



User Guide



Linksys EA6500

Contents

Product Overview

EA6500	1
------------------	---

Setting Up: Basics

How to create a home network.	4
What is a network?	4
How to set up a home network	4
Where to find more help.	4
How to install your router	5
How to configure your router.	6
How to connect to Cisco Connect Cloud	6
How to connect directly to your router	6
How to improve your wireless connection speed	6
How to change your network's name and password	7
How to change your router password	8
How to change your router's time zone	8
How to test your Internet connection speed	8
How to connect devices to your network	9
How to connect a computer to your network	9
How to connect a USB printer	9
How to connect other devices	10
How to view device details	11
How to remove a device from the network	12
How to set up parental controls	13
How to set parental controls	13
How to configure your guest network	14
How to back up your router configuration	15

Setting Up: Advanced

How to manually set up your router.	16
How to manually set up your Internet connection	16
How to get the most out of your dual-band router	16
How to control access to your network.	18
How to improve security using the built-in firewall	19
How to clone a MAC address	20

Port Forwarding and Port Triggering

How to set up port forwarding	22
How to set up port forwarding for a single port	22
How to set up port forwarding for multiple ports	23
How to set up port forwarding for a range of ports	23
How to set up port range triggering for online gaming	24
How to configure your Xbox for online gaming	25

Maintaining and Monitoring

How to back up and restore your router configuration.	27
How to upgrade the router's firmware	28
How to check the status of your router.	28
How to disable the Ethernet port status lights	29
How to test your Internet connection	29

Troubleshooting

During setup	31
Your router was not successfully set up	31
Windows XP Service Pack update	31
<i>Your Internet cable is not plugged in</i> message	32
<i>Cannot access your router</i> message	32
After setup.	34
The Internet appears to be unavailable	34
All other troubleshooting has been unsuccessful	34

Specifications

Linksys EA6500	36
--------------------------	----

Product Overview

EA6500



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

802.11AC technology

Built with leading 802.11AC 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 10x 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

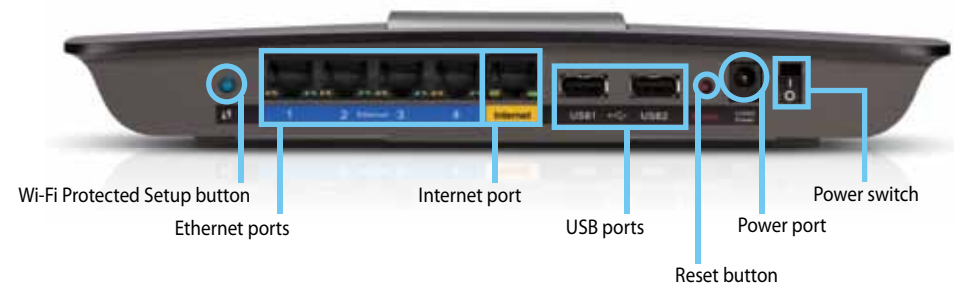
Create a separate, password-protected network for guests.

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. Pulsates slowly during bootup, during firmware upgrades, and during a Wi-Fi Protected Setup connection. Flashes quickly when there is a Wi-Fi Protected Setup error.

Back view

- **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 set up wireless security using Wi-Fi Protected Setup” on page 38.

- **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

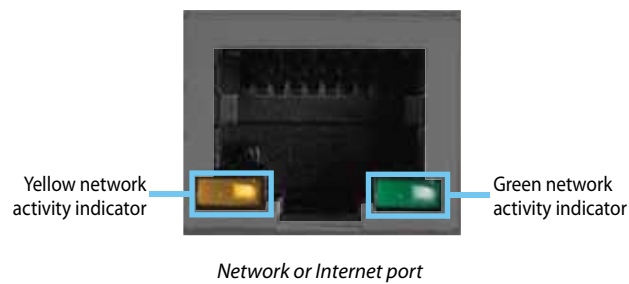
For best performance, use CAT5E or higher rated cables on the Ethernet ports.

