

REPLAY

Learn about the quick and easy mobile scanner that works where you do ►



Canon
ImageFORMULA

The Ultimate Guide to Home Networking

Wired or Wi-Fi? Here's how to pick the right hardware for your PCs, game consoles, Internet-capable HDTVs, and other devices--and how to solve your networking problems.

Loyd Case

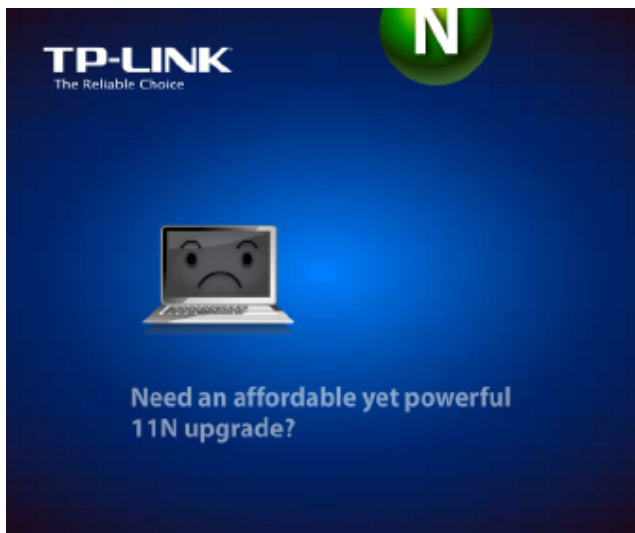
Tuesday, May 11, 2010 06:35 PM PDT

Home networking is never as simple as merely connecting device A to device B. This guide will walk you through the jargon of setting up a [home network](#). I'm focusing on PC networking here, but I will talk about consumer electronics gear in the context of delivering material from your PC to the living room, as well as Internet connectivity.



Some of the following advice may apply to renters as well as to homeowners, but if you rent rather than own, you have much less control over your physical environment. Your landlord may not appreciate your punching holes in the walls to string Cat 5e cabling, for example.

What Do You Need From Your Network?



TP-LINK
The Reliable Choice

N

Need an affordable yet powerful 11N upgrade?

Before whipping out your credit card and buying up gear, figure out what you're trying to accomplish with your home network.

- Are you just looking to connect a couple of laptops and maybe a Wi-Fi-equipped cell phone to the Internet for Web access? You might be able to get by with a single 802.11n access point.
- Do you work at home frequently, and require access to a corporate network through VPN (virtual private

network) technology? You'll need a good router that can handle VPN passthrough.

- Are you a serious online gamer? Do you connect to massively multiplayer online games or through services like PlayStation Network or Xbox Live frequently? You'll need not only to buy a good router but also to steep yourself in key router capabilities such as port forwarding.
- Do you watch TV through the Internet, using services like Hulu or the networks' own Websites? If you're streaming video from the Internet to multiple locations in your home, you'll want a reliable networking infrastructure--probably a wired network.

Determining the answers to such questions will go a long way toward ensuring that you build a network suitable for your home without spending too much in the process.

Next: Your Network Infrastructure Options

Your Network Infrastructure Options

Most homeowners have three basic choices for moving data around their abode: wired ethernet, Wi-Fi, and HomePlug (powerline networking).

Wired Ethernet



Nothing today beats [gigabit ethernet](#) for moving data around the home. (While 10-gigabit ethernet is starting to make inroads in corporate environments, it's still too expensive for most homeowners.) Gigabit ethernet translates to a maximum throughput of 125 megabytes per second, but you'll rarely see that speed; this is about as fast as a midrange hard drive, although networking overhead will make gigabit seem slower.

The primary standard for gigabit today is 1000Base-T, or IEEE 802.3ab. 1000Base-T runs over twisted-pair copper wiring. If you plan on using gigabit ethernet, you'll need Cat 5e (Category 5e) wiring. (You can also use Cat 6 cabling, though that's overkill for gigabit ethernet.)

Be careful when buying Cat 5e, however--some cheaper cables labeled "Cat 5e" may not be solid copper, or may be smaller than the standard 24-gauge, and your throughput on such lower-cost cables may be reduced. Make sure you buy cabling from a reputable manufacturer, and take care to avoid the cheapest cables.

