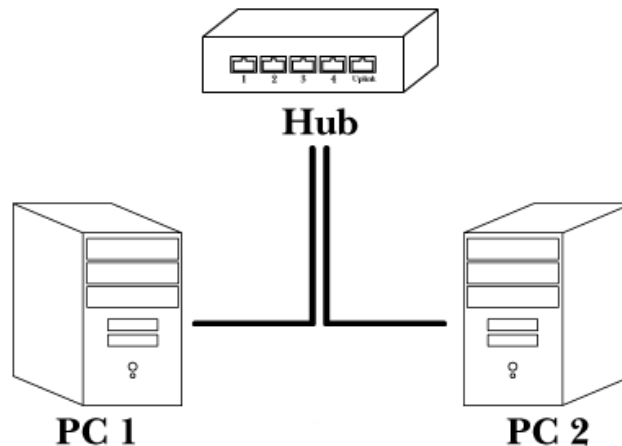


Networks Untangled

In the good old days, the only people that ever had to know anything about networks were network engineers. Due to the explosion of the Internet and the connected world in which we live today, those days are gone. Computer networks are everywhere, connecting computers in the largest corporations and the smallest homes. As a result, so many advances have been made in networking technology that it's hard to keep up. This article, the first of two about networking, will help untangle the mess of wires and peripherals and help you make sense of it all.

All networks, no matter how simple or complicated, have one and only one goal: to connect two or more computers together so they can talk to each other. So, how do they do that? Let's look at a simple example:



In the figure above, two ordinary computers have a network card installed in them, and a network cable connecting each of them to a network hub or switch. In a simple network, that's really all there is to it. But, like most things in life, there's more than meets the eye.

First, let's talk about network speed. Every part of a network has a speed rating associated with it, generally measured in terms of how much data in millions of bits it can handle per second (megabits per second, usually written as "Mbps"). Modern network components are generally rated at either 10 Mbps, 100 Mbps, or more recently, 1000 Mbps (also known as "gigabit ethernet"). (Wireless networks, however, have different speed ratings entirely). When purchasing, it's important to match the speed ratings of the various components so that they can talk to each other correctly. These days, most devices in use are rated for 10/100 Mbps, meaning they can "talk" at either 10 or 100 Mbps. Newer network cards and most cabling on the market can now support 10/100/1000 Mbps. Although gigabit ethernet hubs and switches are readily available, they are still considerably more expensive than their 10/100 counterparts.

Now, let's look at the three parts of this simple network in a bit more detail:

Network Card



The network card's job is to send and receive data to and from other computers. It is the computer's interface to the network, so network cards are often referred to as Network Interface Cards, or simply NIC cards. A network card comes with the necessary software ("drivers") that allows the computer to talk to it. Since a network card is not smart enough to know where other computers are on the network, it sends all the data to a central hub.

Hub / Switch



The job of the network hub or switch is to receive data from one computer and help send that data along to its final destination. Its job is to know where the other computers are, and to deliver the data to the destination computers. Think of a hub or switch as a traffic cop, directing network

traffic to its destination. Note that although hubs and switches perform the same function, there are some important technical differences between the two that are worth knowing about. Hubs tend to be cheaper than switches, because they rely on simpler technology. A hub, when it receives a piece of data from a computer on the network, will simply broadcast that data out to all the computers connected to it, rather than attempting to determine which specific computer the data is destined for. Although less expensive, this results in a less efficient network, with more useless traffic clogging the network. A switch, on the other hand, is designed to forward data only to the computer that it is intended for, often significantly reducing network traffic as a result. In practice, the question is becoming academic, as the industry is slowly phasing hubs out in favor of switches.

Network Cable



The network cable, of course, carries the data between the network card inside the computer and the network hub. Amazingly enough, network cables cause more confusion than any other part of this system, due to the different types and grades of cabling there are out there. In this section, we'll look at the most important characteristics of network cables and what they mean.