- **Internet port**—Connect an Ethernet cable (also called a network or Internet cable) to this port, color coded yellow, and to your modem.
- **USB ports**—To easily share disk storage with other users on your network or on the Internet, connect a USB drive to one of these ports. For more information, see “Using an External Drive” on page 43. 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 9.
- **Reset button**—Press and hold this button for 5-15 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 56.
- **Power port**—Connect the included AC power adapter to this port.
- **Power switch**—Press the top of this switch to turn on your router.

CAUTION

Use only the adapter that came with your router.

Port activity indicators



- **Green network activity 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 5.
4. To connect a computer or other network device to the network, see "How to connect a computer to your network" on page 9 and "How to connect other devices" on page 10.

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)



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.
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.



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	

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 from anywhere in the world.

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.

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.



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**.



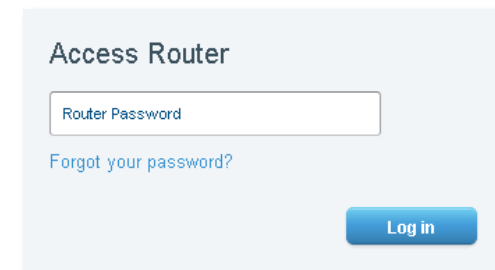
4. Click **OK**.

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. Open your computer's web browser.
2. Go to myrouter.local and log into your router using the router password you created when you installed your router.



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:

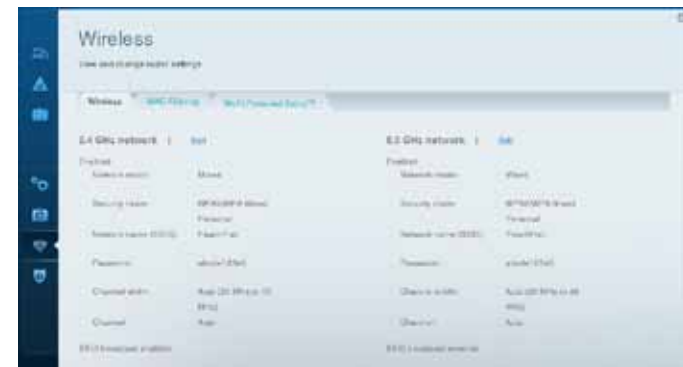
- For the widest coverage area, install your router near the center of your home, and near the ceiling, if possible.
- Avoid placing the router on or near metal objects (such as file cabinets and metal furniture), reflective surfaces (such as glass or mirrors), or masonry walls.
- Any obstruction can 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.

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 6.)
2. Under **My Router**, click **Wireless**.



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

Network name (SSID):	<input type="text" value="PeachFish"/>
Password:	<input type="text" value="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.

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

TIP

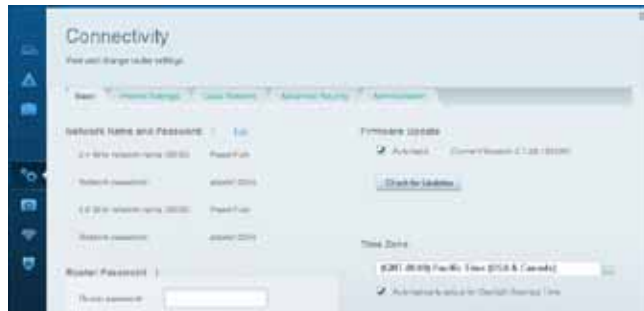
If you have a dual-band router, each band (2.4 GHz and the 5 GHz) can have a separate network name and password.

How to change your router password

Your router's 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.

To change your router password

- Log into Cisco Connect Cloud. (See "How to configure your router" on page 6.
- Click **Connectivity** under *Router Settings*.
- Click the **Basic** tab.
- Under **Router Password**, type the new password, then click **OK**.

