Regardless Of Which Type You Select

With a home network, you can connect multiple computers in your home.

Once, home networks were primarily the realm of technophiles -- most families either didn't need or couldn't afford more than one computer. But now, in addition to using computers for e-mail, people use them for schoolwork, shopping, instant messaging, downloading music and videos, and playing games. For many families, one computer is no longer enough to go around. In a household with multiple computers, a home network often becomes a necessity rather than a technical toy.

A home network is simply a method of allowing computers to communicate with one another. In this article, you'll learn about the different types of home computer networks, how they work and what to keep in mind if you're considering creating one. We'll look at the hardware that creates and protects home networks in the next section. In both of these types, the router does most of the work by directing the traffic between the connected devices. By connecting a router to your dial-up, DSL or cable modem, you can also allow multiple computers to share one connection to the Internet.

If you're going to connect your network to the Internet, you'll need a firewall. A firewall is simply a hardware device or software program that protects your network from malicious users and offensive Web sites, keeping hackers from accessing or destroying your data. Although they're essential for businesses looking to protect large amounts of information, they're just as necessary for someone setting up a home network, since a firewall will secure transactions that might include Social Security numbers, addresses, phone numbers and credit card numbers. Most routers combine wireless and Ethernet technology and also include a hardware firewall. In this way, a software firewall can learn which types of information you want to allow into your network. Symantec, McAfee and ZoneAlarm are popular companies that produce software-based firewalls. These companies usually offer some free firewall protection as well as advanced security that you can buy.

Other Network Options

If neither wireless nor Ethernet seems right for you, you have other options for connecting your computers. If your computers have USB or FireWire ports, you can use cables, jump drives or file transfer devices to move files from place to place. Other options include power-line and phone-line networks. Both power- and phone-line networks use existing wiring in your home to connect your computers, so you don't need to worry about concealing extra cable. Check out "How Power-line Networks Work" and "How Phone-line Networks Work" for more information.

Wired Networks

This Belkin router provides wireless and Ethernet connections, while also acting as a firewall.

Ethernet and wireless networks each have advantages and disadvantages; depending on your needs, one may serve you better than the other. Wired networks provide users with plenty of security and the ability to move lots of data very quickly. Wired networks are typically faster than wireless networks, and they can be very affordable. However, the cost of Ethernet cable can add up -- the more computers on your network and the farther apart they are, the more expensive your network will be. In addition, unless you're building a new house and installing Ethernet cable in the walls, you'll be able to see the cables running from place to place around your home, and wires can greatly limit your mobility. A laptop owner, for example, won't be able to move around easily if his computer is tethered to the wall.

There are three basic systems people use to set up wired networks. An Ethernet system uses either a twisted copper-pair or coaxial-based transport system. The most commonly used cable for Ethernet is a category 5 unshielded twisted pair (UTP) cable -- it's useful for businesses who want to connect several devices together, such as computers and printers, but it's bulky and expensive, making it less practical for home use. A phone line, on the other hand, simply uses existing phone wiring found in most homes, and can provide fast services such as DSL. Finally, broadband systems provide cable Internet and use the same type of coaxial cable that gives us cable television. If you want to connect several computers or other devices, you'll need an additional piece of equipment: an Ethernet router. You'll also need a cable to connect each computer or device to the router.

Once you have all of your equipment, all you need to do is install it and configure your computers so they can talk to one another. Exactly what you need to do depends on the type of network and your existing hardware. For example, if your computers came with network cards already installed, all you'll need to do is buy a router and cables and configure your computers to use them. Regardless of which type you select, the routers, adapters and other hardware you buy should come with complete setup instructions.

The steps you'll need to take to configure your computers will also vary based on your hardware and your operating system. User manuals usually provide the necessary information, and Web sites dedicated to specific operating systems often have helpful tips on getting several different computers to talk to each other.

Next, we'll examine the advantages and disadvantages of wireless networks.

Nervous about Networking?

Most people who have a basic familiarity with computers can set up a network without much help. But the idea of installing cards and making connections makes some people nervous. Many Internet service providers (ISPs) offer home networking packages. For a monthly fee (and sometimes an initial setup cost), the ISP will provide you with the hardware and support you need to build and maintain your network. The absence of physical wires makes this kind of network very flexible. For example, you can move a laptop from room to room without

fiddling with network cables and without losing your connection. The downside is that wireless connections are generally slower than Ethernet connections and they are less secure unless you take measures to protect your network.

If you want to build a wireless network, you'll need a wireless router. Signals from a wireless router extend about 100 feet (30.5 meters) in all directions, but walls can interrupt the signal. Depending on the size and shape of your home and the range of the router, you may need to purchase a range extender or repeater to get enough coverage. You can add printers and other devices to the network as well. Some new models have built-in wireless communication capabilities, and you can use a wireless Ethernet bridge to add wireless capabilities to devices that don't. Any devices that use the Bluetooth standard can also connect easily to each other within a range of about 10 meters (32 feet), and most computers, printers, cell phones, home entertainment systems and other gadgets come installed with the technology.

