NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

LOCAL AREA NETWORK

Graduation Project
COM- 400

Student: **Amir Tayseer SARAYREH**

Supervisor: **ASST.PROF.DR.Firudin Muradov**

NICOSIA-2005

ACKNOWLEDGEMENTS

Foremost I would like to pay my special thank to the **GOD,** then thanks to my family. I am very much thankful and grateful to my mother and father whose prayers and love for me has encouraged me so make this day come true.

Secondly I want to thank to my project's adviser Asst. Prof. Firudin Muradov for his helping and advices. And special thank to his great relation with all the students, he is really an exellent adviser.

I would also like to thank my all friends .Mohammad al-sharaf, Saad al Mohiesen and who helped me so much in doing my project.And special thank to Mr. Murat Turk who was encouraged and stay with me on every phase of my life.

Finally I will never forget the persons who They boosted me up about my studies as well as my life. I am very much thankful and grateful to them. Mrs. Fahriye Bakkaloglu and Mrs Bedia Bakkaloglu. It is only because of them that today I am capable of completing my degree.

ABSTRACT

A Network is a group of computers and other devices that connected to each other. The most common types of Networks are LAN, WAN MAN. LANs are networks usually restricted to a geographic area, such as a single building, office. LANs can be small, linking as few as three computers, but often link hundreds of computers used by thousands of people. The growth of typical networking protocols and media has resulted in universal propagation of LANs all the way through business organizations. Users can also use the LAN to communicate and share information as well as data with each other. Most LANs are built with relatively inexpensive hardware such as Ethernet cable and network interface cards. Specialized operating system software is also often used to configure a LAN. LANs are usually faster than WANs, ranging in speed from 230 Kbps up to and beyond 1 Gbps. They have very small delays of less than 10 milliseconds.
Protocols and a reference model defined my ISO hold communication between different devices. Some special softwares are installed on the communicating devices on the LAN, which help and facilitate in communication.

TABLE OF CONTENTS

CHAPTER TWO:LAN TOPOLOGIES AND REFERENCE MODELS

CHAPTER THREE: LAN HARDWARE

Introduction

When computers first became available, the typical institute consisted of one single large, expensive machine which catered for many users, perhaps hundreds of users at a university campus. This single machine is usually called a *mainframe*. Each user was connected to the mainframe by means of a serial, low speed, line and a terminal (which simply displayed the information in text mode). No connection existed between the mainframe and any other computer.

This is quite adequate for many purposes and was the only practical solution at a time when computers were very expensive items. By the mid 1970's, experiments were made in connecting computers to each other. The benefit of having computers talking to each other is that instead of duplicating valuable and expensive resources on each machine, it makes it possible for these resources to be made available on all machines which are on the network. The connections that were made in those early days involved computers situated in close proximity to each other (in the same building). The connections were accomplished by connecting each computer with coaxial cable. This allows much higher data transfer rates than the serial lines which connect terminals to computers.

Local area networks (LANS) are those networks usually confined to a small geographic area, such as a single building or a college campus. LANs are not necessarily simple in design, however, as they may link many hundreds of systems and service many thousands of users. The development of various standards for networking protocols and media has made possible the proliferation of LANs worldwide for business and educational applications.

At SAAO we have two LANS: one in Cape Town and another one in Sutherland. The two LAN's are connected to each other by means of a (slow) telephone line (to be replaced this week by a faster 68 Kb/s Diginet link). The network in Cape Town is itself connected to a network which spans the whole world using telephone lines - the Internet.

1. LOCAL AREA NETWORKS IN WORKPLACE

1.1 What is Computer Network?

A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN).

Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions.

There are many different types of LANs Ethernets being the most common for PCs. Most Apple Macintosh networks are based on Apple's AppleTalk network system, which is built into Macintosh computers

1.2 How and Why Network Exists?

The concept of linking a large numbers of users to a single computer via remote terminal is developed at MIT in the late 50s and early 60s. In 1962, Paul Baran develops the idea of distributed, packet-switching networks. The first commercially available WAN of the Advances Research Project Agency APRANET in 1969. Bob Kahn and Vint Cerf develop the basic ideas of the Internet in 1973.