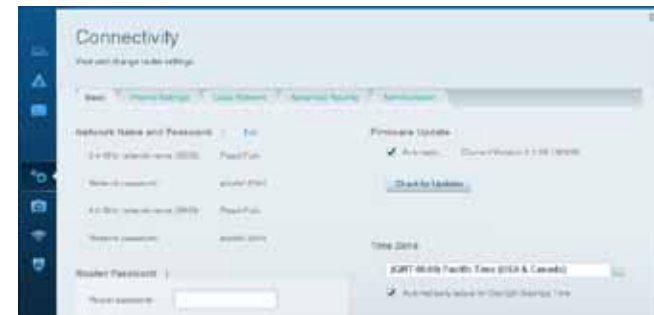


How to change your router's time zone

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

To set your router's time zone:

- Log into Cisco Connect Cloud. (See "How to configure your router" on page 6.
- Click **Connectivity** under *Router Settings*.
- Click the **Basic** tab, then select your time zone in the **Time Zone** drop-down list and click **OK**.



How to test your Internet connection speed

To test your Internet connection speed:

- Log into Cisco Connect Cloud. (See "How to configure your router" on page 6.
- Click **Speed Test** under *Router Settings*. The *Internet speed test* screen opens.
- Follow the on-screen instructions to complete the test.

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.

TIP

You can use the Device List to detect and disconnect unauthorized users on your network.

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 set up wireless security using Wi-Fi Protected Setup" on page 39.

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 6.
2. Click Device List, then click **Add a Device**.



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



4. Follow the on-screen instructions for downloading and installing the VUSB (virtual USB) software for your computer.
5. Log into Cisco Connect Cloud, then click **Device List** to confirm that your router recognizes the new printer.

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 30
- "How to set up port forwarding" on page 22
- "How to set up port range triggering for online gaming" on page 24

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 6.)
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.



- 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**.



- 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.

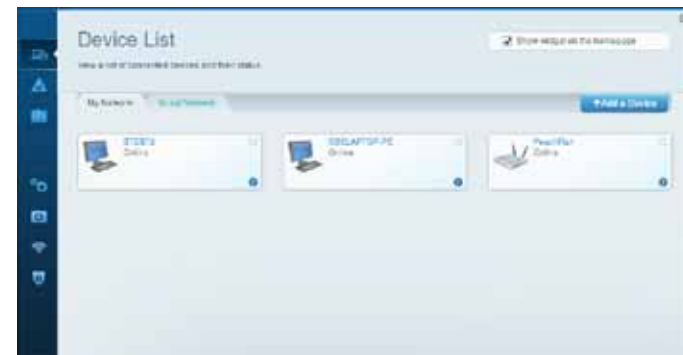


How to view device details

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

To view network device details:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 6.)
2. Under **My Apps**, click **Device List**. The *Device List* screen opens.



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



Information about the device appears on the screen.



4. Click **OK**.

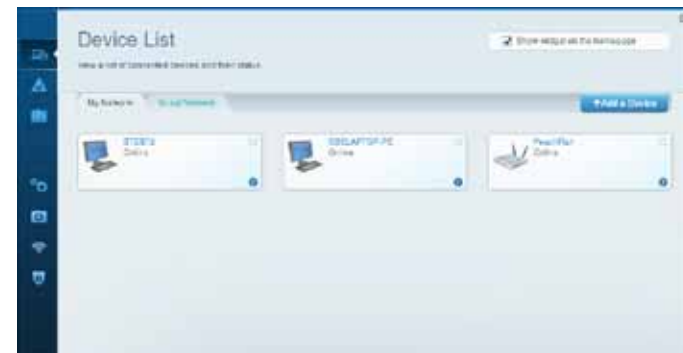
How to remove a device from the network

You can remove a networked device in several ways:

- Unplug its network cable (if attached)
- Turn off its wireless connection (if active)
- Remove it using Cisco Connect Cloud

To remove a connected device by using Cisco Connect Cloud:

1. Log into Cisco Connect Cloud. (See "How to configure your router" on page 6.)
2. Under **My Apps**, click **Device List**. The *Device List* screen opens.



