The Home Network

Section Two

Making personal computers cooperate with each other...

Introduction

GENERAL

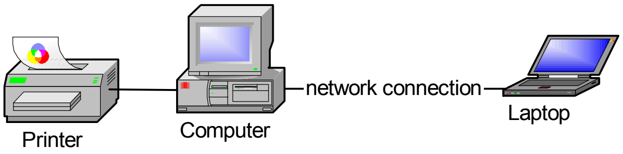
More and more homes have two or more computers. Many homes have a desktop (as a stationary system with all peripherals attached) and laptop (for portability) computers. To cut costs these home computers are connected together using a simple local area network. This section describes several scenarios in which a home network might be put together.

The Two Computer Network

SIMPLY LAN

Local area networks (LANs) are based on two or more computers *somehow* connected together to share resources. I say *somehow* because there are many ways to connect two or more computers and these ways involve many options and technologies. The bottom line is that these computers combine to create a “team” of devices to accomplish tasks. If we look again at our example in chapter 1 (figure 1 below), we see that two computers share one printer.

FIGURE 2 - 1. **Two Computer Network**



We have not defined a network connection at this point -- only that there must be *something* between both computers in order for a LAN to exist.

The *computer* in figure 1 is directly connected to the *printer* and acts as the *print server* sharing that device with the *laptop*. Without server software, this LAN is considered a *peer to peer* network. The *computer* and *laptop* can print to the *printer* as long as the *computer* and *printer* are both on.

If all of this seems a bit confusing then we understand each other. My description of figure 1 is that of one a network engineer might offer. To the average person this would not really describe what they see. Let’s take a moment to recap and explain figure 1 a little bit better.

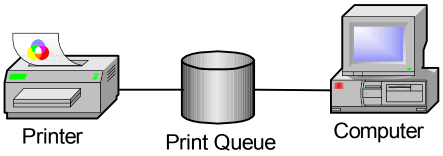
We actually see five things in figure 1:

1. Printer
2. Printer connection
3. Computer
4. Network Connection
5. Laptop

THE PRINTER/COMPUTER RELATIONSHIP

The printer is connected to the computer by either a cable (Parallel, serial, USB) or wireless (infrared, microwave, etc.) - at this point the communication media is not our concern. The computer communicates to the printer in the same way it would without the LAN (at this point the LAN is also a mute concern). As all printers do, it is fed by a *print queue* (a folder on the computer that temporarily holds the print job until the printer is ready to process its content). As the print buffer (a memory space on the printer) is fed by the print queue, the size of the file in the print queue folder is reduced. Once the print job is emptied the file in the print queue folder is removed.

FIGURE 2 - 2. **Printer/Queue/Computer**



What is most important to understand here is that the computer processes print jobs for the printer through a folder found on the *computer*. The print queue is a folder for temporary files that have been modified from the files you create in your application (such as a word processing file) to a format that your printer understands. Embedded in the original file is commands that tell the printer how the output should be processed. These files can have commands for fonts, formatting and page layout.

This is what would be printed on a page from the printer:

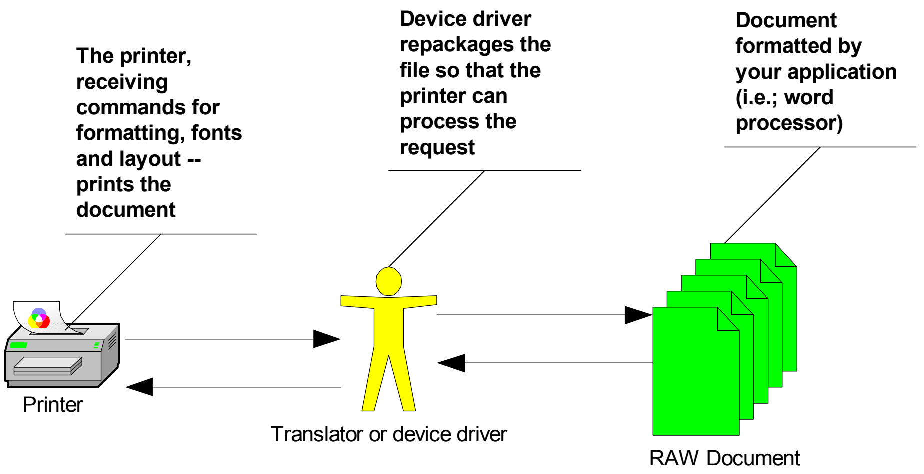
Hi there

This is a sample of what is sent to the printer:

```
E□%-12345X@PJL ENTER LANGUAGE=PCL3GUI
□E□&u600D□*o5W□    □□□□&l2A□&l1H□&l-
2H□&l0M□*o0M□*g26W□□□X□X□□□,□,□□□,□,□□□,□,□□□&l0O□&l0E□*p0y0X□&l0L□*r1A
□*b0m296y2m18v¶□□□üþ□□□ü□?Àû□□□ü18v¶□□□üþ□□□ü□?Àû□□□ü12vÛ□□ □
□€þ□□À13vÜ□□□@□□□þ□□□ 13vÜ□□□`□□□þ□□□`12vÛ□□€□
□€þ□□€12vÛ□□
À□
```

The formatting process converts your document into a language it understands (this formatting process is mirrored throughout computer interactions with other devices as well). It is the *device driver* that modifies information so that each device can complete their assigned tasks. So it can be said that the device driver is the translator for information from one device (computer) to the other (printer). These languages are optimized for their device so that you get the best performance from each device you buy.

FIGURE 2 - 3. Document Translation Process

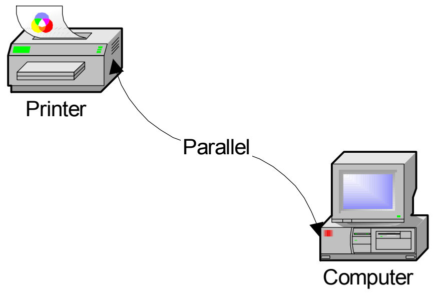

The printer, receiving commands for formatting, fonts and layout -- prints the document
Device driver repackages the file so that the printer can process the request
Document formatted by your application (i.e.; word processor)
Printer
Translator or device driver
RAW Document

The printer driver resides in the computer. The print queue acts as the stagging area for the repackaged document (processed by the print driver). What is delivered to the printer is the processed document. The print driver (repackaging the document for the printer) also controls the communication from the computer to the printer negotiating the job and feeding the document until the close of the print job (terminating the job and releasing the printer for the next job to begin). It is this process that allows many documents to be printed in succession and maintaining the print job until completion even when something stalls or stops the printing process.

