Home Networking in 5 Easy Steps

Building a home network? First question: Why would you want to? Only ten years ago you could have answered that question easily: "I'm an incurable geek." But nowadays there are so many products and services being offered for home networks that it's really a question of "why wouldn't you want to?"

A home network will let you share high-speed Internet access with any computer in the house the Spouse's, the kids', even Grandma's iPhone when she drops by for a visit is within reach. A network lets you control what the kids are doing on the Web, share data and multimedia files across all your computers, automate backups for those system, and even use webcams to see what that new puppy is doing in the living room while you're at work.

With a network, the bedroom computer upstairs can print to the color printer in the downstairs study, and the media PC in the living room can show a movie on the PC-connected TV in the master bedroom. That's all accomplished simply by hooking your PCs together. Adding on network-oriented products and peripherals makes the setup even more useful. Network attached storage lets you create—for each family member—shared folders that can be accessed both from the home network or from the Internet if you're away from home. These folders are also a great place to store all those backup files. Network printers, webcams, and even phones are all available in home network flavors and can help maximize the return on your time and effort. Getting in the game isn't hard. All you have to do to get started is set up that basic home network, which means following just a few initial steps.—Next: Step 1: High-Speed Internet

Step 1: High-Speed Internet

You can run a home network without high-speed Internet, but that's a little like building a boat and then parking it in your backyard. The Internet makes home networking worthwhile, and starting there means you'll begin at the right place: the home Internet router.

First, you'll need to choose a high-speed Internet provider, generally from cable TV providers, the phone company (fiber or DSL lines), or your satellite TV operator, if you live in a remote area (it's still better than dial-up). If you're in a rural area, you can also consider a WISP, or wireless Internet service provider. WISPs act like upside-down satellite dishes, reaching down into the ground to connect to fiber-optic lines, while long-range wireless routers installed in each customer's house point sideways toward the tower. Regardless of the tech you choose, pick the one with the most throughput (measured in megabits per second, or Mbps) for the lowest monthly cost, and you're good to go. In our annual Service and Reliability Survey, the favorite of our readers, hands down, is fiber, which you can get via the highly rated Verizon FiOS service (in very select areas of the United States, that is).

Setting up high-speed Internet service is much, much simpler than it used to be. As a first option, you can make an at-home service appointment with the phone or cable company, then wait for that highly precise, "anywhere between 8 a.m. and 4 p.m." arrival time. Some providers may require this, or at the very least insist that you visit their local office to get the modem kit, because they won't allow use of a third-party modem.

If they do allow it, your other option is to purchase a DSL or cable modem kit at your local electronics store. The kit usually includes a name-brand router, a definite plus. You can find these packages at stores like Best Buy or Wal-Mart, and online at Buy.com and Amazon. In addition to the modem and router—or, in some cases, one integrated modem/router unit—there are setup instructions and info on how to register your new service automatically with the provider. Again, these kits used to be a nightmare of bad instructions and nonfunctioning automation. Today's packages, however, are easy-peasy.

Stick the quick-start CD into your computer and follow the on-screen instructions. Typically, it will ask you to plug your router into the phone or cable TV line first; then take a minute or so to find itself on the provider's network (the Internet) and register. After that, you'll plug your computer into the other side of the router, fill out some identification and billing information, make sure your computer's network settings are set to "Automatically get an IP address," and that's it. You'll be on the Internet.

Any other computers you plug into the back of that router will not only see the Web, they'll also see each other (or they will after you run Microsoft's home-networking wizard)—and hey, you've got a basic network. Don't have a router yet? See the sidebar, "New Wireless Routers Add Speed, Drop Price."—Next: Step 2: Smartening Up Your Computers

Step 2: Smartening Up Your Computers

Once your router is functioning and your computers are plugged in, you've got to make sure all the computers can see not just the Internet, but each other as well. For Vista and Windows 7 machines, you're not going to have to do much besides wait. These versions of the Windows operating system are much smarter about networking. Vista PCs will simply find one another on the network, as long as they're all in the same IP subnet—a logical division of a local area network, which is created to improve performance and provide security (see below). If your computers don't see one another, Vista has a couple of network fix-it wizards as well as the "Set up a home network" wizard for you to fall back on.

Windows XP machines, on the other hand, are a mixed bag. Those in the same IP subnet should see one another, but there's a chance they won't. You'd be best off running the "Set up a home network" wizard right away for XP, which is available off the Network Neighborhood screen. Just run this wizard on every XP machine individually. The most thinking you'll have to do is picking a workgroup name for your network. (But that's an important step: You can't share files or printers between PCs that don't have the same workgroup name.)—Next: Step 3: Understanding Your Router

Step 3: Understanding Your Router

The router is the heart of your home network—which is good. That's because it's doing several important jobs. First, it's the outward face of your Internet connection. To the phone, cable, or satellite company, your Internet account is represented by just one Internet address. If you look on your router's basic setup or status Web page, you'll see that address at the top, generally labeled something like "WAN IP address" or "Internet IP address." This is all that the provider or anyone on the Internet can see of your network. The router maintains that external address and simultaneously hands out a bunch of internal addresses to the computers in your house, using an IP addressing scheme that's different from the public one that your provider uses. The process of translating traffic between the internal and external addresses is called *Network Address Translation* (NAT), and the process for handing out those internal addresses automatically is called the *Dynamic Host Configuration Protocol* (DHCP).