3. Click the **x** in the upper-right corner of the device you want to disconnect.



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.

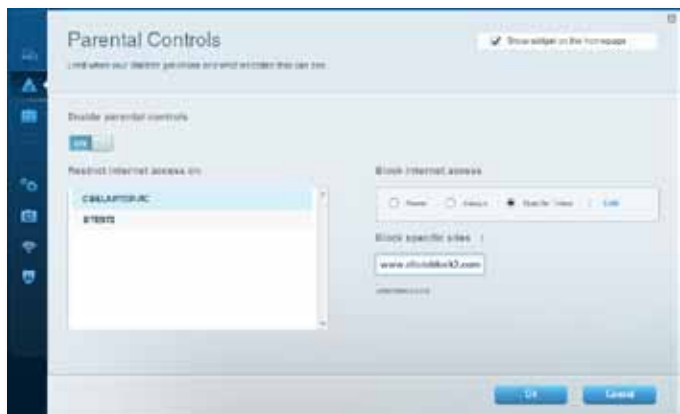
TIP

When someone tries to open a blocked website, a window opens asking for the parental controls password. Enter the password to view the blocked content.

How to set parental controls

To set parental controls:

1. Log into Cisco Connect Cloud. (See “How to configure your router” on page 6.
2. Under **My Apps**, click **Parental Controls**. The *Parental Controls* screen opens.



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

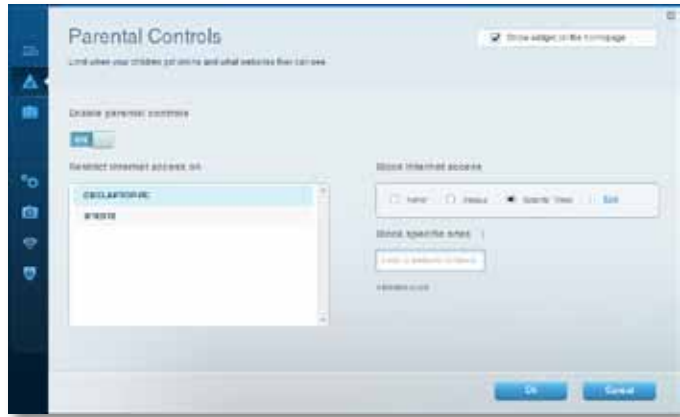
TIP

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.



6. To block specific websites:
 - a. Under **Block specific sites**, click **Add**.



- b. Type the web address (URL) of the website to block, then click **OK**.

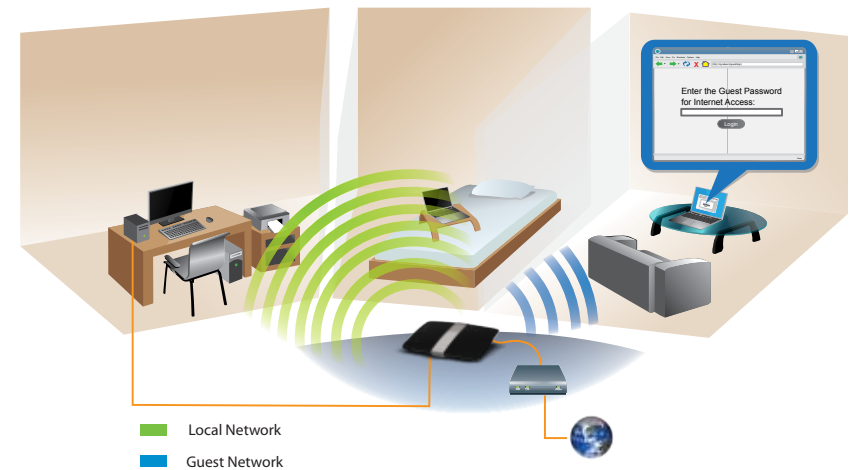
TIP

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.



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 6.
2. Under **My Apps**, click **Guest Access**. Your guest network, which was set up during your router installation, is displayed.



