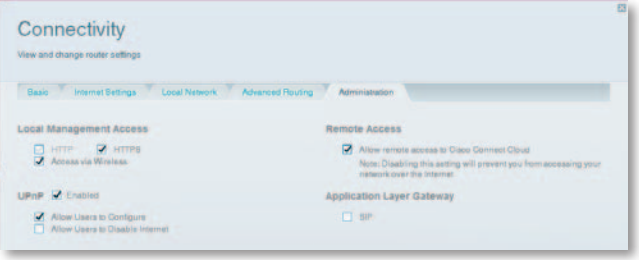
How to disable remote access

If you want to configure your router only while you are on your home network, you should disable remote access.

To disable remote access:

1. Log into Cisco Connect Cloud.
2. Under **Router Settings**, click **Connectivity**.

3. Click the **Administration** tab, then deselect **Allow remote access to Cisco Connect Cloud**.



Connectivity

View and change router settings

Local Management Access

☐ HTTP ☑ HTTPS
☑ Access via Wireless

UPnP ☑ Enabled

☑ Allow Users to Configure
☐ Allow Users to Disable Internet

Remote Access

☑ Allow remote access to Cisco Connect Cloud

Note: Disabling this setting will prevent you from accessing your network over the Internet.

Application Layer Gateway

☐ SIP

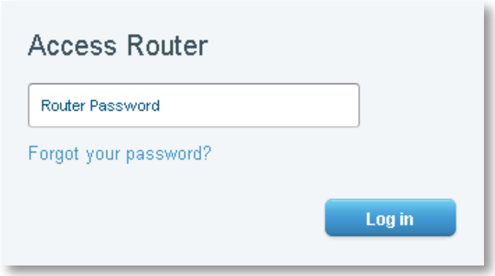
4. Click **OK**.

How to connect directly to your router

You can configure your router by directly accessing it on your home network instead of through the Internet-based Cisco Connect Cloud.

To connect to your router while you are on your home network:

1. Disconnect the cable from the yellow **Internet** port on the back of your router. If you do not have Internet access, this step is not necessary.
2. Open your computer's web browser.
3. Go to **www.ciscoconnectcloud.com** and log into your router using the router password you created when you installed your router. (When there is no Internet connection, this address re-routes directly to your router.)



Access Router

4. After you finish configuring your router, reconnect the cable to the router's **Internet** port.

How to improve your wireless connection speed

Follow these tips to improve your network's wireless connection speed:

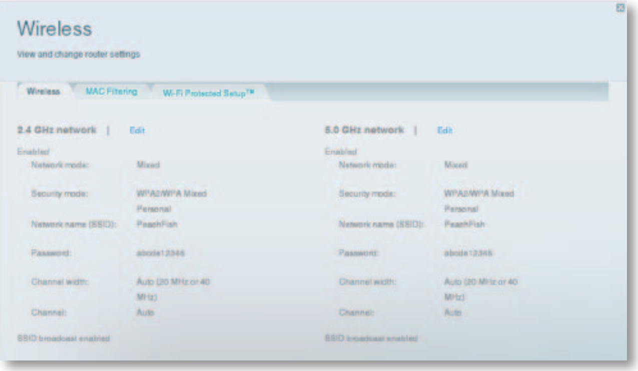
- Make sure that your router is in a good location:
  - For the widest coverage area, install your router near the center of your home, and near the ceiling, if possible.
  - Avoid placing the router on or near metal objects (such as file cabinets and metal furniture), reflective surfaces (such as glass or mirrors), or masonry walls.
  - Any obstruction can weaken the wireless signal (even non-metallic objects), so the fewer obstructions between the router and the wireless device, the better.
  - Place the router in a location away from other electronics, motors, and fluorescent lighting.
  - Many environmental variables can affect the router's performance, so if your wireless signal is weak, place the router in several locations and test the signal strength to determine the ideal position.
- If possible, upgrade wireless network interfaces (such as wireless network cards in computers) from older wireless standards to 802.11n. If a wirelessly networked device uses an older standard, the performance of the entire wireless network may be slower.
- If your router is a dual-band router, split your network traffic so the high-bandwidth traffic uses the 5 GHz band. For more information, see "How to get the most out of your dual-band router" on page 24.

How to change your network's name and password

You can change the name (SSID) and password of your network, but if you do so, all wireless devices connected to your router will lose their Internet connection until you reconnect them using the new network name and password.

To change your router's name and password:

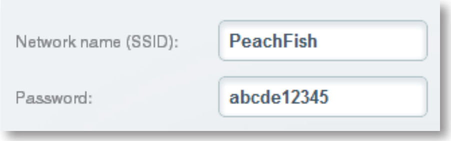
1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Router Settings**, click **Wireless**.



2.4 GHz network | Edit
Enabled
Network mode: Mixed
Security mode: WPA2/WPA Mixed Personal
Network name (SSID): PeachFish
Password: abcde12345
Channel width: Auto (20 MHz or 40 MHz)
Channel: Auto
SSID broadcast enabled

5.0 GHz network | Edit
Enabled
Network mode: Mixed
Security mode: WPA2/WPA Mixed Personal
Network name (SSID): PeachFish
Password: abcde12345
Channel width: Auto (20 MHz or 40 MHz)
Channel: Auto
SSID broadcast enabled

3. Click the **Wireless** tab, then click **Edit**.



Network name (SSID): PeachFish

Password: abcde12345

- To change the network name, type a new name in the **Network name (SSID)** box.
- To change the network password, type a new password in the **Password** box.

4. Click **OK** to apply your changes.

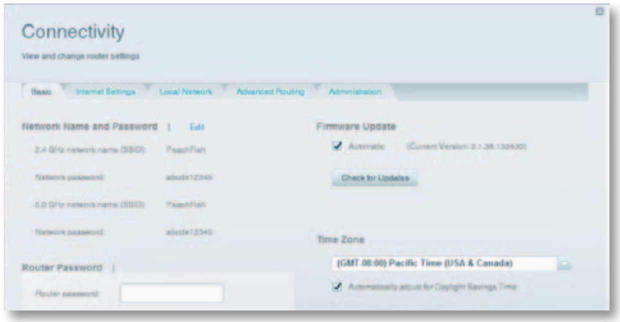
> **TIP**
> If you have a dual-band router, each band (2.4 GHz and the 5 GHz) can have a separate network name and password.

How to change your router's local access password

Your router's local access password was set when you ran the router's setup software, but you can change it at any time. You need the router password to change router settings when you don't have an Internet connection. When you do have an Internet connection, log into your Cisco Connect Cloud account by following the directions under "How to connect to Cisco Connect Cloud" on page 11.

To change your router's local access password

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Click **Connectivity** under *Router Settings*.
3. Click the **Basic** tab.
4. Under **Router Password**, type the new password, then click **OK**.



Network Name and Password | Edit
2.4 GHz network name (SSID): PeachFish
Network password: abcde12345
5.0 GHz network name (SSID): PeachFish
Network password: abcde12345

Router Password |
Router password:

Firmware Update
☑ Automatic (Current Version: 2.1.38.132430)

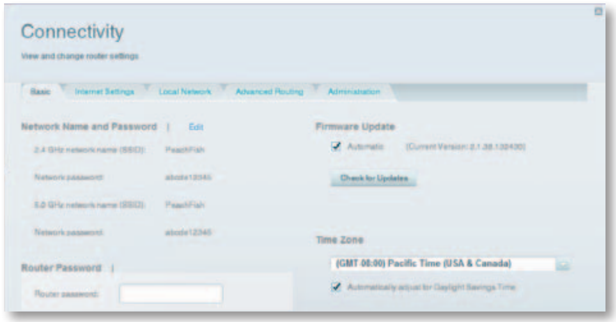
Time Zone
(GMT-08:00) Pacific Time (USA & Canada)
☑ Automatically adjust for Daylight Savings Time

How to change your router's time zone

Your router's time zone should be set to your local time zone.

To set your router's time zone:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Click **Connectivity** under *Router Settings*.
3. Click the **Basic** tab, then select your time zone in the **Time Zone** drop-down list and click **OK**.



Connectivity

View and change router settings

Network Name and Password

2.4 GHz network name (SSID): PeachFish

Network password: abcde12345

5.0 GHz network name (SSID): PeachFish

Network password: abcde12345

Router Password

Router password:

Firmware Update

☑ Automatic (Current Version: 2.1.38.132430)

Time Zone

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

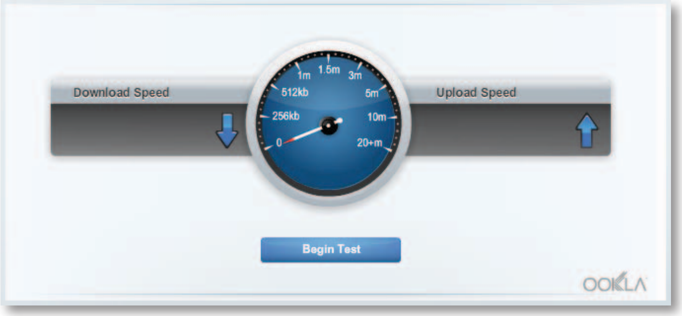
☑ Automatically adjust for Daylight Savings Time

How to test your Internet connection speed

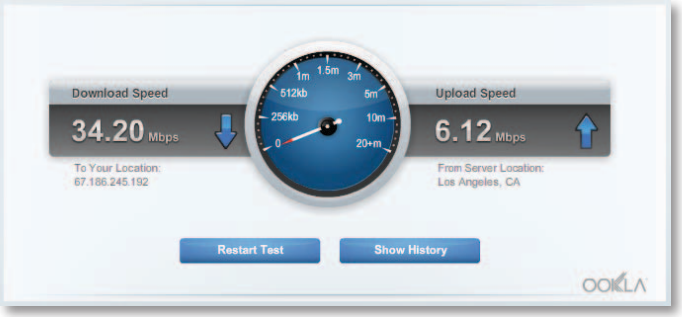
NOTE
To run the speed test, you must be accessing the Internet by using the router you are testing. You cannot run the speed test remotely.

To test your Internet connection speed:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Click **Speed Test** under **Apps**. The *Speed Test* screen opens.



3. Click **Begin Test**. The test measures your download and upload speeds.



Download Speed 34.20 Mbps

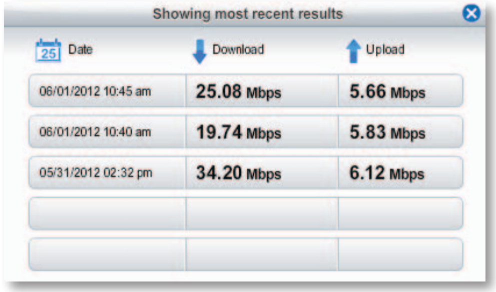
To Your Location: 67.186.245.192

Upload Speed 6.12 Mbps

From Server Location: Los Angeles, CA

NOTE
Internet connection speeds are determined by a variety of factors, including ISP account type, local and worldwide Internet traffic, and number of devices in your home that are sharing the Internet connection.

4. Click **Restart Test** to run it again, and click **Show History** to display the results of past tests.



Showing most recent results

Date	Download	Upload
06/01/2012 10:45 am	25.08 Mbps	5.66 Mbps
06/01/2012 10:40 am	19.74 Mbps	5.83 Mbps
05/31/2012 02:32 pm	34.20 Mbps	6.12 Mbps

How to connect devices to your network

Your Linksys router is the nerve center of your home network. Your router safely opens the Internet to your network, and all of your computers and network devices rely on your router to pass files, media, and network commands in an organized, error-free way. Whether connected wirelessly or with cables, each part of your network needs the router in order to work reliably with the other parts of your network.

How to connect a computer to your network

To connect a computer to your network:

1. At the computer you want to connect, enter your network's connection information into your wireless manager.
2. After that computer connects to your network, log into Cisco Connect Cloud, then click **Device List** to confirm that your router recognizes the new computer. You can use the Device List to monitor all network-attached devices.

How to connect a USB printer

When you install a printer that requires a cable, you can:

- Follow the printer's instructions for setting it up, then follow your computer's operating system instructions to share the printer with your network.

  - OR -

- If your router is a Linksys EA3500 or EA4500, you can connect a USB printer to the router's USB port to make the printer available to any networked computer.

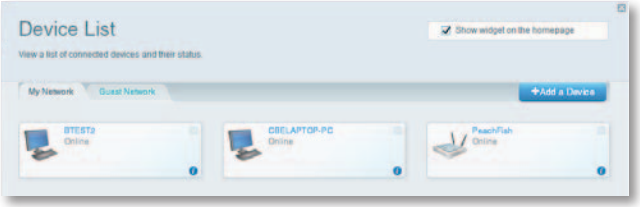
When you set up a wireless printer, you need to make sure that:

- Your printer has been completely set up except for being connected to the network.
- Your printer supports the WPA/WPA2 wireless encryption standard.
- If your wireless printer supports WPS (Wi-Fi Protected Setup), you should use WPS to connect it to your network. See "How to connect a network device using Wi-Fi Protected Setup" on page 16.

To connect a USB printer to your network through the router's USB port:

For EA3500 EA4500

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Click Device List, then click **Add a Device**.

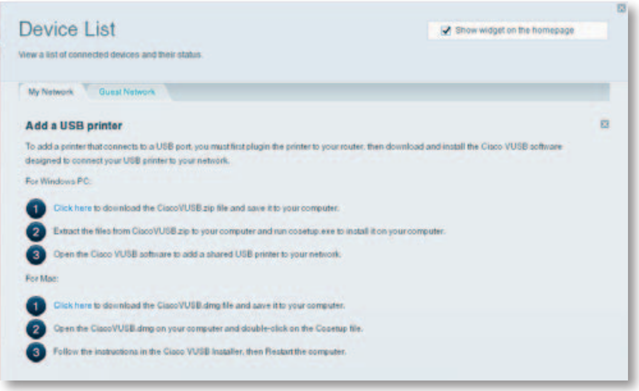


Device List

View a list of connected devices and their status.

☑ Show widget on the homepage

3. Under *Select the type of device to add to your network*, click **USB Printer**. The *Add a USB printer* screen opens.



Device List

☑ Show widget on the homepage

View a list of connected devices and their status

Add a USB printer

To add a printer that connects to a USB port, you must first plugin the printer to your router, then download and install the Cisco VUSB software designed to connect your USB printer to your network.

For Windows PC:

1. Click here to download the CiscoVUSB.zip file and save it to your computer.
2. Extract the files from CiscoVUSB.zip to your computer and run cosetup.exe to install it on your computer.
3. Open the Cisco VUSB software to add a shared USB printer to your network.

For Mac:

1. Click here to download the CiscoVUSB.dmg file and save it to your computer.
2. Open the CiscoVUSB.dmg on your computer and double-click on the Cosetup file.
3. Follow the instructions in the Cisco VUSB Installer, then Restart the computer.

4. Follow the on-screen instructions for downloading and installing the VUSB (virtual USB) software for your computer.

To connect a wireless printer to your network:

1. Follow the printer's instructions to connect it to your network. Use the connection information available in Cisco Connect Cloud or saved to your computer desktop.
2. After that printer connects to your network, log into Cisco Connect Cloud, then click **Device List** to confirm that your router recognizes the new printer.

How to connect other devices

Many other types of wireless network devices can connect to your home network, including:

- Game consoles
- Internet-capable TVs and media players
- Digital music players
- Smart phones

Because of the wide variety of devices and methods of connecting, you must manually enter network information into the devices for a successful network connection.

TIP

For more instructions on connecting a game console to your network, see also:

- "How to optimize your router for gaming and voice" on page 32
- "How to set up port forwarding" on page 48
- "How to set up port range triggering for online gaming" on page 50

How to manually connect a network device

To manually connect a device to your network:

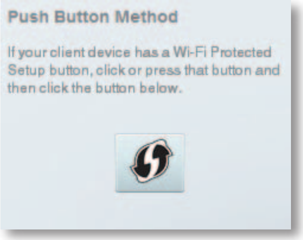
1. Follow the device's instructions to connect it to your network. Use the connection information available in Cisco Connect Cloud or saved to your computer desktop.
2. After the device connects to your network, log into Cisco Connect Cloud, then click **Device List** to confirm that your router recognizes the new device.

How to connect a network device using Wi-Fi Protected Setup

To connect a device using Wi-Fi Protected Setup™:

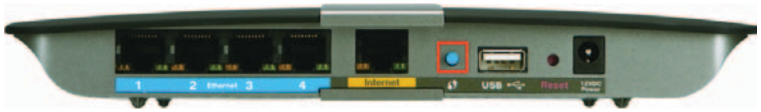
1. Plug in and turn on the network device. If the device does not support Wi-Fi Protected Setup, follow its instructions for a standard network installation.
2. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
3. Under **Wireless**, click the **Wi-Fi Protected Setup** tab.
4. Use one of the following methods to complete the setup:

- If the device has a Wi-Fi Protected Setup button, press that button, then click the **Wi-Fi Protected Setup** button in Cisco Connect Cloud or press the button on the back of your router.

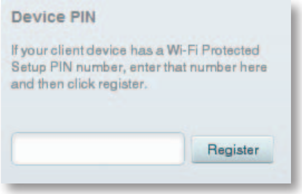


Push Button Method

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



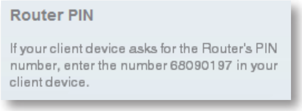
- If the device has a Wi-Fi Protected Setup PIN, type that number into the **Device PIN** box in Cisco Connect Cloud, then click **Register**.



Device PIN

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

- If the device's own setup asks for the router's Wi-Fi Protected Setup PIN, enter the number that appears under *Router PIN* in Cisco Connect Cloud.



Router PIN

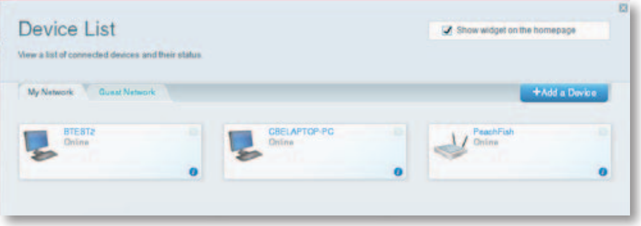
If your client device asks for the Router's PIN number, enter the number 68090197 in your client device.

How to view device details

You can use Cisco Connect Cloud to view any network device's network infomation.

To view network device details:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Apps**, click **Device List**. The *Device List* screen opens.