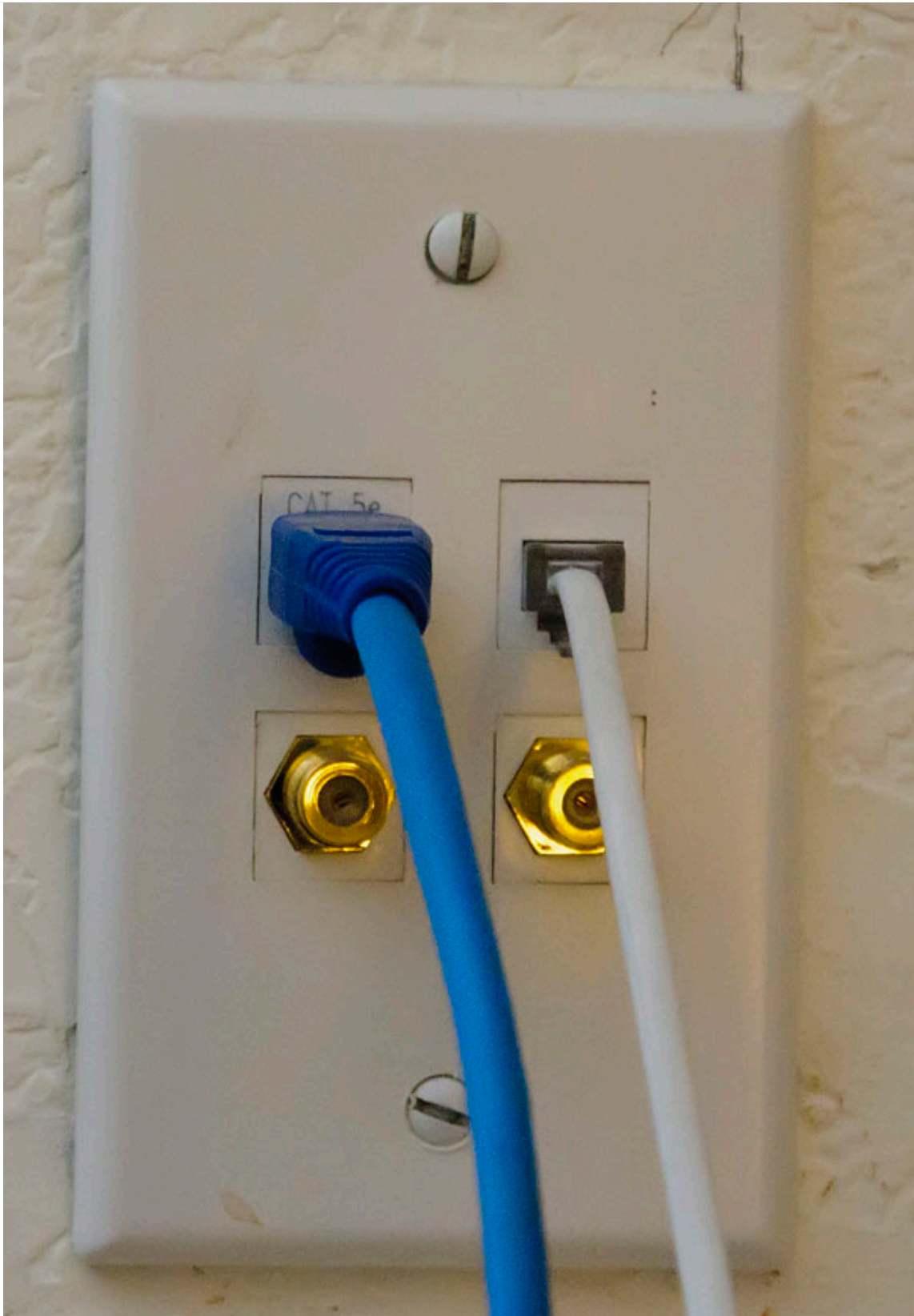
The weakness of gigabit ethernet lies within its strength: It requires physical wiring. So you'll need to string Cat 5e to any room where you want that level of connectivity.

Structured Wiring



If you're running other kinds of wiring around the house (telephone, fiber-optic, coax, or the like), you might be able to kill two birds with one stone with structured wiring, which bundles all of them in a single sheath. The term "structured wiring" actually encompasses a range of products, including wiring panels, junction boxes, and other items, but I'm mainly discussing the actual wiring here.

While the structured bundle is thicker than individual cables, it makes running cable throughout a home easier, though you'll still have to punch holes in your walls.



In my home office, which is a basement room, I have Cat 5e running on the floor, in gathered bundles. This approach is fine in a single room that isn't intended for lots of visitors, but it's a less-than-optimal solution for social-gathering locations, like living rooms--you'll want to run the wires behind the walls there. (Check out

[SWHowto.com](#) for more structured-wiring tips.)

If you can't (or won't) run cables through your house, the next best setup is Wi-Fi.

Next: Wi-Fi

Wi-Fi

I'll say it up front: if you're planning on using Wi-Fi for whole-house networking, think again. While 802.11n sounds great--offering throughput up to 300 megabits per second, and no wiring hassles--it isn't ideal if you want to do lots of media streaming and moving big files around.