- To turn guest access on or off, click the **Allow guest access** button.
- 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**.



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 27.

To back up your router configuration:

1. Log into Cisco Connect Cloud. (See “How to configure your router” on page 6.
2. Under **Router Settings**, click **Troubleshooting**.
3. Click the **Diagnostics** tab.
4. Under **Router configuration**, click **Backup**.



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. Open a web browser on the computer and go to **myrouter.local**.
4. Enter **admin** as the user name, then enter the default password (**admin**). The main menu opens.
5. 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. Open your computer's web browser.

3. Go to **myrouter.local** and log into your router using the default router password, **admin**.
4. Under *Router Settings*, click **Connectivity**. The *Connectivity* page opens.
5. Click the **Basic** tab.
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**.

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. If you are connecting to your router with a computer that has a dual-band wireless network adapter, you might not be able to determine which band you're using. 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.

3. Click the **Wireless** tab, then click **Edit** next to the network band you want to modify. Change any of the settings below:

- a. **Enabled**—Unselect this checkbox to disable the network band.
- b. **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-A Only** (802.11a only)
- **Wireless-N Only** (802.11n only)

On the 2.4 GHz band, you can select:

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

- c. **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 WPA2-Personal security mode for best performance.

- d. **Network name (SSID)**—You can provide a unique SSID for each band of your wireless network. The name must not exceed 32 characters.

- e. **Password**—You can provide a unique password for each band of your wireless network.
- 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, unselect 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.

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.

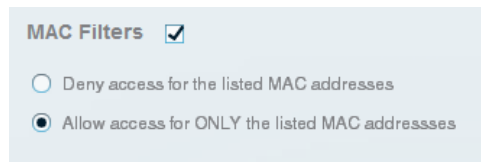
To set up MAC filtering to allow one wireless device access to your network:

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.



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



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



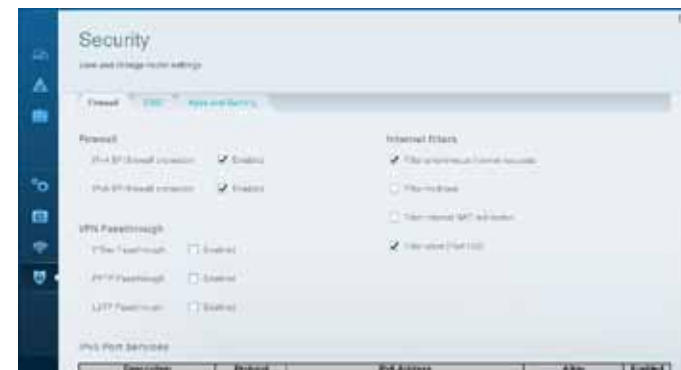
How to improve security using the built-in firewall

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.

General 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.
3. Click the **Firewall** tab.



4. Modify each setting that you want to change.

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**—
 - **PPTP Passthrough**—
 - **L2TP Passthrough**—
- **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.

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

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.



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

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 23)
- A range of ports (see “How to set up port forwarding for a range of ports” on page 23)

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.

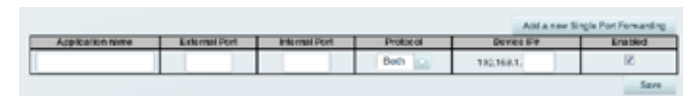
To set up single port forwarding:

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 27).
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.



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



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.

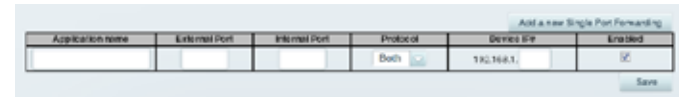
Example: You want to set up your computer so you can remotely access it using VNC software. By default, VNC uses TCP ports 5800 and 5900.

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 27).
4. Under **Router Settings**, click **Security**.
5. Click the **Apps and Gaming** tab.
6. Click **Single Port Forwarding**. The *Single Port Forwarding* screen opens.



