PDHonline Course G245 (2 PDH)

PC Networking for Design Professionals

Instructor: Jack H Warner, P.E.

2020

PDH Online | PDH Center

5272 Meadow Estates Drive
Fairfax, VA 22030-6658
Phone: 703-988-0088
www.PDHonline.com

An Approved Continuing Education Provider

PC Networking for Design Professionals

Jack H Warner Jr, PE

Introduction

Networks are all around us. Most of us work in offices with networks; many of us even have networks in our homes. When you visit the grocery store, chances are that all the check-out registers are networked to a server that can tally sales and track inventory, and even order more carrots straight from the producer when supplies get low. We may soon be to the point where we even wear a network!

While we walk around minding our own business, our PDA may be wirelessly networking with our cell phone to keep the contacts up to date, and synchronizing schedules with our computer when we come within wireless range. Our schedule could then automatically be made available to our co-workers all over the country via the internet. So, before we become walking web-servers, let's catch up with the current networking technology.

What is a Network?

A network is a group of interconnected computers and related devices. A network can be as small as two computers connected to each other via a single cable, or as large as you can imagine… people are already designing standards for interplanetary networks (they'd better be wireless!). Most networks fall comfortably within these extremes. For many reasons, networks have become a necessary part of working as a design professional these days. We are going to cover today's most commonly used networking technologies.

Why Network?

I'll share two basic benefits to networking. The first involves working with others. I'm primarily speaking of people in your design office, though these benefits now extend to people who are remotely connected. Before PC's, if an office had a computer, everyone shared it, either via dumb terminals that allowed several simultaneous users, or by waiting in line until it was your turn to use it. This was a pain, for sure, but all the data was in one place, and accessible to each user. Also, printers and plotters were connected to this computer, so they were always available to the user of the computer. Once PC's came on the scene, people were happy to not have to share the computer anymore. There was no more waiting in line, or having the computer slow to a crawl as someone else ran some humongous finite element problem.

The down-side was that these PC's were not connected. It was difficult to share data and peripherals. Most early PC users were forced to use a network called "Sneaker Net". This involved copying your data to a floppy disk, and walking over to another computer (wearing sneakers, of course). This is how you would share a design document or other data with a colleague. You would also have to do this to get your designs plotted or printed, as most offices could not afford to put high-quality printers and plotters on every PC. Networking fixes this, by allowing files, as well as peripherals such as high-speed printers and large-format plotters, to be shared among computers.

The second reason dates back to the years BC (Before Computers). The logistics of sharing information was a significant resource drain in a design and construction environment. A typical design office might have a full-time "gopher" (as in: go-fer this, go-fer that) running around town

getting the latest copies of the design codes, delivering base plans to the various designers involved in a project, picking up the specialty designs, taking finished plans to the blueprint shop, delivering plans to contractors and job sites, picking up shop drawings, etc. I remember times that we would have people involved for hours simply trying to figure out the quickest yet most cost effective way to get plans moved from office to office. Some of this still goes on, for sure, but networking has the potential to eliminate most of it.

Networking Basics

Here we are going to cover some fundamentals of networking. Some of it I'm sure you've heard of before, but other parts will be brand new. If some of it gets a bit hairy, don't worry. I'm going to go into a bit more detail in spots than most folks need to know, but it will be helpful down the road so you won't be as likely to go running away like a scared rabbit the next time some computer geek starts spouting off some of these terms. For example, the network in your home or office (or the one you will soon have) is probably an "Ethernet" network. But what is Ethernet? I could say it is a "net" of "ether", but that would not be very helpful. To find the truth of the matter, we have to start with something called "protocols".

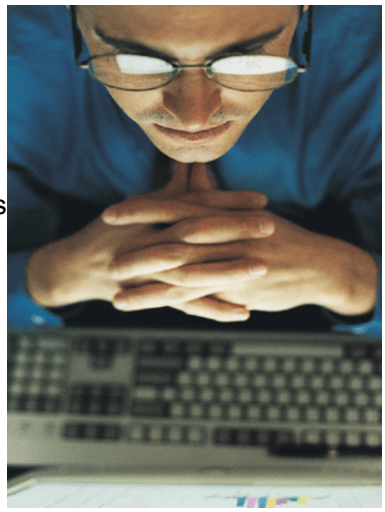
Protocols

First we'll cover something that is a bit deep, but will be handy to know later on. I'm sure you've used networked computers before, but have you ever wondered how they really "talk" to each other? I mean, you buy a computer that was made in Taiwan, and plug it into some device that was made in California, and somehow they can communicate. How do they understand each other? Well, it's not exactly English, but it is a common language. Every device on a network needs to send your data in a manner that every other device can understand, and needs to verify that it made it there correctly. Plus, there might be hundreds of devices in the network, and the data has to get to the correct device! You certainly don't want your files being saved to the wrong computer's hard drive, or your files being printed on randomly selected printers throughout the building!

