CyberScience Lab Report

Introduction
To
Basic Networking

May 15, 2003

Produced By:
CyberScience Laboratory
A Program of the National Institute of Justice

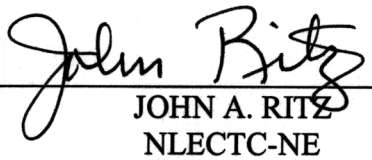
National Law Enforcement and Corrections Technology Center
Northeast Region (NLECTC-NE)
26 Electronic Parkway
Rome, NY 13441

Revision Date 15 May 2003
Joshua G. Bartolomie – josh@dolphtech.com (315)838-7057

Introduction To Basic Networking

CyberScience Laboratory Report

This project is supported by CyberScience Laboratory.



JOHN A. RITZ
NLECTC-NE
Director

MARTIN NOVAK
Program Manager
Office of Science & Technology

DISCLAIMER

This report was prepared for the United States Government by the CyberScience Laboratory (CSL).

With respect to information provided in this document, neither the United States Government nor any of its employees nor CSL nor any of its employees make any warranty, expressed or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose. Further, neither the United States Government nor any of its employees nor CSL nor any of its employees assume any legal liability for the accuracy, completeness, or usefulness of any information, apparatus, product or process disclosed.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or CSL. The information and statements contained in this document shall not be used for the purpose of advertising, nor to imply the endorsement or recommendation of the United States Government or CSL.

Acknowledgement:

This study was sponsored by the National Institute of Justice. The National Institute of Justice is a component of the Office of Justice Programs. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Justice.

INTRODUCTION

The purpose of this whitepaper is to introduce several concepts of networking to an audience that does not deal with them on a daily and intimate basis. Areas that will be covered in this paper are: A general overview on "What networks are"; "How networks actually work"; and "An overview of the general equipment used to build or operate a network." We will introduce the different types of hardware needed to create a network, along with the various protocols that make the network function. With this knowledge, we will then look at how the Internet works as well as what is popular in today's networking field, and some of what the future holds for the networking of tomorrow.

This paper will not make you a networking expert. It is designed to give you a firm foundation of the concepts and hardware behind networking in general. Many of the in depth, technical issues are either skipped over or simply mentioned, as they are outside of the scope of this paper. Several of the higher functions and issues have been overly simplified for better explanation and understanding. For more in depth details on the inner workings of networks please refer to the suggested reading links at the end of the paper.

WHAT ARE NETWORKS?

So what are networks? What do they do? How do they do it? Why do we need them? These are all great questions, and are constantly asked in today's fast-paced world, where you hear on a daily basis such buzzwords as: Internet, Intranet, LAN, WAN, and Ethernet.

Let us start with the first question, "What exactly is a network?" Loosely defined, a network is a collection of entities that exchange information, goods or services. For the sake of this paper, we will define a network as a collection of computers and peripherals that are inter-connected utilizing specific hardware, with the distinct purpose of sharing information, services and connectivity amongst each other.

Ok, so now we have these computers 'connected' to each other, what does that allow us to do and why do we need them? Simply put, you may now transfer and share information between these computers, a feat that would be difficult or time consuming without the network that connects them. Not only that, but you may now utilize various services and peripherals connected to remote computers, thereby extending your computers usefulness. As a simple example, say you are in an office of fifteen computers and five printers. With those five printers, each connected to one computer, there are ten people that cannot print directly from their desks. Those ten would have to save their work to some form of portable media (floppy disk, CDROM Etc…) and carry it across the room or across the building to the computer with the printer connected to it. If they were on a network however, each of the computers (utilizing the proper network hardware) would now be able to print to any of the five printers – thereby saving you valuable time and energy.

That example is one of the primary reasons for establishing a network. The network allows for the sharing of resources between many systems, regardless of their location. This means less time spent trying to get to the computer with the printer, fewer printers for the various offices, and your time spent more productively. In addition to the savings on equipment, a more efficient work environment is

created. This sharing of peripherals is by no means limited to just printers, you can pretty much share any piece of computer equipment or information, such as CD burners, DVD Players, disk space and pure data.

In addition to sharing equipment and resources, networks are the vehicle that all computers use to share data in its many forms and mediums. Some computers connect to each other thru satellites or phone lines, but the majority of them connect to each other thru these computer networks. Without a network, we could not send email, perform online chats or discussions. Web pages, search engines and streaming audio or video, even voice and fax data, all of the tools of modern age communications are made possible and more powerful by the computer network. In many ways, the Internet has improved long distance communications the same way that the invention of mail service, the telegraph and the telephone did. Information once took days, weeks or months to travel and share from coast to coast or across the sea. Now it flies across the miles in seconds or minutes, thanks to computer networks.