In early 1980s, when desktop computers began to proliferate in the business world, then intent of their designers was to create machines that would operate independently of each other. Desktop computers slowly became powerful when applications like spreadsheets, databases and word processors included. The market for desktop computers exploded, and dozens of hardware and software vendors joined in the fierce competition to exploit the open opportunity for vast profits. The competition spurred intense technological development, which led to increased power on the desktop and lower prices. Businesses soon discovered that information is useful only when it is communicated between human beings. When large information being

handled, it was impossible to pass along paper copies of information and ask each user to reenter it into their computer. Copying files onto floppy disks and passing them around was a little better, but still took too long, and was impractical when individuals were separated by great distances. And you could never know for sure that the copy you received on a floppy disk was the most current version of the information-the other person might have updated it on their computer after the floppy was made.

For all the speed and power of the desktop computing environment, it was sadly lacking in the most important element: communication among members of the business team. The obvious solution was to link the desktop computers together, and link the group to shared central repository of information. To solve this problem, Computer manufactures started to create additional components that users could attach to their desktop computers, which would allow them to share data among themselves and access centrally located sources of information. Unfortunately the early designs for these networks were slow and tended to breakdown at critical moments.

Still, the desktop computers continued to evolve. As it became more powerful, capable of accessing larger and larger amounts of information, communications between desktop computers became more and more reliable, and the idea of a Local Area Network (LAN) became practical reality for businesses. Today, computer networks, with all their promise and power, are more complicated and reliable than stand-alone machines. Figure 1 shows the network connectivity of the world.

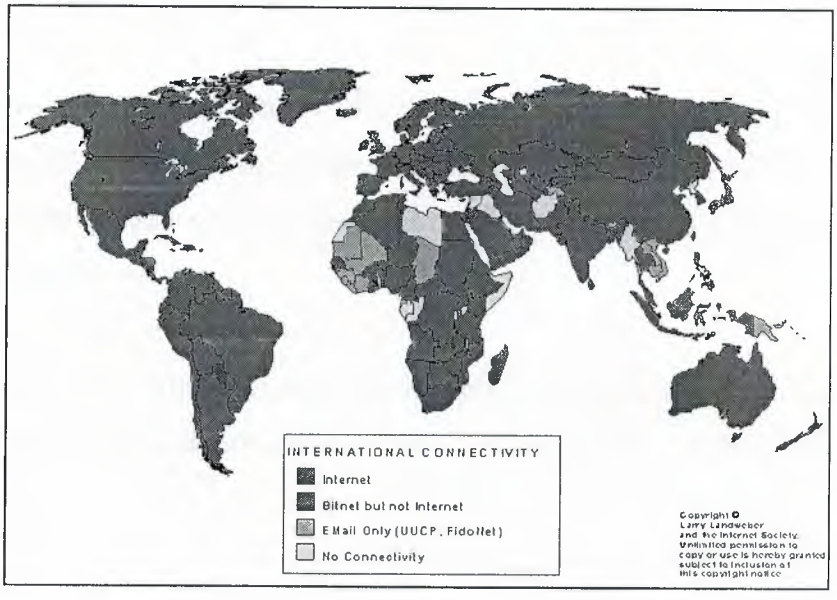


Figure 1 Computer Network Connectivity of the World

1.3 Goals of Computer Networks

The main goal of networking is "Resource sharing", and it is to make all programs, data and equipment available to anyone on the network with out the regard to the physical location of the resource and the user.

A second goal is to provide high reliablity by having alternative sources of supply. For example, all files could be replicatied on two or three machines, so if one of them is unavailable, the other copies could be available.

Another goal is saving money. Small computers have a much better price/performance ratio than larger ones. Mainframes are roughly a factor of ten times faster than the fastest single chip microprocessors, but they cost thousand times more. This imbalance has caused many system designers to build systems consisting of powerful personal computers, one per user, with data kept on one or more shared file server machines. This goal leads to networks with many computers located in the same building. Such a network is called a LAN (local area network).