This is where network protocols come in. They are a set of internationally recognized standards that define how the bits and bytes need to be sent through the wires to ensure that everything on the network is speaking the same language. The overall architecture of protocols is well described by the **ISO's (International Standards Organization) OSI (Open System Interconnection) Reference Model**. You might notice that ISO OSI is the same backwards as forwards... I don't know if they plan this stuff or what! This standard defines a framework for networking. It also leaves many details open for others to specify. The OSI, for example, does not define how Ethernet works, but provides a framework which allows for Ethernet to be specified in such a way that it will interoperate with other protocols. This graphic depicts the 7 layers in the OSI model:

Layer 7	Application Layer
Layer 6	Presentation Layer
Layer 5	Session Layer
Layer 4	Transport Layer
Layer 3	Network Layer
Layer 2	Data Link Layer
Layer 1	Physical Layer

DON'T PANIC! You don't need to memorize the names of all the layers! I just want to give you an overall picture of the number of pieces that all have to work together behind the scenes to make networking work. Most of this stuff is hidden from the user, even when installing the network, by the operating system and user-friendly installation and configuration software.



All the other standards for protocols that we use fit more or less within this ISO OSI model. Ethernet, for example, is defined by **IEEE standard 802.3.** The Ethernet standard is primarily concerned with the **Physical** layer (cabling design and such) and the **Data Link layer** (how the controller card listens for openings in traffic, and deals with collisions). If you copy a file to another computer on your network, protocols populating all of these layers could be used. The Application and Presentation layer could be the first involved, as they would be the layers the operating system (such as Windows) would communicate with. These layers would then work with the Session layer to make sure the whole file makes it to the same place. The transport layer would then ensure that the file makes it over with no errors, while the network layer would route the file across the network to the desired destination. The data link layer and the hardware layer would handle the grunge-work of getting the data in packets and sent over the Ethernet. Depending upon the network configuration, protocols may be present that represent all of these 7 layers, or just a few. Many network configurations combine functions from several layers into a single standard. As mentioned earlier, Ethernet is an example, as it covers both layers 1 and 2.

OK, this is probably more than you wanted to know, but it does at least explain why so many protocols get installed on your computer to get the network to work. In addition to getting the correct protocols installed, there are additional setup tasks required, such as naming your computer (everyone must have a unique name!), but these are usually handled easily by software installation wizards.

Let me mention just a few of the more common protocols:

Ethernet: Ethernet is the most commonly used protocol that defines the lowest two layers of the OSI. It defines how the cables are made that will connect the computers, how long they can be, how they connect, and how the basic bits and bytes are sent across the cables. Although there are alternatives to Ethernet, such as “token ring” or “ATM”, they are far less common in typical office situations. So, most computer equipment for networking that you encounter will adhere to the IEEE 802.3 Ethernet standard… and therefore work with one another.

TCP/IP: TCP/IP is actually two separate protocols, but they are used together, so I’m grouping them together here as well. IP, short for Internet Protocol, works within layer 3, the Network layer. Its job is to route data from one computer to another. It does this via Internet addresses. Every computer using IP is assigned a unique Internet address, and IP routes data through the network using these addresses. TCP, short for Transmission Control Protocol, resides in layer 4, the Transport layer. Its job is to ensure that there are no errors getting the data from one place to another. If data somehow gets garbled while traveling, TCP arranges for that data to be re-sent, and reassembles everything back to the correct order.

HTTP: The HyperText Transfer Protocol runs at the very top level: layer 7. It is the most common protocol used when viewing web pages. You might even notice it mentioned in the address bar of your web browser:

It is a protocol that is understood by your machine, and the web server, so they can communicate with each other to serve up and display web pages.

Bandwidth

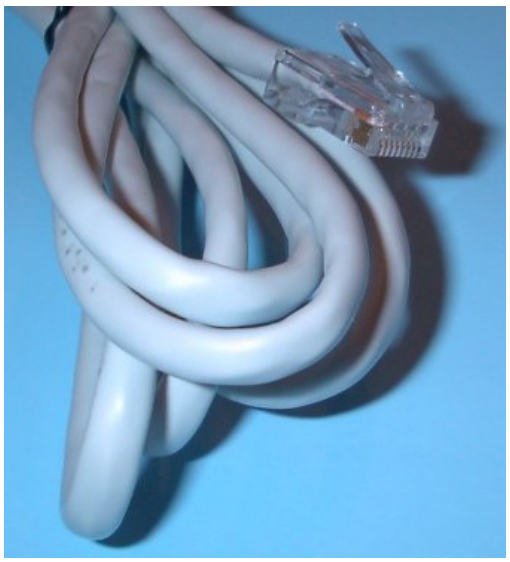
Before we get into connections and hardware and stuff, we need to make sure we all understand bandwidth. What is bandwidth? Bandwidth is essentially the *speed* with which data can be transferred from one place to another. For slower connections such as modems, bandwidth is measured in thousands of bits per second (kbps). For faster connections, bandwidth is measured in millions of bits per second (Mbps) or billions of bits per second (Gbps). If bits don't mean much to you (which they may not, as file sizes are usually given in Bytes, not bits), you can divide bits per second by 8 to convert to Bytes per second. You might notice that distance seems to have nothing to do with perceived speed... it is not measured in bits/sec/mile or anything like that. The speed of electrons, photons, and radio waves is instantaneous compared to the technology that we use to get data converted and encoded into an electron stream, photon stream, or a radio transmission.