So not only do we have the added value of shared resources, but also the ability to share data, thoughts, images, and access to the Internet. In addition to using the network to share data or resources, an organization's Internet connection may be shared amongst many users. Just like the printer example from earlier, many computers may share Internet access, rather than having each one connect directly to the Internet; a topic that will be discussed in greater detail later in this paper.

The type of network that has been outlined at this point is commonly referred to as a Local Area Network (LAN). Most LANs are confined to a single building or group of buildings that are in close proximity to each other. To go further with this, you can connect two LANs together, two or more buildings, even if they are separated by extreme distance. This interconnection of two or more LANs is commonly referred to as a Wide Area Network (WAN). This gives you all of the benefits of a LAN, but with greater distance. For example, say you have an office building in New York City, and one located in San Francisco. If the two LANs (one in each building) are connected as a WAN, you can now easily share data and services even though you are separated by many thousands of miles.

WHAT IS THE INTERNET?

Now that you have a basic level of understanding as to what a network is, the question might arise as to what exactly is the Internet.

The best way to describe the Internet is to say that it is a network, made up of many different networks. It is essentially one giant WAN that connects LANs from all over the globe. This allows us to browse and search through an enormous amount of information, searching for whatever our needs are. It also allows us to instantly communicate and share information with others, regardless of their physical location. When you obtain an Internet connection, you are actually adding your computer to the hundreds of millions that are already connected. With this connection, you have the ability to now browse through information that these other computer users have made available for that distinct purpose.

There are currently six hundred and forty nine million people utilizing the Internet, according to a March 2003 report done by Global Internet Statistics[1]. It is further estimated that by 2004 there will be over nine hundred and forty million users. As you can see, the Internet is –and has been for quite a while- experiencing tremendous growth. Each day, more and more users flock to the Internet, each of them

bringing with them additional information, sometimes new data, sometimes merely copies of existing data, all in all causing the amount of data available on the Internet to grow at an amazing rate. This makes the Internet a larger repository of knowledge with each new system, the largest information network in the world.

The Internet is not a utopia, not by any means. Like any other tool, it has its good and decent uses, as well as its dark and abusive side. There are many scam artists, individuals with fraudulent agendas and swindles, pedophiles, illicit porn traders, and other malicious individuals that utilize its services for nefarious deeds and activities. With proper usage, caution, and common sense, it is possible to avoid most of these situations and utilize the wealth of the Internet for safe, productive applications.

When someone talks of the Internet, many people automatically think of the World Wide Web (WWW), and 'surfing' the Internet, chatting or simply sending Email. Quite a few people believe this is all that the Internet is, and all that it can be used for. This is far from the truth. The Internet is a vast entity that offers numerous services that extend well beyond the scope of just simple web browsing. You have the ability to utilize email, access newsgroups, transfer or download files, participate inside 'chat rooms' as well as a myriad of other Internet related services that utilize this gigantic WAN to connect and communicate around the globe. Going into a break down of each of these services is outside of the scope of this paper, but for a brief synapses of these items, please refer to the recommended reading section at the end of this paper.

The Internet not only contains a wealth of knowledge, but it is also a medium for information exchange. By utilizing the infrastructure that is already in place, an individual on the east coast can easily interact and share information with someone on the west cost, without having to create or maintain a separate infrastructure just for that purpose.

The best analogy is to think of the Internet as a giant water pipe encircling the globe; this would be called the Internet Backbone. Additionally, thousands of Internet Service Providers (ISPs) connect themselves to this pipe, thereby extending the actual coverage, or availability, of the 'Internet'. To go further with this analogy, some ISPs connect their 'pipe' to other ISPs, forming a mesh of networking pipes that span the world. Off of these ISP connections, you have the connections of home and business users. With all of these 'pipe' connections, you now have connections to practically every part of the globe. Through this series of pipes, you can reach any one of the others connections, no matter how distant they are from you.

Should any one section of the pipe fail, the specialized networking equipment that helps connect all the pipes together routes the water thru other pipes to help the water continue to flow, albeit somewhat slower. Occasionally, a critical section of pipe may fail, be damaged or tampered with, causing the flow to halt or be directed in the wrong direction. In a data heavy world that is relying on their networks more and more each day, this can mean loss of critical communications, services or revenues.