The most important characteristic of any network cable is its performance rating. These days, all network cable follows a particular performance rating, of which three are in more-or-less common use today:

Category 5

Generally abbreviated as "Cat 5", this was the industry standard for years and is still the most prevalent in existing networks. Recently, it has given way to Category 5E cable. Properly installed Category 5 rated cable is able to support 10/100 Mbps network speeds.

Category 5E

Category 5E (or simply, "Cat 5E") cable is currently the most commonly used cable in new installations. Properly installed Category 5E cable is capable of supporting 10/100 Mbps as well as Gigabit ethernet (1000 Mbps). Until about three years ago, Category 5E cable was not as popular a choice as Cat 5 cable, especially since gigabit ethernet devices were not very common in the marketplace and Cat 5E was more expensive. However, today, Cat 5 cable and Cat 5E cable are virtually the same price, and true Category 5 cable is rarely sold now. (Category 5 cables are now often used for phone lines, especially with the rise of DSL usage).

Category 6

The Category 6 standard was just released on June 24, 2002. Its performance rating characteristics define a cable that can handle twice the bandwidth of Category 5E cables. In practice, there are few (if any) commercially available products that require Category 6 cabling, and it is still priced somewhat at a premium. However, it is considered the "recommended choice" for new installations.

In our next article, we'll visit these three levels again and provide some more guidance as to which to choose for a given situation.

Beyond these performance levels, there are a few other characteristics we have to know about. The first is whether or not a cable is shielded. You will typically see one of the following two designations:

UTP: Stands for "Unshielded Twisted Pair," which means that the cable is not shielded. The vast majority of network patch cables fall into this class.

STP: Stands for "Shielded Twisted Pair." This cable will have an aluminum foil shield wrapped around the wires inside. The primary purpose of the shield is to reduce interference from noise caused by electrical lines (called electromagnetic interference, or EMI), which can cause data errors. Although most commercially available shielded cable comes in 1000' spools, shielded patch cables are also available.

Finally, network cables (more typically, spools of network wire) are often designated as "solid" or

"stranded" wire. The difference lies in whether each of the eight wires in a network cord are made up of a single solid copper wire or many fine strands of copper wire. Stranded wire (typically more expensive) is more flexible and is almost always used when making short cables. Solid wire is typically reserved for longer runs inside walls. Again, we will look at these two more closely in the next article.

That's all we're going to say about network cables for now. However, no networking overview would be complete without at least mentioning these other common terms:

Bridge: A bridge is any network device that connects one network to another.

Router: Conceptually, a router is a specialized type of bridge. Many devices that act as routers physically look like hubs or switches, although they perform many more functions than an average hub or switch. A router is capable of analyzing network traffic and redirecting or blocking it as necessary.

Firewall: A firewall is actually a piece of software whose purpose, generally speaking, is to protect networks from "bad" network traffic (i.e., hackers trying to break into a network). Firewalls look at individual bits of network traffic and make decisions (based on rules that network administrators set up) about whether to allow that traffic to continue into the network or not.

Well, that's all for this month. Please note that networking is still a vast and complicated topic and this article only scratches the surface. In Part II, we'll look at how to set up a simple network in your home or small office (including identifying when it's time to bring in a professional).

Now for a more practical approach, and to show you how you might want to set up a home or small office network.

Before we begin, however, we should carefully consider whether or not this is something you should do yourself or something that should be handled by a qualified network installer. Like any other do-it-yourself project, it comes down to how complicated the particular project is compared with how much time you have and what your skill level is. Having said that, there are definite situations where a qualified network installer should be brought in. For example, if network speed and reliability are of primary concern (such as with an Internet service provider, or if you are going to host a web site on this network), and you do not have experience in setting up a network, you should definitely consider bringing in a professional. Also, if you are going to run network cable through the walls or ceilings of a commercial building, there are building electric codes that have to be followed, and a qualified installer can advise you best.

At a minimum, you will need the following in order to network two or more computers together:

1. A network switch or hub
2. One network cable for each computer
3. One network card for each computer

Note that more and more computers are offering a network card already built in, so check your computer before purchasing one.