PRINTER CONNECTION

A printer connection is the physical relationship between the printer and the computer. By this I refer to either the cable or wireless connection that acts as the conduit for information to travel to and from both devices. This must be a two way connection since a file may be larger then the printer can store in order to process to print job. As previously stated, the print driver must negotiate the full download of the print job so that the printer knows when the job is done and the next one begins. Cables give the best visual description for understanding a printer connection. When dealing with wireless printer connections it is always a good practice to think of it as a physical connection so that you can troubleshoot problems more simply.

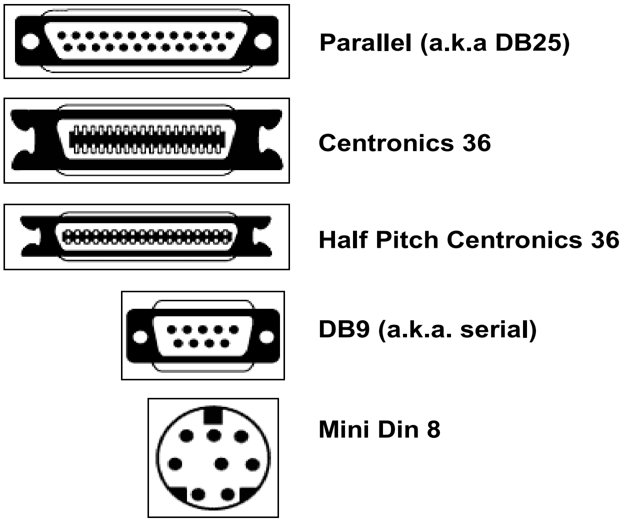
FIGURE 2 - 4. **Printer Cable**



The traditional printer connection is the parallel[53] cable (figure 4 represents a parallel printer connection). In this case a physical twenty-five pin cable is connected from the printer to the computer. As long as this connection is maintained the only thing that can stop the printer from processing each print job is either the loss of power (to either device), lack or supplies (paper/ink) or a failure of the device driver to translate the request. Usually when the print driver fails the printer starts spewing out nonsensical data (random characters). If there is no power to the printer (or you ran out of supplies) then the print queue will broadcast a message to you noting that the printer is off line.

[53] In the context of the Internet and computing, parallel means more than one event happening at a time. It is usually contrasted with *serial*, meaning only one event happening at a time. In data transmission, the techniques of time division and space division are used, where time separates the transmission of individual bits of information sent serially and space (in multiple lines or paths) can be used to have multiple bits sent in parallel.

FIGURE 2 - 5. **Printer Connections**



- **DB25** is also called a D-shell 25 pin connector or a Type A connector. A DB25 is a typical parallel printer connection on the PC end. These are IEEE 1284[54] compliant connectors.
- **Centronics36** are also called Type B connectors. A Centronics36 is the typical parallel printer connection on the printer end. These are IEEE 1284 compliant connectors.
- **Half Pitch Centronics36** connectors are also called Type C connectors. These are often used on laptops because of their compact size. These are IEEE 1284 compliant connectors.
- **DB9** is a typical serial printer connector. This connector is found on monochrome monitors, serial mice, and other serial devices.
- **Mini Din 8** Macintosh Image Writer and Laser Writer connector. Also used for some serial printers.
- **Universal Serial Bus** (USB) is the latest printer cable scheme that improves performance and adaptability. We will discuss this technology in greater detail later in this book.

Most (excluding centronics) of these connection ports are located in the back of your computer. The bottom line is that there are only so many places that the printing process can fail:

1. Printer - power, paper, or ribbon
2. Print Driver or queue
3. Printer Connection

[54] The 1284 standard defines 5 modes of data transfer. Each mode provides a method of transferring data in either the forward direction (PC to peripheral), reverse direction (peripheral to PC) or bi-directional data transfer (half duplex).

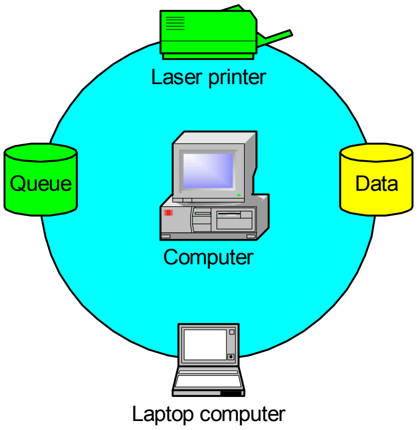
COMPUTER

The computer is the base for processing information to the printer and the laptop in our example. It acts as the *print server* (connected directly with the printer) and communicates with the laptop using a network interface. Further it acts as the desktop for creating documents and processing data. The computer is a multiprocessing[55] tool that also coordinates other tools.

The computer *hosts* disk space, printer queues and communication with the laptop. Printer and file sharing must be offered by the computer for this to happen. By default, most operating systems do not turn sharing on because sharing resources can open security holes and make the computer vulnerable to attack. In sharing the local printer with the laptop, the computer must allow the laptop to copy files to the print queue folder on the computer. In figure 5 the computer also offers data storage for the laptop to copy non-printer related files as well. In allowing the laptop to copy files to the computer, there is always the chance that damage can occur.

In performing these chores, our computer is also multitasking[56], running more then one program (keeping track of each program) so that you can hop from one open application to the other. Our computer also hops from one program to another in the background (printing to the printer and communicating with the laptop) without you realizing it.

FIGURE 2 - 6. Juggling Devices



[55] Multiprocessing is the coordinated processing of programs by more than one computer processor. Multiprocessing is a general term that can mean the dynamic assignment of a program to one of two or more computers working in tandem or can involve multiple computers working on the same program at the same time (in parallel).

[56] In a computer operating system, multitasking is allowing a user to perform more than one computer task (such as the operation of an application program) at a time. The operating system is able to keep track of where you are in these tasks and go from one to the other without losing information. Microsoft Windows 2000, IBM's OS/390, and Linux are examples of operating systems that can do multitasking (almost all of today's operating systems can). When you open your Web browser and then open word at the same time, you are causing the operating system to do multitasking.