NAT is used because the TCP/IP network protocol was never intended to support the millions of users, devices, and Web sites that currently populate the Internet. There simply aren't enough addresses to go around, so one per customer is all ISPs can manage—and even then they need to play cycling games, so your WAN IP address will probably change every few weeks.

On the internal side, you can set up whatever IP addressing scheme you'd like using your router's DHCP settings. This looks like Sanskrit, but don't panic: For the most part you can leave the default settings. Most routers default to a 192.168.*X*.*X* address scheme. It's those last two Xs—technically, they're called *octets*—that concern you. The second-to-last variable determines your subnet. So PCs addressed as 192.168.1.*X* are all in the same subnet and should see and network with each other just fine. One that's addressed as 192.168.0.*X* will be left out in the cold.

That last octet will be different for every device you plug into the network. The router, for example, might be 192.168.1.1. The first PC might be 192.168.1.2; your laptop might have .3; the Xbox might be assigned .4; and so on. That last octet can be any number from 1 to 254, so you've got plenty of addresses to go around inside your home—don't worry about running out. The reason to stick with the default 192.168.0.*X* or 192.168.1.*X* scheme is because that particular range is not routable on the Internet. Consequently, anything hacking past the firewall that's built into your router will have some trouble accessing the PCs behind it. Another non-routable addressing scheme is 10.10.*X*.*X*. You can set your scheme to run any way you'd like, but those schemes are safest.

Speaking of safe, your router, as mentioned, is also your firewall. This is critical to a safe network. A good firewall using *stateful inspection* (which ensures that all inbound packets are the result of an outbound request) keeps the bad guys off your home network—and believe me, the bad guys are out there! At PCMag Labs, we once plugged an open PC into a non-firewalled Internet connection and recorded how long it took the PC to become hacked or infected. The low record was 20 minutes. Watch out.

You should also install a software firewall on every Windows PC and make sure it stays updated. Just open the app every few weeks, and the firewall will tell you if it needs a software update. That's as easy as downloading a file and hitting Save. Vista and Windows 7 have pretty good firewalls built into the operating system. For XP, our Editors' Choice is Comodo Firewall Pro 3.0.—Next: Step 4: Set Up Wireless

Step 4: Set Up Wireless

Finally, your router is likely capable of providing wireless access using Wi-Fi. The giveaway used to be whether or not it had antennas, but more and more routers today remain stylish by hiding the antenna—even multiple antennas—inside the bezel. Actually, it's hard to find a router today that *isn't* Wi-Fi-capable. PCs with Wi-Fi will see the router almost immediately, but you shouldn't let it go at that.

Wireless networking works on RF (radio frequencies), meaning it's essentially a radio: Anyone within 300 feet (indoors) or 600 yards (outdoors) can tune in to your signal. Some people are quite open to sharing their Internet connection this way, but doing so can leave your PCs vulnerable. Unless you want anyone parked outside your driveway to have access to what's on your network, your PCs, your hard drives, and more, it's a good idea to use some security.

Your router will offer several wireless security options. The two most popular are WEP (Wired Equivalent Privacy) and WPA2 (Wi-Fi Protected Access). Either will give you enough basic protection, though WPA2 is tougher. But many folks still use WEP, because Windows XP has trouble with more advanced forms of wireless security. Moreover, if you've got any older Wi-Fi products around your house using 802.11b technology, WEP is probably all they support. WEP is easy to crack by anyone with the right tools and the time to put in, however, so don't trust it for important data. Windows Vista handles either with aplomb, so stick with WPA2 there.

Setting up wireless is again just a short series of steps. First pick a channel (you can stick to the default unless there are a lot of other wireless routers around, as there probably are in an apartment building). Stick with channels 1, 6, or 11: They don't "overlap" and thus have less interference. Set all your wireless devices to the same channel. The router will then ask you to name its wireless network—this is called the SSID in Wi-Fi-speak. Definitely do not to stick with the default here, which is usually "Linksys" or "DLink" or something similar. Use something personal like "BobsWireless." When asked which security option you'd like to use, opt for WPA2 if you know all the devices on your network support it. After that, simply pick a security key, which boils down to a password-type phrase. Try and go strong here, so not just "password," but "P4ssW0rd1234"—a mix of capitalization, numbers, and symbols with the letters is much harder to crack, let alone guess. Avoid words found in the dictionary. The balance here is finding something easy to remember. Even then, it's a good idea to change that security key every few months.