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



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:

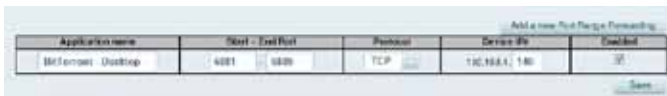
1. Log into Cisco Connect Cloud. (See “How to configure your router” on page 11.)
2. Set up a DHCP reservation for the IP address of the computer on which you installed the software. (See “How to set up the DHCP server on your router” on page 27). In this example, the IP address of the desktop computer 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.



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



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**.



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.)

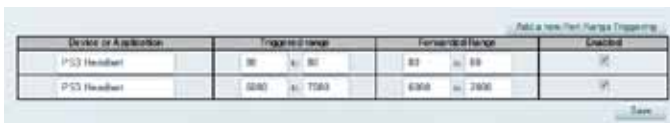
3. Under **Router Settings**, click **Security**.
4. Click the **Apps and Gaming** tab.
5. Click **Port Range Triggering**. The *Port Range Triggering* screen opens.



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



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.



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.

How to configure your Xbox for online gaming

Why would I set up my Xbox for online gaming? Online gaming adds another dimension to using your Xbox. As with other online gaming applications and gaming consoles, you need to forward multiple ports to use your Xbox for online gaming. The procedure for setting up your Xbox is almost identical to setting up multiple port forwarding for VNC remote control. (See "How to set up port forwarding for multiple ports" on page 23).

NOTE

For more information on configuring your router for online gaming, see "How to optimize your router for gaming and voice" on page 30.

Refer to your game console documentation to determine the ports used by your device. The Xbox uses four ports:

- TCP port 80
- UDP port 88
- TCP/UDP port 53
- TCP/UDP port 3074

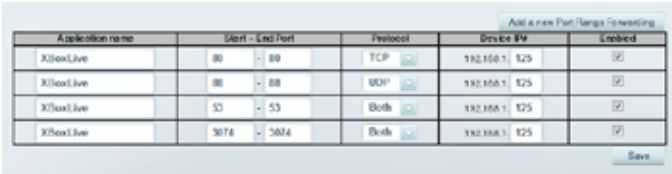
To set up an Xbox using multiple entries of single port forwarding:

Applications & Gaming > Single Port Forwarding

1. Connect your Xbox 360 to your router.
2. Log into Cisco Connect Cloud. (See "How to configure your router" on page 11).
3. Set up a DHCP reservation for the IP address of the Xbox. (See "How to set up the DHCP server on your router" on page 27).
 - OR –

Refer to your game console's documentation to set a static IP address for your device.

- Under **Router Settings**, click **Security**.
- Click the **Apps and Gaming** tab.
- Click **Single Port Forwarding**. The *Single Port Forwarding* screen opens.
- Click **Add a new Single Port Forwarding**. The Xbox uses four ports, so create four entries on this page.
- Enter the information as shown in the image below. In the **To IP Address** field, enter a 1- to 3-digit number that corresponds to the last three digits of the IP address of the Xbox 360. The rest of the IP address is already completed.



The screenshot shows a web interface for configuring port forwarding. At the top right, there is a button labeled "Add a new Port Range Forwarding". Below this is a table with the following columns: "Application name", "Start - End Port", "Protocol", "Device IP", and "Enabled". There are four rows of data, all for "XboxLive". The "Start - End Port" values are 80-80, 88-88, 53-53, and 3074-3074. The "Protocol" values are TCP, UDP, Both, and Both. The "Device IP" values are all 192.168.1.125. Each row has a checkbox in the "Enabled" column, all of which are checked. A "Save" button is located at the bottom right of the table.

Application name	Start - End Port	Protocol	Device IP	Enabled
XboxLive	80 - 80	TCP	192.168.1.125	<input checked="" type="checkbox"/>
XboxLive	88 - 88	UDP	192.168.1.125	<input checked="" type="checkbox"/>
XboxLive	53 - 53	Both	192.168.1.125	<input checked="" type="checkbox"/>
XboxLive	3074 - 3074	Both	192.168.1.125	<input checked="" type="checkbox"/>

- Click **Save**. If you don't want to use the settings but want to keep the information in the table, unselect the checkboxes.