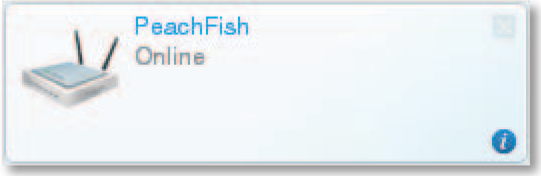


Device List

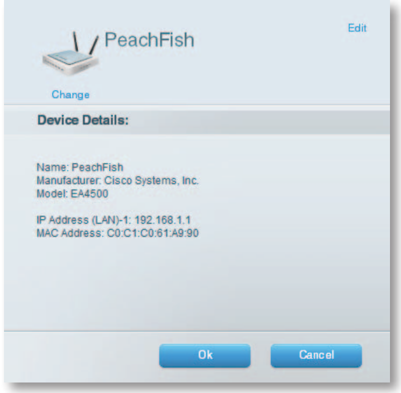
View a list of connected devices and their status

☑ Show widget on the homepage

3. Click the ***i*** in the lower-right corner of the device.



Information about the device appears on the screen.



Device Details:

Name: PeachFish
Manufacturer: Cisco Systems, Inc.
Model: EA4500

IP Address (LAN)-1: 192.168.1.1
MAC Address: C0:C1:C0:61:A9:90

4. Click **OK**.

How to set up parental controls

With your router, you can use parental controls to:

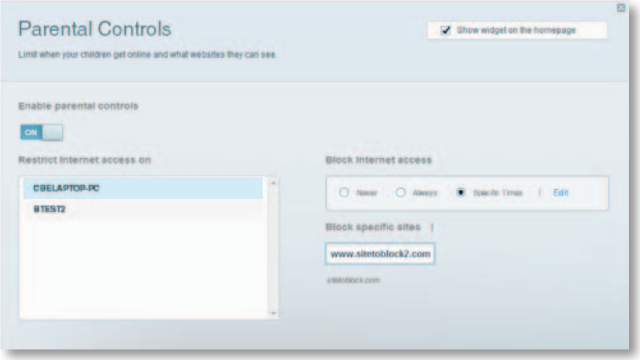
- Set the times that Internet access is allowed.
- Block websites that you specify or based on their content.
- Set the above restrictions for specific computers.

> **TIP**
> When someone tries to open a blocked website, a Cisco Connect login page appears. To view the blocked content, you must log into your Cisco Connect Cloud account and change the parental control restrictions.

How to set parental controls

To set parental controls:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Apps**, click **Parental Controls**. The *Parental Controls* screen opens.



Limit when your children get online and what websites they can see.

☑ Show widget on the homepage

Enable parental controls: ON

Restrict Internet access on:
CBELAPTOP-PC
BTEST2

Block Internet access: ○ Never ○ Always ● Specific Times | Edit

Block specific sites |

www.sitetoblock2.com

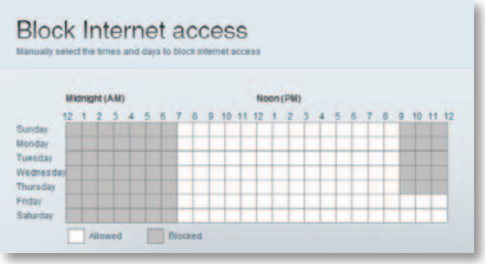
sitetoblock.com

3. To turn on parental controls, click the **Enable parental controls** button so that **ON** is displayed.

> **TIP**
> It's not necessary to set parental controls over each computer on your home network. You can set the controls on only those computers that children can access.

4. To select a computer to apply parental controls to, click the name of the computer in the **Restrict Internet access on** list.
5. To block Internet access on the selected computer(s), under **Block Internet access**:
   - Click **Never** to allow Internet access.
   - Click **Always** to always block Internet access.
   - Click **Specific Times** to set the times when Internet access is allowed.

- Click **Edit** to change the Internet access schedule. You can click and drag to select or deselect a block of time.



Block Internet access

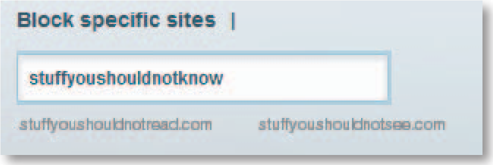
Manually select the times and days to block internet access

	Midnight (AM)												Noon (PM)											
	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sunday	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	▨	▨	▨
Monday	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	▨	▨	▨
Tuesday	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	▨	▨	▨
Wednesday	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	▨	▨	▨
Thursday	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	▨	▨	▨
Friday	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Saturday	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

□ Allowed ▨ Blocked

6. To block specific websites:

   a. Under **Block specific sites**, click **Add**.



Block specific sites |

stuffyoushouldnotknow

stuffyoushouldnotread.com

stuffyoushouldnotsee.com

   b. Type the web address (URL) of the website to block, then click **OK**. You can block up to ten websites.

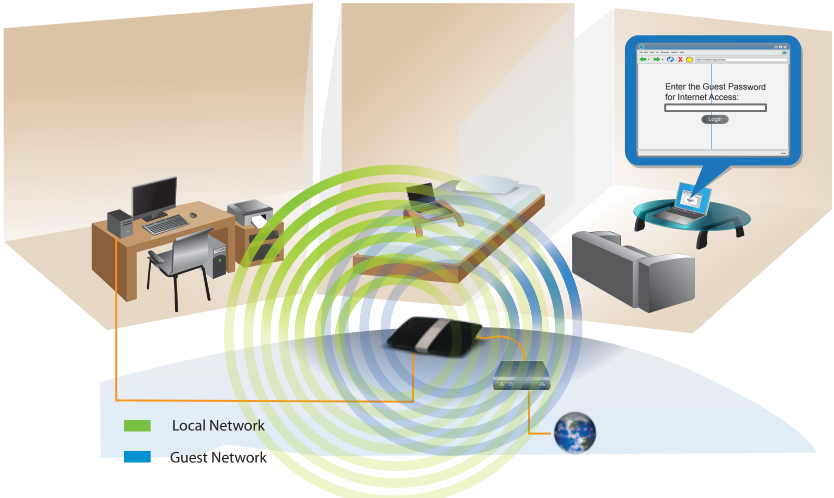
TIP

It's easier to copy and paste a web address than it is to type it in. Copy the address from your browser's web address box, then paste it into an available box in the *Block Specific Sites* screen of Cisco Connect Cloud.

7. Click **OK** to apply your changes.

How to configure your guest network

You can use your router's guest network to provide your guests with access to the Internet, while restricting their access to other resources on your local network. To prevent unauthorized users from using your Internet access, your guest network requires that a password be entered for Internet access. The guest network is enabled by default.

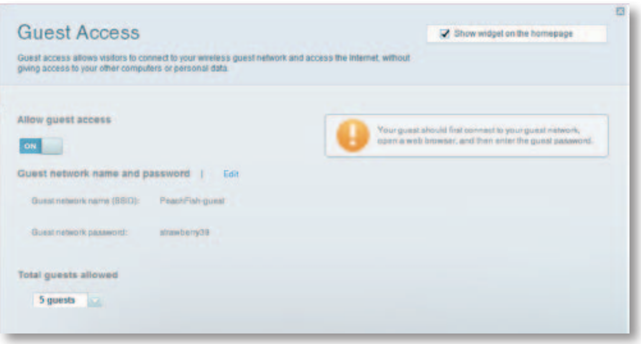

http://mynetwork/guestlogin
Enter the Guest Password for Internet Access:
Login
Local Network
Guest Network

Local Access and Guest Access Diagram

Your wireless network's guest network and password were set when you ran the router's setup software, but you can change them at any time.

To set up guest access to your network:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Apps**, click **Guest Access**. Your guest network, which was set up during your router installation, is displayed.



Guest Access

☑ Show widget on the homepage

Guest access allows visitors to connect to your wireless guest network and access the Internet, without giving access to your other computers or personal data.

Allow guest access

ON

Your guest should first connect to your guest network, open a web browser, and then enter the guest password.

Guest network name and password | Edit

Guest network name (SSID): PeachFish-guest

Guest network password: strawberry39

Total guests allowed

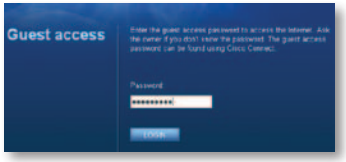
5 guests

- To turn guest access on or off, click the **Allow guest access** button.
- The guest network name is based on your 2.4 GHz network name and is automatically generated.
- To change the guest network password, click in the box next to **Guest network password**, then type the new password.
- To change the number of simultaneous guest network users you want to allow, click the drop-down box under **Total guests allowed**, then click the number that you want.

TIP
To keep your guest network secure, click **Change** to change the guest password when the guest no longer needs access to the account.

3. Click **OK** to apply your changes.

TIP
The first time your guest tries to access the Internet through a web browser, they will see the *Guest access* screen. To continue, they must enter the password you provided in the **Password** field, then click **LOGIN**.



Guest access

Enter the guest access password to access the Internet. Ask the owner if you don't know the password. The guest access password can be found using Cisco Connect.

Password

●●●●●●●●●●

LOGIN

How to back up your router configuration

When you are done setting up your router, you should back up its settings so that you can restore them later, if necessary. For instructions, see "How to back up and restore your router configuration" on page 52.

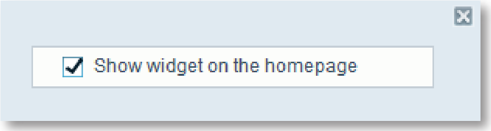
How to customize Cisco Connect Cloud

You can customize your Cisco Connect Cloud home page by adding or removing *widgets*. Widgets are miniature versions of menus that let you change basic settings or check the status of your network.

Using widgets

To add a widget:

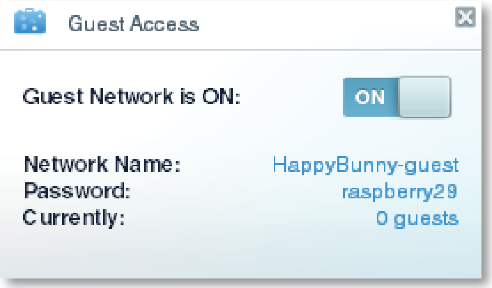
1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Open a menu, then select **Show widget on the homepage** in the upper-right corner.



☑ Show widget on the homepage

To remove a widget:

1. On the home page, click the × in the upper-right corner of the widget you want to remove.



Guest Access

Guest Network is ON: ON

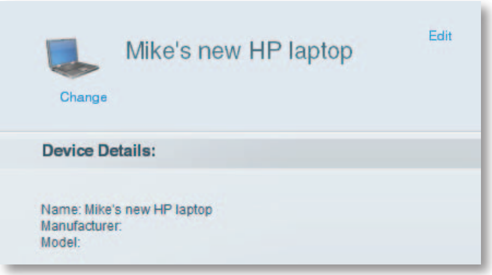
Network Name: HappyBunny-guest
Password: raspberry29
Currently: 0 guests

Customizing the Device List

You can change the icon and text description of each device on your network.

To change the device appearance:

1. In the Device List, click the device you want to change the appearance for. The device's information screen opens.



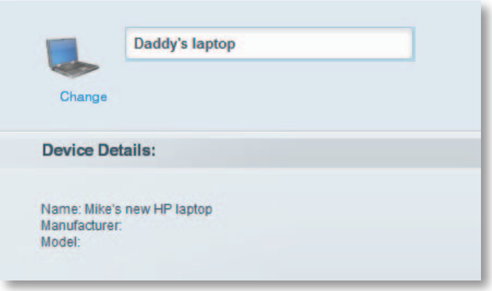
Mike's new HP laptop Edit

Change

Device Details:

Name: Mike's new HP laptop
Manufacturer:
Model:

2. To change the description, click **Edit**, type the new name, then click **OK**.



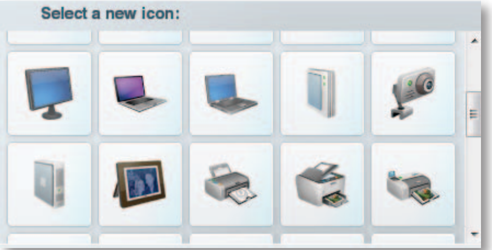
Daddy's laptop

Change

Device Details:

Name: Mike's new HP laptop
Manufacturer:
Model:

3. To change the icon, click **Change**, click a new icon, then click **OK**.



Select a new icon:

Setting Up: Advanced

How to manually set up your router

Although running your router's setup software is the easiest way to set up and maintain your router, advanced users may want to manually configure their router. Be careful when changing settings using this method.

To manually set up your router:

1. Connect your router's power adapter to a power outlet.
2. Connect an Ethernet cable to the computer and to an available numbered **Ethernet** (blue) port on the back of your router.
3. Disconnect the cable from the router's **Internet** port.
4. Open a web browser on the computer, then go to **www.ciscoconnectcloud.com**. (When there is no Internet connection, this address re-routes directly to your router.)
5. Enter **admin** as the user name, then enter the default password (**admin**). The main menu opens.
6. After you finish changing settings, click **Save** and close the browser window.

TIP
For descriptions of the settings, click **Help** at the top of the screen.

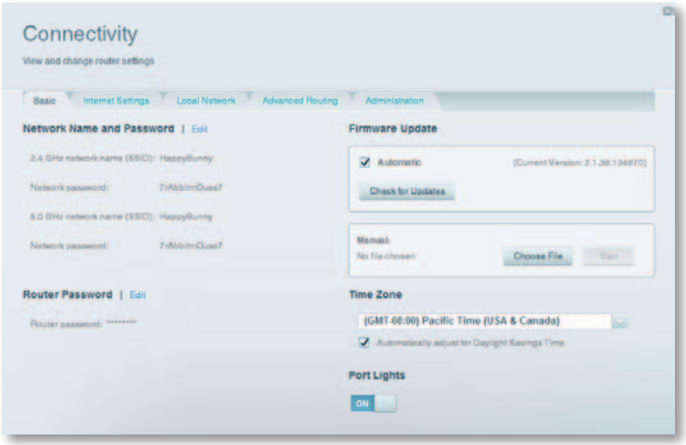
How to manually set up your Internet connection

Running Setup configures your router's Internet connection. However, for some *ISPs* (Internet Service Providers), especially those outside of the United States, you may need to manually configure your router's Internet connection.

How to configure basic Internet connection settings

To manually configure your router's Internet connection:

1. Use an Ethernet cable to connect an Ethernet port on your router to the Ethernet port on your computer.
2. Disconnect the cable from the router's **Internet** port.
3. Open a web browser on the computer, then go to **www.ciscoconnectcloud.com**. (When there is no Internet connection, this address re-routes directly to your router.)
4. Log into your router using the default router password, **admin**.
5. Under *Router Settings*, click **Connectivity**. The *Connectivity* page opens to the **Basic** tab.



Network Name and Password | Edit

2.4 GHz network name (SSID): HappyBunny
Network password: 7rAbbitmOusa7
5.0 GHz network name (SSID): HappyBunny
Network password: 7rAbbitmOusa7

Router Password | Edit

Router password: ********

Firmware Update

☑ Automatic (Current Version: 2.1.38.134870)

Manual:
No file chosen

Time Zone

(GMT-08:00) Pacific Time (USA & Canada)
☑ Automatically adjust for Daylight Savings Time

Port Lights

ON

6. Next to *Type of Internet Connection*, click **Edit**.

7. Select your ISP's Internet connection type from the drop-down list. Complete the *Optional Settings* only if required by your ISP.

> **TIP**
> For field descriptions, click **Help** at the top of the screen.

8. Click **OK**.

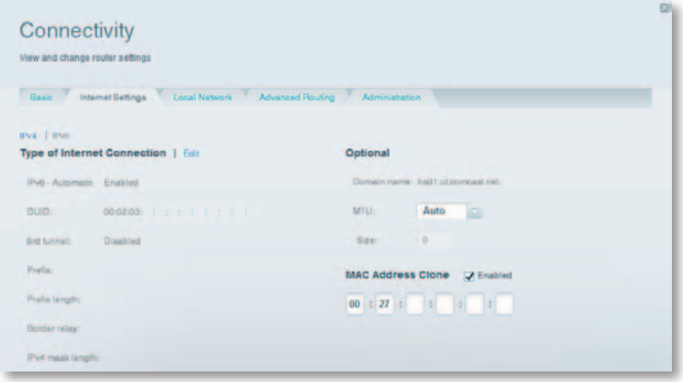
IPv6 Internet connection settings

IPv6 is a new IP protocol that uses simplified packet headers and requires IPSec. It also has improved support for mobile IP and computing devices.

> **NOTE**
> To use your router's IPv6 Internet connection settings, IPv6 service from your ISP (Internet service provider) is required. For more information on this service, ask your ISP.

To manually configure your router's IPv6 settings:

1. Use an Ethernet cable to connect an Ethernet port on your router to the Ethernet port on your computer.
2. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
3. Under *Router Settings*, click **Connectivity**. The *Connectivity* page opens.
4. Click the **Internet Settings** tab, then click **IPV6**.



Connectivity

View and change router settings

Type of Internet Connection | Edit

IPv6 - Automatic: Enabled

DUID: 00:02:03: : : : : : : : :

6rd tunnel: Disabled

Prefix:

Prefix length:

Border relay:

IPv4 mask length:

Optional

Domain name: hsd1.ut.comcast.net.

MTU: Auto

Size: 0

MAC Address Clone ☑ Enabled

00 : 27 : : : :

5. Click **Edit**. You can now change the following settings:
   - **IPv6 - Automatic**—Select **Enabled** to use IPv6 for all network addressing.
   - **DUID** (device user ID)**—**Used by DHCP to identify network clients.
   - **6rd Tunnel**—Allows your router to send IPv6 IP addresses over IPv4 networks. To enable this option, **IPv6 - Automatic** must be unselected. To let your router handle the 6rd Tunnel settings (such as prefixes and address masks), change the **6rd tunnel** setting to **Automatic**. Select **Manual** to change these settings manually.
   - **Prefix**—Enter the prefix address used for the tunnel provided by your ISP.
   - **Prefix Length**—Enter the prefix length used for the tunnel provided by your ISP.
   - **Border Relay**—Enter the border relay address used for the tunnel provided by your ISP.
   - **IPv4 mask length**—Enter the IPv4 address mask length used for the tunnel provided by your ISP.
6. Click **OK**.

How to associate a router with your Cisco Connect Cloud account

To associate an additional router to your Cisco Connect Cloud account:

1. Run **Setup** for the additional router. When Setup is complete, you are prompted to create a new Cisco Connect Cloud account.
2. Instead of creating a new account, click **Login** at the top of the screen. You are prompted to enter your account user name (e-mail address) and password.
3. Enter your original Cisco Connect Cloud account user name and password, then click **Log in**. The additional router is added to your Cisco Connect Cloud account.
4. To configure the additional router, log into Cisco Connect Cloud, then select the router's SSID (network name) from the drop-down list at the top of the screen.

How to get the most out of your dual-band router

I bought a dual band router, but I'm not sure that I'm getting the most out of it. What should I check? Of the many reasons for owning a dual-band router, the most common is to ensure available bandwidth for streaming high-definition video. At the same time, owners want to make sure that their video streams won't be interrupted by other wireless network traffic. To get the most out of your dual-band router, you can:

- Upgrade your wireless clients
- Split your traffic

Upgrade your wireless clients

If you have network adapters that support only legacy wireless network standards such as 802.11b, you should consider upgrading them with Wireless-N (802.11n) network adapters. Wireless-B (802.11b) devices can slow your entire wireless network. For the best performance, all of your wireless devices should support Wireless-N. You can then select *Wireless-N Only* as your Network Mode below.