For example, in my home we have a Windows Home Server with several user accounts. We also use the server as a repository for applications. Installing large apps over wired gigabit ethernet takes only a little more time than installing from a CD. But installing software over an 802.11n link can take a very long time.

On the other hand, if you simply want to connect a small number of PCs, Wi-Fi may be the right way to go for you. Wi-Fi is a quick and easy way to connect several business laptops, Wi-Fi-enabled cell phones, and light-duty devices such as an Apple iPad or a netbook.

If you like the convenience of Wi-Fi for connecting laptops and phones, you might consider a mixed network, using a combination of Wi-Fi and gigabit ethernet. I'll discuss one possible scenario for a mixed-mode network on the next page.

What Kind of Wi-Fi Do You Need?

If Wi-Fi is your only alternative, definitely go with 802.11n. The prices of 802.11n routers and access points have dropped substantially, so there's no point in using older 802.11g gear unless your networking needs are minimal. (Check out PCWorld's [wireless router and networking reviews](#), while you're at it.)

Before you start shopping for Wi-Fi equipment, make sure you know what kind of equipment you're looking for--you'll see both "wireless routers" and "wireless access points" out there.



Routers take incoming traffic from the Internet and route the traffic to the correct system inside the network. They handle the task through a built-in NAT (network address translation) capability. Routers also act as firewalls between the internal network and the outside Internet, but that's an additional function.

Traditionally, access points simply existed to connect Wi-Fi-equipped PCs, and didn't handle routing functions. Early access points needed to be connected to a router. These days that definition has become a little fuzzy, and most home-oriented access points have built-in routers but lack wired-ethernet switches.

Home routers include wired-ethernet switches. Note that you can still find routers that connect only via wired links and don't have built in access points.

For our purposes here, I'll use the term "router" to mean a wired router with a built-in Wi-Fi access point. An access point, for this article, is a Wi-Fi router without built-in wired-ethernet switching. Routers don't cost much more than most access points, though, so consider one anyway--you never know if you'll need the added flexibility at some point.

The key to good 802.11n performance is to pick the right router. Routers can vary widely in features and performance, though if you have a small living area and only one or two systems connected to the router, you might never notice.

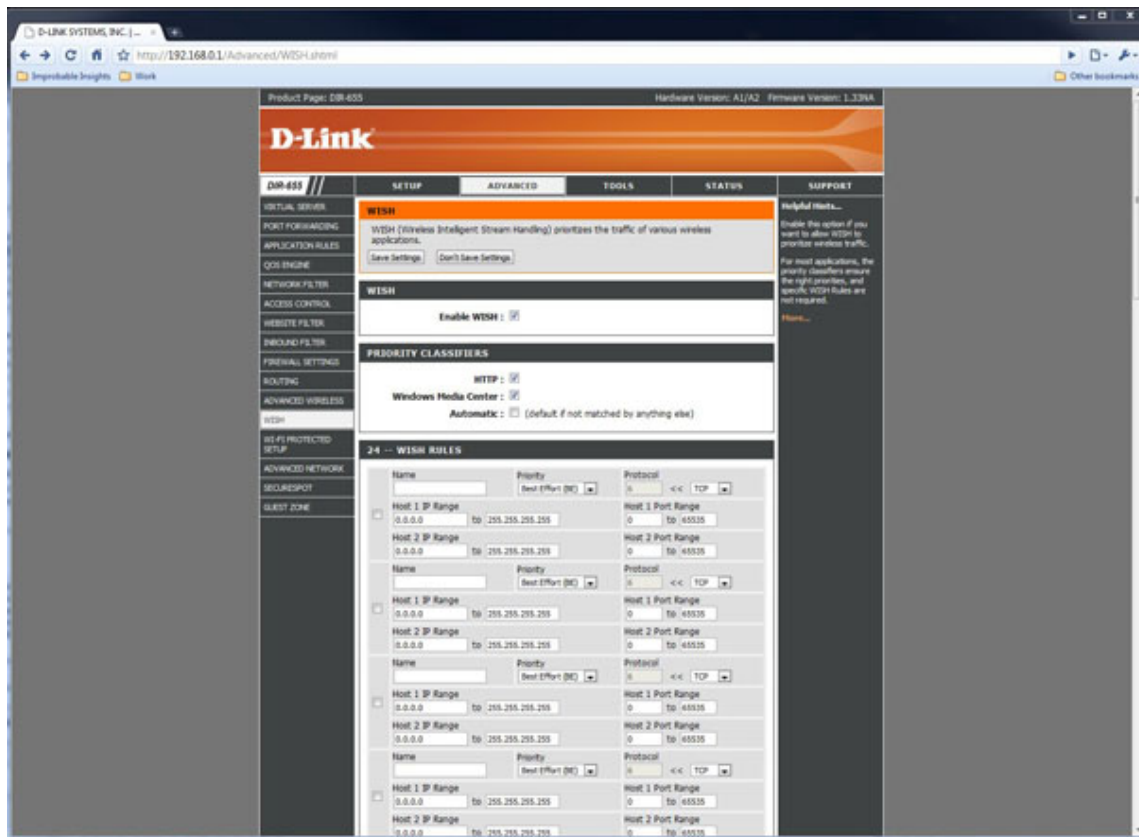
[Small Net Builder](#) offers more-detailed performance reviews, if you're concerned about throughput or area coverage. Lower-cost routers may have only fast ethernet support, and only a single Wi-Fi radio. When you're shopping for equipment, here are several key features to look for.