Another closely related goal is to increase the systems performance as the work load increases by just adding more processors. With central mainframes, when the system is full, it must be replaced by a larger one, usually at great expense and with even greater disruption to the users.

Computer networks provide a powerful communication medium. A file that was updated/modified on a network, can be seen by the other users on the network immediately

1.4 Classification of Computer Networks

Network Classification Like snowflakes, no two networks are ever alike. So, it helps to classify them by some general characteristics for discussion. A given network can be characterized by its:

Size: The geographic size of the network

Security and Access: Who can access the network? How is access controlled?

Protocol: The rules of communication in use on it (ex. TCP/IP, NetBEUI, AppleTalk, etc.)

Hardware: The types of physical links and hardware that connect the network

Computer experts generally classify computer network into following categories:

Local Area Network (LAN): A computer network, with in a limited area, is known as local area network (e.g in the same building)

Wide Area Network (WAN): A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.

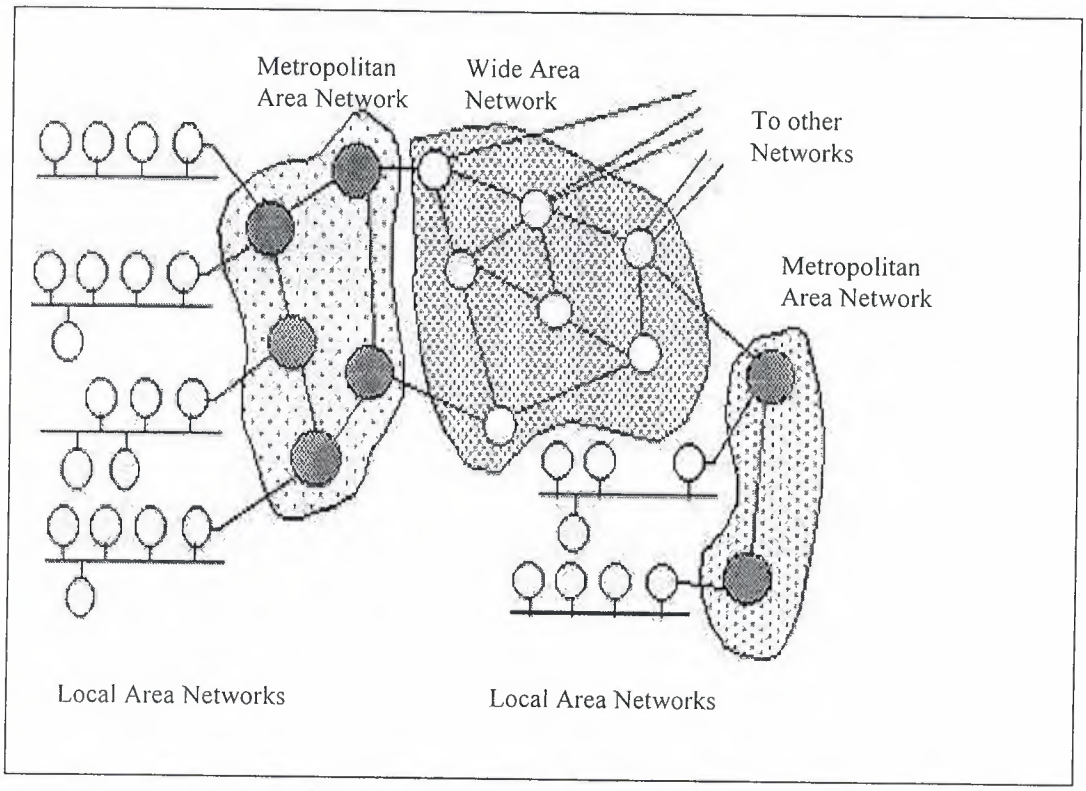
Metropolitan Area Network (MAN): A data network designed for a town or city. In terms of geographic breadth, MANs are larger than local-area networks (LANs), but smaller than wide-area networks (WANs). MANs are usually characterized by very high-speed connections using fiber optical cable or other digital media.

Campus Area Network (CAN): The computer network within a limited geographic area is known as campus area network such as campus, military base etc.