> **NOTE**
> If you select *Wireless-N Only*, you may need to temporarily change your network settings to Mixed to provide access to guests without Wireless-N networking.

Split your traffic

The best way to improve your multimedia wireless performance is to split your wireless traffic between your router's two bands (ranges of radio frequencies). Your router supports the 2.4 GHz band and the 5 GHz band, and handles the two bands as two separate wireless networks to help manage the traffic.

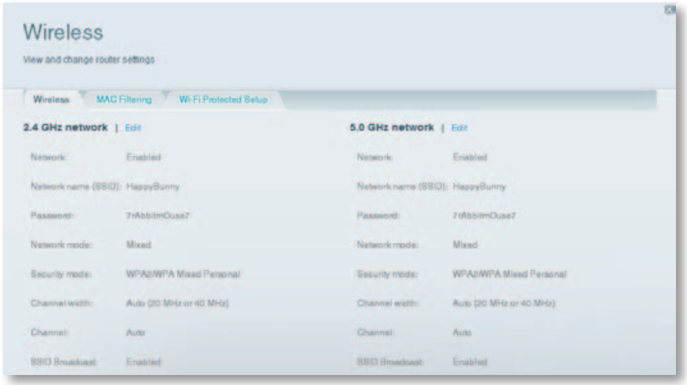
The most common way to split wireless traffic is to use the 2.4 GHz band for basic Internet tasks such as web browsing, email, and downloads, and use the 5.0 GHz band for streaming multimedia. There are several reasons for this approach:

- Although the 2.4 GHz band may be more crowded with wireless traffic from your neighbors, it's fine for basic Internet traffic that is not time-sensitive (such as e-mail).
- Even though you are connected to your own wireless network, you are still sharing "air time" with nearby networks.
- The 5 GHz band is much less crowded than the 2.4 GHz band, so it's ideal for streaming multimedia.
- The 5 GHz band has more available channels, so it is more likely that you will have your own, interference-free channel for your wireless network.

By default, your dual-band router uses the same network name on both the 2.4 GHz band and the 5 GHz band. The easiest way to segment your traffic is to rename one of your wireless networks. With a separate, descriptive name, it will be easy to connect to the right network.

To reconfigure your wireless network:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under *Router Settings*, click **Wireless**. The *Wireless* page opens to the *Wireless* tab.



2.4 GHz network | Edit		5.0 GHz network | Edit	
Network:	Enabled	Network:	Enabled
Network name (SSID):	HappyBunny	Network name (SSID):	HappyBunny
Password:	7rAbbitmOuse7	Password:	7rAbbitmOuse7
Network mode:	Mixed	Network mode:	Mixed
Security mode:	WPA2/WPA Mixed Personal	Security mode:	WPA2/WPA Mixed Personal
Channel width:	Auto (20 MHz or 40 MHz)	Channel width:	Auto (20 MHz or 40 MHz)
Channel:	Auto	Channel:	Auto
SSID Broadcast:	Enabled	SSID Broadcast:	Enabled

3. Click **Edit** next to the network band you want to modify. Change any of the settings below:
   a. **Enabled**—Deselect this checkbox to disable the network band.
   b. **Network name (SSID)**—You can provide a unique SSID for each band of your wireless network. The name must not exceed 32 characters.
   c. **Password**—You can provide a unique password for each band of your wireless network.

d. **Network mode**—Your choice depends upon the clients that will connect to your network. If all of your devices are Wireless-N capable, you can select **Wireless-N Only** for either or both bands.

   On the 5 GHz band, you can select:

   - **Mixed** (default), which accepts connections from 802.11a or 802.11n clients
   - **Wireless-N Only** (802.11n only)
   - **Wireless-A Only** (802.11a only)

   On the 2.4 GHz band, you can select:

   - **Mixed**
   - **Wireless-B/G Only**
   - **Wireless-N Only**
   - **Wireless-G Only**
   - **Wireless-B only**

e. **Security mode**—You can set up different security options for the 5 GHz and 2.4 GHz networks. If the security mode you select requires a passphrase, a *Passphrase* field appears, and you must enter a passphrase. You can select:

   - **None** (no security)
   - **WEP**
   - **WPA Personal**
   - **WPA Enterprise**
   - **WPA2 Personal**
   - **WPA2 Enterprise**
   - **WPA2/WPA Mixed Personal**
   - **WPA2/WPA Mixed Enterprise**

TIP
Wireless-N networks should use the *WP2-Personal* security mode for best performance.

f. **Channel width**—We recommend that you keep the default (Auto) setting for each band. In *Auto* mode, the router and the network clients automatically switch to the *40 MHz* mode if:

   - Your wireless clients support the 40 MHz mode (sometimes called *Bonded* mode) in which two 20 MHz channels are bonded together for better performance.
   - There is no adjacent interference.

   With more available channels and less chance of interference on the 5 GHz band, you have the option to force the 40 MHz mode.

   On the 2.4 GHz band, you can select:

   - **Auto (20 MHz or 40 Mhz)**
   - **20 MHz Only**

   On the 5 GHz band, you can select:

   - **Auto (20 MHz or 40 Mhz)**
   - **20 MHz Only**
   - **40 MHz Only**

g. **Channel**—Choose the operating channel for each band. Your router will automatically select the channel with the least amount of interference if you leave the default **Auto** setting. We recommend keeping the default settings for both bands.

h. **SSID broadcast**—When wireless clients look for wireless networks to connect to, they detect the *SSID* (wireless network name) broadcast by the router. In other words, anyone within range of your network can see your network name. To broadcast your router's SSID, keep the default setting (Enabled). If you do not want to broadcast the router's SSID, deselect the **SSID broadcast** checkbox. We recommend keeping the default setting (**Enabled**) for both bands.

4. To save your changes, click **OK**.

How to control access to your network

Why would I need to control access to my wireless network? If you used the Setup CD to install your router, your wireless network is already secure. By default, Setup enables industry-standard *WPA* (Wi-Fi Protected Access) security using WPA2/WPA mixed mode. If you set up your wireless network manually and have not enabled wireless security, your wireless network will be an "open" network that almost anyone nearby with a Wi-Fi-enabled device could access.

What is MAC filtering? If you choose not to use the built-in security features of your router, you can still control access to your wireless network using MAC filtering. Every network device has a unique, 12-digit *MAC* (Media Access Control) address. Using MAC filtering, you can allow only known MAC addresses (known devices) onto your network. You can also exclude specific MAC addresses or deny them access to your wireless network.

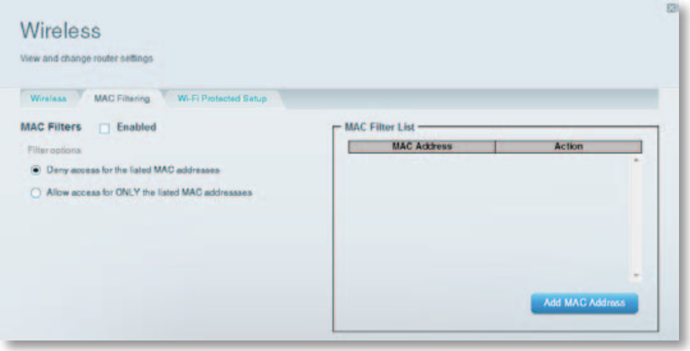
TIP
MAC filtering is not strong security. The best way to secure your network is to use the router's WPA2 security setting.

Example: Because each MAC filtering configuration is unique, the following procedure uses the simplified example of setting up MAC filtering to allow one wireless device access to the network.

TIP
You can also use MAC filtering to prevent specific PCs from accessing your network by selecting **Deny**. However, it's easier to select **Allow** to permit only known devices than to exclude unknown devices.

To set up MAC filtering to allow one wireless device access to your network:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under *Router Settings*, click **Wireless**. The Wireless page opens.
3. Click the **MAC Filtering** tab.



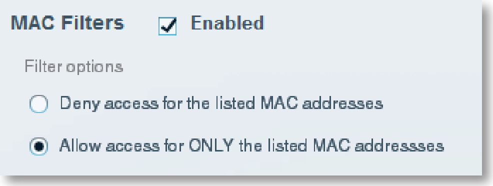
Wireless
View and change router settings

MAC Filters □ Enabled
Filter options
● Deny access for the listed MAC addresses
○ Allow access for ONLY the listed MAC addresses

MAC Filter List

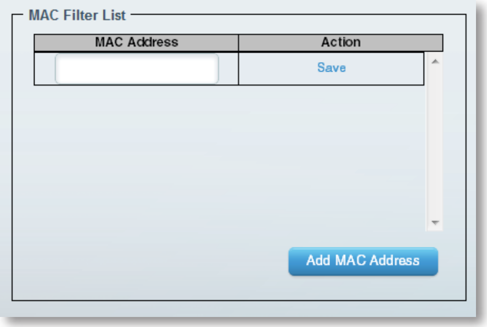
MAC Address	Action

4. Select **Enabled** next to *MAC Filters*, then select **Allow access for ONLY the listed MAC addresses**.



MAC Filters ☑ Enabled
Filter options
○ Deny access for the listed MAC addresses
● Allow access for ONLY the listed MAC addressses

5. Click **Add MAC Address**, then enter the MAC address into the **MAC Filter List** and click **Save**.



MAC Filter List

MAC Address	Action
	Save

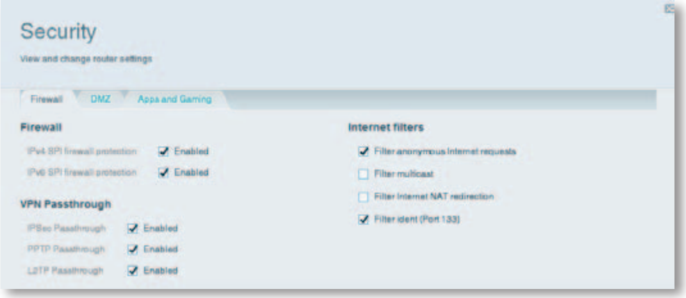
How to improve security using the built-in firewall

Why would I need to change my security settings? By default, the firewall settings in your router have been optimized for most home environments, so no changes are needed. The *SPI* (Stateful Packet Inspection) firewall is enabled by default. In addition, anonymous Internet requests and IDENT requests are filtered by default. All web filters are disabled, because enabling them may cause problems for sites that depend on ActiveX controls, Java, or cookies.

Changing firewall settings

To change your firewall settings:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Router Settings**, click **Security**. The *Security* page opens to the *Firewall* tab.



Security

View and change router settings

Firewall

IPv4 SPI firewall protection ☑ Enabled

IPv6 SPI firewall protection ☑ Enabled

VPN Passthrough

IPSec Passthrough ☑ Enabled

PPTP Passthrough ☑ Enabled

L2TP Passthrough ☑ Enabled

Internet filters

☑ Filter anonymous Internet requests

□ Filter multicast

□ Filter Internet NAT redirection

☑ Filter ident (Port 133)

3. You can now change the following settings:

TIP
For more descriptions of each setting, click **Help** at the top of the screen.

- **Firewall: SPI firewall protection**—This helps protect your local network from Internet threats. This option is enabled by default. On some router models, this setting is separated into IPv6 and IPv4 options so that each can be handled separately.

CAUTION
To help protect your network, you should keep this option enabled.

- **VPN Passthrough:**
  - **IPSec Passthrough** – *IPSec* (Internet Protocol Security) is a suite of protocols used to implement secure exchange of packets at the IP layer. The VPN clients on the local network can establish an IPSec VPN tunnel through the router. This option is enabled by default.
  - **PPTP Passthrough** – *PPTP* (Point-to-Point Tunneling Protocol) allows the *PPP* (Point-to-Point Protocol) to be tunneled through an IP network. The VPN clients on the local network can establish a PPTP VPN tunnel through the router. This option is enabled by default.
  - **L2TP Passthrough** – *L2TP* (Layer 2 Tunneling Protocol) enables point-to-point sessions using the Internet on the Layer 2 level. The VPN clients on the local network can establish an L2TP VPN tunnel through the router. This option is enabled by default.
- **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 block 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. On some router models, this setting applies to IPv4 Internet only.
  - **Filter ident (Port 133)**—This filter prevents port 133 from being scanned by devices from the Internet. This option is enabled by default.

4. Click **Save** to save your changes.

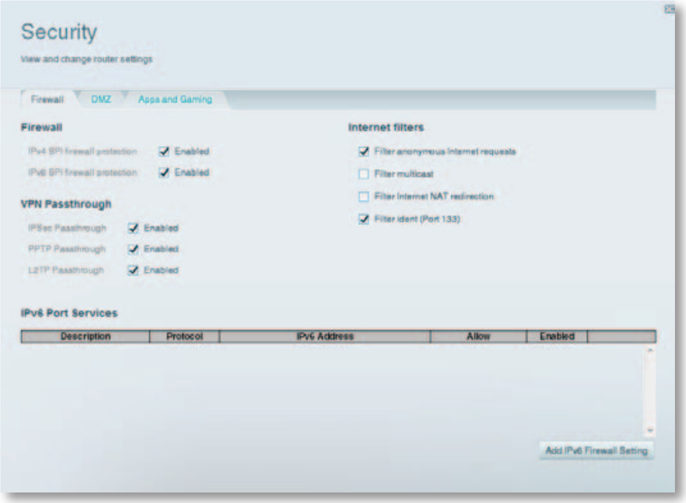
Changing IPv6 firewall settings

On some router models, the IPv6 firewall lets you customize IPv6 port services for applications. When users send these types of requests to your network via the Internet, the router will allow those requests to the appropriate computers.

> **NOTE**
> To use your router's IPv6 Internet connectino settings, IPv6 service from your ISP (Internet service provider) is required. For more information on this service, ask your ISP.

To set IPv6 firewall settings:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Router Settings**, click **Security**. The *Security* page opens to the *Firewall* tab.



Firewall
IPv4 SPI firewall protection ☑ Enabled
IPv6 SPI firewall protection ☑ Enabled

VPN Passthrough
IPSec Passthrough ☑ Enabled
PPTP Passthrough ☑ Enabled
L2TP Passthrough ☑ Enabled

Internet filters
☑ Filter anonymous Internet requests
□ Filter multicast
□ Filter Internet NAT redirection
☑ Filter ident (Port 133)

IPv6 Port Services

Description	Protocol	IPv6 Address	Allow	Enabled

3. Click Add IPv6 Firewall Setting. You can now change the following fields:
   - **Description**—Enter a description of the application.
   - **Protocol**—Select **TCP**, **UDP**, or **Both** (default).
   - **IPv6 Address**—Enter the IPv6 address of the computer that should receive the traffic.
   - **Allow**—Select the range of port(s) used by incoming traffic.
4. Click **Save** to save your changes. The list is updated to show the settings you have saved.
   - To change a saved setting, click **Edit** next to the setting.
   - To delete a saved setting, click **Remove** next to the setting.

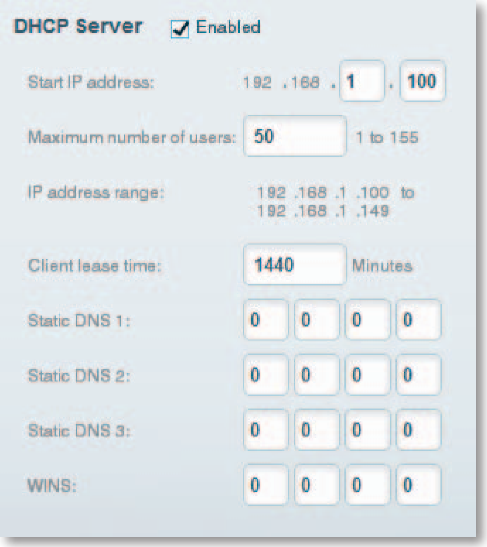
How to set up the DHCP server on your router

Your router can be used as a *DHCP* (Dynamic Host Configuration Protocol) server to automatically assign an IP address to each computer or device on your network. The DHCP server is enabled by default. If you already have a DHCP server on your network, or if you do not want to use your router as a DHCP server, you should disable this setting.

To configure your router's DHCP server settings:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Router Settings**, click **Connectivity**.

3. Click the **Local Network** tab.



DHCP Server ☑ Enabled

Start IP address: 192 . 168 . 1 . 100

Maximum number of users: 50 1 to 155

IP address range: 192 .168 .1 .100 to 192 .168 .1 .149

Client lease time: 1440 Minutes

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

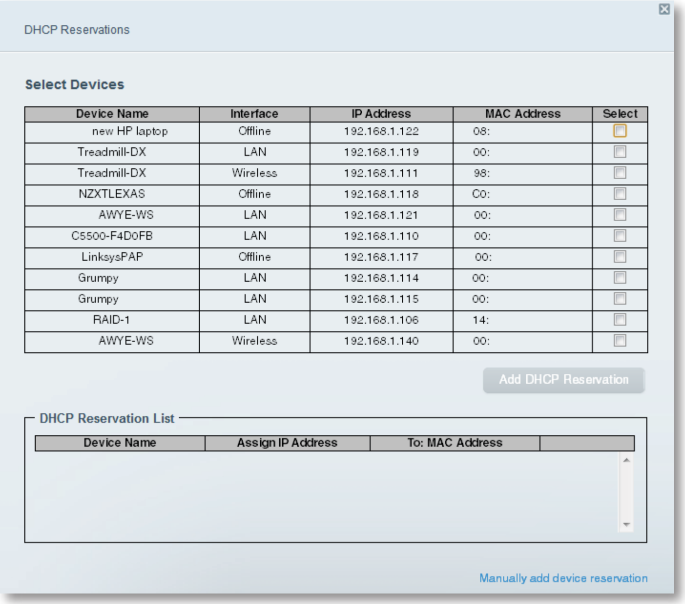
4. To disable the DHCP server, deselect the **Enabled** checkbox.
5. Leave the **Enabled** checkbox selected to edit the following settings:
   - Start IP address
   - Maximum number of users
   - IP address range (not editable)
   - Client lease time
   - Static DNS values
   - WINS
6. Click **OK** to save changes.

How to set up DHCP reservation

Why would I use it? *DHCP reservation* allows you to assign a unique, fixed IP address to a specific device on your network. Assigning a fixed IP address is a good way to manage devices such as print servers, web cameras, network printers, and game consoles. A fixed IP address is also recommended if you want to use port forwarding for devices that need to receive inbound traffic from the Internet ("How to set up port forwarding" on page 48).

To configure DHCP reservation:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Router Settings**, click **Connectivity**.
3. Click the **Local Network** tab, then click **DHCP Reservations**. The *DHCP Reservations* list opens, which lists attached network devices and current DHCP reservations.