Before going out and purchasing a bunch of supplies, the first thing to do is plan your network. Look at your floorplan and decide where you think computers are going to be placed. Then, decide on an appropriate central location for a network switch. For a simple setup, running network cables along floorboards may be acceptable. But for many environments, it is likely that you will want to run the cabling inside walls or through ceilings. Knowing this in advance will help you plan what accessories to buy. Once you know this, you can measure out how long each cable run is going to be. Network signals can travel a

maximum of 100 meters (328 feet), so no single network cable run should ever be longer than that. (If you find you need to travel further, you can use a hub in between to connect two cables, although it's not a good idea to string more than about three hubs together along a network run.)

The other decision you'll need to make is what sort of network card to purchase. These days, you can purchase an internal network card that gets installed inside the computer (traditionally, the most common choice), or, if your computer supports USB, you can use a USB Ethernet adapter that you simply plug in to the USB slot. USB Ethernet adapters are much easier to install, but they tend to be a bit more expensive and run the slight risk of becoming disconnected from the computer.

Constructing a simple network

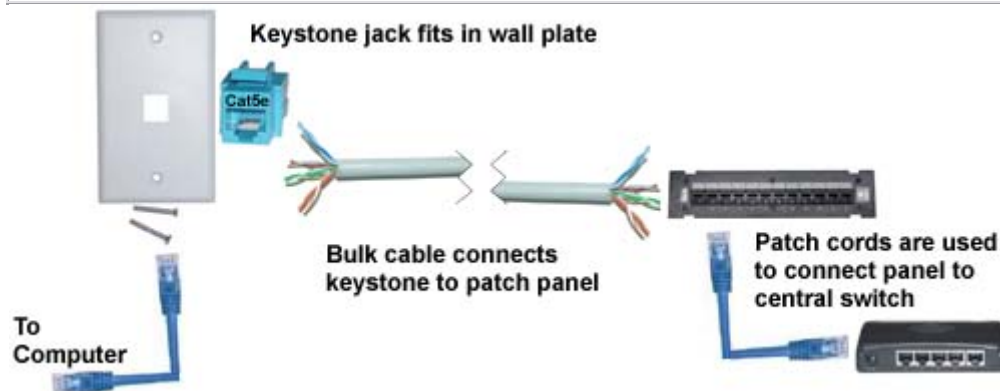
In the simplest case, you do not have to run cables through walls or ceilings, and no run happens to be more than 150 feet. In this case, the best choice may be to purchase pre-manufactured network patch cables rather than attempting to make your own. At this point, it's simply a matter of installing the network card in your system, plugging one end of each cable into the computer and the other end into the network switch, and then configuring the computers to "see" the network. (These days, most operating systems can usually do this automatically, and simply accepting the default choices when the network card is being configured will get you on the network and able to share files and printers. However, this can become a complicated task, and the services of a qualified network engineer may be appropriate.)

A Step Further...

The problem with simply using pre-made network patch cables is that keeping a neat (and safe) cable run is not easy. In particular, you will likely find that, while you can run a patch cable along a floorboard, there comes a point where it has to leave the wall to connect to the computer or switch. A more desirable installation will have most of the cabling run through walls. Here's where things start to get interesting. In this scenario, you're most likely going to want to connect a patch cable from your computer to a network wall jack, and then run bulk network cable through the walls to wall jacks or a patch panel next to your hub.

Should you make your own patch cables?

We see many customers purchase 1000' spools of bulk network cable, along with bags of connectors, boots, and crimp tools, with the intention of making their own cables and saving money. While this is certainly doable, there are some things to consider. First of all, unless you're quite experienced at making patch cables, it can be a time-consuming process. Also, if you don't invest in a decent network cable tester, you can waste a lot of time trying to figure out whether you have a miswired cable or other issue. Generally speaking, we recommend using bulk cable to wire into patch panels and wall jacks (a relatively easy task) and sticking with pre-manufactured patch cables for connecting devices together.



