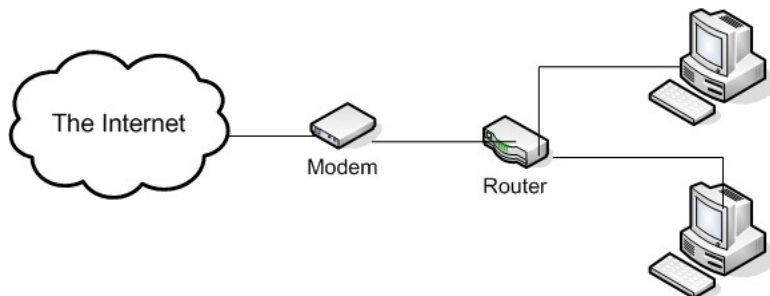


Routers & Firmware

Home networking routers are stand-alone devices that allow you to connect multiple computers or devices to one Internet connection (such as a DSL or cable modem). A router also allows for file and printer sharing between computers on the local network. Modern routers also provide a firewall for security purposes, among other features. Wireless routers are available, which, in addition to normal routing features, also provides a wireless access point for wifi-enabled computers to connect to. These devices are reasonably inexpensive (generally \$60 or less), and can be a bit tricky to set-up, but are very easy to use once configured.

A router generally has several Ethernet ports on the back, one of which connects to the modem, the other ports are for PC's. The port for the modem is usually labeled "WAN" (short for Wide Area Network) or simply "modem". The PC ports are generally labeled "LAN" (Local Area Network). Most common home routers have 1 WAN port and 4 LAN ports. Here's an example of a common home router wiring diagram:



Many of you may already have a router. The most common brands are Linksys, Netgear, DLink, Belkin. If you don't already have one, I highly recommend Linksys products.

Basic Theory of Routers

The primary purpose of a router is to allow multiple computers to share one Internet connection. This is achieved by using what's called NAT, or Network Address Translation. Your ISP issues your modem one single IP address – for example, 64.32.16.8 . For more than one computer to use this Internet connection, they'll both have to share this IP address, and somehow keep each one's traffic separate from the other's. To do this, the router issues each machine INSIDE the network with it's own unique IP address, frequently called a local IP. Most local IP's start with 192.168. So for instance, if we had two computers connected to a router, they might be 192.168.1.100 and 192.168.1.101. These IP addresses only exist within the local network; no one outside your router can access your machine using it's local IP.

A wireless router does double-duty; in addition to routing, it acts as a "base station" very much like a cordless phone – in this analogy, the wifi router is the base station and the computers are "handsets".

Configuring your Router

For hard-wired applications, routers are reasonably plug-and-play devices and require very little configuration besides plugging the hardware in. For a wireless setup, things are slightly more complicated. In either case, routers have an HTTP interface – meaning, you access your router's control panel through your Web browser. First you need to find your router's IP address. To do this, open your Network Connections folder and double-click your connection (probably labeled Local Area Connection). In the "Local Area Connection Status" window that pops up, go to the Support tab. Your router's IP address will be listed as "Default Gateway" and generally starts with 192.168.*.*. Write it down. By the way, your machine's local IP is listed here, simply as IP Address.

Next, open Internet Explorer or Firefox (best not to use the AOL or MSN browsers for this) and put in <http://> followed by your router's IP address, for instance, <http://192.168.1.1> , and press Enter.

If you haven't set a username and password for your router, it will still be the factory default. For most routers, this is a blank username (or "admin") and the password is "admin" , "password" , "1234", or blank. If you've lost your username/password, you can reset the router back to factory defaults by holding down the little teeny reset button on the back of the router for 10 seconds.

Once you're logged into the router, browse around a bit and get to know the menus – don't change any settings you aren't familiar with though. If you haven't done so before, set a password on your router.

If you have a wireless router, you'll want to take some time to setup the wireless features. Here are the specific features you want to set. You can leave the rest default.

- § SSID – this is the name of your wifi network and is usually broadcast over the airwaves. Name your wifi network something easy to remember, but avoid using any identifying info such as your last name or a password.
- § Channel – There are 12 wifi channels for the US. If there are multiple networks in your neighborhood, there can be signal interference if two routers within close proximity are on the same channel – to avoid this, you can change to a different channel. If you experience weak signal or if your computer drops off of the wifi network periodically, try changing channels.
- § Encryption or Security – this is what prevents your neighbors and passerby's from accessing your network. If your equipment supports it, the WPA(PSK) encryption protocol is best for home use. If your equipment doesn't support it, the older WEP encryption protocol is adequate.
 - The Encryption Key or Passphrase is essentially the password required to access the wifi network. For WPA and WPA2, the password can be anything you choose, but should ideally include some numbers and symbols as well as regular characters. For WEP, you must use a hexadecimal password – I recommend using a password generator – just search Google for “wep key generator”. Make sure you write down your encryption key.
 - MAC Authentication – each machine's networking card (wireless or hardwired) has a unique identifying number called a MAC (Media Access Control). You can setup your router to use a MAC whitelist, allowing only pre-authorized MAC ID's to connect to your router. This requires entering the MAC ID from every wireless computer. To find a machine's MAC ID, click start > run > “cmd” > “ipconfig /all”. MAC ID will be listed as “Physical Address”. Some machines have multiple networking cards, so make sure you're entering the MAC ID for the wireless card.

Firmware

Firmware, as the name indicates, lies somewhere between hardware and software. A device's firmware is like it's built-in operating system. Many peripheral devices such as routers, modems, printers, even some mp3 players and cameras, have user-upgradeable firmware. Updating firmware is particularly important for routers, because their firewall plays a central role in your network's security.

Generally, traditional wisdom is to not update the firmware on other devices (except routers) unless there's a need to (such as a problem with the device) – “if it ain't broke, don't fix it”.

First things first, you'll need to determine the brand and model number of your router. The brand is generally quite obvious and is written right on the front, but the model number is frequently on the back or bottom of the router. If you've updated your router in the last year, you may still have the current version, as some device's firmware isn't updated very frequently. Now is a good time to check. Login to the router as described above, and find the Firmware page. It's sometimes under Advanced or Help, etc... The Firmware page should list a version number and give you an option to upload a new firmware.

Now, you'll want to go download the latest firmware from the router manufacturer's website. Go to the manufacturer's website (linksys.com, netgear.com, dlink.com, etc....) and find the Downloads page (sometimes under Support). Enter the model of your router, and the webpage should direct you to the proper firmware. Download the file to your computer. Sometimes (but not usually) the file will come in a zip, which will need to be extracted (right-click it, Extract All). The firmware is now on your PC, and needs to be uploaded to the router. To do this, log in to the router and go back to the Firmware page. Click the “Browse” button, select the firmware file you downloaded on your PC, and click OK. **DO NOT UNPLUG OR DISTURB THE ROUTER DURING THE FIRMWARE UPDATE!** Disturbing the router during the firmware update will turn a router into a very expensive doorstop. The firmware update process generally takes less than two minutes.