As you may have started to realize, the computer requires additional resources (memory, diskspace, etc.) to serve printing and communication resources for the laptop and printer. The printing process alone will noticeably slow down the computer when the laptop is printing material.You should gauge your resources to meet those needs.

NETWORK CONNECTION

The Network connection can be made two ways (depending on security and the physical environment):

1. Cable
2. Wireless

There is a variety of options for both cable and wireless. Since the price of wireless network connections have gone down in recent years there are many who believe that the home wired network is coming to an end. I believe that you should think carefully before considering wireless. The most common wire-based network connectors found in the home is RJ45 (see figure 7). The second most common wire-based network connection found in the home is BNC (see figure 7). All other wire-based network connectors displayed here are more common to older networks found in industry or office environments. Most national brand personal computers come with RJ45 network interface cards (also known as 100BaseT[57])

Properties of a wired network are:

Advantages

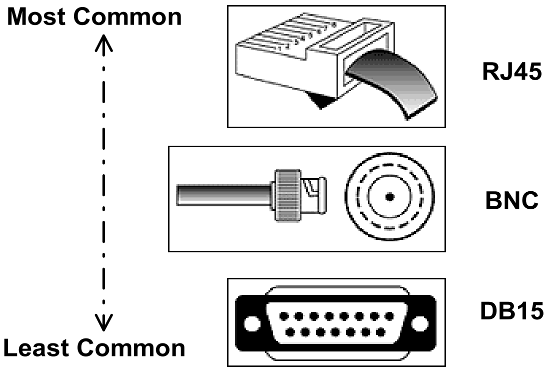
- Simplicity
- Distance (328 feet and up)
- Reliability
- 802.11a and 802.11b standards
- Security

Disadvantages

- Messy
- Difficult to hide
- not upgradable
- Fixed positioning of equipment
- Hard to add connections

[57] A.K.A. Fast Ethernet - 100BaseT: 100BaseT is an extension of the 10BaseT standard, designed to raise the data transmission capacity of 10BaseT from 10Mbits/sec. to 100Mbits/sec.

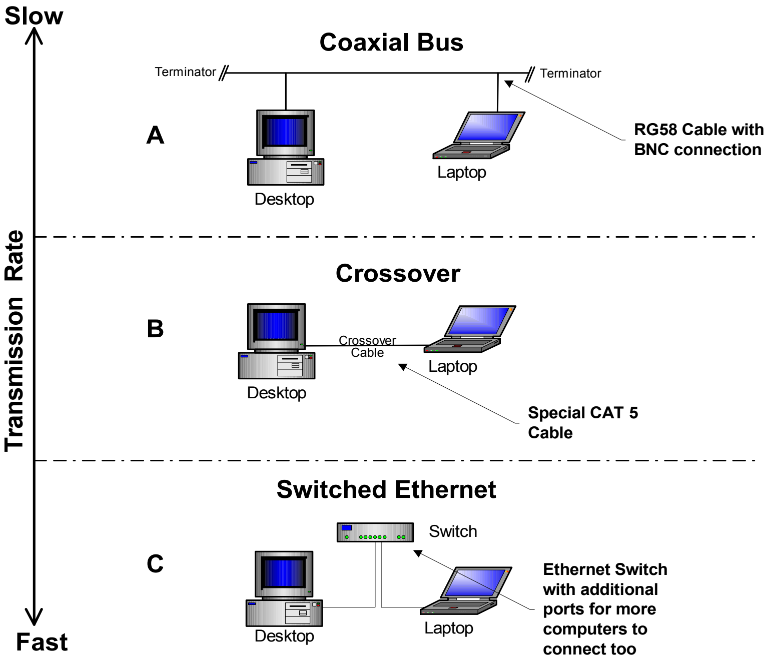
FIGURE 2 - 7. **Wire-Based Network Connectors**



- Short for **Registered Jack-45**, an eight-wire connector used commonly to connect computers onto a local-area networks (LAN), especially Ethernet.
- The **BNC** (Bayonet-Neil-Councelman) connector is very common in many different applications. You will see this connector on many different devices, from monitor cables to network patch cables. Most commonly this connector will be found in a 10Base2 network environment attached to RG58 coax ("ThinNet") cables.
- Another versatile connector, the **DB15** is used for everything from connecting your joystick to your PC to connecting a 10Base5 network. In a network setting you will often find DB15's attached to bulky coax ("ThickNet"). This connector is often called an AUI connector.

Topology[58] (how cables are physically deployed)

FIGURE 2 - 8. **Common Topologies**



In figure 8, we see three basic topologies that can be used for wired networks in the home:

- **A** - **Coaxial Bus** - using RG58 coaxial cable (looks much like the cable used in cable TV). This cable is fairly thick by modern standards and must be terminated at both ends by a 60 Ohm resister. The Coax bus was one of the most common topologies in early networking.
- **B** - **Crossover**[59] - using a special cable that connects to both RJ45 connectors, this is the cheapest method for connecting two computers together. It offers better speed then the Coax Bus and is less messy. A crossover network (such as in figure 8) is limited to two computers.
- **C** - **Switched Ethernet** - Using common CAT 5[60] cables, connected to a "switch" that allows for many connections. Usually 5 or more ports are available to connect

[58] A topology (from Greek *topos* meaning place) is a description of any kind of locality in terms of its layout. In communication networks, a topology is a usually schematic description of the arrangement of a network, including its nodes and connecting lines. There are two ways of defining network geometry: the physical topology and the logical (or signal) topology.

[59] A crossover cable is a cable that is used to interconnect two computers by "crossing over" (reversing) their respective PIN contacts. Either an RS-232C or a telephone jack connection is possible. A crossover cable is sometimes known as a null modem.

[60] CAT 5 is a 100 bit per second version of twisted pair used with RJ45 connectors.

computers together. This topology allows for greater expansion then the crossover topology and easier to deploy then the coax bus.