Save that and all you have to do is go to each of your wireless computers and let them scan for the SSID (BobsWireless). When a device finds it, it will ask you for the security key. Type it in, hit Save, and those PCs will automatically connect whenever they're turned on and in range. To enhance your security, nearly all routers will let you opt not to broadcast your SSID. All this

means is that you must know the ID and input it manually before connecting a laptop for the first time. After that, the SSID will be stored—though outsiders won't be able to see it when they scan the airwaves.—Next: Step 5: Last Thoughts on Wires and Ports >

Step 5: Last Thoughts on Wires and Ports

Congratulations! You've got a working home network. Those wireless computers should be able to see both one another and any wired computers you've got plugged directly into the back of the home router. And speaking of wired, stick with Category 5e or Category 6 Ethernet patch cables. Both of these are capable of running Gigabit-speed Ethernet. The highest-end home routers have Gigabit, which has a data rate of 1,000 Mbps—ten times faster than "Fast Ethernet."

Gigabit will be especially useful if your network winds up carrying movies and high-def TV content around the house, or if you play multiplayer games. And who doesn't? If those ports on the back of your router aren't enough, drop around $30 on a Gigabit-capable switch. Plug it into a Gigabit port on your router and then all the ports on the switch will function the same as those on the router. You'll instantly go from four available Ethernet ports to 8, 12, or 20, depending on how big a switch you choose. You can even plug a second switch into the first.

If you've got areas of the house where Wi-Fi won't reach and you don't want to thread Ethernet cable through the walls or around doors, you can sometimes take advantage of existing wires in the walls. If you're lucky enough to have coaxial cable running from room to room, a set of MoCA-capable adapters (short for Multimedia over Coax Alliance) on either end will use the wire as if it were Ethernet. You can even do the same with power lines in your house, using adapters that support HomePlug. Those are even easier, because they just plug into existing outlets, then have an Ethernet cord that comes out to attach to the router and switch.

There are plenty of ways you can now add to or modify your home network. You can add more security for wireless, another wireless access point, webcams for watching the house while you're away, parental controls so the kids stay safe on the Web, picocells that use the Internet to extend the range of your cellular phone—the list goes on and on. But what you've done in these five steps is the foundation for everything else to come.—Next: New Wireless Routers Add Speed, Drop Price >

New Wireless Routers Add Speed, Drop Price

03.16.09

Discuss Total posts: 1

by Jeremy A. Kaplan

To take real advantage of your home network, you'll want a wireless router. A router negotiates traffic between your network and the Internet. The switch and wireless access point integrated with the router handle traffic among the various devices in your home network, be they PCs,

laptops, media devices, or whatever else you've plugged in or linked up wirelessly. The latest crop adds a slew of neat features beyond mere speed, but speed is definitely at the heart of these gadgets.

Today's wireless routers are built around the 802.11n specification, meaning they can hurl data around your house at an incredible gallop: 300 megabits per second (Mbps), theoretically. In our testing, the routers we reviewed actually moved bits at speeds ranging from 63 Mbps to 133 Mbps. Two of the routers we tested, the Netgear RangeMax Wireless-N Gigabit Router WNR3500 and the Belkin N+ Wireless Router (F5D8235-4) include Gigabit Ethernet connections, so wired connections can really zip. The third, the D-Link RangeBooster N Dual-Band Router (DIR-628), uses the more common 10/100-Mbps Ethernet.

New routers like these place a real emphasis on ease of setup. Many have a WPS (Wi-Fi Protected Setup) button, such as the one you'll find on the Belkin and Netgear router. Pressing the buttons on the client adapter and router simultaneously automatically sets up networking between the two, without your having to set channel, SSID, and WPA encryption key. For WPS devices without a button—like a laptop with integrated Wi-Fi—you have to enter a PIN code manually.

The Belkin router's claim to fame is that it's an easy way to add network storage: Simply plug an external hard drive into the router's USB 2.0 port. The included software utility works well and maps the drive as a local drive, letting you access it from anywhere on the network. The combination of this storage manager software and the port provides a tremendously useful feature you won't find on many routers at this price. The Netgear router's wireless repeater function takes networking up a notch over its competitors. A repeater makes possible wireless meshing of a sort—a way for Wi-Fi devices to talk to each other wirelessly. It establishes ad hoc connections or direct connections using MAC addresses, a very cool feature. With the wireless repeating function turned on, the router can extend the range of your wireless network. When you add it all up, the router can work well either in a home or in a small business.

The D-Link, our Editors' Choice among these routers, supports a wealth of fancy features: channel auto-scanning for both bands and mixed channel widths, a quality of service (QoS) engine, VPN gateways, and access control policies. The router's firewall even supports IPsec VPN and includes some nifty network address translation (NAT) filtering capabilities to limit traffic at the protocol level. In addition, the low price (it's just $119.99 direct) is a sign that wireless-n, now at draft 2.0, is finally hitting the mainstream