As you now know from your study of protocols, there is extra data being sent along the wire with your data to make sure it makes it to the correct location intact. This means that you cannot directly calculate the number of seconds it will take to transfer a file over the network by taking its size and dividing by the network connection's bandwidth; but you can at least get an idea of the relative speeds of the various technologies that we are going to discuss.

Connections

Let's cover some basics of connecting devices together. I'm only going to discuss Ethernet, since it is by far the most common. There is still, however, some variety in how devices are connected together.

Wired: There are several ways to cable Ethernet devices, but **Unshielded Twisted Pair (UTP)** cable is by far the most common. It gets its name because it contains several pairs of wires, each pair twisted around each other. These wires are then covered with an insulating jacket. The ends are terminated with RJ-45 connectors, which look a lot like large modular phone connectors.



There are a few different grades of UTP cable, and the grade you use depends upon the data speed you design your network for. **Category 3** is good enough for 10 Mbps (million bits per second), and is often called 10baseT. The T stands for “twisted”, and the 10 indicates the speed in Mbps. The "base" stands for baseband. Ethernet is a baseband protocol, as opposed to broadband. What does that mean? Well, it just means that there is only one data stream, rather than several. If you have an internet connection from your cable company, for example, it is broadband, as your internet data is coming through the cable at the exact same time as *Cosby Show* re-runs.

Category 5 (“cat-5” for short) is the preferred UTP cable these days. It is a higher quality cable, and it is good enough for “Fast Ethernet”, transferring data at up to 100 Mbps. This is also called **100baseT**. The devices connected to the network, such as the network interface cards, determine the speed of the network. To avoid problems, make sure to use the correct grade of cable that is compatible with that speed. UTP cables can run the length of a football field, so cable length will not be a problem in normal situations.

There are even faster versions of wired Ethernet available. **Gigabit Ethernet (1000baseT)**, which runs at 1000 Mbps, is becoming more common in high-demand networks, and requires **Category 5e** UTP cable. Beyond that, there is 10-Gigabit Ethernet and faster, but these are not yet common. However, if you were having your office wired for networking, and wanted to make sure it was ready for the next few generations of technology, you might think about using **Category 6** cables. After all, it's only money!

I should at least mention the other types of cable that you may run into. If it is not UTP, it will be some form of **coaxial cable** or **optical fiber**. If the term coaxial, or "coax", sounds familiar, it is probably because it is the same basic construction as the cable feeding all your favorite shows from the cable company into your television. Optical fiber sounds pretty snazzy, and it is. It is made with thin strands of very pure glass, and transmits data using light. UTP is by far more common, but you will occasionally see these other two types in long distance runs, or situations with demanding specifications.

Wireless: This is becoming a very common option. By using network cards and other network devices with small radio transceivers, devices can be moved about freely within the range of the signal, with no network cabling. This is convenient in several situations, such as offices with people who like to roam about with notebook computers and PDA’s, or buildings where it is difficult to run cables. Wireless Ethernet is again governed by standards, such as IEEE’s 802.11a, 802.11b, or 802.11g. The “b” and “g” variety are the most common and least expensive. Network cards are available for notebooks, PDA’s, and desktops. Access Points, which connect the wireless devices to the wired network, are also abundant in a wide variety of configurations. You can get a device which just acts as a wireless access point, or combines that function with other conveniences, such as this device (see photo), which combines the wireless access point with a router, firewall, and a 4-port switch. The access point in the photo is an 802.11b device. This class of wireless can transfer data at speeds up to 11 Mbps for distances of up to 300 feet indoors. The “a” variety is newer than “b”, but is not nearly as common. Its big feature is that it offers speeds of up to 54 Mbps, but only at distances of about 60 feet indoors, and it is not compatible with “b”. The newest variety is 802.11g, which combines the best of both "a" and "b". You get roughly the distance of "b", with

the speed of "a", plus it is compatible with the ubiquitous "b". Even faster ones will soon be available, with standards such as 802.11n. Actually, you can purchase “pre-n” devices today, even though the standard has not yet been ratified. Buying these devices now carries a small risk of incompatibility when the standard becomes final, but many people are taking that risk in order to get the fastest speeds possible.