Properties of a wireless network are:

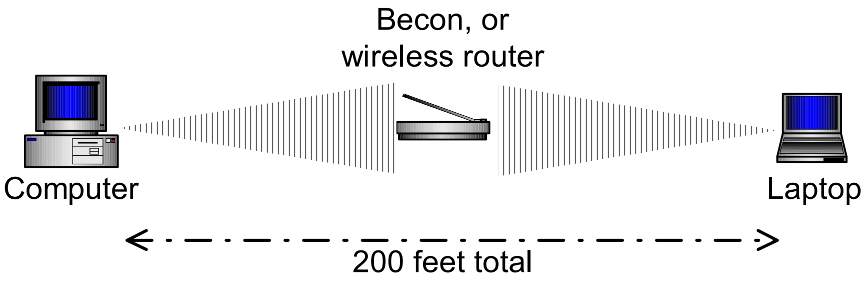
Advantages

- Less visible
- Easy installation
- Mobility
- Easy to add connections

Disadvantages

- Limited distance (100 feet)
- 802.11a and 802.11b standards are incompatible
- No connection tracking
- No security

FIGURE 2 - 9. **Wireless network diagram**



You can see in figure 8, as long as you are within 100 feet of the beacon (or wireless router), and you have a wireless network card installed, you are part of the network. The most common current wireless network protocols[61] are in the 802.11x[62] family, sometimes referred to as Wi-Fi (Wireless Fidelity). Problems arise when someone from outside your network is within communication range and has a wireless network interface card -- they can gain access to your network as if they were wired to it. Unless you have the knowledge to lock out unwanted users, the default configuration for a wireless network is to give access to everyone who asks.

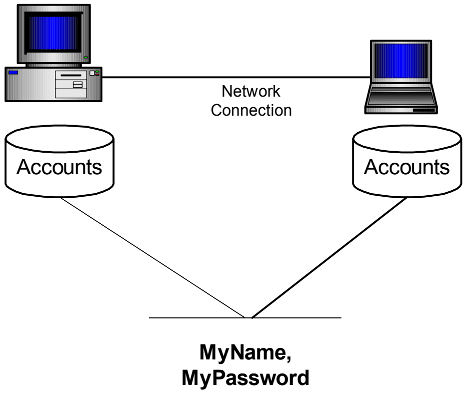
[61] A preliminary basis of which negotiations are carried on. Protocol is the common communication bond by which two entities can disseminate and resolve differences.

[62] 802.11 is a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). There are currently four specifications in the family: 802.11, 802.11a, 802.11b, and 802.11g. All four use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.

LAPTOP

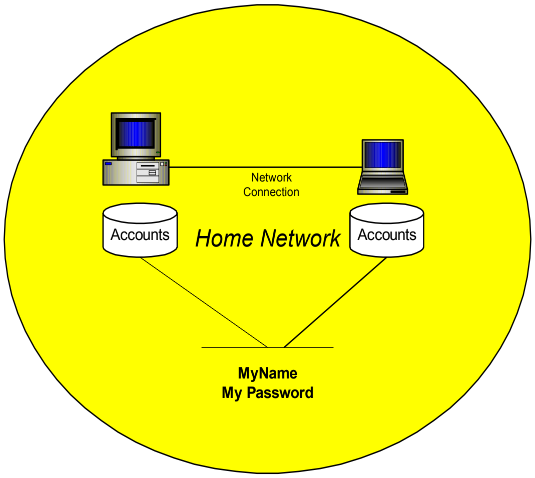
Finally, our laptop acts as another computer (often in networking referred to as a “node” or “host”) on the network. The laptop also requires access to the printer through the print queue (offered by the computer). Although the purpose of the laptop is less pivotal then the “computer” in our example, it must have many things in common.

FIGURE 2 - 10. **Authentication**



For the laptop to use printer resources and/or the computer’s shared folders, both computers must have the same user accounts. These accounts must also have the same passwords. There should also be a peer-to-peer *workgroup* to localize what you would see in your local network browser[63]. Figure 10 displays a workgroup named Home Network.

FIGURE 2 - 11. **Workgroup**



[63] Network browser - an application that allows the display of local and remote resources available in either your workgroup or domain. Objects are displayed as computers, servers, shares or printers. Some network browsers reflect additional objects such as pda’s and mobile devices.

The main problem with peer-to-peer networks is the hastle of updating each computers account/password information. The more computers you add to a peer-to-peer network (a.k.a. workgroup) the more times you have to update each of the individual account/password information. If you add another printer to the mess, you have to update all of the accounts/passwords for each computer in the workgroup as well as any additional printer information. The bottom line is that workgroups are for small networks.

The greatest troubleshooting problem with workgroups is the failure to keep all account information the same. It is too easy to loose track of which system is up to date. The errors you receive when they are not up to date is generally ambiguous and misleading. The baseline for reaching the limits of a workgroup (or peer-to-peer) network is generally ten computers on the same network. Once you exceed ten computers on the same network, having to keep track of all the accounts and passwords, printers and queues, becomes an overwhelming task for any one person. Don't get me wrong, it can be done by a single person -- but that will be the primary task of that person.

NETWORK PROTOCOL

As you have begun to see, there is this thing called "protocol". It helps the printer communicate with the computer, and other computers communicate with each other. Just as in politics, protocol represents an agreement between two or more entities so that they know how to react with the other. Previously, we discussed a protocol between a computer and it's printer. Here we discuss the standard protocol used for computers on a common network. While there are many protocols available (and many better then the most commonly used one we will discuss here), TCP/IP[64] is the defacto standard.

TCP/IP (Transmission Control Protocol/Internet Protocol) has become the defacto standard for most (if not all) modern operating systems designed for personal computers. This is much like designating a single etiquette for all the Earth's population to interact. We will look more closely at TCP/IP and it's many layers further on, for now we want to address the immediate concerns of how it is used in a home computer.

What the average person must know:

- Installation
- Configuration
- Troubleshooting

Installation

Installing TCP/IP is fairly straight forward. Since most modern operating systems use TCP/IP as the default network protocol, connecting an active network to the network interface card will usually prompt the operating system to let you know that something has changed. Usually, if an installation CD is required, you will be prompted for any additional software (drivers). The key is to review your documentation and follow the

[64] TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

directions provided by either your computer or operating system. Since each operating system has their own dialog for installing drivers and/or software you should review all supporting manuals regarding TCP/IP.

Configuration

Configuring TCP/IP requires a little forethought. Assuming you have two or more computers, you will need to verify the following:

- If your computer lets you get to a command prompt (for Windows "C:\:) type **IPCONFIG** and note the information you get back.