NETWORKING PROTOCOLS

What exactly is a 'network protocol'?

A protocol is the pre-defined way that someone (who wants to use a service) talks with or utilizes that service. The "someone" could be a person, but more often it is a computer program like a Web browser. What does this mean in English? Simply put, for one computer (or computer program) to talk to another computer (or computer program) they must both be talking the same language, this language is called a protocol.

Where do protocols come from and who defines them? A protocol is based on an agreed upon and set standard, this way all manufactures of hardware and software that are utilizing the protocol in question, do so in a similar fashion to allow for interoperability. The Institute of Electrical and Electronics Engineers[2] (IEEE) is the governing body that determines these standards. Through extensive testing, collaboration, and industry feedback, these standards are solidified into working entities, or blueprints for communicating.

There are dozens of different types of protocols out there today; some are old and obsolete while some are so new they have yet to be implemented. For the purpose of this paper, we will just touch on a few of the most popular ones in use today. [3]

One of the most popular protocol families out there today is given the IEEE designation as 802.3[4], more commonly referred to as Ethernet. This IEEE 802.3 standard is actually compromised of dozens of specific protocols that fall under the Ethernet umbrella. Please refer to the mentioned reference for more information on the details of this family of protocols, as a full breakdown of them would be a paper unto itself.

Most businesses, old and new, utilize some form of Ethernet networking. Due to its robustness, scalability and speed, Ethernet is pretty much the 'de-facto' family of protocols for networking.

Under this umbrella lie the protocols that are used in controlling and directing traffic on the Internet. Specifically speaking, this is the TCP/IP suite of protocols.

1. What is TCP/IP?

   TCP/IP is the protocol, or set of protocols, utilized by a majority of today's networks, including the Internet. TCP/IP is actually two different sets of protocols, one being TCP and the other being IP. TCP stands for Transmission Control Protocol, and IP stands for Internet Protocol.

   TCP and IP were developed by a Department of Defense (DOD) research project aimed at connecting a number of different networks designed by different vendors into a network of networks (the "Internet"). It was successful because it delivered services that everyone needed (file transfer, electronic mail, remote logon) across a very large number of systems.

   TCP is responsible for verifying the correct delivery of data. Data can be lost in transit. TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received.

IP is responsible for moving data from computer to computer, from hardware piece to hardware piece. IP forwards each packet based on a four byte destination address - the IP ADDRESS. An IP address is like a mailing address, it is your location on the Internet, and if you are connected to the Internet you have a unique IP address.

When you want to interact with something over a network, you send your request out using the TCP protocol. This request is kind of like a regular letter you would send through the postal service. You have an envelope that has your return address (YOUR IP address), your destination address (The other computers IP address) and the contents of the envelope (your data, or request).

As mentioned, this "IP number" is a four byte value. By convention, this value is expressed by converting each byte into a decimal number (0 to 255) and separating the bytes with a period. For example, www.yahoo.com has an IP address of 66.218.79.230.

Wait a minute, when you go to www.yahoo.com you don't type in 66.218.79.230 to get there – do you? So if you don't tell it 'where' to go by the definition above, how does it know that you want to go there? This is accomplished by another service that is called DNS.

2. What is DNS?

Ok, while DNS isn't a protocol per-say, we do want to touch on it briefly here so that you can obtain a firm understanding of what it is, and why it is useful

Based on the information above, it can be stated that there are roughly 649 million users on the internet. Each one of these users has an IP address that is assigned to them, one way or another. This includes all of the websites and email servers that you probably utilize on a daily basis without even thinking about it. Now, what you are used to seeing and using when you 'surf the net' are called domain names. Domain names are just that, names of specific domains on the internet. Microsoft.Com, BestBuy.com, Yahoo.com; these are all examples that you are probably familiar with, these are all domain names. So how do these domain names point to these IP addresses we went over earlier?? With DNS, that's how.

DNS matches your domain name with your IP number, and DNS servers are running everywhere all over the internet. When you type in an address, which is commonly referred to as a URL (Uniform Resource Locator – it's a fancy way of saying domain name) in your web browser, you are led to the page you want by DNS. Your DNS record can contain many different types of information which can tell networking hardware where to send certain requests. DNS was created so that you wouldn't have to remember these long strings of numbers, it allows for more customizability and easier usage.

NETWORKING HARDWARE

Ok, we now know the basics of what a network and the Internet are, but what about the hardware that is utilized in all of these tasks??