DHCP Reservations

Select Devices

Device Name	Interface	IP Address	MAC Address	Select
new HP laptop	Offline	192.168.1.122	08:	□
Treadmill-DX	LAN	192.168.1.119	00:	□
Treadmill-DX	Wireless	192.168.1.111	98:	□
NZXTLEXAS	Offline	192.168.1.118	C0:	□
AWYE-WS	LAN	192.168.1.121	00:	□
C5500-F4D0FB	LAN	192.168.1.110	00:	□
LinksysPAP	Offline	192.168.1.117	00:	□
Grumpy	LAN	192.168.1.114	00:	□
Grumpy	LAN	192.168.1.115	00:	□
RAID-1	LAN	192.168.1.106	14:	□
AWYE-WS	Wireless	192.168.1.140	00:	□

DHCP Reservation List

Device Name	Assign IP Address	To: MAC Address	

4. Click the **Select** checkbox next to the device you want to reserve, then click **Add DHCP Reservation**.

5. Click **Edit** to change the reservation details, or click **Delete** to delete the reservation.

> **TIP**
> For field descriptions, click **Help** at the top of the screen.

How to access your network on the Internet

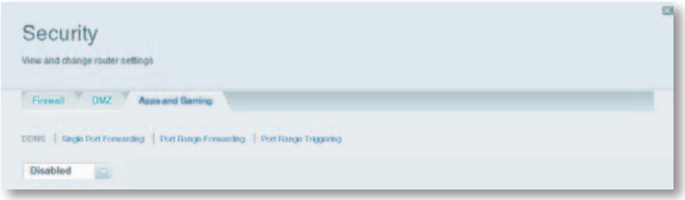
Why would I need to find my network on the Internet? If you want to remotely access a drive attached to your router or view a web camera on your home network, you need to be able to easily enter your network's address into a web browser.

Working with several DDNS (Dynamic Domain Name System) service providers, your router's DDNS feature lets you configure a domain name for your network, which you can then use to easily find your network on the Internet. If your ISP changes your network's IP address (which can happen frequently), the DDNS service providers detect the address change and continue to route your domain name to that address.

> **TIP**
> Before you configure DDNS on your router, you must sign up for DDNS service from a DDNS service provider that's supported by your router.

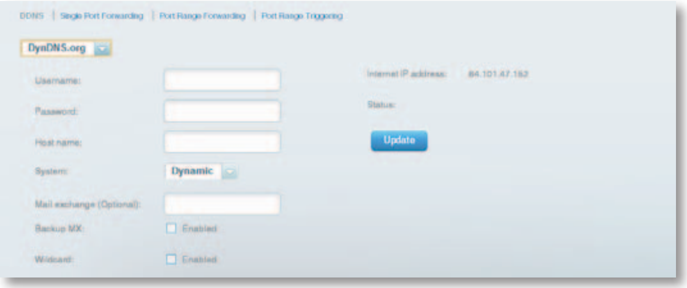
To set up DDNS:

1. Sign up for DDNS service at either **www.dyndns.org** or **www.tzo.com**. Note all of the information provided to you by the DDNS provider.
2. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
3. Under **Router Settings**, click **Security,** then click the **Apps and Gaming** tab. The DDNS screen opens.



Disabled

4. In the DDNS Service drop-down list (the list that has **Disabled** selected by default), select your DDNS service provider.



DynDNS.org

Username:

Password:

Host name:

System: Dynamic

Mail exchange (Optional):

Backup MX: □ Enabled

Wildcard: □ Enabled

Internet IP address: 84.101.47.182

Status:

5. Complete the fields with information provided by your DDNS provider, then click **OK**.
6. To access the network from the Internet, enter the domain name provided by the DDNS service provider.

   To access one of your network devices on the Internet:

   a. Configure the router to use port forwarding for the device (see "How to set up port forwarding for a single port" on page 48). Note the port number used for the device.

   b. Enter the domain name for your network, followed by a colon and the port number. For example, if the domain name registered with your DDNS provider is *HappyBunny.linksysnet.com*, and your Internet camera has been configured to use port 1024, you would enter: **HappyBunny.linksysnet.com:1024**

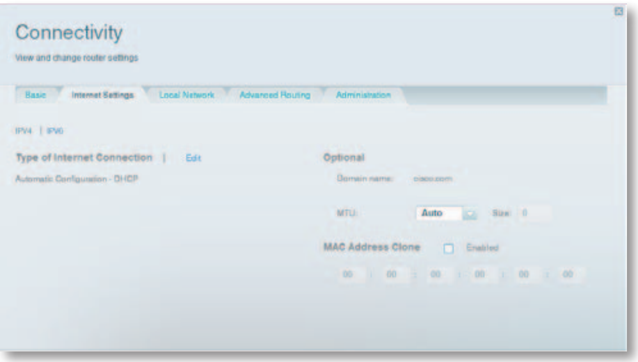
How to clone a MAC address

On any home network, each network device has a unique *MAC* (Media Access Control) address. Some ISPs register the MAC address of the device (usually a router or a computer) connected directly to the modem. If your computer's MAC address is registered with your ISP and you do not want to re-register the MAC address, then you can *clone* the address (assign the registered MAC address of your previous device to your new router). If you want to use the MAC address from an old router that you are replacing with your new router, you should first determine the MAC address of your old router, then manually enter it into your new router.

> **NOTE**
> For many ISPs that provide dynamic IP addresses automatically, the stored MAC address in the modem is reset each time you reset the modem. If you are installing this router for the first time, reset your modem before connecting the router to your modem. To reset your modem, disconnect power for about one minute, then reconnect power.

To clone a MAC address from your computer:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under *Router Settings*, click **Connectivity**. The *Connectivity* page opens.
3. Click the **Internet Settings** tab.



Type of Internet Connection | Edit
Automatic Configuration - DHCP

Optional
Domain name: cisco.com
MTU: Auto Size: 0
MAC Address Clone □ Enabled
00 : 00 : 00 : 00 : 00 : 00

4. Under *MAC Address Clone*, click **Enabled**.
5. Enter the 12-digit MAC address of your old router, then click **OK**.

How to connect to your corporate office using a VPN

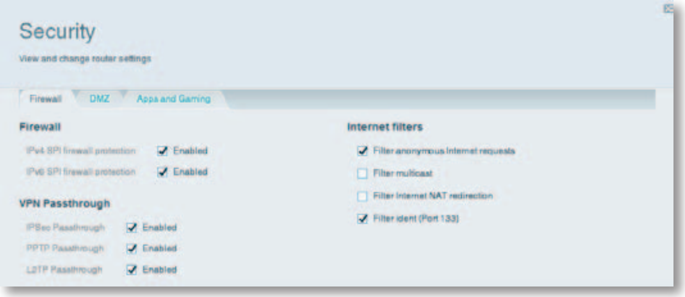
What is a VPN, and do I need to change my router settings? A *VPN* (Virtual Private Network) is a network that uses a public network, such as the Internet, to provide secure communications between a remote computer and another network. Corporations often provide VPN access to their networks to enable employees to work from remote offices or while traveling. Most corporate VPNs use the Internet to provide connectivity between remote employees and the corporate network.

For a typical VPN, the corporation installs a VPN gateway on their corporate network. Employees authorized to work remotely connect to the VPN gateway through the Internet using VPN software and security methods provided by their employers. Robust security and authentication schemes ensure a secure connection and access by only authorized users.

The default VPN settings in your router have been configured to pass through (allow) the most common types of VPN protocols, so usually no changes are needed.

To change your VPN passthrough settings:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Router Settings**, click **Security**. The *Security* page opens to the *Firewall* tab.



Firewall
IPv4 SPI firewall protection ☑ Enabled
IPv6 SPI firewall protection ☑ Enabled

VPN Passthrough
IPSec Passthrough ☑ Enabled
PPTP Passthrough ☑ Enabled
L2TP Passthrough ☑ Enabled

Internet filters
☑ Filter anonymous Internet requests
□ Filter multicast
□ Filter Internet NAT redirection
☑ Filter ident (Port 133)

3. Enable each setting that you want to change.
   - **IPSec Passthrough** – *IPSec* (Internet Protocol Security) is a suite of protocols used to implement secure exchange of packets at the IP layer. The VPN clients on the local network can establish an IPSec VPN tunnel through the router. This option is enabled by default.
   - **PPTP Passthrough** – *PPTP* (Point-to-Point Tunneling Protocol) allows the *PPP* (Point-to-Point Protocol) to be tunneled through an IP network. The VPN clients on the local network can establish a PPTP VPN tunnel through the router. This option is enabled by default.
   - **L2TP Passthrough** – *L2TP* (Layer 2 Tunneling Protocol) enables point-to-point sessions using the Internet on the Layer 2 level. The VPN clients on the local network can establish an L2TP VPN tunnel through the router. This option is enabled by default.
4. Click **OK** to save your changes.

How to optimize your router for gaming and voice

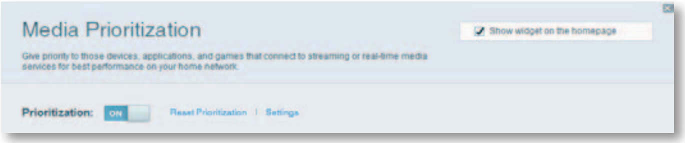
How does my router prioritize traffic to the Internet? Your router can prioritize traffic between your network and the Internet. Performance for demanding, real-time applications, such as online gaming, VoIP calls, video streaming, and videoconferencing, can be improved by configuring *media prioritization*.

Prioritization settings are applied only to traffic that is uploaded to the Internet. The router cannot control the quality of the traffic after it reaches the Internet.

> **TIP**
> For more information on optimizing your router for online gaming, see "Port Forwarding and Port Triggering" on page 48.

To configure media prioritization:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Apps**, click **Media Prioritization**. The *Media Prioritization* screen opens.



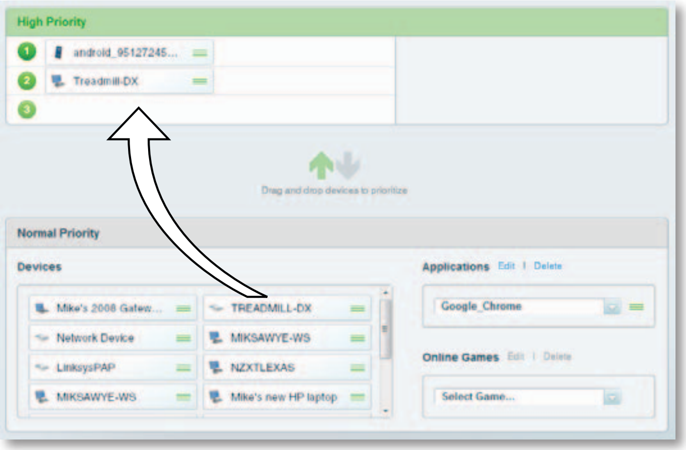
Media Prioritization

Give priority to those devices, applications, and games that connect to streaming or real-time media services for best performance on your home network.

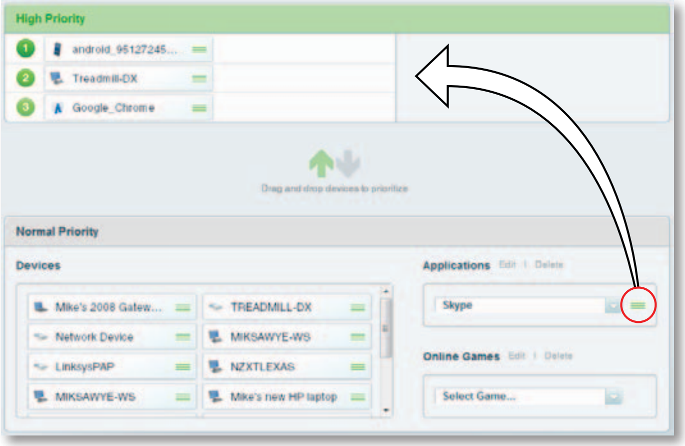
☑ Show widget on the homepage

Prioritization: ON

3. Turn on **Prioritization** if it is not already on.
4. Click and drag high-priority devices from the **Normal Priority** list to the **High Priority** list.



5. To prioritize an application or game, select the name in the drop-down list, then click and drag the ≡ icon next to the name to the **High Priority** list.



High Priority

1 android_95127245... ≡
2 Treadmill-DX ≡
3 Google_Chrome ≡

Drag and drop devices to prioritize

Normal Priority

Devices

Mike's 2008 Gatew... ≡	TREADMILL-DX ≡
Network Device ≡	MIKSAWYE-WS ≡
LinksysPAP ≡	NZXTLEXAS ≡
MIKSAWYE-WS ≡	Mike's new HP laptop ≡

Applications Edit | Delete

Skype ≡

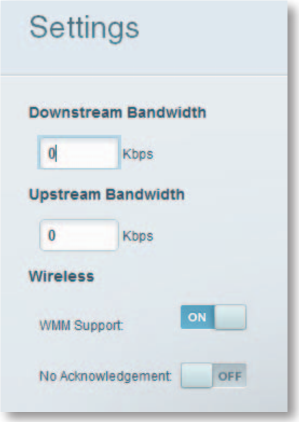
Online Games Edit | Delete

Select Game...

- If the application name isn't listed, click **Edit** and add the name.

> **TIP**
> If you want to add a new application or game, you need to know its port and protocol information (see the application or game's documentation for help).

6. Click **Settings**. The *Settings* screen opens.



Settings

Downstream Bandwidth

0 Kbps

Upstream Bandwidth

0 Kbps

Wireless

WMM Support: ON

No Acknowledgement: OFF

a. Set the maximum **Downstream Bandwidth**. If you set the bandwidth lower than the actual bandwidth of your router, performance may be limited.

b. Set the maximum **Upstream Bandwidth**.

c. To help manage traffic priority with devices that support WMM, turn on **WMM Support**.

> **TIP**
> *WMM* (Wi-Fi MultiMedia) Support is a wireless feature based on the IEEE 802.11e standard. WMM improves quality for audio, video, and voice applications by prioritizing wireless traffic. This feature requires that the wireless client devices in your network also support WMM.

d. To have the router re-send data if an error occurs, turn off **No Acknowledgement**.

> **CAUTION**
> If you specify a maximum bandwidth that is too high, the router cannot apply priorities correctly, and prioritization problems may result.

e. Click **OK**.

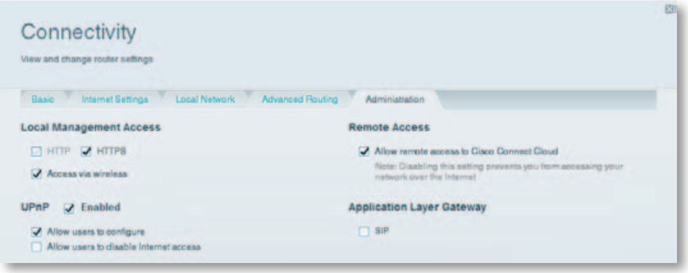
How to enable Voice over IP on your network

Do I need to configure Voice over IP? *VoIP* (Voice over Internet Protocol) is a technology for using the Internet as an interface for telephone communications. To use VoIP, you need to get an account with a VoIP service provider. The VoIP service provider typically provides you with a telephone adapter that connects to your network. If you do not use your network to make phone calls, you don't need to change the default settings.

The *Application Layer Gateway SIP* (Session Initiation Protocol) allows SIP packets, used by some VOIP service providers, to get through your router's firewall.

To configure the router for VoIP:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Router Settings**, click **Connectivity**, then click the **Administration** tab.



Local Management Access

□ HTTP ☑ HTTPS

☑ Access via wireless

UPnP ☑ Enabled

☑ Allow users to configure

□ Allow users to disable Internet access

Remote Access

☑ Allow remote access to Cisco Connect Cloud

Note: Disabling this setting prevents you from accessing your network over the Internet

Application Layer Gateway

□ SIP

3. If your VoIP service uses SIP, select the **SIP** checkbox under *Application Layer Gateway*.

   – OR –

   If your VoIP service uses other NAT traversal solutions such as *STUN* (Session Traversal Utilities for NAT), *TURN* (Traversal Using Relay NAT), or *ICE* (Interactive Connectivity Establishment), deselect the **SIP** checkbox.

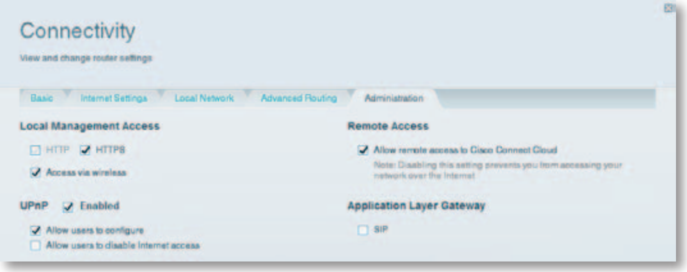
NOTE
You may need to contact your VoIP service provider to determine the type of NAT traversal configuration they use.

How to configure UPnP

What is UPnP? *UPnP* (Universal Plug and Play) allows devices connected to a network to discover each other and automatically create working configurations. Examples of UPnP-capable devices include web cameras, online gaming applications, and VoIP devices. UPnP is enabled by default.

To configure UPnP:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Router Settings**, click **Connectivity**, then click the **Administration** tab.



Local Management Access

□ HTTP ☑ HTTPS

☑ Access via wireless

UPnP ☑ Enabled

☑ Allow users to configure

□ Allow users to disable Internet access

Remote Access

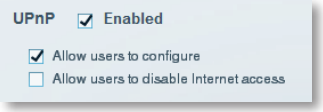
☑ Allow remote access to Cisco Connect Cloud

Note: Disabling this setting prevents you from accessing your network over the Internet

Application Layer Gateway

□ SIP

3. To use UPnP, select **Enabled** (default) next to *UPnP*.
4. To allow changing router settings while using UPnP, select **Allow Users to Configure**.
5. To prevent local network users from disabling your Internet connection through UPnP, deselect the **Allow users to disable Internet access** checkbox.



UPnP ☑ Enabled

☑ Allow users to configure

□ Allow users to disable Internet access

6. Click **OK**.

How to use a router as an access point

How can I use this new router as an access point? If you have a large area to cover with your wireless signal, or if part of your home has weak signals due to interference, you can use this router to extend the range of your old router's wireless network.

To set up your new router as an access point:

1. Use a network cable to connect this router's **Internet** port to the **Ethernet** or **LAN** port on the router that is connected to your modem.
2. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
3. Under **Router Settings**, click **Connectivity**, then click the **Internet Settings** tab.
4. Click **IPv4**.
5. For **Type of Internet Connection**, select **Bridge Mode**.
6. Click **Obtain an IPv4 address automatically**, then click **OK**. The new router's LAN IP address will be changed and obtained from the router that is connected to your modem.

How can I use my old router as an access point? If you have a large area to cover with your wireless signal, or if part of your home has weak signals due to interference, you can use your old router to extend the range of your wireless network. This is a complex process, so this procedure assumes that you have some networking knowledge.