What is the down-side to wireless? Well, there are two points that I can think of. First, the speed is not as fast as wired networks. This is negligible when accessing e-mail, but will be noticed if you are trying to transfer huge CAD drawing files over the network. Second is security. If the security is properly set up, it can be almost as good as the security of your wired network. If it is not set up properly (usually the default configuration out-of-the-box), it's like a screen door on a submarine... not very secure! People have been known to drive around with wireless equipment looking for nearby unsecured wireless networks. When they find one, they can just park their car and access the internet, try to crack your servers, or use your internet connection for sending spam (junk e-mail) at no cost to them. In any case, an unsecured wireless network is not pretty, so be sure to take a few extra minutes to turn the security options on.

Hardware

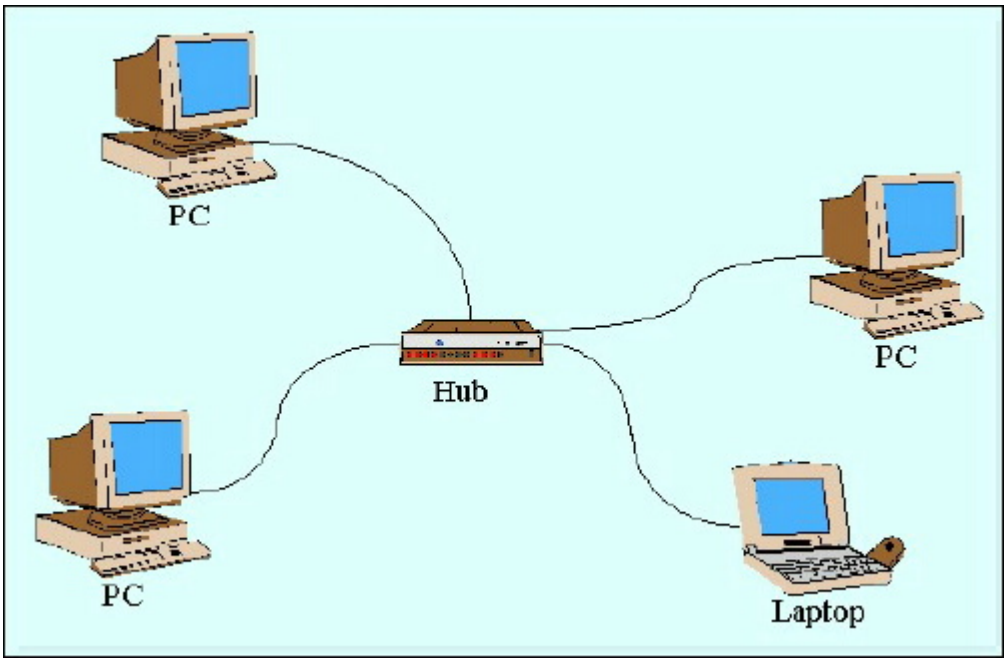
There are a few pieces of hardware that are required for any network, and many that can enhance the functionality of the network as it grows. Before you panic, let me tell you that small networks simply need some network interface cards, a hub, and cables. It’s only as networks get bigger, and need to connect to other networks, that these other devices enter the picture. So, here are a few components you'll hear about:

Network Interface Cards: For any device to connect to a network, it must have some sort of Network Interface Card (NIC). Many computers come with them built into the motherboard of the computer itself. If not, they can be added to desktop systems via add-in cards, and notebooks via a PC-Card. Though not as common, NIC’s can also be attached externally via a USB port or other connection.

Their basic function was mentioned in the protocol section. The NIC performs some of the functions in layer 1 and layer 2. Its job is to take the data that has been processed by the higher protocol layers, and get it passed to the other devices connected to the network via cable or wireless. Ethernet handles traffic much like you and I handle traffic at a 4-way stop. When it has some data to send, it “looks both ways”, and if no one else seems to be sending data, it goes ahead and shoots it out the cable. Of course, just like at a 4-way stop, sometimes two people stop at the same time, and then decide at the same time that it is their turn… and sometimes they collide. Ethernet does the same thing, only nobody has to exchange insurance information… it just says “oops”, looks again, and gives it another try. This helps to explain why, as a network gets more and more devices, it often begins to appear to slow down. Frequent collisions cause a lot of data to be re-sent, thereby slowing things down.

Network cards for typical computers need not be expensive. NIC’s that are to be used in a file server usually deserve a card with some extra features, but typical computers do fine with a run-of-the mill NIC. The *speed* of the card, however, is very important. Cards are specifically designed to run at 10 Mbps, 100 Mbps, or faster. Most are capable of switching between their top speeds and slower speeds to match the equipment at the other end, but this is an important detail to watch when creating or modifying a network.