There are many different pieces of networking hardware out there today. It is as diverse as a home improvement store, with specialty pieces for just about every thing you could ever imagine, and some that you probably couldn't imagine. In keeping to the theme of this paper, we will just cover the most basic and common pieces of equipment that are utilized in the networking field today.

1. Routers

   A router performs two separate but related tasks, it ensures that information doesn't go where it's not needed and it makes sure that the information in question actually makes it to the intended destination These steps are crucial for keeping large volumes of data from clogging the connections of "innocent bystanders."

   A router joins two networks, passing information from one to the other and, in some cases, performing translations of various protocols between the two networks. It also protects the networks from one another, preventing the traffic on one from unnecessarily spilling over to the other. It acts pretty much like a traffic cop; it knows where you need to go (based on your IP and the destination IP) and tells you which road to take to get there.

2. Hubs

   A hub connects devices together. Hubs used to be expensive pieces of equipment used only in larger computer rooms, but now mini hubs are available for a mere fraction of the price that they used to fetch.

   Hubs are used for 'splitting' a connection. Say you have one networking line, yet you want to add 4 computers to it. You can go purchase a 4-port hub from your local electronics store and have an instantaneous solution to your problem. That 4-port hub will take that one connection and split it into 4 connections.

   The problem with hubs is the simple fact that because it 'splits' the connection, any incoming, or outgoing, information is broadcasted to all of the ports on it. This means there is a waste of resources, and that someone that is connected to another port on the same hub might be able to 'sniff' or capture the data you are transmitting.

3. Switches

   A switch is pretty much an 'intelligent hub'. Whereas a hub 'splits' a connection over multiple lines, a switch 'switches' the connection over multiple lines. It might seem like a very small difference, but it is a very important distinction. Think back to our water pipe analogy from earlier, a hub will take that one pipe and run 4 pipes off of it – there by reducing the water pressure across the whole series of pipes (reduction of bandwidth). A switch will take that main pipe and allow the 4 other pipes to utilize it for a predetermined time frame (usually a few milliseconds

every few milliseconds) thereby allowing each pipe to utilize the full pressure potential of the original pipe (maximum bandwidth).

Another benefit of a switch is that the incoming and outgoing data is specifically sent to the requested port. This again differs from a hub, whereas a hub broadcasts to all of the ports, a switch forwards the information only to the one port that is requesting/sending it. This is a viable security feature, as it disallows an individual that is connected to another port from 'sniffing' or capturing your data transmissions, as they would be able to with a hub.

4. Cabling

Ok, how is everything connected together on these networks? You have probably guessed by now, one of the main items needed for networking is networking cable. It's hard to connect devices if there is no way to connect them.

There are many different kinds of cable out there today. Here is a brief overview of some of the more popular ones:

- **CAT5** is an Ethernet cable standard defined by the Electronic Industries Association and Telecommunications Industry Association (commonly known as EIA/TIA). CAT5 is the 5th generation of twisted pair Ethernet cabling and the most popular of all twisted pair cables in use today.

  CAT5 cable contains four pairs of copper wire. It supports Fast (100 Mbps) Ethernet and comparable alternatives such as ATM. As with all other types of twisted pair EIA/TIA cabling, CAT5 cable runs are limited to a maximum recommended run rate of 100m (328 feet).

- **CAT5e** is an enhanced version of Cat5. Although CAT5 cable usually contains four pairs of copper wire, Fast Ethernet communications only utilize two pairs. A new specification for CAT5 cable, CAT5 enhanced (CAT5e), supports short-run Gigabit Ethernet (1000 Mbps) networking by utilizing all four wire pairs and is backward-compatible with ordinary CAT5.

- **CAT6** is a further expansion on CAT5. It allows for faster speeds then is currently allows with CAT5 cabling. CAT6 cabling is fairly new to the networking scene, and is used mainly for Gigabit Ethernet networking runs.

- **Coax** is the type of cable you are probably familiar in seeing connected to your home TV set. Coax is a type of communication transmission cable in which a solid center conductor is surrounded by an insulating spacer which in turn is surrounded by a tubular outer conductor (usually a braid, foil or both). The entire assembly is then covered with an insulating and protective outer layer. Coaxial cables have a wide bandwidth and can carry many data types, voice and video conversations, simultaneously. If you have a 'cable' Internet connection, you utilize Coax as your networking medium.