  - **Host Name** - *can be anything you like (as long as there are no two computers in your network with the same host name).*

  - **IP Address** - *based on what your computer finds or how you wish to define it -- we'll get into the details in a little bit.*

  - **Gateway** - *is the address to a routing device connected to another network (such as the internet).*

  - **Subnet Mask** - *a filter used to speed up the search process for local network objects, also used to separate and seclude network sections on a given local area network.*

  - **Primary and secondary DNS**[65] - *database servers that are responsible for providing name resolution on the local network - this will also be discussed in more depth later on.*

  - **Domain or Workgroup** - *a group definition for your local area network (domain is usually associated with large networks while workgroups are generally small groups of computers. There's more to Domains but we will discuss this further).*

The following is an example of what a common home TCP/IP configuration might look like:

[65] The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

FIGURE 2 - 12. IPCONFIG /ALL

```
Windows IP Configuration
Host Name . . . . . . . . . . . . : MyPC
Primary Dns Suffix  . . . . . . . :
Node Type . . . . . . . . . . . . : Unknown
IP Routing Enabled. . . . . . . . : No
WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : Cabletron DE500B PCI
Fast Ethernet Adapter (21143-PC)
Physical Address. . . . . . . . . : 00-00-FF-06-7B-38
Dhcp Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . . . . . . . . : 169.254.1.2
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . :
DHCP Server . . . . . . . . . . . :

Lease Obtained. . . . . . . . . . :
Lease Expires . . . . . . . . . . :
```

Troubleshooting

Figure 12 looks a bit confusing to the untrained eye, but if we take a moment to look at the information we can better understand what going on and how we should use the information to troubleshoot our network configuration.

- **Host name** - randomly generated if you don't name it yourself. In this case I have named the computer "Mypc"
- **Primary DNS Suffix**[66] - is empty indicating that this system is not connected to the internet nor part of a larger network domain.
- **Node Type** - unknown
- **IP Routing Enabled** - No - meaning that this machine is not part of any network routing scheme (this will become more understandable later on).
- **WINS**[67] **Proxy Enabled** - No - meaning that this is not part of a network using Microsoft's LAN Manager name resolution.
- **Connection-specific DNS Suffix** - empty - meaning that this machine is not configured to work in a larger "domain centric" network.
- **Description** - the NIC driver name bound to the physical hardware (or NIC Card).

[66] The domain suffix provides you with a clue about the purpose or audience of a Web site or domain. The domain suffix might also give you a clue about the geographic origin of a Web site. Many sites from the United Kingdom will have a domain suffix of.uk.

[67] Windows Internet Naming Service (WINS), part of the Microsoft Windows NT and 2000 Servers, manages the association of workstation names and locations with Internet Protocol addresses (IP addresses) without the user or an administrator having to be involved in each configuration change.

- **Physical Address** (or MAC address) which is applied at the factory and unique to all NIC cards.
- **DHCP**[68] **Enabled** -yes - the default for any network configuration not set up manually.
- **Autoconfiguration Enabled** - yes - also the default for any network configuration not manually set up.
- **IP Address** - 169.254.1.2 - the *169.254.x.x* address, when assigned to your computer, means that a DHCP server could not be found and that a default IP address will be used for troubleshooting purposes.
- **Subnet**[69] **Mask** - 255.255.255.0 - in this case computers on the network will only discover other computers by the last octet (last number in the IP address series (in this case ".2"). It will ignore all other computers that *do not* have the 169.254.1 number series. The 255.255.255.0 subnet mask indicates that the first three octets must be identical for each computer to be in the same network. This is also better explained later on in this book.
- **Default Gateway**[70] - blank - meaning there is no access to other networks or the internet currently available.
- **Default DHCP Server** - blank - meaning that there is no DHCP server available.
- **Lease Obtained** - blank - no configuration information was gathered from outside your computer.
- **Lease Expired** - blank - no configuration information will expire on a given date.

The information gathered from your machine through the IPCONFIG command tells you that this computer is not part of a larger network, nor is it connected to the internet. Further, there are no network management servers (such as the DHCP and DNS servers) to organize the computers. This network setting will allow our two computer network to work as long as it is not part of the internet. We can print, copy files back and forth, but we can not share outside of our little environment.

SUMMARY

The two computer network is actually simple to put together. If you did not read most of this section, by simply plugging computer NICs together (either by crossover cable or using an ethernet switch) by default you would be able to have both computers talk to each other. The only problem you might face is in getting the printer to be accessed by both computers.

[68] Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address.

[69] A subnet (short for "subnetwork") is an identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN)

[70] A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes.

Remember, you would have to "share" the printer (this is generally not the default) and then access the "networked" printer (on the computer not attached to the printer) by browsing the network until you found the printer. In either case both computers would have to have the same logon accounts with the same passwords.

In this environment the network would be called a peer-to-peer network because each computer acts independently and shares no single logon account database. Since there are no special computers to manage network resources (DNS and DHCP) administering all those independent accounts and passwords gets more difficult as you add more computers to the mix.

The main benefits of this type of network are:

- *Reduced cost*
  - One printer for two computers.
  - No network management software required.
  - Works with almost any OS and networking hardware.
- *Scalable*
  - By using an Ethernet switch, wireless router or coaxial bus you can add more computers easily.

The main disadvantages are:

- *Harder to manager* as you add more computers
  - You must administrate each computer logon account database individually.
  - All passwords and accounts must be identical across the board.
- *Limited to workgroup* configurations
  - You can not create a domain with a single logon account database.
  - No real security.