If you decide to build a wireless network, you'll need to take steps to protect it -- you don't want your neighbors hitchhiking on your wireless signal. Wireless security options include:

Wired Equivalency Privacy (WEP)

WiFi Protected Access (WPA)

Media Access Control (MAC) address filtering

You can choose which method (or combination of methods) you want to use when you set up your wireless router. The IEEE has approved each of these security standards, but studies have proven that WEP can be broken into very easily. If you use WEP, you may consider adding Temporal Key Integrity Protocol (TKIP) to your operating system. TKIP is a wrapper with backward compatibility, which means you can add it to your existing security option without interfering with its activity. Think of it like wrapping a bandage around a cut finger -- the bandage protects the finger without preventing it from carrying out its normal functions.

In the next section, we'll learn about some innovative home network technologies on the rise.

Faster Wireless

Most home wireless networks use 802.11g wireless networking, which transmits data at 2.4 GHz with a speed of 54 megabits. A newer wireless standard is 802.11n, which is faster and has a longer range than 802.11g. Some of the most exciting advances are in healthcare and housing.

In healthcare, Wireless Sensor Networks (WSNs) let doctors monitor patients wirelessly. Patients wear wireless sensors that transmit data through specialized channels. These signals contain information about vital signs, body functions, patient behavior and their environments. In the case of an unusual data transmission -- like a sudden spike in blood pressure or a report that an active patient has become suddenly still -- an emergency channel picks up the signal and sends medical services to the patient's home. Bill Gates

owns one of the few smart houses in existence, but someday, we might all live in one. A smart house is a fully networked structure with functions that can be controlled from a central computer, making it an ideal technology for homeowners who travel frequently or for homeowners who simply want it all.

Builders are beginning to offer home network options for their customers that range from the primitive -- installing Ethernet cables in the walls -- to the cutting-edge -- managing the ambient temperature from a laptop hundreds of miles from home. In one trial experiment called Laundry Time, Microsoft, Hewlett Packard, Panasonic, Proctor & Gamble and Whirlpool demonstrated the power of interfacing home appliances. The experiment networked a washing machine and clothes dryer with a TV, PC and cell phone. This unheard-of combination of networked devices let homeowners know when their laundry loads were finished washing or drying by sending alerts to their TV screens, instant messaging systems or cell phones. Research and development also continues for systems that perform a wide variety of functions -- data and voice recognition might change the way we enter, exit and secure our homes, while service appliances could prepare our food, control indoor temperatures and keep our homes clean.

This technology is promising, but it's not quite ready for the consumer market yet. By wow dad can't afford a WSN or a smart house, and if he could, there's a good chance he or she wouldn't be able to operate these sophisticated systems. Another issue is security -- until developers find a way to secure these networks, consumers risk sharing medical information and leaving their homes open to attack.

For lots more information about home networks, installation and technology, see the links on the next page. "(In)Security of the WEP algorithm." Berkeley University. (10/2/2007) http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Coyle, Karen. "The Technology of Rights: Digital Rights Management. Based on a talk originally given at the Library of Congress, Nov. 19, 2003."(10/1/2007) http://www.kcoyle.net.drm_basics.pdf

Haskin, David. "FAQ: 802.11n wireless networking." Computerworld. May 16, 2007. (10/2/2007) http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=9019472

Lange, Peter. "WiFi Update." PC Update Online. April 2004. (10/2/2007) http://www.melbpc.org.au/pcupdate/2404/2404article6.htm

Larkin, Eric. "WinHEC: Gates on Mobile Computing, Home Networks, Windows Server." Today@PC World. May 15, 2007. (10/1/2007) http://blogs.pcworld.com/staffblog/archives/004390.html

Linux. "Home entertainment networks coming on strong." July 6, 2006. (10/1/2007)

http://www.linuxdevices.com/news/NS4342517630.html

Marriott, Michel. "I Know It's Here Somewhere…" The New York Times. 2/19/2004 (9/28/2007) http://query.nytimes.com/gst/fullpage.html?res=9D02E2D6123DF93AA25751C0A9629C8B63

McNamara, Paul. "Your washer's calling and the dryer's on IM." Network World. July 17, 2006. (9/28/2007) http://www.networkworld.com/columnists/2006/071706buzz.html

Regan, Keith. "Ten Scary Things About Home Networks, Part 1." TechNewsWorld. 2/22/2007 (10/1/2007) http://www.technewsworld.com/story/55882.htm

Regan, Keith. "Ten Scary Things About Home Networks, Part 2." ECommerce Times. March 2, 2007. (10/1/2007) http://www.ecommercetimes.com/story/65022.html

Snyder, Joel and Rodney Thayer. "Explaining TKIP." Network World. Oct. 4, 2004 (10/2/2007) http://www.networkworld.com/reviews/2004/1004wirelesstkip.html

Stankovic, John A. "Wireless Sensor Networks for In-Home Healthcare: Potential and Challenges." Department of Computer Science, University of Virginia. (9/28/2007) http://www.cs.virginia.edu/papers/wlsn_health_HCMDSS05.pdf

Universities and Colleges Information Systems Association. "Choosing Cat 5e or Cat6 Cabling." (10/2/2007) http://www.ucisa.ac.uk/groups/ng/docs/ChoosingCat5Cat6.htm

Ward, Mark. "Troubled times for home networks." BBC News. Aug. 21, 2007. (10/1/2007) http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/technology/6949607.stm

Wilson, James M. "The Next Generation of Wireless LAN Emerges with 802.11n." White paper: Intel Communications Technology Lab. Sept. 9, 2004. (10/1/2007) http://www.intel.com/technology/magazine/communications/wi08041.pdf