- **Simultaneous dual band:** Such routers can support both 2.4GHz and 5GHz or 5.8GHz. Only a few routers fully support 5.8GHz; you'll get increased bandwidth, but you'll also sacrifice some range, particularly through walls. Some newer routers may include a pair of 5GHz radios.

- **Multiple antennas:** You'll want an 802.11n router with two antennas at a minimum. Some home routers may have no visible antennas, but carry multiple antennas embedded in the case. That's okay for moderately sized homes.
- **Replaceable antennas:** If you have longer range requirements, consider a router with external, replaceable antennas. These typically attach to a small, coax-style connector. Antennas are widely available from a number of sources, and come in a variety of sizes and configurations.

Depending on your needs, you might also want to look for routers with [QoS \(quality of service\) support](#) for better media streaming, gaming support (if you're an online gamer), and guest access (if you have a stream of friends dropping by who might want to connect).

One key issue to note with Wi-Fi networks is that your bandwidth splits among multiple client connections. Think about an 802.11n router with 300-mbps bandwidth. Now imagine connecting ten PCs to that router via Wi-Fi. All ten systems must share that 300 mbps. Fortunately, most modern routers are pretty smart about allocating bandwidth as needed, and some routers allow you to set up bandwidth allocation limits.



Another feature that some routers support is WISH (wireless intelligent stream handling), which allows you to prioritize certain types of traffic to specific clients or sets of clients. You might want to enable WISH if you're streaming video from one system (a home server) to another (a living-room PC or network-equipped HDTV). Similarly, WISH is useful for making sure that VoIP connections remain reliable.

Extending Wi-Fi

There may be times you'll want to extend your Wi-Fi network to wired-only devices, like the Xbox 360 game console or BD 2.0 network-equipped Blu-ray players.

A wireless bridge is just the thing you need. You can find bridges with a single ethernet port for connecting one device, as well as bridges with a built-in ethernet switch for setting up several devices at the same time in one

area.

Alternatively, you could just increase the range of your network. Standard access points often have a bridge or extender mode, but you can also find dedicated range extenders that essentially act as relays for your Wi-Fi signal.

Next: Powerline Networking, Mixed-Mode Networks

Powerline Networking (HomePlug)



If you want reliable bandwidth to particular computers or devices, but aren't able to string Cat 5e wiring, consider a HomePlug [powerline networking](#) setup. HomePlug uses your home's existing power lines for carrying network signals. The HomePlug standard has been evolving over the years, and current products include QoS (quality of service) settings and offer maximum throughput of up to 200 mbps.

That's less total bandwidth than 802.11n, but HomePlug connections are for single clients. You can plug an ethernet switch into a HomePlug connection, of course, but at the cost of splitting that bandwidth.

The problem with HomePlug is that your total bandwidth is at the mercy of your electrical wiring. Actual speeds vary wildly--brand-new adapters might get over 100 mbps in an ideal home but only 10 to 15 mbps in an older building.

Newer construction often means better wiring, but how that wiring is laid out can also be a factor. In my home, we have discontinuous wiring--the only way to route a signal from the basement to the top-floor bedrooms is through the circuit-breaker panel. That's often a bottleneck, and it can sometimes even completely block a HomePlug signal.

Mixed-Mode Networks

In my home, we use a mixed-mode, wired and Wi-Fi network. As I noted earlier, my basement office has bundles of Cat 5e wiring running along the baseboards. We also paid to have professional electricians run structured wiring to several key rooms in the house, including the living room, the family room, and the kids' bedroom. Everything is tied together with structured wiring into a central panel in the basement, in the storage area adjacent to one of the two home offices.

This works well for us: We have wired networking where we need it, and Wi-Fi access throughout the house. Of course, your needs may be simpler--you might want wired networking in just one room, and Wi-Fi in the rest of the house.

I've seen other people install their cable modem connection in the living room, along with an 802.11n router. As a result, their networked entertainment devices can have wired connections, while various laptops connect via Wi-Fi.