Home Area Network (HAN): A network contained within a user's home that connects a person's digital devices. It connects a person's digital devices, from multiple computers and their peripheral devices to telephones, VCRs, televisions, video games, home security systems, fax machines and other digital devices that are wired into the network.

In figure 2 the connecttivity of local area networks to metropolitan area networks and typical use of metropolitan area networks to provide shared access to a wide area network is shown.

Figure 2 A typical use of MANs to provide shared access to wide area network



Computer networks are used according to specified location and distance. In table 1 it is shown that which technology can be applied to the specific location and specific distance.

Table 1 Network Techonologies that Fit in Different Communication Spaces

NETWORK TYPE	DEFINITION	DISTANCE RANGE	COMMUNICATION SPACE
LAN	Local Area Network	0.1 to 1 Km	Building, floor, Room
WAN	Wide Area Network	100 to 10000+ Km	Region, Country
MAN	Metropolitan Area Network	10 to 100 Km	City
CAN	Campus Area Network	1 to 10 Km	Campus, Military base, Compnay site
HAN	Home Area Network	0.1 Km	Home

In Figure 3 a chart is shown which specifies the distances and speeds of different networks.

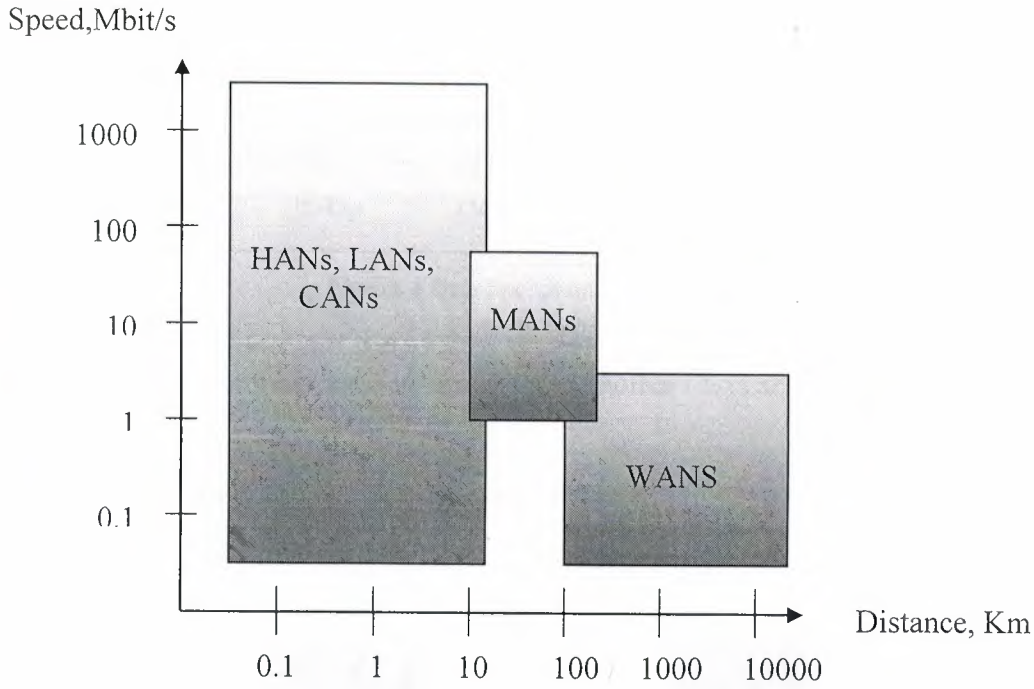


Figure 3 Distances and Speeds of the Different Networks

1.5 Local Area Networks

LANs are networks usually confined to a geographic area, such as a single building, office. LANs can be small, linking as few as three computers, but often link hundreds of computers used by thousands of people. The development of standard networking protocols and media has resulted in worldwide proliferation of LANs throughout business organizations. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions. Most LANs are built with relatively inexpensive hardware such as Ethernet cable and network interface cards (although wireless and other options exist). Specialized operating system software is also often used to configure a LAN. For example, some flavors of Microsoft Windows -- including Windows 98 SE, Windows 2000, and Windows ME -- come with a package called Internet Connection Sharing (ICS) that support controlled access to resources on the network.

