Configuring a Wireless Router

Setting up a wireless router is straightforward as long as you have a PC with a wireless network adapter, as well as an active high-speed Internet connection. You might also need a computer with a wired network adapter and router-specific setup software, which is typically included on a disc packaged with your router or available for download on the router manufacturer's support site.

Set Up Your Wireless Router on a Windows 7 PC

- Connect the wireless router to your modem using an ethernet cable.
- Connect your wireless router to a power source. Wait about a minute, and then continue to the next step.
- Click the network icon in the notification area; the icon should look like a series of vertical bars, or a tiny PC with a network adapter alongside it.
- Select your wireless network from the list of available networks to complete the setup process. By default, your network name will be the name of your router manufacturer.

Although newer routers connected to Windows 7 PCs are generally simple to set up, some problematic wireless routers might require a little more attention. If you can’t set up your wireless router as explained above, follow the directions included with it. Chances are, you'll need to use one of the following two strategies.

Set Up Your Router Using the Setup Software

- Make sure that your wireless router is completely disconnected from the modem, the computer, and the power source.
- On your PC, insert the disc that came with your router, or download and run the latest version of the router's software from the vendor website.
- Follow the on-screen instructions. The setup routine will ask you to connect components (including your modem and PC) in a certain order, and it may request that you temporarily connect your wireless router to a computer via an ethernet cable. You will also create a wireless network name and password at this point. If something goes wrong, you may want to consider manually configuring your wireless router.

Manually Configure Your Router Without Setup Software

- Connect your wireless router to the modem, using an ethernet cable.
- Connect the wireless router to a power source. Wait about a minute to ensure that your router is fully operational.
- Connect the wireless router to your computer using an ethernet cable.
- Log in to your router’s Web interface by opening a browser and entering the IP address of your router into the address bar. The IP address should be listed within your router’s documentation; if you can't find it, most routers use a common IP address such as http://192.168.1.1, http://192.168.0.1, or http://192.168.2.1.
- Enter the default username and password, which you should find within your router’s documentation. Alternatively, visit Port Forward’s Default Router Passwords page.
- Use the Web interface to set up a network name and password.
- Disconnect your computer from the wireless router and then reconnect wirelessly. Finally, check out our router tips to speed up your wireless connection.

Caution: Be sure to use a password to protect your wireless network. Unauthorized parties can easily connect to an unprotected network, stealing your bandwidth as well as your personal data. Include a combination of letters, symbols, and numbers to build a better password, and don’t use words found in the dictionary. Don’t worry about memorizing your password; just write it down and file it away. The one-time minor inconvenience of connecting a computer to a password-protected network is worth the huge security advantage.

DCHP

The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

Encryption Options

Wi-Fi Security: Should You Use WPA2-AES, WPA2-TKIP, or Both?

On our Comcast Xfinity router, WPA2-PSK (TKIP), WPA2-PSK (AES), and WPA2-PSK (TKIP/AES) are all different options. Choose the wrong option and you'll have a slower, less-secure network.

The last option — both TKIP and AES — was the default on our router. That's actually a bad choice, but just understanding the options requires some knowledge of Wi-Fi encryption standards.

AES vs. TKIP

It's important to secure your wireless network with WPA2 encryption and a strong passphrase. TKIP and AES are two different types of encryption that can be used by a Wi-Fi network. TKIP stands for "Temporal Key Integrity Protocol." It was a stopgap encryption protocol introduced with WPA to replace the very-insecure WEP encryption at the time. TKIP is actually quite similar to WEP encryption. TKIP is no longer considered secure, and is now deprecated. In other words, you shouldn't be using it.

AES stands for "Advanced Encryption Standard." This was a more secure encryption protocol introduced with WPA2, which replaced the interim WPA standard. AES isn't some creaky standard developed specifically for Wi-Fi networks; it's a serious worldwide encryption standard that's even been adopted by the US government. For example, when you encrypt a hard drive with TrueCrypt, it can use AES encryption for that. AES is generally considered quite secure, and the main weaknesses would be brute-force attacks (prevented by using a strong passphrase) and security weaknesses in other aspects of WPA2.

The "PSK" in both names stands for "pre-shared key" — the pre-shared key is generally your encryption passphrase. This distinguishes it from WPA-Enterprise, which uses a RADIUS server to hand out unique keys on larger corporate or government Wi-Fi networks.

IP Filtering

IP filtering is simply a mechanism that decides which types of IP datagrams will be processed normally and which will be discarded. By discarded we mean that the datagram is deleted and completely ignored, as if it had never been received. You can apply many different sorts of criteria to determine which datagrams you wish to filter; some examples of these are:

- Protocol type: TCP, UDP, ICMP, etc.
- Socket number (for TCP/UPD)
- Datagram type: SYN/ACK, data, ICMP Echo Request, etc.
- Datagram source address: where it came from
- Datagram destination address: where it is going to

It is important to understand at this point that IP filtering is a network layer facility. This means it doesn't understand anything about the application using the network connections, only about the connections themselves. For example, you may deny users access to your internal network on the default telnet port, but if you rely on IP filtering alone, you can't stop them from using the telnet program with a port that you do allow to pass trhough your firewall. You can prevent this sort of problem by using proxy servers for each service that you allow across your firewall. The proxy servers understand the application they were designed to proxy and can therefore prevent abuses, such as using the telnet program to get past a firewall by using the World Wide Web port. If your firewall supports a World Wide Web proxy, their telnet connection will always be answered by the proxy and will allow only HTTP requests to pass. A large number of proxy-server programs exist. Some are free software and many others are commercial products. The Firewall-HOWTO discusses one popular set of these, but they are beyond the scope of this book.