Depending on your needs, just a single router with four ethernet ports and Wi-Fi access-point capability may get the job done. Or your requirements may be more complex, in which case you'll prefer to run wires to multiple rooms, as well as to include wireless repeaters or range extenders as necessary.

Next: Setting Up Your New Network

Setting Up Your New Network

Okay, so you've installed your networking infrastructure (if you're using wired or HomePlug networking). Now it's time to set everything up. I'll assume that you're starting from scratch. (If you're having problems with your network, check out "[Set Up Your Home Network: Windows 7 Edition](#)" for more tips.)

The steps are pretty straightforward, but keep in mind that these are general rules of thumb. Various models and brands of access points and routers may differ on specific configuration details. Note that when I refer to "routers" in this section, most of this advice also applies to access points in Wi-Fi-only networks.

Also, don't assume that experience with older routers means you'll just be able to jump in and configure new ones. Some recent routers have substantially automated the setup process, but it's useful knowing how to manually set up your router if there are exceptions to the rules you've followed before.

Configure the Router to Connect to One PC

Typically, you'll connect your router or access point to your PC via an ethernet cable. Routers usually have multiple ethernet ports, so connecting a PC is easy. An access point may require something called a *crossover cable*, which is a special ethernet cable with two of the pins reversed. Some access points come with a short crossover cable, but you may need to obtain one before proceeding.

Some routers require you to configure your PC to a specific IP address in order to perform setup. Recently released products may be bundled with a software CD that walks you through the configuration process. Note that different brands may have different default IP addresses for the router itself. For example, Linksys routers default to 192.168.1.1, while D-Link users have 192.168.0.1. You'll need to consult your router or access-point documentation for specifics.

Set Up Router and Wi-Fi Security

Every router comes with a default admin account that has a default password, which is usually listed in the documentation. It's startling how many users simply leave the admin password at the default, which allows random people to hijack your router. So the first thing you should do is change the admin password.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode :

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode :

Cipher Type :

Group Key Update Interval : (seconds)

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key :

The next step is to set up wireless security. A general rule of thumb is to configure for the highest level of security: WPA2, which uses AES encryption. However, some applications and older hardware may not work with WPA2, so you may need to opt for WPA with TKIP encryption for compatibility. Some *much* older devices may support only the original WEP security scheme, but that has been shown to be relatively insecure. I recommend upgrading to newer devices.

One important step here is to enter a password that acts as an encryption key. Though you want to remember the password easily, you don't want it to be so easy as to be hackable by an outsider. Pick a long, relatively arcane password. (WEP keys are more limited--but you're not using WEP, right?)

Connect the Router to Your ISP

If you have a recent-generation router, it may come with software that will autoconfigure the ISP settings, but you might want to do this manually anyway. Connecting to the Internet means entering key information about your ISP into the router.

- Connect your cable modem, DSL modem, or other gateway that your ISP supplied to the port labeled "WAN" or "Internet" on the router.
- Set the IP address of the router as indicated by your service provider, if you use a static IP. Otherwise, simply set the router to be assigned an IP address by your service provider automatically via DHCP. Note that this is

different from the gateway address you'll set in any client hardware that connects to the router.

Routers isolate your internal network from the Internet by presenting a single IP address to the Internet. But your home network sees a different IP address as the router gateway, typically 192.168.0.1 or 192.168.1.1.

- If your ISP provides you with a modem that acts as a gateway device, as some do, you'll need the IP address for that device. The gateway adds another layer, which has yet another IP address. Your ISP should have configured that piece of hardware earlier.
- If you use alternate DNS providers, such as [OpenDNS](#), you'll want to enter that information. (If you don't know what this is, then you can ignore this step.)

Next: Connect Any Wired Devices to the Router

Connect Any Wired Devices to the Router

If you want to connect some PCs or other hardware via wired ethernet, now is the time to hook them up. Also, if you have an ethernet switch, attach that to one of the router's standard ports (not the port labeled "WAN").

I'm assuming that you left the router set to supply IP addresses to your internal network automatically, via DHCP. If you did, any client hardware should pick up an IP address from the router.

Connect Wi-Fi Hardware

The last step to getting your network running is to configure Wi-Fi hardware. When you fire up your hardware and tell it to connect via Wi-Fi, you'll need to enter the encryption key (Wi-Fi password) you set up in the router.

Some routers implement something called "Wi-Fi protected setup," which can automate the process of connecting wirelessly to the router. You may still need to enter the password, but you won't need to tell the device what type of security you're using, or other connectivity details. Again, check the documentation for each piece of hardware.

Configure for Software

You may need to configure your router for particular software needs. For example, you may be a heavy user of videoconferencing or VoIP (voice over IP). Or maybe you're a serious online gamer. In any of those cases, you may need to configure features such as port forwarding or virtual servers.