> **TIP**
> Check the documentation for your old router. Some brands of routers include either a switch on the outside of the case or a software option to convert it to an access point. If either of these options is available, follow your old router's instructions to convert it to an access point.

You need to take note of your new router's settings, then apply some of those settings to the old router so it can work as an access point.

To view your new router's settings:

1. Make sure that your new router is connected to the Internet.
2. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
3. Under **Router Settings**, click **Wireless**, then take note of the *Network name (SSID)*, *Password*, *Security mode*, and *Channel*.
4. Under **Router Settings**, click **Connectivity**, then click the **Local Network** tab. Take note of the DHCP server's IP address range (192.168.1.100 to 192.168.1.149 by default)

To use your old router as an access point:

1. With your computer connected to your old router, log into its browser-based administration utility.

> **NOTE**
> Save your changes after finishing each step below.

2. Open the setup page for the local network (LAN).
3. In the **Router IP address** field, enter an unused IP address for the LAN network of your new router.

   For example, if your new router has an IP address of 192.168.1.1, you should choose an IP address on the 192.168.1.0 network. You can choose any address within the range of 192.168.1.2 to 192.168.1.254. You should exclude addresses in the range that will be used by the DHCP Server of your new router (192.168.1.100 to 192.168.1.149). A safe choice might be 192.168.1.250. Take note of this address, because this will be the address that you will use to manage your old router in the future.
4. In the **Subnet Mask** field, enter **255.255.255.0** or, if available, select that subnet mask from a drop-down list.
5. Disable the DHCP server on your old router. (Because your old router will be operating as an access point instead of a router, you don't want it to distribute IP addresses. There should be only one active DHCP server on your network, and that should be your new router.)
6. To reconfigure the wireless network on your old router:
   a. Open the wireless network setup page.

b. Change the network name (SSID) to match the name of your new network. Having the same network name and security settings enables you to seamlessly roam between your new router and your old router.

c. Change the security mode to match the security mode on your new router.

d. Change the passphrase (sometimes called the pre-shared key) on your old router to match the passphrase on your new router.

e. Change the wireless channel to a non-conflicting channel. Some manufacturers have an "Auto" function for channel selection that automatically selects a wireless channel that does not interfere with other nearby wireless networks. If your old router supports an Auto function, select that. Otherwise, you may need to manually select the wireless operating channel on your old router. In the 2.4 GHz wireless spectrum, there are only three non-overlapping channels: 1, 6, and 11. Pick a channel that does not overlap the operating channel of your new router. For example, if your new router is operating on channel 11, configure your old router for either channel 1 or channel 6.

7. Connect an Ethernet network cable to one of the LAN/Ethernet ports on your old router and an Ethernet port on your new router.

> **CAUTION**
> Do **not** connect the cable to the Internet port on your old router. If you do, you may not be able to set up the router as an access point on the current network.

How to put your new router behind an existing router

Why would I put my new router behind an existing router? There are several possible scenarios in which you might want to use your new router "behind" another router:

1. You might be in an environment that shares the landlord's Internet connection with all tenants. In this case, you should put your own router behind the landlord's router in order to create your own private network and to isolate computers on your network from the rest of the building.
2. You are sharing an office building Internet connection, and you want to control Internet access or the content viewed by your employees.
3. You already have an existing network and you want to extend the network's range or add wireless capabilities to your network.
4. You want to separate older, less secure network devices from the rest of the network.

To add your router to an existing router or gateway

In most cases, you can easily add your router to an existing wireless network by running Cisco Connect. If you are unable to set up the additional router using the instructions below, see "To share an Internet connection" on page 37 or "To extend your network" on page 39.

To add your router to your existing wireless network:

1. Insert your router's setup CD into a CD/DVD drive on your computer, then follow the on-screen instructions until you are told to connect your router's **Internet** port to the **LAN/Ethernet** port on your modem.
2. Instead, connect your router's **Internet** port to the **LAN/Ethernet** port on your existing (upstream) router or gateway.
3. Follow the remaining on-screen instructions until setup is complete.

To share an Internet connection

NOTE
This is a complex process, so this procedure assumes that you have some networking knowledge.

To add another router to share an Internet connection:

This topic covers cases one and two above

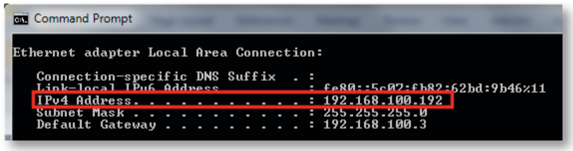
1. Determine the IP address range for your upstream (office or building) network.

   To determine the address range by using a Windows computer:

   a. Connect your computer into your upstream network's router.

   b. Click **Start**, **Run**, type **CMD**, then click **OK**. The command prompt window appears.

   c. Type **ipconfig**, then press **Enter**.