- **Fiber Optic** cables are actually strings, or fibers, of glass. By utilizing a glass fiber, varying frequencies of light are transmitted back and forth utilizing specialized lasers. Fiber Optics offer an extremely high level of bandwidth, small space needs and protection from electromagnetic interference, eavesdropping and radioactivity. Because of these issues, Fiber Optic cable forms the backbone for many networks throughout the world.
  The high costs and specialized equipment needed for fiber optics keeps this technology out of normal day to day networking uses.

5. Modems

   Modems are devices that allow you to connect your computer to networks remotely. There are several different types of modems in use today.

   - Dial-Up Modems are what most people think of when modems are discussed. These have been around for quite a number of years, and they are utilized by a majority of those that connect to the Internet. Dial-Up modems allow you to connect to a network via your phone line. It converts your digital transmission into an analog one that the phone lines can handle. Most people use modems to connect back to their office network remotely, or to connect to such ISP's as American Online, or Earthlink.
   - Cable Modems are the connection device that is utilized by those that have cable Internet service. This device basically looks at the input coming in from your cable line and filters out all that is not related to your Internet connection.
   - DSL Modems are connection devices that are used if you have a DSL Internet connection. If you are lucky enough to have updated telephone wiring in your community, you might be able to subscribe to a DSL ISP for your Internet service. DSL utilized existing phone lines (higher quality and newer lines then most areas have at the moment) and share the signal, in a similar fashion as a cable connection. This modem performs the same function, it filters out that which isn't related to your Internet and converts it into information your computer can recognize and use.

6. Network Interface Cards (NICs)

   Some of you are probably saying, ok that defines how we get hooked up at home, but at work I don't have any modems hooked up – all I have is a cable coming into the back of my computer. Well most computers now days have what are called NICs installed. NIC is short for Network Interface Card. These are the devices in which you can plug your networking cable (Cat5 as an example) directly into. It is usually an internal card on your computer.

POPULAR TRENDS IN NETWORKING

So what is the most popular type of network out there today? The items that are discussed in this paper are the most prevalent in today's networking field. Ethernet networking utilizing CAT5 or CAT5e cabling are the most common types of items you will see.

Due in part to the drop in prices that the technology field has experienced over the past few years, it is possible to walk right into your local electronics/computer store and purchase anything, and everything, you would need to easily and quickly setup a small to medium sized network just about anywhere. As many home users have begun doing, allowing the home user to share resources and data amongst their household, as easily as they do at work.

As people connect to the Internet from their homes and business, they realize that having a dial-up ISP has severe disadvantages. With streaming audio and video, and the prevalence of multimedia laden webpage's, having a fast connection is sometimes a must. This fast connection is called Broadband[5]. Broadband is utilized all over the world; it is how someone gets onto the Internet fast. In a recent article that was published by PCWorld[6], it was reported that the U.S. broadband audience accounts for about 50 million people, or nearly one-third of all Internet users. Of those 50 million, 17 million are households.

It would be safe to give an educated guess that approximately 50-75% of the 17 million households quoted above have some form of small network set up behind their broadband connection. This is so they can share their high-speed Internet connection with several computers throughout their homes, instead of just one.

This 'broadband' connection can come in many forms. Cable, DSL, Satellite, and ISDN are all ways a fast connection can enter your house, and all of these are termed as broadband connections.

As broadband networking is becoming more prevalent with the population (it is expected to double in the next two to three years), more and more people desire the ability to connect more then one computer to their Internet Connection. This ties in all of the information that we have covered so far in this paper, and it accounts for why the Internet is experiencing a tremendous surge in growth. More and more people are adding more and more computers to the Internet, thereby making the Internet surge in size.

One item that has seen an abnormal amount of growth, in relation to other networking trends, is that of Wireless networking.

THE FUTURE OF NETWORKING

So what do we expect the future to hold for us? Based on current market trends, and the apparent attitude of the networking field, it would be a safe bet to assume that there is going to be tremendous push into Wireless networking.

Now, wireless networking was mentioned before, but was given no detail. Below is a brief synapses as to what wireless networking is, and what its key points are. For a more detailed look at Wireless networking, please refer to the series of papers that the CyberScience Laboratory has created based on this specific topic.

1) What is Wireless Networking?

   Briefly, Wireless networking has been around for decades. The concept of transmitting data over the airwaves is nothing new (example: radio). The parts that are relatively new are the concepts and standards that have come out of IEEE in regards to wireless networking. At its

most basic, wireless networking is networking without any wires. You have the freedom and mobility to perform your work, or to maintain a network (Internet) connection regardless of your location, within certain limits.