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.

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**.

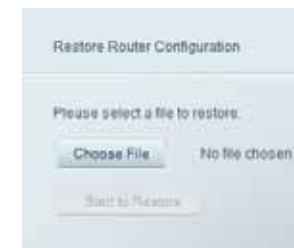


You are prompted to save the file.

5. Specify a file location, then click **Save**.

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.



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 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.



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.

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.



The image shows a web interface for tracing a route. It has a title "Trace route" and a label "IP or host name:" next to a text input field. Below the input field is a button labeled "Start to Traceroute".

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

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 5-15 seconds, then run the **Setup** program again on the router's CD.



- 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, Cisco Connect Cloud 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.

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:

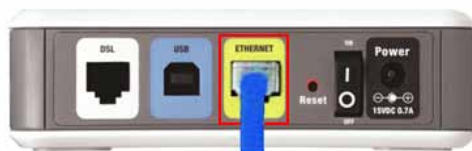
1. Make sure that an Ethernet or Internet cable (or a cable like the one supplied with your router) is securely connected to the yellow **Internet** port on the back of the router and to the appropriate port on your modem. This port on the modem is usually labeled **Ethernet**, but may be named **Internet**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

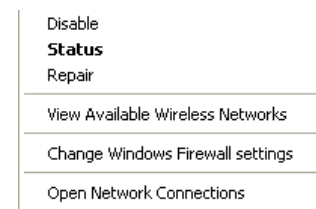
1. On your Windows desktop, click or right-click the wireless icon in the system tray.



Windows XP

Windows 7

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



- 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.



- 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**.

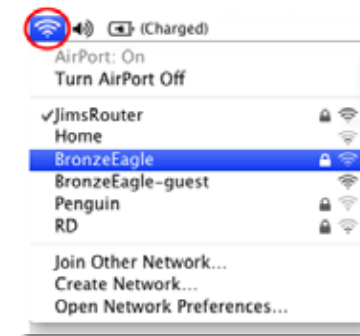


Your computer connects to the network, and you should now be able to access the router.

To fix the problem on Mac computers:

- 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.



- Click the wireless network name of your Linksys E-Series router (*BronzeEagle* in the example).
- Type your wireless network password (Security Key) into the **Password** field, then click **OK**.



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*.

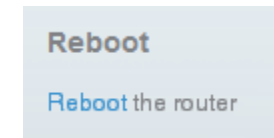
Rebooting your router

To reboot your router using the power cord:

1. Disconnect the power cord from the router.
2. Wait 10 seconds, then reconnect the power cord. The router’s power indicator flashes while it reboots. When the power indicator stops flashing, your router has finished rebooting and is ready to use.

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**.



A confirmation screen opens.



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

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 53.

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 5-15 seconds.



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.



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

Specifications

Linksys EA6500

Model Name	Linksys EA6500
Description	Dual-Band AC Router with Gigabit and 2xUSB
Model Number	EA6500
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 (2), Internet, Ethernet (1-4)
Buttons	Reset, Wi-Fi Protected Setup, power (EU models only)
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 4 or higher, Google Chrome 10 or higher, and Safari 4 or higher

Environmental

Dimensions	10.8" x 1.58" x 7.25" (256 x 40 x 184 mm)
Unit Weight	17.67 oz (501 g)
Power	12V, 3A
Certifications	FCC, IC, CE, Wi-Fi a/b/g/n/draft ac, Windows 7, DLNA, Energy Star
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



Cisco, the Cisco logo, and Linksys are trademarks or registered trademarks of Cisco and/or its affiliates in the United States and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. All other trademarks mentioned in this document are the property of their respective owners.

© 2012 Cisco and/or its affiliates. All rights reserved.

3425-0xxxx

111216MS