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5c07:fb82:62bd:9b46%11
   IPv4 Address. . . . . . . . . . . : 192.168.100.192
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.3
```

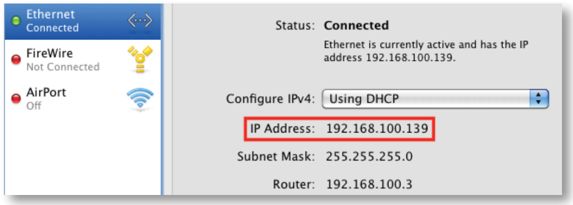
TIP
Although you can determine your computer's IP address in many ways, this method is quick and relatively easy.

   d. Take note of the IP address. In this example, the IP address is *192.168.100.192*.

To determine the address range by using a Mac computer:

a. Connect your computer into your upstream network's router.

b. From the *Dock*, click **System preferences**, click **Network**, then click **Ethernet** in the window to the left. A network status window opens.



Status: Connected
Ethernet is currently active and has the IP address 192.168.100.139.

Configure IPv4: Using DHCP

IP Address: 192.168.100.139

Subnet Mask: 255.255.255.0

Router: 192.168.100.3

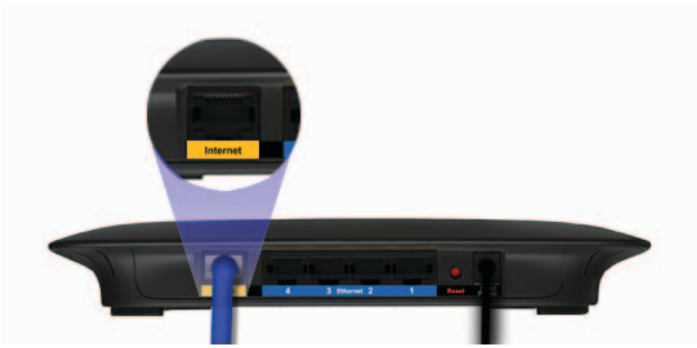
c. Take note of the IP address. In this example, the IP address is *192.168.100.139*.

Example: The above examples show that upstream IP addresses are on the 192.168.100.0 network. (The "0" indicates the entire network.) Your upstream network's address may be different. The default address of your new Linksys router is 192.168.1.1. In setting up one router behind another, you must make sure that the local network on your new router is different than the network of your upstream router. In the above example, because the default local network on your Linksys router 192.168.1.0 is on a different subnet than the office network's 192.168.100.0, you will be able to place your Linksys router behind the other router.

2. Connect an Ethernet network cable to a **LAN/Ethernet** port on your upstream network to the yellow **Internet** port on your router.

> **CAUTION**
> Connect the upstream network to your router's yellow **Internet** port, *not* one of the blue Ethernet ports. If you connect to an Ethernet port, you create IP addressing problems for the office network.

> **TIPS**
> An office network often has a wall plate with an Ethernet port that you can connect to.
>
> If you are doing this in a home environment (without wall ports), connect an Ethernet network cable between a LAN port on your upstream router and the **Internet** port on your Linksys router.



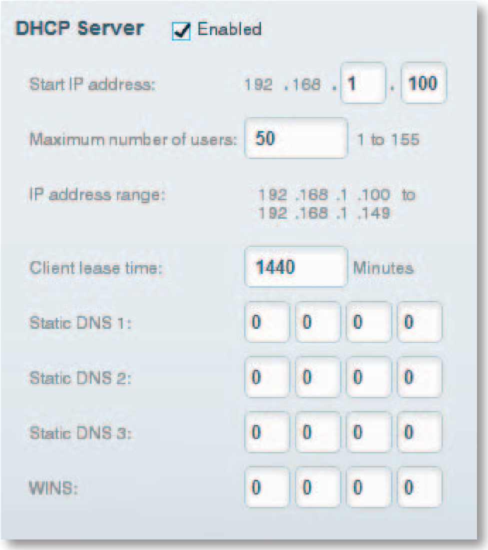
3. Run your router's setup CD on each computer that you want to connect to the Linksys router. Each computer needs either a wired or wireless connection to the Linksys router. For more information, see "How to connect a computer to your network" on page 15.

The computers that are connected to the Linksys router are now on the same network, and are isolated from the upstream network. However, you will still have access to the Internet through the upstream router (by way of your Linksys router). Because two routers are between your computer and the Internet, Internet traffic undergoes two network address translations. This is sometimes referred to as *Double NAT*.

Your computers can also use the built-in capabilities of your Linksys router, such as parental controls. If you need further control over the type of content your employees or family access, you can create an account with an Internet filtering site such as **www.opendns.com** or **www.bsecure.com**. After you create an account with them, use their DNS in place of your ISP's DNS.

To use their DNS:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Router Settings**, click **Connectivity**.
3. Click the **Local Network** tab.



DHCP Server ☑ Enabled

Start IP address: 192 .168 . 1 . 100

Maximum number of users: 50 1 to 155

IP address range: 192 .168 .1 .100 to 192 .168 .1 .149

Client lease time: 1440 Minutes

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

4. Complete the **Static DNS** fields with the information provided by your content filtering provider.
5. Click **OK**.

To extend your network

This topic covers cases three and four above.

NOTE
This is a complex process, so this procedure assumes that you have some networking knowledge.

To extend your network or add wireless capabilities:

1. If you want to extend your network, you may also follow the instructions above. One example of this might be to provide a separate wireless network for your children to keep their wireless network traffic separate from your wireless network. You might also want to isolate one network from another network so that network shares aren't visible across networks. In this case, use an Ethernet cable to connect the **Internet** port of the downstream router to one of the LAN ports of the upstream router. Make sure that the local network subnets on the two routers are different.

   - OR -

   You can extend your network by turning the downstream router into an access point. (See "How to use a router as an access point" on page 35). When you use a router as an access point, computers connected to the access point are on the same IP subnet as all other devices connected to the router. File, printer, and media sharing is much easier if all devices are on the same subnet.

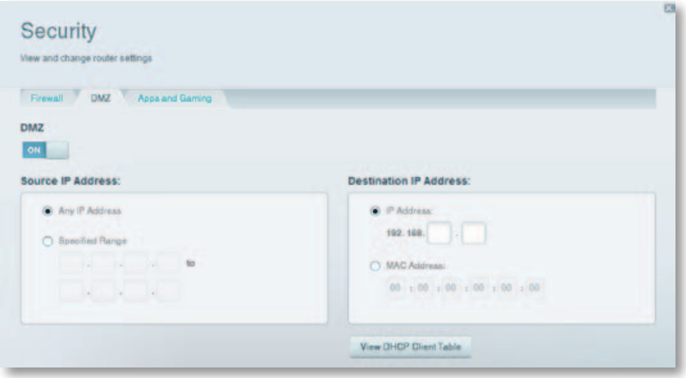
How to expose a device to the Internet

Why would I expose a device to the Internet? If you are operating a web server, a mail server, or a web camera, you may want to expose that device to the Internet so anybody can access it. Your router includes a *DMZ* (Demilitarized Zone) feature that forwards all inbound ports presented on the WAN interface, except those that are specifically forwarded, to an individual IP address or MAC address. This feature is normally not used, because it presents significant security risks to the device that you designate for the DMZ. The DMZ device is not protected by the built-in firewalls, Internet filters, or router web filters, and is open to attacks from hackers.

A much safer way of "exposing" devices to the Internet would be to use port forwarding. See "How to set up port forwarding" on page 48.

To set up a device in the DMZ:

1. Configure your device with a static IP address. See your device's documentation for help with setting a static IP address or use DHCP reservation (see "How to set up the DHCP server on your router" on page 28).
2. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
3. Under **Router Settings**, click **Security**, then click the **DMZ** tab.

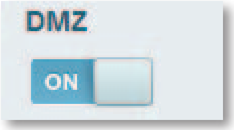


DMZ: ON

Source IP Address:
● Any IP Address
○ Specified Range . . . to . . .

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

4. Click the setting for **DMZ** to turn it on.



DMZ

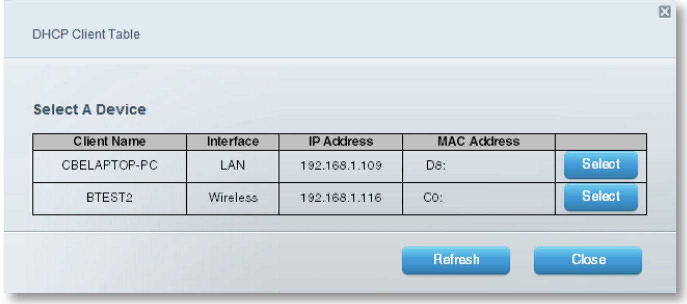
ON

5. Select **Enabled**.
6. In the *Source IP Address* section, select **Any IP Address** to allow access to your DMZ device from the entire Internet, or select the alternate button and enter a range of allowed source addresses.
7. In the *Destination IP Address* section, enter the last three digits of the IP address of the device that will be in the DMZ. The rest of the IP address is already completed.

   - OR -

   If you want to specify the 12-digit MAC address of the device instead of setting up a DHCP address reservation, you can replace Step 6 with the following steps:

   a. In the *Destination IP Address* section, select **MAC Address**, then click **View DHCP Client Table**. The *DHCP Client Table* screen opens.



DHCP Client Table

Select A Device

Client Name	Interface	IP Address	MAC Address	
CBELAPTOP-PC	LAN	192.168.1.109	D8:	Select
BTEST2	Wireless	192.168.1.116	C0:	Select

   b. Click **Select** next to the device that you want to place in the DMZ, then click **Close**. The corresponding MAC address is copied into the *MAC Address* field.

   c. Click **OK**.

Using an External Drive

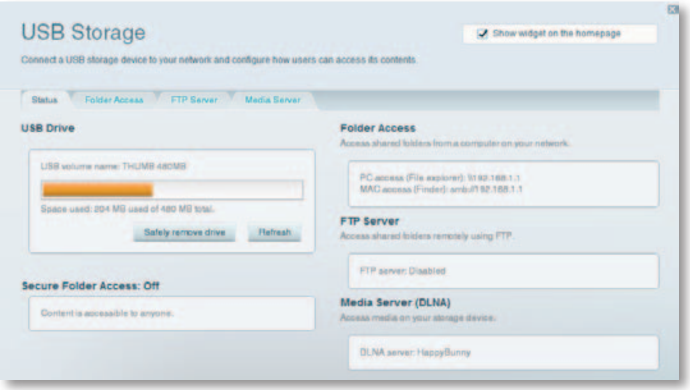
For EA3500 EA4500

Overview

You can attach most USB drives (including a thumb drive or a high-capacity external drive) to the USB port on your router. You can then use the drive as networked storage, as a media server (for media-enabled devices such as a networked TV), and as an FTP (File Transfer Protocol) server. You can also specify which users can access the content on the drive. (The media server feature is not available on the EA3500.)

To view the status and settings of your attached drive:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Click **USB Storage** under **Apps**. The *Status* tab displays information such as:
   - Drive capacity and use
   - Secured folder access status
   - Addresses for accessing shared folders, the FTP server, and media server



USB Storage

☑ Show widget on the homepage

Connect a USB storage device to your network and configure how users can access its contents.

USB Drive

USB volume name: THUMB 480MB

Space used: 204 MB used of 480 MB total.

Secure Folder Access: Off

Content is accessible to anyone.

Folder Access

Access shared folders from a computer on your network.

PC access (File explorer): \\192.168.1.1
MAC access (Finder): smb://192.168.1.1

FTP Server

Access shared folders remotely using FTP.

FTP server: Disabled

Media Server (DLNA)

Access media on your storage device.

DLNA server: HappyBunny

How to attach a USB drive

For EA3500 EA4500

If a USB drive is already connected to the router, and you want to attach a different drive to that USB port, you should safely disconnect the old drive first.

To safely remove a USB drive from the router:

1. Log into Cisco Connect Cloud, then click **USB Storage** under **Apps**.
2. In the **Status** tab, click **Safely remove drive**.
3. Disconnect the old drive from the router.

To attach a USB drive to the router:

1. Connect the USB drive to an available USB port on the back of your router. Your router detects the drive.
2. To update the *USB Storage* screen, you may need to click **Refresh**.

How to use secured folder access

For EA3500 EA4500

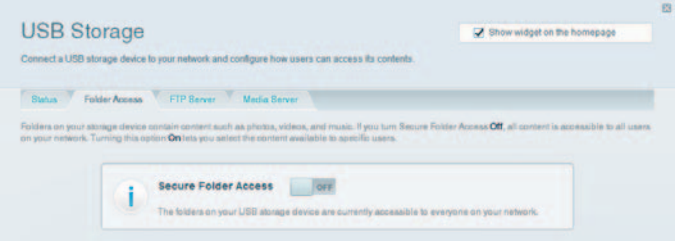
Why would I need to use secured folder access? By default, when you connect a USB drive to your router, the entire contents of the drive are available for read and write access to anyone on your local network (no login credentials are required). However, you can also make the drive and its folders secure, so that only authorized users can access the drive's contents.

> **TIP**
> When Secure Folder Access is on, the entire USB drive is secured.

How to set up authorized users and shared folders

To enable access to shared folders:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Click **USB Storage** under *Apps*, then click the **Folder Access** tab.



USB Storage

☑ Show widget on the homepage

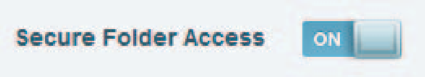
Connect a USB storage device to your network and configure how users can access its contents.

Folders on your storage device contain content such as photos, videos, and music. If you turn Secure Folder Access **Off**, all content is accessible to all users on your network. Turning this option **On** lets you select the content available to specific users.

Secure Folder Access OFF

The folders on your USB storage device are currently accessible to everyone on your network.

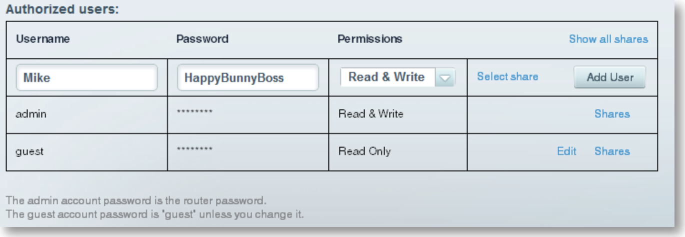
3. Click the setting for **Secure Folder Access** to turn it on.



Secure Folder Access ON

The *Authorized users* list appears.

4. In the *Authorized users* list, type a **Username** and **Password** for each new user.



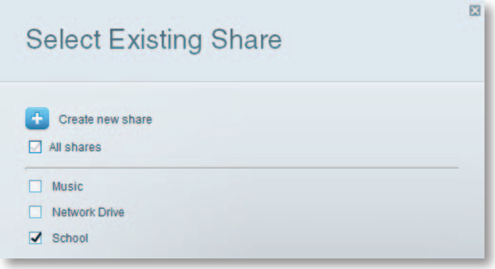
Authorized users:

Username	Password	Permissions	Show all shares
Mike	HappyBunnyBoss	Read & Write	Select share Add User
admin	********	Read & Write	Shares
guest	********	Read Only	Edit Shares

The admin account password is the router password.
The guest account password is "guest" unless you change it.

> **TIP**
> Two accounts, *Admin* and *Guest*, are already set up and cannot be deleted.

5. Select the permissions to give the user.
   - **Read Only** lets the user read (open) the file.
   - **Read & Write** lets the user read, rename, overwrite, or delete the file. The user can also save new files to the folder.
6. Click **Select Share**. The *Select Existing Share* dialog box opens.
7. If you already have the shared folder set up:
   a. Select the check box next to each share you want to grant access to, then click **OK**.



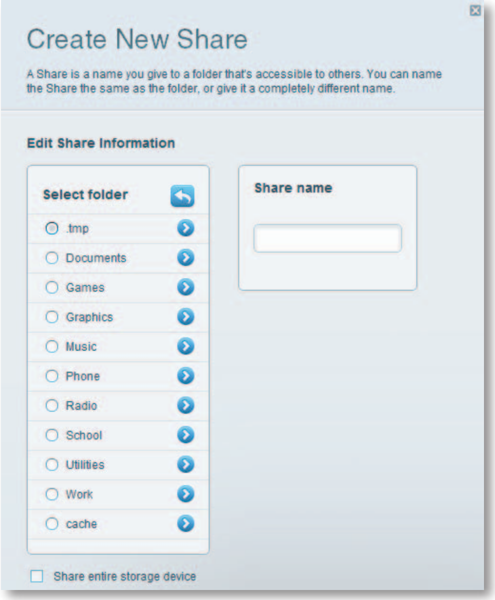
Select Existing Share

□ All shares

□ Music
□ Network Drive
☑ School

8. If you need to set up the shared folder:

   a. Click **Create new share**. The *Create New Share* dialog box opens.



Create New Share

A Share is a name you give to a folder that's accessible to others. You can name the Share the same as the folder, or give it a completely different name.

Edit Share Information

   b. Click the button next to the folder that you want to share.
      - To view subfolders, click the › icon next to the folder name.
      - To return to a parent folder, click the ↶ icon at the top of the list.
      - To select the entire drive, select **Share entire storage device**.

> **TIPS**
> - The share name automatically changes to the name of the folder you selected.
> - You cannot select more than one folder for each share.

      - To use a different share name, type the name in the **Share name** field.

   c. Click **OK**.

   d. Select the check box next to each share you want to grant access to, then click **OK**.

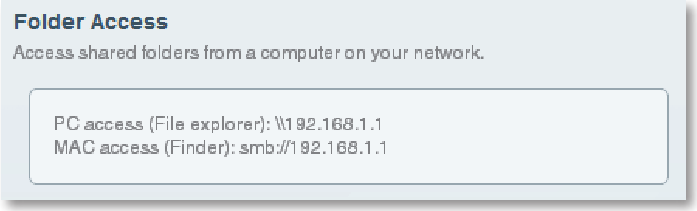
9. Click **Add User**.

10. In the *Authorized users* list, you can also:
    - Click **Edit** to change a user's credentials.
    - Click **Shares** to change the shares that a user can access.
    - Click **Delete** to delete the user account.

How to access shared folders

To access shared folders while on your network:

1. While in Cisco Connect Cloud, click **USB Storage** under **Apps**.
2. In the *Status* tab, note the information under *Folder Access*. This is the address you will need to access the shared folders from a file manager.



Folder Access

Access shared folders from a computer on your network.

PC access (File explorer): \\192.168.1.1
MAC access (Finder): smb://192.168.1.1

3. Enter the access address into your file manager.

> **TIP**
> You can also usually locate the folder by browsing through your computer's file manager.

4. Enter your user account name and password. The drive's contents (files and folders) appear in a window.
5. Use the file manager to open, copy, or view the folder's contents.

TIPS

File managers display content in many ways, but you can usually use these common actions to navigate through folders:

- Click or double-click a folder name to open it.
- Click, double-click, or right-click a file to open, copy, or view it.
- Drag a file from another window and drop it into the shared folder's window to copy it to the shared folder. (To copy a file to the shared folder, your user account must have write access.)

How to set up your router as a media server

For EA4500

What is a media server and how would I use it? A media server lets you share media content across your network. Your router can act as a media server if it has a USB drive attached and if you have UPnP AV (Audio and Video)-enabled or DLNA (Digital Living Network Alliance)-certified devices in your home. Examples of UPnP AV-enabled devices include digital media players, gaming consoles with a built-in media player, and digital picture frames.

For example, if you have a digital media adapter that sends content to your entertainment system, and if your router's set up as a media server, then the digital media adapter can access your router's attached USB drive.

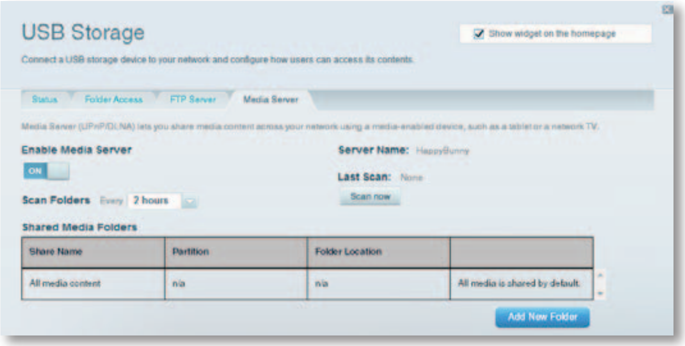
You can specify which folders are used by the media server, add and delete folders, and specify how often the folders are scanned for new content.

NOTE

The EA3500 does not support the media server feature.

To configure your router as a media server:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Click **USB Storage** under *Apps*. The *USB Storage* screen opens.
3. Click the **Media Access** tab.



USB Storage

☑ Show widget on the homepage

Connect a USB storage device to your network and configure how users can access its contents.

Media Server (UPnP/DLNA) lets you share media content across your network using a media-enabled device, such as a tablet or a network TV.

Enable Media Server: ON

Server Name: HappyBunny

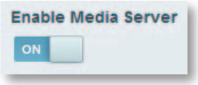
Last Scan: None

Scan Folders Every 2 hours

Shared Media Folders

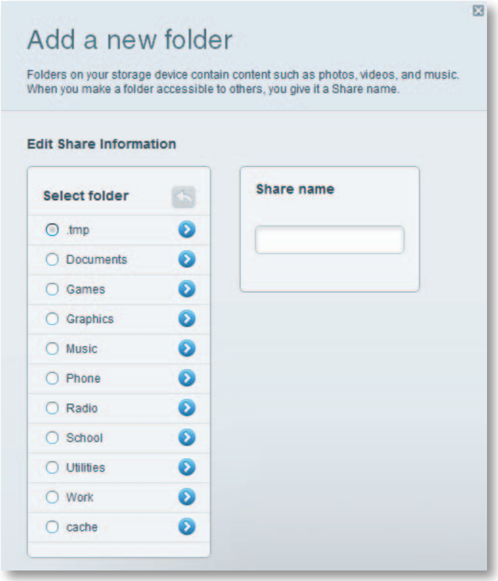
Share Name	Partition	Folder Location	
All media content	n/a	n/a	All media is shared by default.

4. Click the setting for **Enable Media Server** to turn it on.



Enable Media Server: ON

5. Click **Add New Folder**. The *Add a new folder* dialog box opens.



Add a new folder

Folders on your storage device contain content such as photos, videos, and music. When you make a folder accessible to others, you give it a Share name.

Edit Share Information

6. Click the button next to the folder that you want to share, then click **OK**.
   - To view subfolders, click the › icon next to the folder name.
   - To return to a parent folder, click the ↶ icon at the top of the list.

TIPS

- The share name automatically changes to the name of the folder you selected.
- You cannot select more than one folder at a time.

7. Click **OK** again to save changes.

How to connect your UPnP device to the media server

After you set up your router's media server, you need to connect an UPnP-compatible device (such as an UPnP-compatible game console or digital media player) to the network so that you can play the media server's content.

To connect an UPnP device to your router's media server:

1. Connect your UPnP device to your home network with wired (Ethernet cable) or wireless networking. If you are connecting wirelessly, you need to know your network's name and password. See your device's documentation for help.
2. On your UPnP device, change the media source to the media server name you specified on your router. (See "How to set up your router as a media server" on page 44)
3. See your UPnP device's documentation for help with playing media on the device.

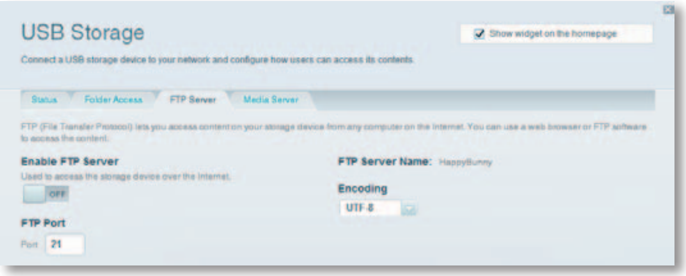
How to remotely access storage

For EA3500 EA4500

Why would I need to access my router's storage remotely? After you enable the router's FTP (File Transfer Protocol) server, you can access the attached drive's files from anywhere by using either a web browser or FTP software.

To set up the FTP server:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Click **USB Storage** under *Apps*. The *USB Storage* screen opens.
3. Click the **FTP Server** tab.



USB Storage

Connect a USB storage device to your network and configure how users can access its contents.

☑ Show widget on the homepage

FTP (File Transfer Protocol) lets you access content on your storage device from any computer on the Internet. You can use a web browser or FTP software to access the content.

Enable FTP Server

Used to access the storage device over the Internet.

OFF

FTP Port

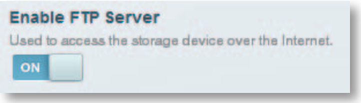
Port 21

FTP Server Name: HappyBunny

Encoding

UTF-8

4. Click the setting for **Enable FTP Server** to turn it on.

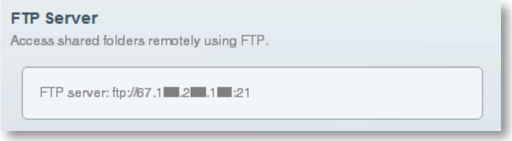


Enable FTP Server

Used to access the storage device over the Internet.

ON

5. We recommend that you keep the default settings for **FTP Port** and **Encoding**, unless you are an advanced user and have reason to change them.
6. Click **OK**.
7. Click the **Status** tab.
8. Note the information under *FTP Server*. This is the information you will need to access the attached storage remotely.



FTP Server

Access shared folders remotely using FTP.

FTP server: ftp://67.1[redacted].2[redacted].1[redacted]:21

9. To access the attached storage using a web browser:
   - **a.** Open a web browser.
   - **b.** In the browser's **Address** or **URL** field, type the address that was provided on the *Status* tab above, starting with **ftp://**... If you have *DDNS* (Dynamic Domain Name Service), you can use your router's domain name instead.
   - **c.** Enter your user account name and password. This is the same User Name and Password that were set up in the shared folders *Authorized users* list. See "How to set up authorized users and shared folders" on page 42.

     The drive's contents (files and folders) appear in a browser window.
   - **d.** Click a file to download it to your computer, or click and drag a file from your computer's file manager to the browser window to upload a file (only if you have read and write access).
10. To access the attached storage using FTP client software:
    - **a.** Run your FTP client software.
    - **b.** Refer to the software's help to determine how to connect to an FTP site. Use the following information to connect:
      - The address that was provided on the *Status* tab above, starting with **ftp://**... If you have *DDNS* (Dynamic Domain Name Service), you can use your router's domain name instead.
      - The user account name and password. This is the same User Name and Password that were set up in the shared folders *Authorized users* list. See "How to set up authorized users and shared folders" on page 42.
      - The port and encoding specified during your FTP server setup (usually port 21, and UTF-8 encoding)
    - **c.** Refer to the software's help to determine how to download and upload files.

TIPS

FTP software and web browsers display FTP content in many ways, but you can usually use these common actions to navigate through FTP folders:

- Click a folder name to open it.
- Click a double period (..) or **Up to a higher level directory** to open a parent folder.
- Click or right-click a file to download or view it.
- Drag a file from another window and drop it into the FTP window to upload it. (To upload a file, your user account must have write access.)

Port Forwarding and Port Triggering

How to set up port forwarding

Why would I use port forwarding? Port forwarding is a feature that forwards inbound traffic from the Internet on a specific port or ports to a specific device or port on your local network. You can set up port forwarding for:

- A single port (see "How to set up port forwarding for a single port" below)
- Multiple ports (see "How to set up port forwarding for multiple ports" on page 49)
- A range of ports (see "How to set up port forwarding for a range of ports" on page 49)

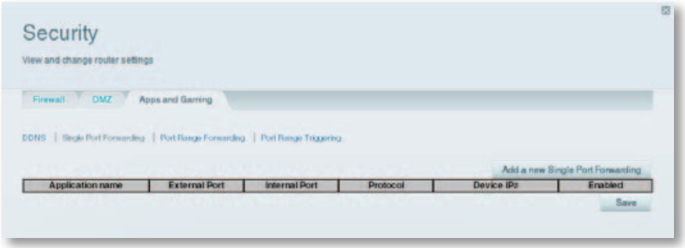
How to set up port forwarding for a single port

Why would I use port forwarding for a single port? Single port forwarding is a feature that forwards inbound traffic from the Internet on a specific port to a single device on your local network. An example of single port forwarding would be to forward inbound web requests, typically on port 80, to a web server.

> **TIP**
> See the device's documentation for port and protocol information.

To set up single port forwarding:

1. Follow your device's instructions for configuring it with a static IP address or use DHCP reservation to assign it a permanent address (see "How to set up the DHCP server on your router" on page 28).
2. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
3. Under **Router Settings,** click **Security**.
4. Click the **Apps and Gaming** tab.
5. Click **Single Port Forwarding**. The *Single Port Forwarding* screen opens.



Security

View and change router settings

Firewall | DMZ | Apps and Gaming

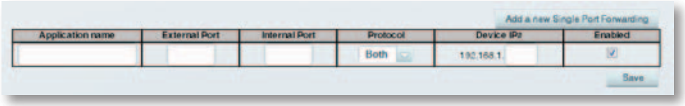
DDNS | Single Port Forwarding | Port Range Forwarding | Port Range Triggering

Add a new Single Port Forwarding

Application name	External Port	Internal Port	Protocol	Device IP#	Enabled

Save

6. Click **Add a new Single Port Forwarding**.



Add a new Single Port Forwarding

Application name	External Port	Internal Port	Protocol	Device IP#	Enabled
			Both	192.168.1.	☑

Save

7. In the **Application name** field, enter a descriptive name.
8. In the **External Port** field, type the external port number (not always required).
9. In the **Internal Port** field, type the internal port number (not always required).
10. In the **Protocol** drop-down list, select **TCP**, **UDP**, or **Both** (default).
11. In the **Device IP#** field, enter the last three digits of the IP address you have reserved for the computer you want to forward Internet traffic to. The rest of the IP address has already been completed for you.
12. Select **Enabled**, then click **Save**. If you don't want to use port forwarding but want to keep the information in the table, unselect the checkbox.

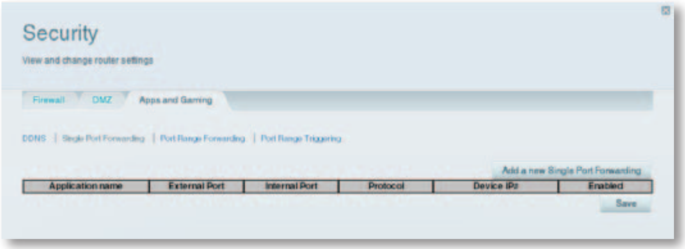
How to set up port forwarding for multiple ports

Why would I set up port forwarding for multiple ports? Port forwarding is a feature that forwards inbound traffic from the Internet on a specific port to a single device on your local network. Unlike a web camera that typically only requires a single port to be forwarded, some applications require forwarding of multiple ports. *VNC* (Virtual Network Computing) software that allows you to operate your computer remotely from anywhere on the Internet is an example of an application that requires multiple ports to be forwarded. To forward to multiple ports, just create additional entries to forward additional ports to the same IP address.

Example: You want to set up your computer so you can remotely access it using VNC software. By default, VNC uses TCP ports 5800 and 5900.

To set up single port forwarding for multiple ports:

1. Make sure that the software you want to use has been installed onto a networked computer.
2. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
3. Set up DHCP reservation for the IP address of the computer on which you installed the software. (See "How to set up the DHCP server on your router" on page 28).
4. Under **Router Settings,** click **Security**.
5. Click the **Apps and Gaming** tab.
6. Click **Single Port Forwarding**. The *Single Port Forwarding* screen opens.



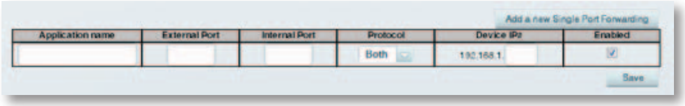
Security

View and change router settings

Firewall
DMZ
Apps and Gaming
DDNS | Single Port Forwarding | Port Range Forwarding | Port Range Triggering
Add a new Single Port Forwarding
Save

Application name	External Port	Internal Port	Protocol	Device IP#	Enabled

7. Click **Add a new Single Port Forwarding**.



Application name	External Port	Internal Port	Protocol	Device IP#	Enabled
			Both	192.168.1.	☑

8. In the **Application name** field, enter a descriptive name.
9. Enter in the same port number for the **External Port** and the **Internal Port**.
10. In the **Protocol** drop-down list, select **TCP**, **UDP**, or **Both** (default).
11. In the **Device IP#** field, enter the last three digits of the IP address you have reserved for the computer you want to forward Internet traffic to. The rest of the IP address has already been completed for you.
12. Select **Enabled**, then click **Save**. If you don't want to use port forwarding but want to keep the information in the table, unselect the checkbox.

> **NOTE**
> If you want to use software such as VNC on multiple computers, you will need to reconfigure the default ports that VNC uses on each additional computer. Then, create additional port forwarding entries for each additional computer. See your software's documentation for help.

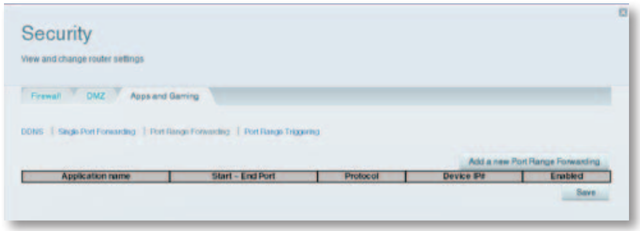
How to set up port forwarding for a range of ports

Why would I set up port forwarding for a range of ports? Port forwarding is a feature that forwards inbound traffic from the Internet on a range of ports to a single device on your local network. Unlike a web camera that typically only requires a single port to be forwarded, some applications require forwarding to a range of ports.

Example: You want to set up your computer so you can use BitTorrent, a popular peer-to-peer file sharing application. BitTorrent uses port 6881 by default. If that port is busy, the requesting BitTorrent client tries the next port in sequence. The most common configuration for home routers with a single BitTorrent computer is to set up port forwarding using a range of ports starting with 6881 and ending with port 6889.

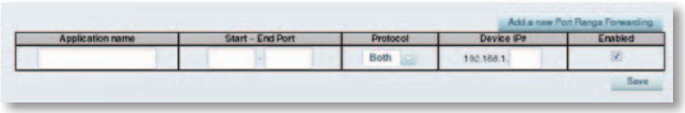
To set up port range forwarding:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Set up a DHCP reservation for the IP address of the computer on which you installed the software. (See "How to set up the DHCP server on your router" on page 28). In this example, the IP address of the desktop computer with BitTorrent installed is 192.168.1.140.
3. Under **Router Settings,** click **Security**.
4. Click the **Apps and Gaming** tab.
5. Click **Port Range Forwarding**. The *Port Range Forwarding* screen opens.



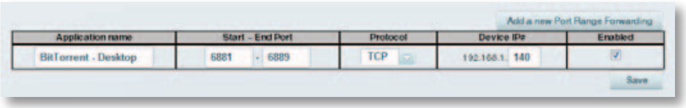
Application name	Start ~ End Port	Protocol	Device IP#	Enabled

6. Click **Add a new Port Range Forwarding**.



Application name	Start ~ End Port	Protocol	Device IP#	Enabled
	-	Both	192.168.1.	☑

7. In the **Application name** field, enter a descriptive name.
8. In the **Start ~ End Port** fields, enter the range or ports. In this example, the range is **6881** to **6889**.



Application name	Start ~ End Port	Protocol	Device IP#	Enabled
BitTorrent - Desktop	6881 - 6889	TCP	192.168.1. 140	☑

9. Select **TCP** as the protocol.
10. In the **To IP Address** field, enter the last 3 digits of the IP address of the device running the software. The rest of the IP address fields already completed. In this example, you would enter **140**.
11. Select **Enabled**, then click **Save**. If you don't want to use port range forwarding but want to keep the information in the table, unselect the checkbox.

TIPS
To use software like BitTorrent on multiple computers on your network, create additional entries with a unique range of ports as shown above. BitTorrent works only with ports between 6881 and 6999.

Depending on your computer's firewall software, you may need to open a range of ports in your firewall to enable software that uses port range forwarding.

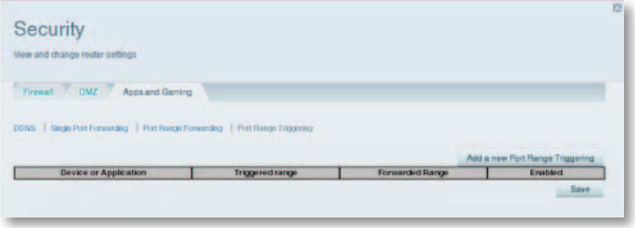
How to set up port range triggering for online gaming

Why would I use port triggering instead of port forwarding? Port range triggering 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 routed back to the proper computer. An example of port range triggering would be to enable a USB or Bluetooth headset for online chat and gaming.

To set up port range triggering for multiple entries:

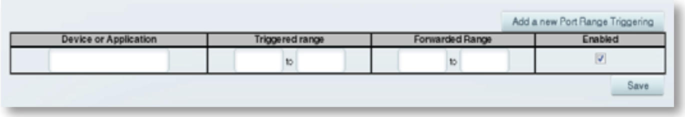
1. See your device documentation for information on the ports that the device uses.
2. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.

3. Under **Router Settings,** click **Security**.
4. Click the **Apps and Gaming** tab.
5. Click **Port Range Triggering**. The *Port Range Triggering* screen opens.


Security
View and change router settings
Firewall
DMZ
Apps and Gaming
DDNS | Single Port Forwarding | Port Range Forwarding | Port Range Triggering
Add a new Port Range Triggering
Save

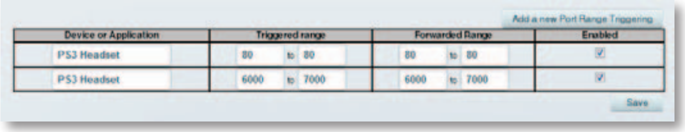
Device or Application	Triggered range	Forwarded Range	Enabled

6. Click **Add a new Port Range Triggering**.



Device or Application	Triggered range	Forwarded Range	Enabled
	to	to	☑

7. In the **Device or Application** field, enter a descriptive name (such as *PS3 Headset*).
8. For single ports, enter the same port number in each **Triggered range** and **Forwarded range** field.
9. For port ranges, enter the same number ranges in each set of **Triggered Range** and **Forwarded Range** fields.



Device or Application	Triggered range	Forwarded Range	Enabled
PS3 Headset	80 to 80	80 to 80	☑
PS3 Headset	6000 to 7000	6000 to 7000	☑

10. Select **Enabled**, then click **Save**. If you don't want to use port range triggering but want to keep the information in the table, unselect the checkbox.

Maintaining and Monitoring

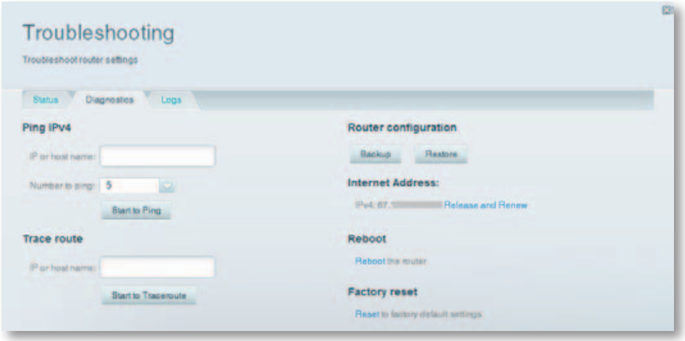
How to back up and restore your router configuration

Why do I need to back up my router configuration? As with any valuable data, you should back up your router configuration. Your router might contain many customized settings. Those settings would be lost if you reset your router to its factory defaults, and you would need to re-enter all of them manually. If you back up your router configuration, restoring settings is easy.

> **NOTE**
> You can only back up the router configuration locally (not remotely).

To back up your router configuration:

1. Log into Cisco Connect Cloud. (See “How to configure your router” on page 11.
2. Under **Router Settings,** click **Troubleshooting**.
3. Click the **Diagnostics** tab.

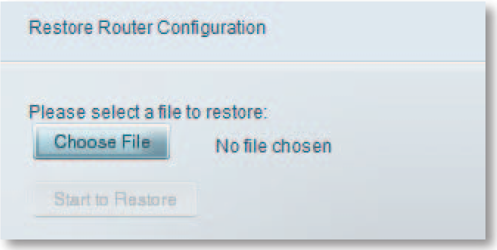


4. Under *Router configuration*, click **Backup**. You are prompted to save the file.
5. Specify a file location, then click **Save**.

> **TIP**
> For save multiple backup files, include the backup date in the filename as you save.

To restore your router configuration:

1. Log into Cisco Connect Cloud. (See “How to configure your router” on page 11.
2. Under **Router Settings,** click **Troubleshooting**.
3. Click the **Diagnostics** tab.
4. Under **Router configuration**, click **Restore**. The *Restore Router Configuration* dialog box opens.


Restore Router Configuration
Please select a file to restore:
Choose File
No file chosen
Start to Restore

5. Click **Choose File** to navigate to the location of your configuration file, then select the file and click **Open**.
6. To restore the configuration, click **Start to Restore**.

How to upgrade the router’s firmware

Why would I need to upgrade my router’s firmware? Linksys may periodically publish a firmware upgrade either to fix a problem or to add features to your router.

> **IMPORTANT**
> Do not interrupt the upgrade process. You should not turn off the router or press the Reset button during the upgrade. Doing so may permanently disable the router.

> **TIPS**
> Your router automatically checks for available updates and installs them by default. Use the following instructions only if the automatic firmware update has been turned off.

To upgrade the router’s firmware:

1. Log into Cisco Connect Cloud. (See “How to configure your router” on page 11.
2. Under **Router Settings,** click **Connectivity**.
3. Click the **Basic** tab.
4. Under **Firmware Update**, click **Check for Updates**.
5. If an available update is found, follow the on-screen instructions to install it.

> **TIP**
> To have your router automatically check for updates and install them, select **Automatic** under **Firmware Update.**

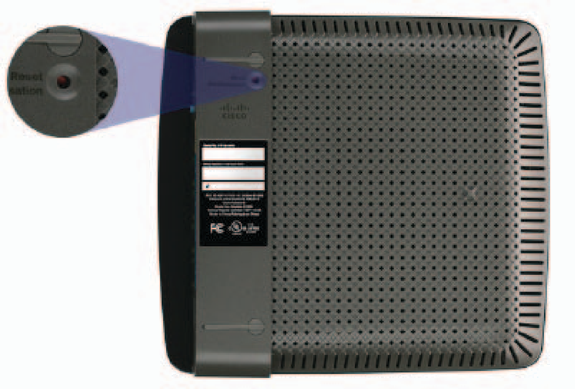
How to restore factory defaults

If you’ve tried previous troubleshooting steps and your network still doesn’t work, you may need to restore your router’s factory defaults. To restore your router to factory defaults, you can use the *Reset* button on the router or use Cisco Connect Cloud.

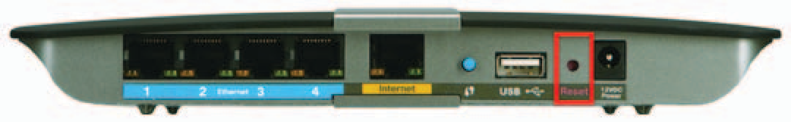
To reset your router using the reset button:

> **CAUTION**
> Whenever you restart the router, all logs that are not saved will be lost.

1. With your router connected to power and turned on, press and hold the **Reset** button on the bottom or back of your router for about 15 seconds (until the power indicator flashes).



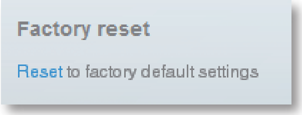
EA2700 and EA3500 Reset button



EA4500 Reset button

To reset your router to factory defaults using Cisco Connect Cloud:

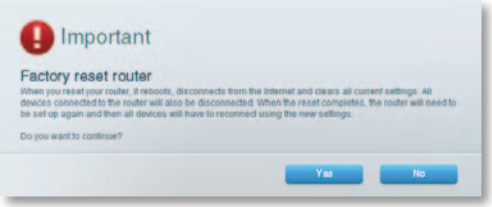
1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Router Settings,** click **Troubleshooting**.
3. Click the **Diagnostics** tab.
4. Under **Factory reset**, click **Reset**.



Factory reset

Reset to factory default settings

A confirmation screen opens.



Important

Factory reset router

When you reset your router, it reboots, disconnects from the Internet and clears all current settings. All devices connected to the router will also be disconnected. When the reset completes, the router will need to be set up again and then all devices will have to reconnect using the new settings.

Do you want to continue?

5. Click **Yes** to confirm. All settings and logs are deleted, and your router is returned to its factory default settings.

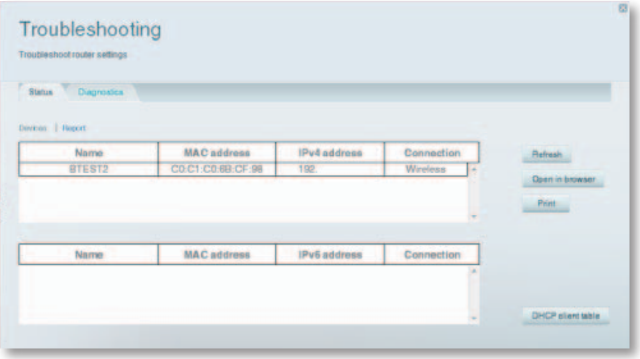
How to check the status of your router

Why would I want to check the status of my router? Your router status tells you whether you have a secure Internet connection and informs you about the status of your network-connected devices.

To check your router status:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Router Settings,** click **Troubleshooting**.
3. Click the **Status** tab. Detailed information about your router status is displayed.

TIP
For field descriptions, click **Help** at the top of the screen.



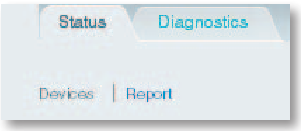
Troubleshooting

Troubleshoot router settings

Name	MAC address	IPv4 address	Connection
BTEST2	C0:C1:C0:6B:CF:98	192.	Wireless

Name	MAC address	IPv6 address	Connection

4. To view a list of connected network devices, click **Devices**. To view a full report of your router status, click **Report**.



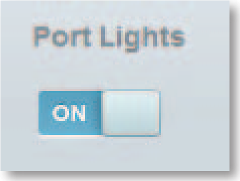
5. Click **OK** to close the screen.

How to disable the Ethernet port status lights

Why would I want to disable the Ethernet port status lights? Depending on the placement of the router in a home, you might find the lights distracting. You can easily disable the lights using Cisco Connect Cloud.

To disable the lights:

1. Log into Cisco Connect Cloud. (See “How to configure your router” on page 11.
2. Under **Router Settings,** click **Connectivity**.
3. Click the **Basic** tab.
4. Under **Port Lights**, click the **ON**/**OFF** button.

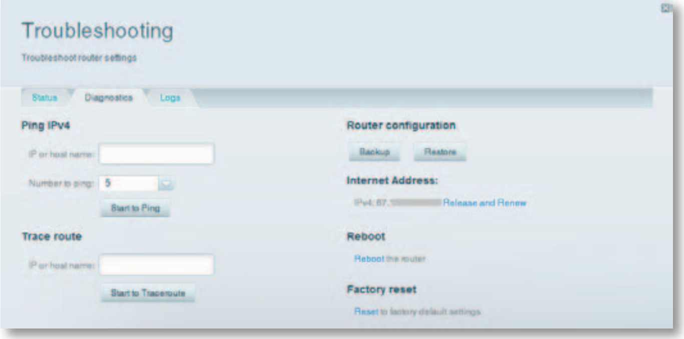


How to test your Internet connection

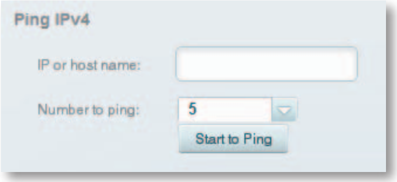
What utilities are included in my router to test my Internet connection? Your router includes two diagnostic tests, Ping and Traceroute, that let you check network connections, including network devices and your Internet connection.

To diagnose your Internet connection:

1. Log into Cisco Connect Cloud. (See “How to configure your router” on page 11.
2. Under **Router Settings,** click **Troubleshooting**.
3. Click the **Diagnostics** tab.

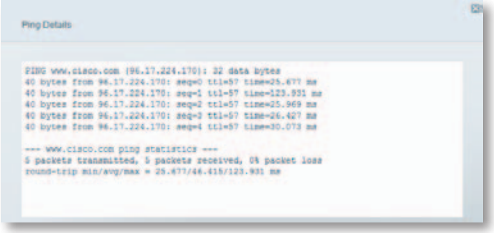


4. To check whether an address can be reached:
   a. Under **Ping IPv4**, enter an IP address or URL into the **IP or host name** field.



b. Select a number of times to ping from the **Number to ping** drop-down list.

c. Click **Start to Ping**. A window opens showing the ping test results. You will see a response for each successful ping.



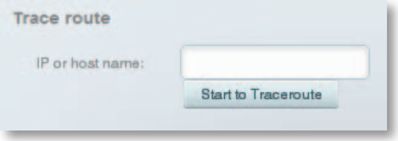
```
PING www.cisco.com (96.17.224.170): 32 data bytes
40 bytes from 96.17.224.170: seq=0 ttl=57 time=25.677 ms
40 bytes from 96.17.224.170: seq=1 ttl=57 time=123.931 ms
40 bytes from 96.17.224.170: seq=2 ttl=57 time=25.969 ms
40 bytes from 96.17.224.170: seq=3 ttl=57 time=26.427 ms
40 bytes from 96.17.224.170: seq=4 ttl=57 time=30.073 ms