IEEE designated the protocol of 802.11 for its wireless networking. Like the 802.3 Ethernet one, there are many different protocols within this family that cover the many different ways in which wireless networks may be used, secured, and implemented.

The most popular protocol for wireless today is the one called 802.11b. This protocol is commonly referred to as WiFi (Wireless Fidelity). As mentioned above, wireless networking has seen an enormous amount of growth in the past few years; with most of the growth is concentrated with products that conform to the 802.11b protocol. Due to the relative inexpensiveness of the hardware, WiFi connections are popping up everywhere – even in peoples homes. As referenced, people have a growing desire to add multiple computers to their broadband connections. What better way to add something, then without utilizing wires. This way you can be outside sitting on your deck or in your bedroom laying down with your laptop and still enjoy the benefits of full Internet access, without all those messy cables dragging around your feet, and the hassle of drilling holes in your walls.

CONCLUSION

The aim of this paper, was to narrow the gap of instructional or educational information available on networking. Many of the tutorials or papers available are written with high technical explanations of networking, often written with a technical or engineering reader in mind. Or they overly simplify the concepts for an audience that has never seen email or a network in their lives.

Hopefully this paper has helped to close that gap and given you a better understanding as to what networks are and how they work. Many people today, even some in the IT field, take networks for granted. Never thinking about the fact that there are people that might not have been taught the underlying concepts of networking.

If you are interested in obtaining more detailed information about any of the topics discussed in this paper, please refer to the references at the end of the paper.

APPENDIX

For more information on the subject matter discussed in this paper, we recommend the following sites. These recommendations do not signify endorsement of any products or content by the CyberScience Laboratory (CSL). These websites may contain links or advertisements to other websites which are not under the control or maintenance of the CSL.

Please be advised that the links or advertisements on sites we refer to may contain links to adult material, or malicious code. Please be aware that pop-up advertisements may exist. The CSL is not responsible for any of the content on these sites.

RECOMMENDED READING

ITToolBox	A site with numerous papers and brief tutorials in regards to networking hardware, protocols, and concepts.	http://networking.ittoolbox.com/default2.asp
Hardware Central	"The Ultimate Guide to Networking – Part One"	http://www.hardwarecentral.com/hardwarecentral/tutorials/158/1/
Hardware Central	"The Ultimate Guide to Networking – Part Two"	http://www.hardwarecentral.com/hardwarecentral/tutorials/3/1/
Hardware Central	"The Ultimate Guide to Networking – Part Three"	http://www.hardwarecentral.com/hardwarecentral/tutorials/143/1/
Walrus Computers	A decent higher level networking primer	http://www.walruscomputers.com/tomes/Tomes_Volume_Six-Networking_Tutorial.htm
JC's WWW Resource	A site of links that pertain to networking tutorials	http://www.angelfire.com/tx/jcr/Tutorials.html
Comms Design	Some decent 'Home Networking' tutorials	http://www.commsdesign.com/centers/homenetworking_tutorials.html
University of Georgia Center for continuing Education	A nice little primer on the WWW	http://www.gactr.uga.edu/exploring/netweb.html
Paul Griffiths	How the Internet Works	http://www.paulgriffiths.net/web/intro.html#top
PC Mechanics	Some decent Networking informational files.	http://www.pcmech.com/networking.htm
WaterWheel	Basic networking introduction	http://www.waterwheel.com/Guides/networking_basics_0001.htm

REFERENCES

1. Global Reach. Global Internet Statistics. Modified 30-Sept-02
URL: http://www.glreach.com/globstats/index.php3

2.The Institute of Electrical and Electronics Engineers (IEEE) Inc. Modified: 01-Jan-02
URL: http://www.ieee.org/portal/index.jsp

3.Protocols.Com. Protocol Directory Index. Accessed 5-May-03
URL: http://www.protocols.com/pbook/index.htm

4.The Institute of Electrical and Electronics Engineers (IEEE) Inc – 802.3. Modified: 25-Mar-03
URL: http://grouper.ieee.org/groups/802/3/index.html

5.Mehlman, Bruce. Assistant Secretary for Technology Policy. Modified 28-Apr-2003
URL: http://www.ta.doc.gov/Speeches/BPM_030428_broadband-rev.htm

6.PCWorld Magazine. What's up for the Internet in 2003? Modified 31-Dec-02.
URL: http://www.pcworld.com/news/article/0,aid,108343,00.asp