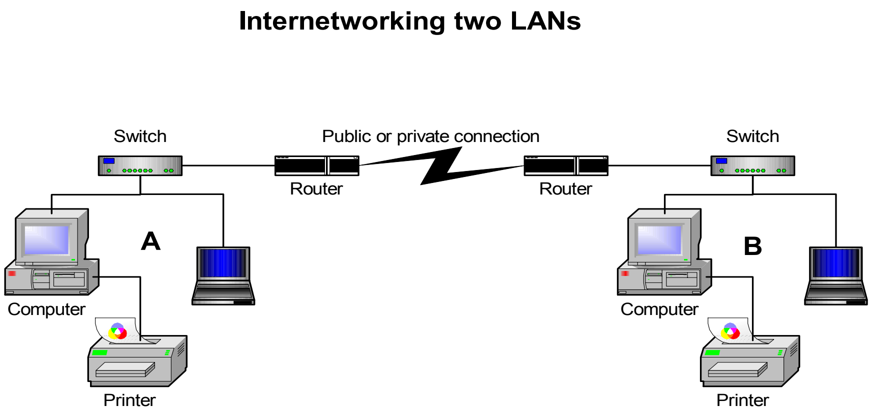
What was learned in this section was the basic parts of a simple network and how they can be put together. The next section will examine how this basic architecture can be molded to work with the internet and it's many resources. Keep in mind that as you add devices to your network you also open it up more each time to security holes. The truth is that no network is fully protected from attack, but you can make things more difficult by limiting the holes added by expanding your environment. Making a drawing of your network topology and listing what each device is programmed to do will help you to lock down your system and create a troubleshooting template as well.

Internetworking

GENERAL

Internetworking[71] two or more local area networks together requires routing[72]so that each network knows when a packet[73] is to remain local or travel to the other network.

FIGURE 2 - 13. Two LANs Combined



If a file or print job is to be sent from the laptop in *LAN A* to the printer in *LAN A*, the router does not need to be informed of the task. If a file from *LAN A* is to go to *LAN B* then the router (on both sides) must know what to do. The link between both routers can be any one of many different strategies (either another ethernet link, Internet, or private phone line (a.k.a. T1/T3[74] etc.). When you use the Internet, you are basically connecting your small LAN to a much larger LAN over a public lines (either fibre or copper). In doing so you keep the same concept as the one displayed in figure 13.

By remembering that the Internet is a collection of networks (small and large) bound together by a bunch of routers and Internet service providers (ISP[75]) that maintain order and provide access, you will find it easier to build your understanding of how things work.

[71] Internetworking is a term used by Cisco, BBN, and other providers of network products and services as a comprehensive term for all the concepts, technologies, and generic devices that allow people and their computers to communicate across different kinds of networks.

[72] On the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination.

[73] A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.

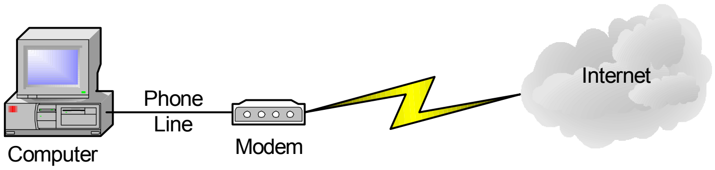
[74] The T-carrier system, introduced by the Bell System in the U.S. in the 1960s, was the first successful system that supported digitized voice transmission. The original transmission rate (1.544 Mbps) in the T-1 line is in common use today in Internet service provider (ISP) connections to the Internet. Another level, the T-3 line, providing 44.736 Mbps, is also commonly used by Internet service providers.

[75] An ISP (Internet service provider) is a company that provides individuals and other companies access to the Internet and other related services such as Web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the Internet for the geographic area served.

MODEMS AND THE INTERNET

Before we talk about sharing the internet connection between both laptop and desktop machines through a single connection, lets talk modems[76]. Modems connect your computer (or laptop) to the Internet via a common phone line (also known as POTS or "plain old telephone system"). Modems connect through an RJ11 connection -- the same connection your phone uses. Modems can either be installed inside your computer or as an external device. The connector looks a lot like the RJ45 connector you use for Ethernet except that it is smaller in size. Your computer *calls* a phone number that your ISP has given you and your computer communicates to a computer on the other side of the phone line giving you access to Internet services. You communicate usually at 56Kb per second. Compression utilities (V.92) allow you even greater communication speeds by compressing information so that data looks smaller in size during the transmission process. As the Internet gets more sophisticated, the speed of your Internet access becomes more important.

FIGURE 2 - 14. Modem/Internet Connection



Modems use the point to point protocol (PPP)[77]. While this protocol is not required for you to actually communicate on the Internet it is required for your computer to communicate with your ISP. When you call your ISP another modem is on the other end of the line de-modulating your communication. Once the link is established, the common protocol TCP/IP is used to establish communication outside the ISP. Your ISP provides a temporary host name, IP address and subnet so that you can act as a host on the Internet. The end result is a low speed connection that provides the same basic functionality as that of the link between routers in figure 13.

Your beginning to see a trend here. There is the protocol to control bandwidth[78], and then there is protocol to manage information. By separating these two (bandwidth and information), we are able to develop both individually without requiring an overall change in everything as new technology comes into being.

[76] A modem modulates outgoing digital signals from a computer or other digital device to analog signals for a conventional copper twisted pair telephone line and demodulates the incoming analog signal and converts it to a digital signal for the digital device.

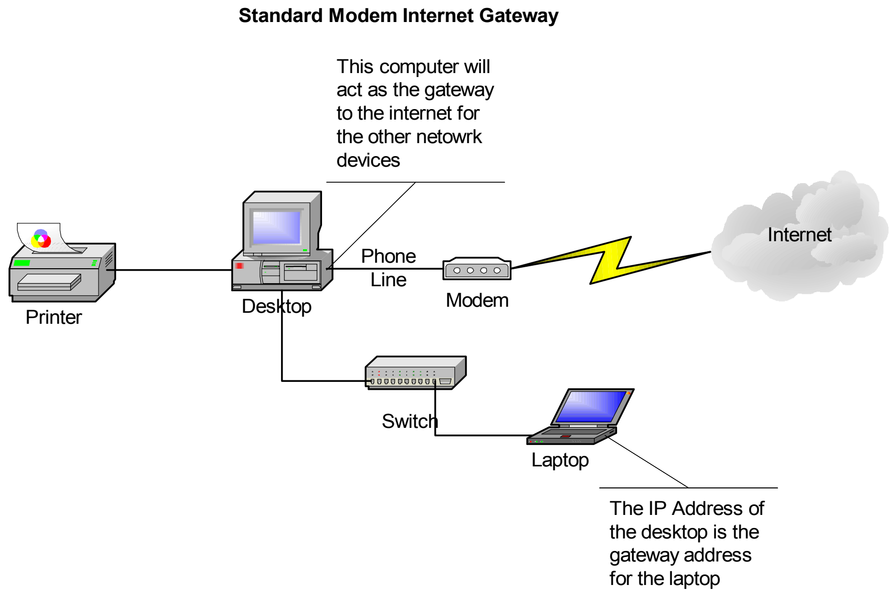
[77] PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you.