--- www.cisco.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 25.677/46.415/123.931 ms
```

NOTE

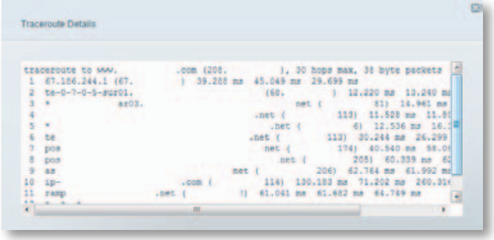
If an Internet URL fails to respond to ping, it doesn't necessarily mean that the site is down. For security reasons, some sites are configured to not respond to ping requests.

5. To trace the route that packets take between your router and a specific address:

   a. Under **Trace route**, enter an address in the **IP or host name** field.



   b. Click **Start to Traceroute**. A window opens with the test results.



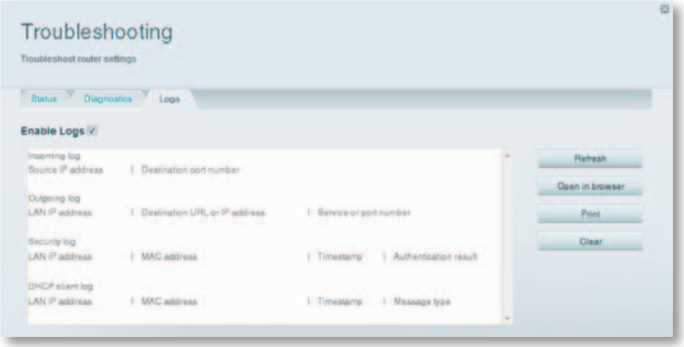
```
traceroute to www.          .com (208.          ), 30 hops max, 38 byte packets
 1  67.186.244.1 (67.          )  39.288 ms  45.049 ms  29.699 ms
 2  te-0-7-0-5-sur01.                            (68.          )  12.220 ms  13.240 ms
 3  *              ar03.                                net (            81)  14.961 ms
 4                                          .net (            113)  11.528 ms  11.8
 5  *                                          .net (            6)  12.536 ms  16.
 6  te                                        .net (          113)  30.244 ms  26.299
 7  pos                                        net (          174)  40.540 ms  58.0
 8  pos                                          .net (          205)  60.339 ms  6
 9  as                                  net (            206)  62.764 ms  61.992 ms
10  ip-                        .com (          114)  130.183 ms  71.202 ms  260.31
11  ramp                  .net (            !)  61.041 ms  61.682 ms  64.749 ms
```

How to configure and use logs

What kind of logging capabilities does my router have? Your router can track all traffic for your Internet connection and record that information in a *log*.

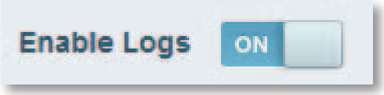
To enable and view logs:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11.
2. Under **Router Settings,** click **Troubleshooting**.
3. Click the **Logs** tab.