Hubs: Ethernet networks using UTP cable to connect 3 or more devices require hubs or switches to connect all the devices to each other. Each computer in the network runs a cable from its NIC to the hub, so it is good to locate it in a central location. They come in all sizes, starting with small ones with only 4 ports (a port is a place for a device to plug in), all the way up to dozens of ports. And if that's not enough, they can be daisy-chained (connected together into a virtual mongo-hub)… but be sure to read the directions to do it right! Interconnected hubs don't even have to be in the same physical location, which can be very convenient. You can locate one hub in a central location, and connect it via a single cable to hubs in different departments, and these hubs can then be wired to each computer in that department. This avoids running lots of really long cables to a central hub.



Just like when choosing NIC's, you must pay attention to the speed of the hub. The ports will be designed for 10 Mbps, 100Mbps, or faster… and often be capable of automatically switching speeds to match the speed of the connected NIC's. Fancy hubs have fancy network-management features, but the inexpensive ones work fine in routine situations.

Switches: A switch is similar to a hub, and everything mentioned about hubs above is true for switches. They contain a bit more complex electronics that can cut down on network congestion, frequently resulting in higher throughput. Now I'll tell you how they accomplish this. When data is sent from a computer to the hub, the hub forwards the data to every port, and therefore to each computer NIC connected to the hub. It's sort of like a shotgun… the data hits it's target, but also every other computer in the network. The NIC's all see the data packets, but ignore it if it is not for them. When you get a large number of computers all sending data all over the network at the same time, things slow down. As I mentioned earlier, the Ethernet NIC needs to wait until there is a quiet moment to send its data. When large amounts of unwanted data arrive at a NIC, it has to wait until it detects "quiet", and the more traffic, the longer it might have to wait. Also, higher traffic results in more of the "collisions" mentioned earlier, resulting in data having to be sent again, and slower performance.

Switches help alleviate some of the unnecessary network traffic by figuring out which port the destination computer is on, and sending the data only out of that port. The price of switches has come down significantly, so anyone shopping for a hub should *seriously* consider using a switch instead.

Bridges: A bridge is a device that connects two separate networks together. It listens to data coming from each network, and determines if it is addressed to a computer on the other network. If it is, it passes it across to the other network. The two networks could be similar, but if they are different, some bridges are capable of transmogrifying (yes, that is a made-up word… if you don't like it, substitute "translating") the data packet into the form expected on the other network. This would be useful if the design department had a new network, and accounting had an older network, and you wanted to connect them together

Routers: A router is a special kind of bridge. They can also connect networks, again either similar or networks with protocol differences. They can also work with other routers on the network to direct the traffic for improved throughput. Routers are commonly used to connect networks together that are quite a distance apart, and connected using phone lines, or the internet.

Firewalls: A firewall is a special type of router that sits between your network and the internet. It routes all outgoing traffic to one internet connection, and most importantly, examines traffic coming from the internet side to make sure it is data that you authorize to come into your network. If it is unauthorized, it is blocked. If it *is* authorized, it allows it onto your network and routes it to the correct machine. A firewall may be a piece of hardware dedicated to just that function, or it may be incorporated as a feature into some other type of device. It can even be an application running on a PC set up for this purpose. This function grows more important each day, as the types of malicious attacks that can affect your machines continue to grow.

Some Different Network Scopes

LAN's

A **Local Area Network**, or **LAN** for short, is what most people imagine when you say "network". The key point here is the word "local". Everyone on a LAN is in the same physical location. A small LAN may connect just a few computers in a small office; but hundreds of computers connected throughout several floors of a large building can also form a LAN. As long as it is constructed as a single network, it needs only consist of devices with interface cards, hubs and/or switches, and cable. These devices will mostly be typical desktop or notebook computers, but can also be several other things. Some printers, scanners, and storage devices have built-in NIC's and can connect directly to the network without attaching to a computer. These types of devices usually cost a little bit more than similar devices that require a connection to a single computer, but allow much more flexibility in use and placement. Another type of device often found connected in a LAN is a "server". Servers are not required, but become beneficial once the network grows beyond just a few people. I'll have more on them just below. Here are two terms commonly used to describe LAN's:

Peer to Peer Network: When you establish a peer-to-peer network relationship, there is no server involved. Say there are two people; I'll call them Bob and Larry, who are connected together over a network. Bob could "share" folders on his computer's hard drive, or share his printer, so that Larry could access them. This capability is built into Windows, and is fairly easy to set up. Bob can require Larry to use a password, thereby giving his files some security. Larry can also share resources so that Bob can use them. Peer-to-peer networks can be set up with more than two people, of course, and each person controls everyone else's access to his files and devices. Those persons who want to participate set their machines to be in the same "workgroup". This is the simplest way for a small office to share files, and share a few high quality printers and plotters.