[78] Bandwidth (the width of a band of electromagnetic frequencies) is used to mean (1) how fast data flows on a given transmission path, and (2), somewhat more technically, the width of the range of frequencies that an electronic signal occupies on a given transmission medium.

SHARING INTERNET ACCESS

Internet access, gained by adding the modem to the desktop, can be shared to other computers by having the other computers point their gateway IP settings to that of the desktops (see figure 15).

FIGURE 2 - 15. **Modem Internet Gateway**


Standard Modem Internet Gateway
This computer will act as the gateway to the internet for the other netowrk devices
Printer
Desktop
Phone Line
Modem
Internet
Switch
Laptop
The IP Address of the desktop is the gateway address for the laptop

The desktop receives an IP address from the ISP which is bound to the modem. In other words the modem acts much like a NIC on the network. Since the desktop already has a NIC connected to the switch, and the modem acting as another NIC, it is therefore capable of becoming a router for internet traffic. Now things can get a little bit complicated because the desktop (having two NICs) has two IP address settings:

- **Internet Service Provider (ISP) IP Address** settings (provided each time you connect your modem to the internet).
- **Internal IP Address** settings created when you built your network.

Having two NICs in a single computer is referred to as multihomed[79]. The ISP IP address information includes:

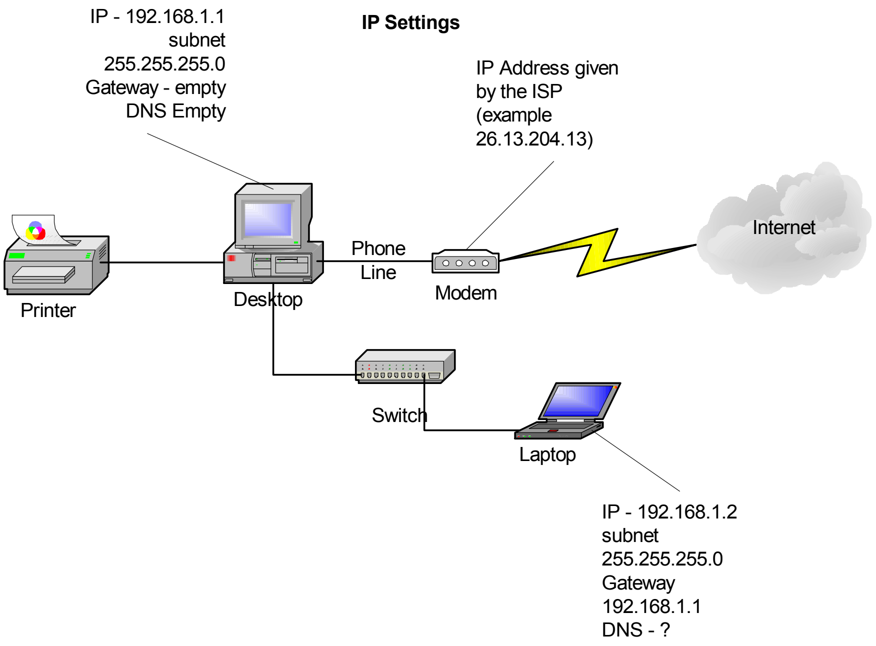
- Routable IP Address
- Subnet Mast
- DNS (primary and secondary)

[79] Multihomed describes a computer host that has multiple IP addresses to connected networks. A multihomed host is physically connected to multiple data links that can be on the same or different networks.

Using the IPCONFIG /ALL command while you are connected to the ISP will provide you with the modem settings as well as your internal NIC settings. You should record the DNS Server IP addresses.

If we were to look more closely at the IP setting for our little network:

FIGURE 2 - 16. **IP Settings**



When we connect our little network to the Internet, it becomes important for us to manually set our network IP settings. Since the modem receives a dynamic address every time it logs onto the ISP connection there is a DHCP server brought on line as well. Since you pay for a single IP through your ISP this can become a problem. By setting your internal IP addresses manually you negate that problem.

If you use the following IP address settings you will be able to attach up to 254 computers internally (the modem will not provide enough bandwidth to support that many but it is possible).

192.168.x.x (whereas the x is a variable) is commonly used in small LANs for several reasons:

1. 192.168.x.x is a *non-routable* address scheme which will not conflict with the ISP IP address scheme.
2. Non-routable addresses are not seen outside the LAN, providing a form of protection against hackers.
3. Free, non-routable IP addresses don't cost anything to use.

192.168.1.x

The key to setting up your internal IP addresses is to follow a consistent plan. If you use 192.168.1.x, all of your computers should have their IP addresses start with 192.168.1.

for example:

computer1 = 192.168.1.1

computer2 = 192.168.1.2

computer3 = 192.168.1.3

If we break down this address scheme you would see that **192.168.1** would be the network and the last number would be the hosts (**1,2,3**). The IP Address 192.168.1.0 (0 is the key) is a special IP address used for broadcasting[80] across your LAN so it can not be used as a Host IP address. 192.168.1.255 can not be used as a host IP address for similar reasons. You can use anything from 192.168.1.1 - 192.168.1.254. It is always a good thing to keep your IP addresses contiguous (192.168.1.*1*, 192.168.1.*2*, 192.168.1.*3*, 192.168.1.*4*, etc.).

255.255.255.0 Subnet Mask

For simplicity, we will use the subnet mask 255.255.255.0 so that any IP address between 192.168.1.1 - 192.168.1.254 can see each other locally. As stated previously, the subnet mask is used to localize the host address to the last octet.

Gateway

The gateway (in figure 16) would be the computer that has the Internet connection (or modem) with the routable IP address. Since the routable IP address is dynamic, you should not add that address as the gateway for other computers locally - you should use the local IP address (in this case 192.168.1.1). By using the local IP address you ensure a stable link to the computer connected to the internet.