In the picture above, we've used the following equipment to achieve a typical in-wall run:

- A one-port keystone wall plate
- A blue CAT-5E keystone jack

- A run of UTP solid-core bulk network cable
- A 12-port wall-mounted CAT-5E patch panel
- A short patch cable to connect the panel to the switch.

Let's look for a moment at the anatomy of network cable, as we will need to understand this in order to wire up keystones and patch panels. Inside a network cable, there are four pairs of color-coded wires twisted together. The colors are:

Orange	Green	Blue	Brown	
Orange / White	Green / White	Blue / White	Brown / White	

Most keystone jacks and patch panels are very easy to wire up, as they have diagrams showing where to connect each of the eight wires. They will generally come with a small tool to help you push the wires into the jack. However, you will generally find two wiring diagrams, typically labelled "568A" and "568B." These are standard wiring conventions that all devices follow. For historical reasons, however, there are two differing standards. In practice, it does not matter which of the two you follow; however, whichever one you choose to use, you must be consistent with that choice throughout your network. Once you have made that decision, wiring the devices involves the following steps:

1. Pull enough wire to run between the patch panel and wall jack so that there's slack in the cable. Make sure you do not bend the wire too sharply (about 2" bending radius is a nice, conservative number). Pull a little more than you think you need, to allow you to trim extra if you make a mistake.
2. Strip about 1" of the outer jacket from the cable. Make sure you do not cut into the jackets of the individual wires.
3. Untwist the pairs of wires only enough to be able to connect them to the panel.
4. Follow the wiring diagram on the panel, using the included tool to "punch" the wire into the panel connections.
5. Repeat steps 2-4 on the keystone jack
6. Use a network tester to verify that the run has been installed correctly.
7. Finally, once you have connected the keystone jack to the wall plate, take the time to label both the jack and the corresponding connection on the patch panel with a code (such as a number) to help you trace the connection in the future.

You can repeat the above procedure for every location where you want to place a jack.

If time and budgets allow, you may want to consider connecting more jacks than you initially anticipate needing. Networks have a way of unexpectedly expanding, and you will appreciate having done that work in the beginning.

Once all of your wall jacks have been wired to the patch panel, you can mount a switch underneath the panel and connect the two together using short patch cords. (Note that although it is possible to bypass the panel and connect the cables direct to the switch, this involves crimping on an RJ45 network connector, which takes some experience and tends to be too time-consuming for the average user. Patch panels also offer a cleaner appearance.) After that, the only step left is to hook up the computers to their respective wall jacks using patch cables, configure the computers (if not already done by the operating system), and your network is up and running.

At this stage, you have a network where computers can talk to each other. While convenient, this is

usually not the only goal. You often want these computers to share a connection to the Internet. Assuming your home or office has a broadband (i.e., DSL, cable modem, or T1) connection to the Internet, connecting your internal network up is a fairly straightforward task. Broadband routers are specifically designed for this task. Simply plug the network connection from the DSL or cable modem into the "uplink" port of the broadband router, and then connect the broadband router to your switch. The router will do the job of providing internet addresses to each of your computers. Note that most broadband routers have a built-in four port switch, so if you have four or fewer computers, the broadband router can serve as both router and switch.

Here are a few other tips that are helpful when building up a network.

- In the U.S., commercial building codes require that electrical cable (including network cable) run through ceilings meet certain fire retardant properties. Generally, the use of CMP, or plenum-rated cable, is required.
- If network cables are going to be run alongside electrical cables, using shielded network cables is highly recommended. Otherwise, interference from the electrical lines can cause data loss.
- Surface mount boxes are convenient when you are running bulk cable along the floorboards instead of inside the walls. They are generally as easy to wire as keystones.
- Patch cables can be connected together using a network cable coupler. Make sure that the coupler is rated for Cat5E or Cat6 cable.

Finally, note that we have not discussed wireless networking in this article. Wireless networking has its own share of products, installation techniques, and technical issues. We will examine wireless networking in a separate technical article.