Virtual servers allow you to configure particular ports as public; the router redirects incoming requests to a specific system. This arrangement can be useful if you're running a Web server or an FTP site.

For gaming, VoIP, and other similar software, you'll want to use port forwarding. If you're not comfortable mucking around with your router settings, check out [Simple Port Forwarding](#).

Ports are specific to individual IP addresses (for example, 192.168.0.100:xxxxx, in which the xxxxx is the port number). Each IP address can support 65,536 ports. For instance, 80 is the port that Web browsers use, and every router automatically recognizes this.

Depending on the application, you may need to configure a TCP (transmission control protocol) port or UDP (user datagram protocol) port--or both.

Product Page: DIR-655 Hardware Version: A1/A2 Firmware Version: 1.33NA

D-Link

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

VIRTUAL SERVER
 PORT FORWARDING
 APPLICATION RULES
 QOS ENGINE
 NETWORK FILTER
 ACCESS CONTROL
 WEBSITE FILTER
 INBOUND FILTER
 FIREWALL SETTINGS
 ROUTING
 ADVANCED WIRELESS
 WISH
 WI-FI PROTECTED SETUP
 ADVANCED NETWORK
 SECURESPT
 GUEST ZONE

PORT FORWARDING

This option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats including, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689). This option is only applicable to the INTERNET session.

Save Settings Don't Save Settings

24 -- PORT FORWARDING RULES

Name	Application Name	Ports to Open	Schedule
Xbox	Xbox Live	TCP 3074	Always
IP Address	Computer Name	UDP	Inbound Filter
0.0.0.0	Computer Name		Allow All
Slingbox	Application Name	TCP 5001	Always
IP Address	Computer Name	UDP	Inbound Filter
0.0.0.0	Computer Name		Allow All
	Application Name	TCP	Schedule
	Application Name		Always
IP Address	Computer Name	UDP	Inbound Filter
0.0.0.0	Computer Name		Allow All
	Application Name	TCP	Schedule
	Application Name		Always
IP Address	Computer Name	UDP	Inbound Filter

Helpful Hints...

Check the **Application Name** drop down menu for a list of predefined applications. If you select one of the predefined applications, click the arrow button next to the drop down menu to fill out the corresponding field.

You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the LAN computer to which you would like to open the specified port.

Select a schedule for when the rule will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools → Schedules** screen and create a new schedule.

You can enter ports in various formats:
 Range (50-100)
 Individual (80, 68, 888)
 Mixed (1020-5000, 689)

More...

Some games and other applications may use only specific ports to connect to the game server or other systems. As a result, you might need to configure your router for particular port numbers. For example, the screenshot here shows a D-Link port forwarding management page, configured for the Xbox Live service (port 3074) and the Slingbox (port 5001).

Port Forwarding, uPnP, and DMZ

Current-generation routers and software are often more sophisticated, and you may not have to configure port forwarding. The general rule is to try to connect with the game first, without port forwarding, and then add it if you can't connect.

If the router has UPnP (Universal Plug and Play) capability, some apps will use it to configure port forwarding while the game is running, and then turn it off when the software shuts down. Some users disable UPnP for security reasons, however. If you do, you may need to configure the proper ports for your app.

You can find [lists of ports](#) and related applications on the Internet, if your game or application manuals don't give you that information.

One thing to avoid, if at all possible, is a firewall DMZ. A DMZ (literally taken from the military term "demilitarized zone") allows you to configure a particular computer to be set up outside the firewall. That PC, as a result, is completely exposed to the Internet. This can be useful for running game servers for older games that are difficult to set up using port forwarding, but you should avoid it if you can. A system in a DMZ is open to all manner of intrusions from the Internet.

Next: Firewalls, Troubleshooting

A Brief Note on Firewalls



Modern hardware routers often ship with fairly sophisticated firewalls built into them. If yours does, you may not need to use a software firewall, such as the Windows firewall, or the firewalls incorporated into [Internet security software](#). In my home, we typically turn off software firewalls. Is that safe? We've never had an intruder get into our home network.

Most routers have logging capability built in, and checking those logs is always illuminating. When we look at the log for our home router, a [D-Link DIR-655](#), we see a few entries that read like the following:

Blocked incoming TCP connection request from IP address xxx.yyy.zzz.123 to [router IP address]

I've changed the IP address above, and I've chosen not to reveal my router IP address for obvious reasons. What this can represent is a serious intrusion attempt, or some software bot simply pinging the router to see if the network is exposed.

No firewall is completely foolproof, but we've had good success with hardware firewalls built into modern routers. While the default settings are often good enough, many have additional capabilities for the truly paranoid. So if you're worried about intruders sneaking into your network, ratchet up all the settings on your hardware firewall.