DNS Primary/Secondary

Using the information you obtained from running the IPCONFIG /ALL command, enter the DNS server IP addresses (primary and secondary) provided for by the ISP. This will give each of your computers the ability to resolve Internet host names and URLs[81]. Since DNS server IP addresses usually remain static, these addresses should not have to change once entered.

[80] In general, to broadcast (verb) is to cast or throw forth something in all directions at the same time.

[81] A URL (Uniform Resource Locator) (pronounced YU-AHR-EHL or, in some quarters, UHRL) is the address of a file (resource) accessible on the Internet. The type of resource depends on the Internet application protocol.

SECURITY

Security is always a concern when connecting computers to the Internet. There are too many people with nothing else to do but break into other peoples computers. In using the non-routable IP address internally for your LAN only the computer directly connected to the modem has an IP address that can be easily hacked. This does not mean that the other computers can not be hacked, it only means that it would be harder. If you store confidential information on your computer make sure you encrypt the files and/or folders containing your confidential information.

Passwords

While there are many ways to break into a system on the Internet, the best way to limit any break-ins begins with a good password. You might say that your the only one using your computers in your house (and in that you might be right), but if you don't have a password for ALL of your accounts on ALL of your computers -- you are exposing your computers to the outside world. Once you are on-line, other Internet users can find your IP and scan that IP for vulnerabilities.

The very first thing they look for is simple or non-existent password. If they can logon to your system using one of your local *privileged*[82] accounts they own everything. Many Crackers[83] gain access to your computer through open passwords and then establish backdoors (usually specialized services to make your computer more vulnerable) so that if you set a password or delete an account, they will continue to get in.

An example of a good password would be:

- The longer the better (usually no more then 14 characters -- too long and you'll have to write it down).
- Mix upper and lower case characters (example: OnETwOThree).
- Add numbers to the password (example" OnE2Three).
- Add meta-characters[84] to the password (example OnE~2~Three).

You want to keep it simple enough for you to remember but hard enough for password cracking programs to have to take time in resolving. Don't forget to change your password occasionally (once every ninety days or so -- sooner depending on the importance of your data).

By the way, don't keep your passwords written down under your keyboard or in your desk drawer, or anywhere. A password written down is an exposed password.

[82] Privileged Accounts -- In UNIX the root (or super user). In Windows the Administrator. In Novell (old = supervisor / New = Admin) In Apple (9.x and older = none, 10.x and above root). These accounts give people complete access to all resources, files and folders on your computer excluding encrypted files or folders.

[83] A cracker is someone who breaks into someone else's computer system, often on a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there.

[84] Meta-characters - @#$%^&*()~

Sharing

Limit your sharing of files and folders internally to a minimal. DON'T put confidential files in an unencrypted folder and share it! Remember that, since you are sharing a printer locally, your file sharing is turned on and available for others to use.

Sockets[85] and Ports

Sockets (a.k.a. ports) are used to let programs access other programs on other computers. Sometimes referred to as *backdoors*, sockets allow other computers access to resources on your computer. Sockets are common to World Wide Web[86] (WWW) applications and are required to utilize the many valuable resources offered by the web.

If you are not offering services (such as web pages) from your home network you can block access to your sockets using a firewall[87]. Most modern operating systems (Windows XP and OS 10) provide a personal firewall built into the operating system. You can also download free personal firewalls from sites on the internet. If you use a personal firewall read the documentation carefully before you apply settings so that you understand what you are blocking. Also apply your settings one at a time so that you can undo those settings if you find that they conflict with your normal access to Internet resources you plan to use.

AntiVirus Software

AntiVirus software is not just a good idea, but essential to keeping your data safe. You need to have something in place to keep your files free from viral contamination. Viruses are so wide spread that it is impossible to not catch one if your on the web. Many virus infections are made via e-mail, but others are caused by accessing contaminated web sites or downloading files and/or applications that are contaminated.

You must keep up with your antivirus software. There are constant definition updates and need to be applied weekly so that your systems continue to remain virus free. Be sure to keep up with all antivirus updates -- this is very important.

[85] Sockets is a method for communication between a client program and a server program in a network. A socket is defined as “the endpoint in a connection.” Sockets are created and used with a set of programming requests or “function calls” sometimes called the sockets application programming interface (API). The most common sockets API is the Berkeley Unix C interface for sockets. Sockets can also be used for communication between processes within the same computer.

[86] A technical definition of the World Wide Web is: all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP). A broader definition comes from the organization that Web inventor Tim Berners-Lee helped found, the World Wide Web Consortium (W3C): "The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge."

[87] A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.)

Service Packs and hotfixes

Service packs and hotfixes are offered freely by the operating system manufacturer (Apple, Sun, Microsoft, etc.) so that you can further tighten down your system and fix problems that are discovered after the operating system was released. It is just as important to keep up with the service packs and hotfixes as you would with your antivirus definitions.

Be sure to read what the service pack offers and why the manufacturer believes it is important for you to apply them before applying them. If you have several computers in your network download the service pack or hot fix to one computer, (test it to make sure it doesn't break anything) and then install the service pack or hot fix to the rest of your computers only after your know it works like it should.

SUMMARY

Internetworking with other networks greatly expands your LAN resources. By adding your LAN to the Internet you make your computers more accessible to attack. Your LAN resources also require greater manual configuration to make everything work right. All-in-all, most people find that the advantages greatly outweigh the disadvantages. Being methodical in building your Internetworking communications and applying all of your security prior to expanding Internet access to other computers in your LAN will help to ensure that your network runs efficiently.

Internetworking Basics

- Take the time to draw out your network and plot the expansion of internetworking resources.
- Accomplish one thing at a time and test it thoroughly.
- Record what did and didn't work right.
- Don't apply changes to more then one computer at a time and make sure you have strong passwords for ALL of your user accounts.
- Don't write down passwords (if you can't remember them pick one you can remember).
- Change passwords occasionally
- Use non-routable IP addresses internally.
- Don't put confidential files or folders in non-encrypted places.
- ALWAYS use antivirus software.
- Keep up to date with all service packs and hotfixes.
- Use personal firewalls when applicable.

The key thing to remember is that no network on the Internet is completely safe. What security you put in place is like locking the doors and windows to your house -- if someone wants to get in bad enough they will. By securing your network you make yourself less vulnerable to others. Organizing all of your configuration settings and keeping it as simple as possible will help you to troubleshoot any problems you might face.