The IP filtering ruleset is made up of many combinations of the criteria listed previously. For example, let's imagine that you wanted to allow World Wide Web users within the Virtual Brewery network to have no access to the Internet except to use other sites' web servers. You would configure your firewall to allow forwarding of:

- datagrams with a source address on Virtual Brewery network, a destination address of anywhere, and with a destination port of 80 (WWW)
- datagrams with a destination address of Virtual Brewery network and a source port of 80 (WWW) from a source address of anywhere

Note that we've used two rules here. We have to allow our data to go out, but also the corresponding reply data to come back in. In practice, as we'll see shortly, Linux simplifies this and allows us to specify this in one command.

Enable and Configure MAC Address Filtering

MAC address filtering (aka link-layer filtering) is a feature for IPv4 addresses that allows you to include or exclude computers and devices based on their MAC address.

When you configure MAC address filtering, you can specify the hardware types that are exempted from filtering. By default, all hardware types defined in RFC 1700 are exempted from filtering. To modify hardware type exemptions, follow these steps:

- In the DHCP console, right-click the IPv4 node, and then click Properties.
- On the Filters tab, click Advanced. In the Advanced Filter Properties dialog box, select the check box for hardware types to exempt from filtering. Clear the check box for hardware types to filter.
- Click OK to save your changes.

Before you can configure MAC address filtering, you must do the following:

Enable and define an explicit allow list. The DHCP server provides DHCP services only to clients whose MAC addresses are in the allow list. Any client that previously received IP addresses is denied address renewal if its MAC address isn’t on the allow list.

Enable and define an explicit deny list. The DHCP server denies DHCP services only to clients whose MAC addresses are in the deny list. Any client that previously received IP addresses is denied address renewal if its MAC address is on the deny list.

Enable and define an allow list and a block list. The block list has precedence over the allow list. This means that the DHCP server provides DHCP services only to clients whose MAC addresses are in the allow list, provided that no corresponding matches are in the deny list. If a MAC address has been denied, the address is always blocked even if the address is on the allow list.

To enable an allow list, deny list, or both, follow these steps:

- In the DHCP console, right-click the IPv4 node, and then click Properties.
- On the Filters tab, you’ll see the current filter configuration details. To use an allow list, select Enable Allow List. To use a deny list, select Enable Deny List.
- Click OK to save your changes.

Note: As an alternative, you can simply right-click the Allow or Deny node, and then select Enable to enable allow or deny lists. If you right-click the Allow or Deny node and then select Disable, you disable allow or deny lists.

Once you've enabled filtering, you define your filters using the MAC address for the client computer or device's network adapter. On a client computer, you can obtain the MAC address by typing the command ipconfig /all at the command prompt. The Physical Address entry shows the client's MAC address. You must type this value exactly for the address filter to work.

When you define a filter, you can specify the MAC address with or without the hyphens. This means that you could enter FE-01-56-23-18-94-EB-F2 or FE0156231894EBF2. You also can use an asterisk (*) as a wildcard for pattern matching. To allow any value to match a specific part of the MAC address, you can insert * where the values normally would be, such as:

FE-01-56-23-18-94-*-F2

FE-*-56-23-18-94-*-*

FE-01-56-23-18-*-*-*

FE01*

To configure a MAC address filter, follow these steps:

- In the DHCP console, double-click the IPv4 node, and then double-click the Filters node.
- Right-click Allow or Deny as appropriate for the type of filter you are creating, and then click New Filter.
- Enter the MAC address to filter, and then enter a comment in the Description field if you want to. Click Add. Repeat this step to add other filters.
- Click Close when you have finished.

Port Filtering

TCP/IP port filtering is the practice of selectively enabling or disabling Transmission Control Protocol (TCP) ports and User Datagram Protocol (UDP) ports on computers or network devices.

Allowing or blocking network packets into or out of a device or the network based on their application (port number)

Web content filtering

On the Internet, content filtering (also known as information filtering) is the use of a program to screen and exclude from access or availability Web pages or e-mail that is deemed objectionable. Content filtering is used by corporations as part of Internet firewall computers and also by home computer owners, especially by parents to screen the content their children have access to from a computer.

Content filtering usually works by specifying character strings that, if matched, indicate undesirable content that is to be screened out. Content is typically screened for pornographic content and sometimes also for violence- or hate-oriented content. Critics of content filtering programs point out that it is not difficult to unintentionally exclude desirable content.

Content filtering and the products that offer this service can be divided into Web filtering, the screening of Web sites or pages, and e-mail filtering, the screening of e-mail for spam or other objectionable content.