Network with a Server: Peer-to-peer has some drawbacks, and as a network grows, it often becomes worthwhile to add a server or two. A server is an application running somewhere on the network to provide a "service" to the users. A network can have one or several server applications running. Server applications are usually run on machines dedicated just to running these services. Servers can be set up to hold files, to manage printers, to manage back-ups, to route e-mail, and many other functions. The most common server on a network is a “file server”. As its name implies, its primary function is to store files so that users can access them.

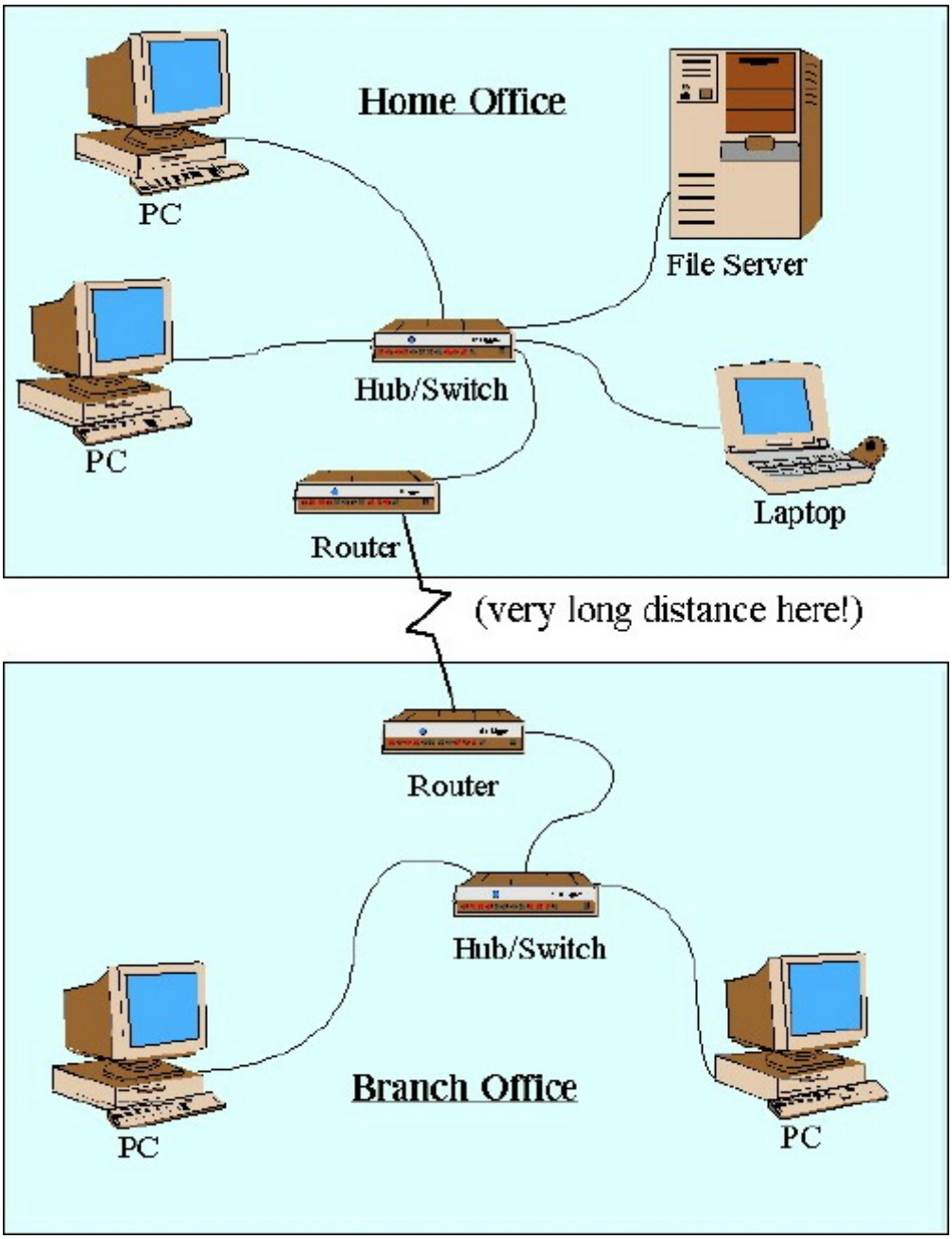
Here are a few of the benefits of keeping shared files on a file server:

- Bob doesn’t have to worry whether Larry remembered to leave his machine on when he left work early. Servers are usually left on 24-7.
- Bob does not have to worry about his program hanging when Larry’s computer freezes up because he was playing a buggy version of “Duke Weingarten and the Aliens from Planet Scum”.
- Larry’s computer does not slow down when Bob runs a program that does a lot of file access on his shared files.
- Servers are usually optimized to make file access faster than in a peer-to-peer configuration.
- With the organization’s important data in one spot, data backups can be done in a more controlled manner.
- The security of the files is controlled in one location, rather than on each user’s machine.