Troubleshooting

I can offer some general troubleshooting tips here, but hardware and software combinations can vary widely. Be prepared to contact your ISP, your router manufacturer, or tech support for each piece of client hardware as appropriate. (For more tips, check out "[How to Fix Anything](#).")



Photograph: Kevin Candland

Can't set up the router: Sometimes, you can't even connect to the router or access point for initial configuration. Make sure you've connected to the correct port; some older routers may allow you to perform initial setup only by connecting to a specific port. Similarly, older routers and most access points may require a crossover ethernet cable.

In addition, you may need to first set up your PC for a specific IP address, and then reboot to actually connect to the router.

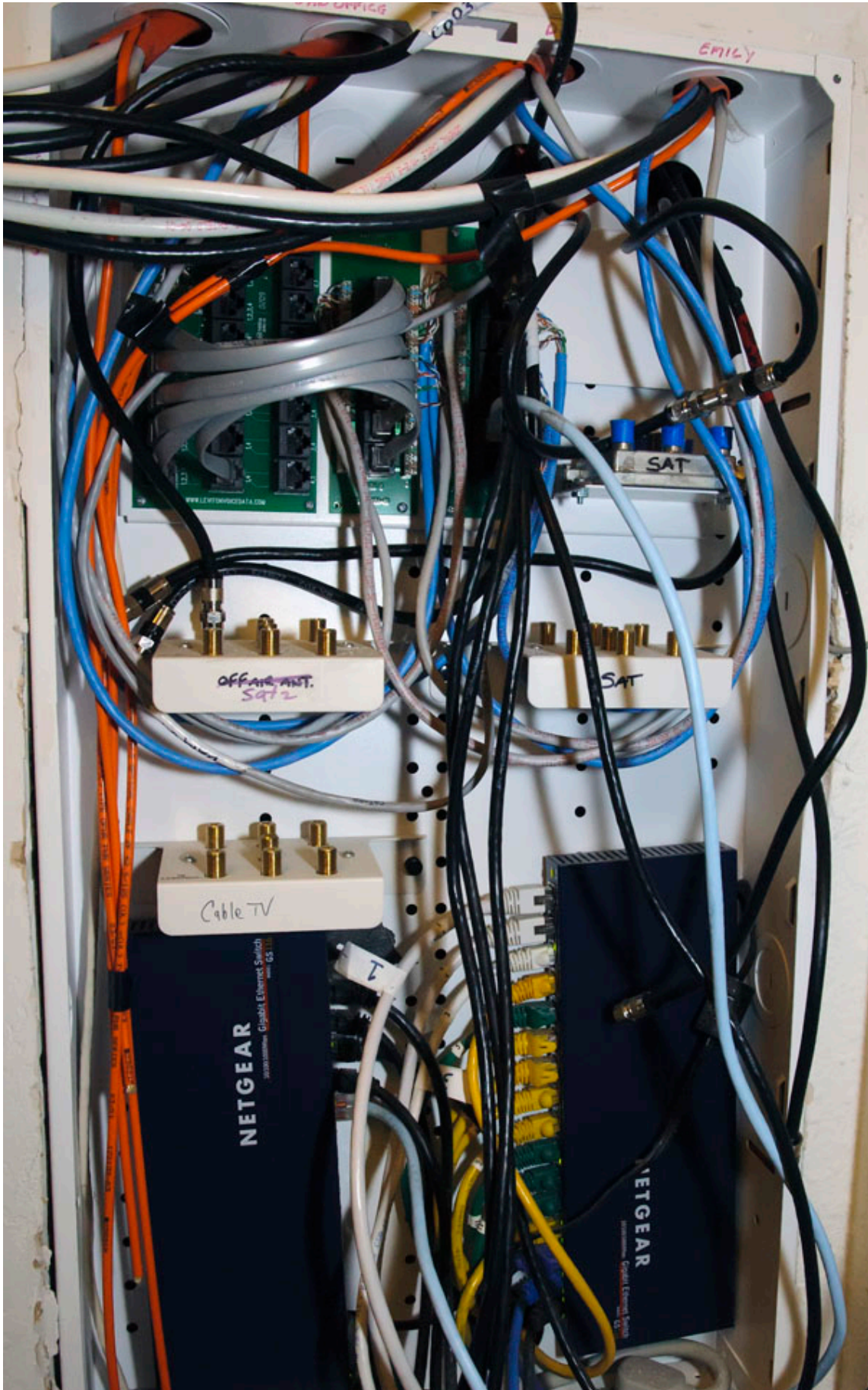
The router doesn't see the ISP: This often happens if the router is set to automatically receive an IP address from the ISP, but you've asked for one or more static IP addresses (or if you've entered a static IP address incorrectly). Also, if your modem doubles as a gateway, you'll have to configure your router differently.