```
Incoming log
Source IP address     | Destination port number

Outgoing log
LAN IP address        | Destination URL or IP address     | Service or port number

Security log
LAN IP address        | MAC address                       | Timestamp  | Authentication result

DHCP client log
LAN IP address        | MAC address                       | Timestamp  | Message type
```

4. To enable logs, click the **Enable Logs** button so that **ON** is displayed.



You can:

- View the logs directly in the list
- Open the logs in a separate browser window
- Print the logs

Troubleshooting

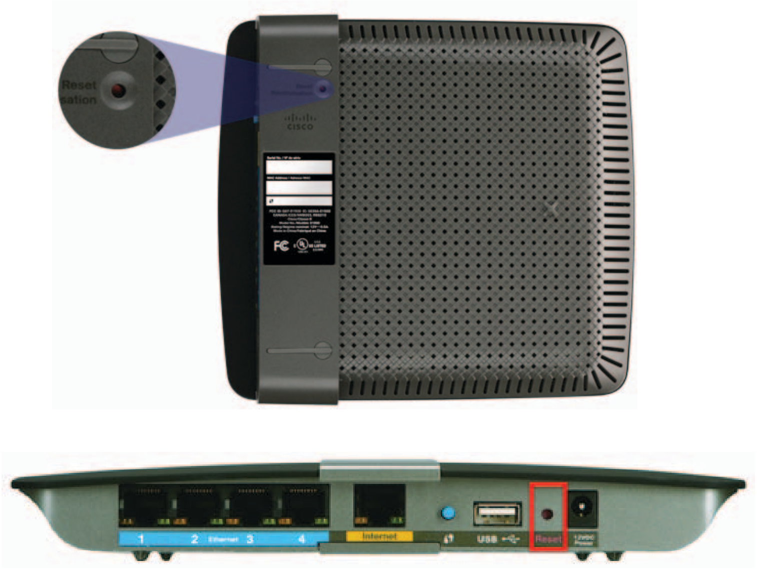
This chapter can help you solve common setup issues and connect to the Internet. You can find more help from our award-winning customer support at **linksys.com/support**.

During setup

Your router was not successfully set up

If Setup did not complete, you can try the following:

- Press and hold the **Reset** button on your router with a paperclip or pin for about 15 seconds (until the power indicator flashes), then run the **Setup** program again on the router's CD.



Your router's appearance may vary

- Temporarily disable your computer's firewall (see the security software's instructions for help), then run the **Setup** program again on the router's CD.
- If you have another computer, use that computer to run the **Setup** program again on the router's CD.

Windows XP Service Pack update

On Windows XP computers, Setup requires Service Pack 3 in order to work. If the currently installed Service Pack is older than version 3, you need to download and install Service Pack 3 before installing your router.

> **TIP**
> To temporarily connect to the Internet and download the required Service Pack, you can use the included Ethernet cable to connect your computer directly to your modem.

To install Service Pack 3:

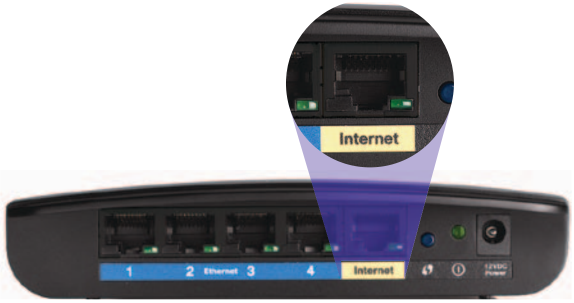
1. Connect to the Microsoft Update website (**update.microsoft.com/windowsupdate**).
2. Follow the instructions on the website or contact Microsoft if you need further help.
3. After downloading and installing Service Pack 3, run the **Setup** program on your router's CD.

Your Internet cable is not plugged in message

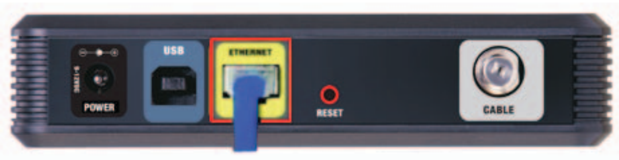
If you get a "Your Internet cable is not plugged in" message when trying to set up your router, follow these troubleshooting steps.

To fix the problem:

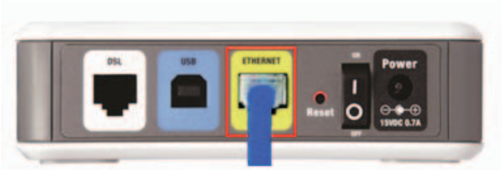
1. Make sure that an Ethernet or Internet cable (or a cable like the one supplied with your router) is securely connected to the yellow **Internet** port on the back of the router and to the appropriate port on your modem. This port on the modem is usually labeled **Ethernet**, but may be named **Internet** or **WAN**.



Back view of router



Back view of cable modem



Back view of DSL modem

2. Make sure that your modem is connected to power and is turned on. If it has a power switch, make sure that it is set to the **ON** or **I** position.
3. If your Internet service is cable, verify that the cable modem's **CABLE** port is connected to the coaxial cable provided by your ISP.

   Or, if your Internet service is DSL, make sure that the DSL phone line is connected to the modem's **DSL** port.
4. If your computer was previously connected to your modem with a USB cable, disconnect the USB cable.
5. Run the **Setup** program again on the router's CD.

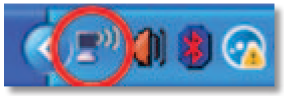
Cannot access your router message

If you cannot access your router because your computer is not connected to your network, follow these troubleshooting steps.

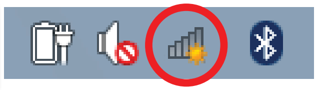
To access your router, you must be connected to your own network. If you currently have wireless Internet access, the problem may be that you have accidentally connected to a different wireless network.

To fix the problem on Windows computers:

1. On your Windows desktop, click or right-click the wireless icon in the system tray.

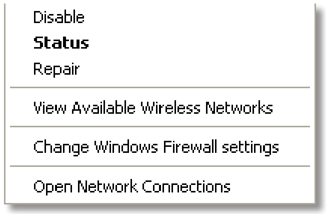


Windows XP



Windows 7

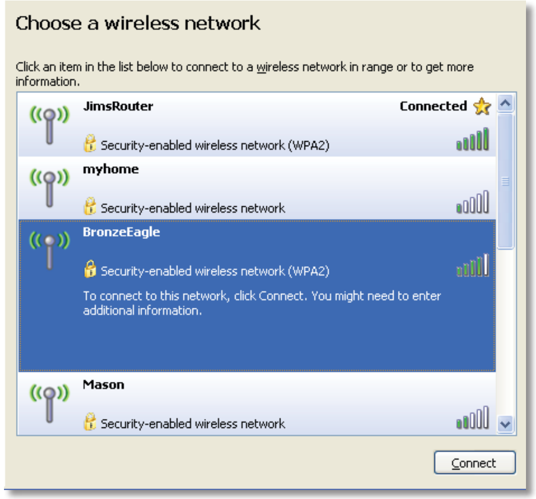
2. Click **View Available Wireless Networks**. A list of available networks appears.



Disable
Status
Repair
View Available Wireless Networks
Change Windows Firewall settings
Open Network Connections

3. Click your own network name, then click **Connect**. In the example below, the computer was connected to another wireless network named *JimsRouter*. The name of the Linksys E-Series network, *BronzeEagle* in this example, is shown selected.

TIP
If you don't see the network name (SSID) you specified during setup, select the name **Cisco***xxxxx* where *xxxxx* is the last five digits of the router's serial number. You can find the router's serial number on the bottom of the router.



Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

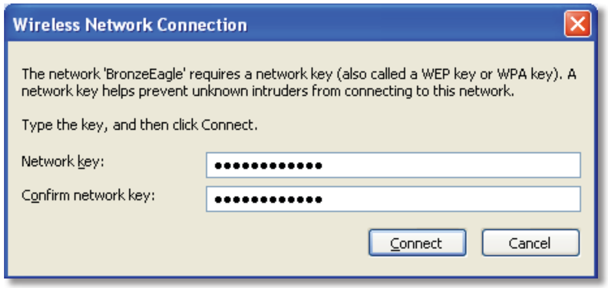
JimsRouter — Connected ☆
Security-enabled wireless network (WPA2)

myhome
Security-enabled wireless network

BronzeEagle
Security-enabled wireless network (WPA2)
To connect to this network, click Connect. You might need to enter additional information.

Mason
Security-enabled wireless network

4. If you are prompted to enter a network key, type your password (Security Key) into the **Network key** and **Confirm network key** fields, then click **Connect**.



Wireless Network Connection

The network 'BronzeEagle' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key: ••••••••••••

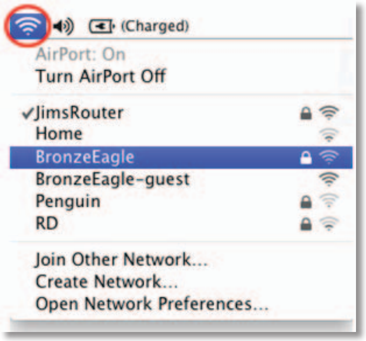
Confirm network key: ••••••••••••

Your computer connects to the network, and you should now be able to access the router.

To fix the problem on Mac computers:

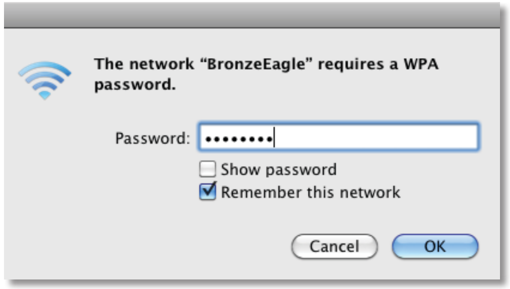
1. In the menu bar across the top of the screen, click the **AirPort** icon. A list of wireless networks appears. Cisco Connect has automatically assigned your network a name.

   In the example below, the computer was connected to another wireless network named *JimsRouter*. The name of the Linksys E-Series network, *BronzeEagle* in this example, is shown selected.



2. Click the wireless network name of your Linksys E-Series router (*BronzeEagle* in the example).

3. Type your wireless network password (Security Key) into the **Password** field, then click **OK**.



The network “BronzeEagle” requires a WPA password.

Password: ••••••••

□ Show password

☑ Remember this network

After setup

The Internet appears to be unavailable

If the Internet has difficulty communicating with your router, the problem may appear as a “Cannot find [Internet address]” message in your web browser. If you know that the Internet address is correct, and if you’ve tried several valid Internet addresses with the same result, the message could mean that there’s a problem with your ISP or modem communicating with your router.

Try the following:

- Make sure that the network and power cables are securely connected.
- Make sure that the power outlet that your router is connected to has power.
- Reboot your router.
- Contact your ISP and ask about outages in your area.

Why would I need to reboot my router? The most common method of troubleshooting your router is to turn off your router’s power, then turn it back on again. Your router can then reload its custom settings, and other devices (such as the modem) will be able to “rediscover” the router and communicate with it. This process is called *rebooting*.

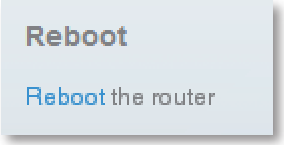
Rebooting your router

To reboot your router using the power cord:

1. Disconnect the power cord from the router and the modem.
2. Wait 10 seconds, then reconnect the power cord to the modem. Make sure it has power.
3. Wait until the modem’s Online indicator has stopped flashing, or wait two minutes, then reconnect the power cord to the router.
4. Wait until the power indicator stops flashing, then wait two minutes before trying to connect to the Internet from a computer.

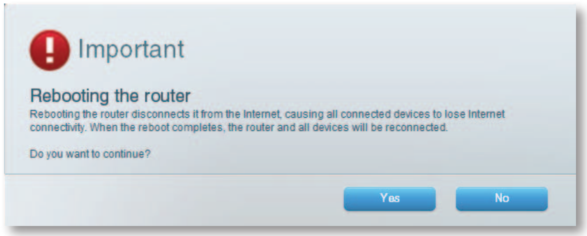
To reboot your router using Cisco Connect Cloud:

1. Log into Cisco Connect Cloud. (See “How to configure your router” on page 11.
2. Under **Router Settings,** click **Troubleshooting**.
3. Click the **Diagnostics** tab.
4. Under **Reboot**, click **Reboot**.



Reboot

A confirmation screen opens.



Important

Rebooting the router

Rebooting the router disconnects it from the Internet, causing all connected devices to lose Internet connectivity. When the reboot completes, the router and all devices will be reconnected.

Do you want to continue?

5. Click **Yes** to confirm. The router reboots. While the router is rebooting, all connected devices will lose their Internet connection.

Cisco Connect Cloud does not open in your web browser

The latest versions of the most common web browsers work with Cisco Connect Cloud. Cisco Connect Cloud works with these web browsers:

- Internet Explorer 8 or higher
- Firefox 8 or higher
- Google Chrome 10 or higher
- Safari 5 (for Mac) or higher

You cannot access Cisco Connect Cloud

To access your router directly, see “How to manually set up your router” on page 22:

All other troubleshooting has been unsuccessful

If you’ve tried previous troubleshooting steps and your network still doesn’t work, you may need to restore your router’s factory defaults.

Why would I need to restore to factory defaults? When all other troubleshooting has failed, you may want to try restoring the router to its basic factory settings, which are the most common settings used in home networks. Resetting the router erases your custom settings, so you must restore the settings after. We recommend that you back up your configuration before resetting your router to factory defaults. See “How to back up and restore your router configuration” on page 52.

To restore your router to factory defaults, you can use the *Reset* button on the router or use Cisco Connect Cloud. For instructions, see “How to restore factory defaults” on page 53.

Specifications

Linksys EA2700

Model Name	Linksys EA2700
Description	Dual-Band N600 Router with Gigabit
Model Number	EA2700
Switch Port Speed	10/100/1000 Mbps (Gigabit Ethernet)
Radio Frequency	2.4 and 5 GHz
# of Antennas	4 (2 per band)
Ports	Power, Internet, and Ethernet (1-4)
Buttons	Reset, Wi-Fi Protected Setup
LEDs	Power/Wi-Fi Protected Setup, Internet, Ethernet (1-4)
UPnP	Supported
Security features	WEP, WPA, WPA2, RADIUS
Security key bits	Up to 128-bit encryption
Browser Support	Internet Explorer 8 or higher, Firefox 8 or higher, Google Chrome 10 or higher, and Safari 5 (for Mac) or higher

Environmental

Dimensions	174 x 190 x 28 mm (6.85" x 7.48" x 1.10")
Unit Weight	297.7 g (10.5 oz)
Power	12V, 1A
Certifications	FCC, IC, CE, Wi-Fi A/B/G/N
Operating Temp.	0 to 40°C (32 to 104°F)
Storage Temp.	-20 to 60°C (-4 to 140°F)
Operating Humidity	10 to 80%, relative humidity, non-condensing
Storage Humidity	5 to 90% non-condensing

NOTES

For regulatory, warranty, and safety information, see the CD that came with your router or go to **Linksys.com/support**.

Specifications are subject to change without notice.

Maximum performance derived from IEEE Standard 802.11 specifications. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions.

Linksys EA3500

Model Name	Linksys EA3500
Description	Dual-Band N750 Router with Gigabit and USB
Model Number	EA3500
Switch Port Speed	10/100/1000 Mbps (Gigabit Ethernet)
Radio Frequency	2.4 and 5 GHz
# of Antennas	6 (3 per band)
Ports	Internet, Ethernet (1-4), USB, Power
Buttons	Reset, Wi-Fi Protected Setup
LEDs	Power, Internet, Ethernet (1-4)
UPnP	Supported
Security features	WEP, WPA, WPA2, RADIUS
Security key bits	Up to 128-bit encryption
Storage File System Support	FAT, and NTFS, and HFS+
Browser Support	Internet Explorer 8 or higher, Firefox 8 or higher, Google Chrome 10 or higher, and Safari 5 (for Mac) or higher

Environmental

Dimensions	6.69" x 0.98" x 7.48" (170 x 25 x 190 mm)
Unit Weight	11.5 oz (326 g)
Power	12V, 2A
Certifications	FCC, IC, CE, Wi-Fi A/B/G/N, Windows 7
Operating Temp.	32 to 95°F (0 to 35°C)
Storage Temp.	-4 to 140°F (-20 to 60°C)
Operating Humidity	10 to 80% relative humidity, non-condensing
Storage Humidity	5 to 90% non-condensing

NOTES

For regulatory, warranty, and safety information, see the CD that came with your router or go to **Linksys.com/support**.

Specifications are subject to change without notice.

Maximum performance derived from IEEE Standard 802.11 specifications. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions.

Linksys EA4500

Model Name	Linksys EA4500
Description	Dual-Band N900 Router with Gigabit and USB
Model Number	EA4500
Switch Port Speed	10/100/1000 Mbps (Gigabit Ethernet)
Radio Frequency	2.4 and 5 GHz
# of Antennas	6 (3 per band)
Ports	Power, USB, Internet, Ethernet (1-4)
Buttons	Reset, Wi-Fi Protected Setup
LEDs	Top panel: Power Back panel: Internet, Ethernet (1-4)
UPnP	Supported
Security Features	WEP, WPA, WPA2, RADIUS
Security Key Bits	Up to 128-bit encryption
Storage File System Support	FAT, and NTFS, and HFS+
Browser Support	Internet Explorer 8 or higher, Firefox 8 or higher, Google Chrome 10 or higher, and Safari 5 (for Mac) or higher

Environmental

Dimensions	8.86" x 0.98" x 6.30" (225 x 25 x 160 mm)
Unit Weight	12.7 oz (360 g)
Power	12V, 2A
Certifications	FCC, IC, CE, Wi-Fi a/b/g/n, Windows 7, DLNA
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, non-condensing
Storage Humidity	5 to 90% non-condensing

NOTES

For regulatory, warranty, and safety information, see the CD that came with your router or go to **Linksys.com/support**.

Specifications are subject to change without notice.

Maximum performance derived from IEEE Standard 802.11 specifications. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions.

Visit linksys.com/support for award-winning 24/7 technical support