Server systems usually run a special network operating system, or NOS. Typical NOS’s are Windows NT Server, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Netware, or Linux. Since a server is responsible for the security of the data or other resources, user accounts are set up on the server for each user, and each user must set up his computer as being in the "domain" of the server.

WAN’s

When you connect users who are geographically separated, you have a Wide Area Network, or WAN. This is very common if a company has branch offices. A WAN allows the branch offices to behave as if they were on the same LAN as the home office. You might remember earlier that we mentioned a component called a “router”. These are very common in a WAN situation. It might look something like this:



The physical connection between the locations used to always be via some sort of telephone line, or radio link. Now it is becoming very common to link locations via a “virtual private network”, or VPN. This solution does not require a dedicated connection. VPN hardware or software encrypts the data on one end, sends it through the internet, and VPN hardware or software on the other end receives the encrypted data, un-encrypts it, and passes it into the LAN. Many routers are available with VPN capabilities built-in.

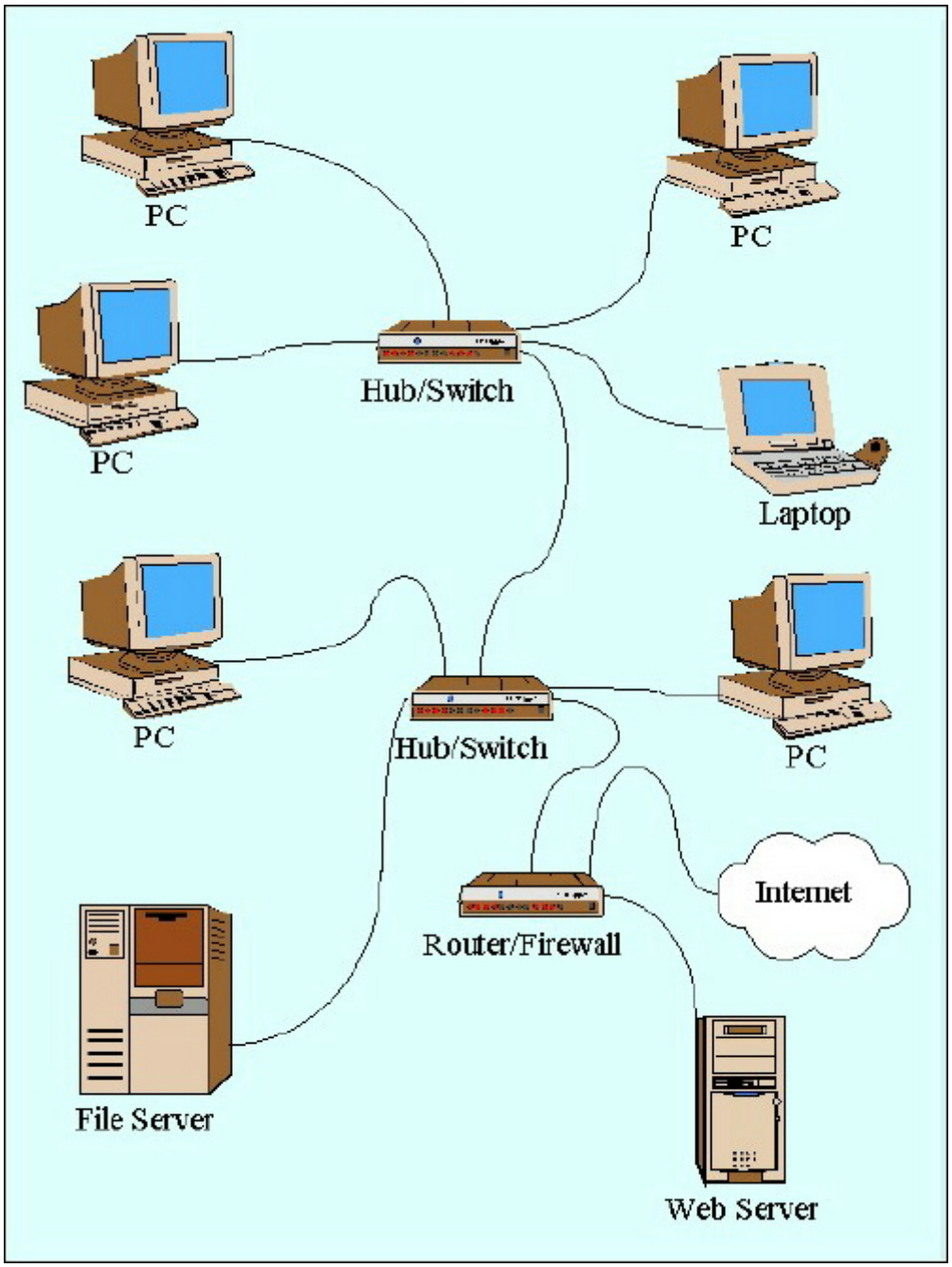
The Internet

The internet is a world-wide network consisting of millions of computers. It started out as sort of a WAN for the US government and University researchers to link up, and grew into the huge world-wide multi-purpose network we know today. Most design professionals have a connection to the internet at work, as well as at home, so you already know there are different types of connections to the internet.

For a single machine at home or at the office, one simply needs to contact an ISP (Internet Service Provider). The ISP has a very fast connection to the internet, and they will provide you with a way to connect to the internet through them. The most common connection to an ISP is through an analog modem and POTS (plain-old telephone service). This is usually the cheapest service (sometimes even free), but is limited in speed, requires dialing-up every time you want to connect, and can result in angry family members or co-workers because you are tying up the phone line.

A single machine can also connect to the internet at higher speeds by paying for extra ISP service from a phone company (DSL) or the cable company. When connecting a LAN to the internet, there are more options, and more issues to be concerned about.

When connecting a LAN to the internet, security becomes a huge issue. You need to make sure that outsiders cannot access your data, that your machines cannot be hijacked for disreputable purposes, and that viruses are kept out. At the minimum, a router is a must to provide some of this security. It provides a simple “firewall” to prevent some mischief. As your network becomes larger, and you find yourself having to provide more internet access for functions such as hosting your web sites, and running VPN’s, the solutions become more complicated and more costly. Though I know some of you are avid do-it-yourselfers, I should mention that these are the sort of things consultants are very useful for. It’s also important to make sure you have good virus protection protecting your servers, your e-mail, and your machines. Though the internet is a necessity in today’s business world, an unprotected connection to the internet can allow all kinds of bad stuff into your network. Here is a small network set up with an internet connection:



There are all kinds of uses for an internet connection. Besides the obvious e-mailing and research, people are even taking advantage of the internet to run programs that they do not own… they just rent them when needed! Companies called **ASP's (Application Service Providers)** license expensive programs, such as finite element analysis software, for use over the internet by the hour or by the month. You can use it to try before you buy, or just to save money on applications you do not often use.

Some Final Points

Networks are a requirement in today's business world, for design professionals, as well as just about anyone else. They have come a long way in just a few decades, in capability, and simplicity. It used to be a major ordeal just to install a network interface card, and a HUGE ordeal to set up a server and connections and everything. We're talking days and days of work, lots of money, and animal sacrifices. Today, simple networks can be set up for much less cost and time, and *NO* sacrifices. A small office with 4 or 5 computers could be set up with a peer-to-peer network and an internet connection in a day by one person with a bit of computer knowledge and the wherewithal to read the manuals and a good do-it-yourself networking book. Servers are still a bit challenging to set up, but again can be done by someone with some computer experience, the desire to learn by reading and doing, and patience. Again, this is a pretty good use for a consultant. As another alternative to traditional servers, vendors are now marketing server "appliances". These are (fairly) user-friendly boxes that can serve a select group of functions, such as acting as some combination of file server, router/firewall, web server, and/or mail server for a small office network.

If your office is less than a dozen people, you may do just fine to find an employee who loves tinkering with computers, and can handle the office network setup and maintenance as an extra item in his job description. There are several good books out there that will assist someone in such an endeavor. When the network gets larger, and the desired uses increase (web-hosting, groupware, etc.), it will be time to bring in consultants as needed, and make "IT" more of a full-time position.

The benefits of networking are numerous. Besides sharing data files and high-quality printers and plotters, there are many types of applications that help a group work together more efficiently.

Here are just a few:

- Group calendars make it easy to see where people are, and when meetings can be scheduled.
- E-mail both within the office and to others via the internet is an indispensable way to avoid telephone tag, and to provide documentation of the communication.
- Groupware allows users to contribute to and view documents, anything from project specifications to employee benefits.
- Job Web sites are becoming more common, as a way for everyone involved in a job to access job information via the internet. Everyone from the architect to the sub-contractors can view drawings, specifications, and change-orders.
- Drawings can be made available on-line for plotting at any location, or at the nearest reprographics shop.
- Internet access is good for many things, such as searching for product specs, doing research, or taking an on-line continuing education course.

So keep your eyes open for new uses. There is no doubt that our networks will continue to grow, and we will find new ways to leverage them for greater functionality and productivity.