The client hardware can't connect: Make sure DHCP is enabled. If you're using a Wi-Fi connection, make sure that security and encryption are set up correctly. For example, many laptops ship with tools from the manufacturer to streamline the configuration process. I've seen some of these tools incorrectly detect the type of security being used, so you may have to go to Windows' own networking utilities to set that.

Next: All Plugged In

All Plugged In







Now for a look at one particular network: the one in my home. Our family's network is relatively complex in scope, but while we do some online gaming, we don't run a Web server or an FTP site from within the house.

As I mentioned, we have bundles of Cat 5e wiring at the baseboards in one home office, plus structured wiring to several key rooms in the house. All this is tied together into a central structured-wiring panel, which houses a pair of Netgear 16-port gigabit ethernet switches.

Outside of the basement lab, the most complex setup in the house is our family room, where we have multiple devices connected to the Internet:

- Microsoft Xbox 360 (wired)
- Nintendo Wii (Wi-Fi)
- Panasonic DMP-BD85k Blu-ray player (wired, though it also has a Wi-Fi option)
- Denon TX-NR3007 A/V receiver (wired)
- HP Premium Fax All-in-One printer (wired)
- Dell Zino HD home theater PC (wired)

That's five wired connections and one Wi-Fi.

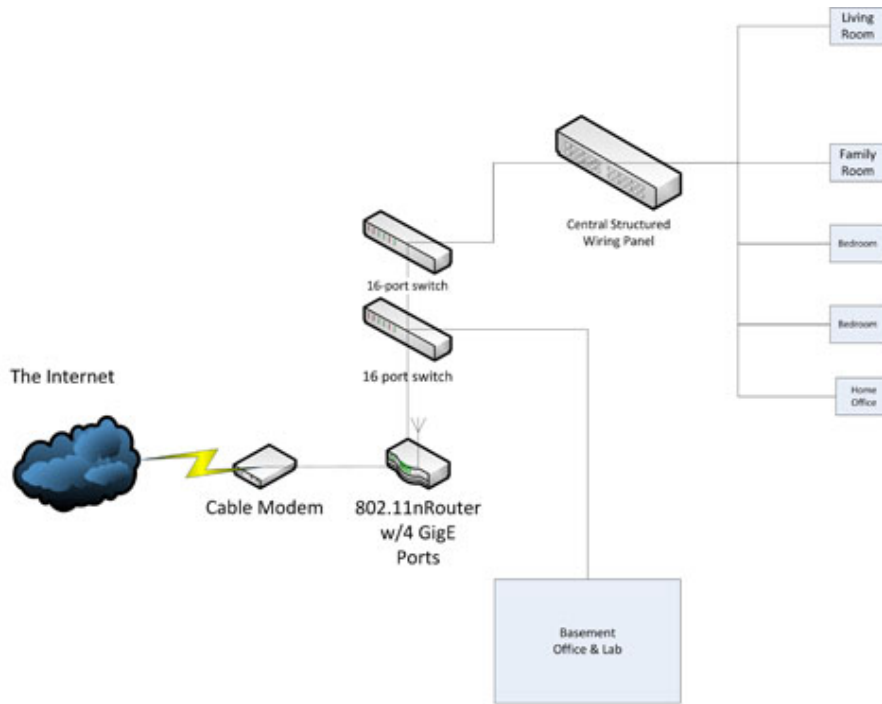
The room has a single Cat 5e wired drop, which connects to a compact Linksys eight-port gigabit ethernet switch. All of the wired devices connect via the switch.

Prior to putting a wired drop in the family room, we were using a D-Link DAP-1522 802.11 wireless bridge. The bridge connected to the router via Wi-Fi, and has four gigabit ethernet ports. Now that we have five wired devices, having a physical drop and an eight-port switch has been incredibly useful.

The Internet connection is through Comcast's Business ISP service, which connects via a cable connection to an SMC gateway. While the gateway also has a built-in router, that's limited to 10/100 fast ethernet, so the router is disabled.

A single cable runs from the gateway to the D-Link DIR-655, which has four gigabit ports. Another cable runs from one of the gigabit ports to one of the Netgear 16-port switches, and the two switches are bridged through a short cable.

Here's a diagram of our home network.



Loyd Case's Home Network

Overall, the network itself has been pretty reliable. In addition to the Nintendo Wii, we have an iPhone and an iPad connecting via Wi-Fi, as well as a couple of laptop PCs. We've never had a problem with network throughput to any device in the house, even with multiple large downloads.

One of us is often taking part in videoconferencing while the other is downloading a large game through Valve Software's Steam gaming service at the same time; neither of us has experienced issues with connectivity, apart from the rare occasions (twice in the past nine months) that the Comcast connection has dropped for brief periods (the longest was about 2 hours).

1998-2010, PCWorld Communications, Inc.