LANs are usually faster than WANs, ranging in speed from 230 Kbps up to and beyond 1 Gbps (billion bits per second) as shown in Figure 4 They have very small delays of less than 10 milliseconds.

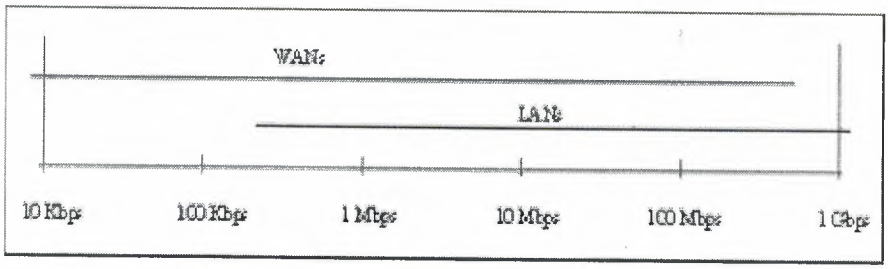


Figure 4 Data Speeds on LANs and WANs

How does one computer send information to another? It is actually rather simple.

The figure 5 shows and explains a simple network.

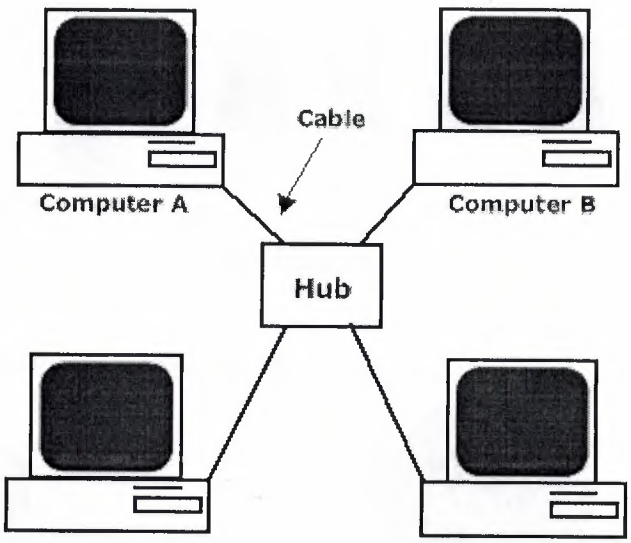


Figure 5 Simple Network

If Computer A wants to send a file to Computer B, the following would take place:
Based on a protocol that both computers use, the NIC in Computer A translates the file (which consists of binary data -- 1's and 0's) into pulses of electricity.
The pulses of electricity pass through the cable with a minimum (hopefully) of resistance.
The hub takes in the electric pulses and shoots them out to all of the other cables.
Computer B's NIC interprets the pulses and decides if the message is for it or not. In this case it is, so, Computer B's NIC translates the pulses back into the 1's and 0's that make up the file.

Sounds easy. However, if anything untoward happens along the way, you have a problem, not a network. So, if Computer A sends the message to the network using NetBEUI, a Microsoft protocol, but Computer B only understands the TCP/IP protocol, it will not understand the message, no matter how many times Computer A sends it.

Computer B also won't get the message if the cable is getting interference from the fluorescent lights etc. or if the network card has decided not to turn on today etc etc.

Figure 6 shows small Ethernet local area network.

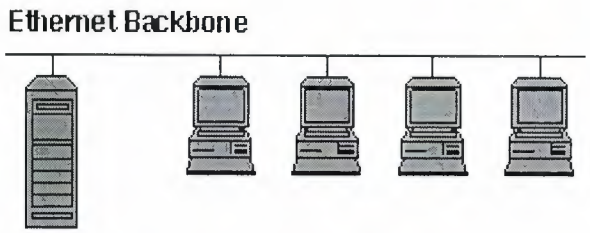


Figure 6 Small Ethernet LAN

The figure 7 shows briefly the interconnection of two LANs

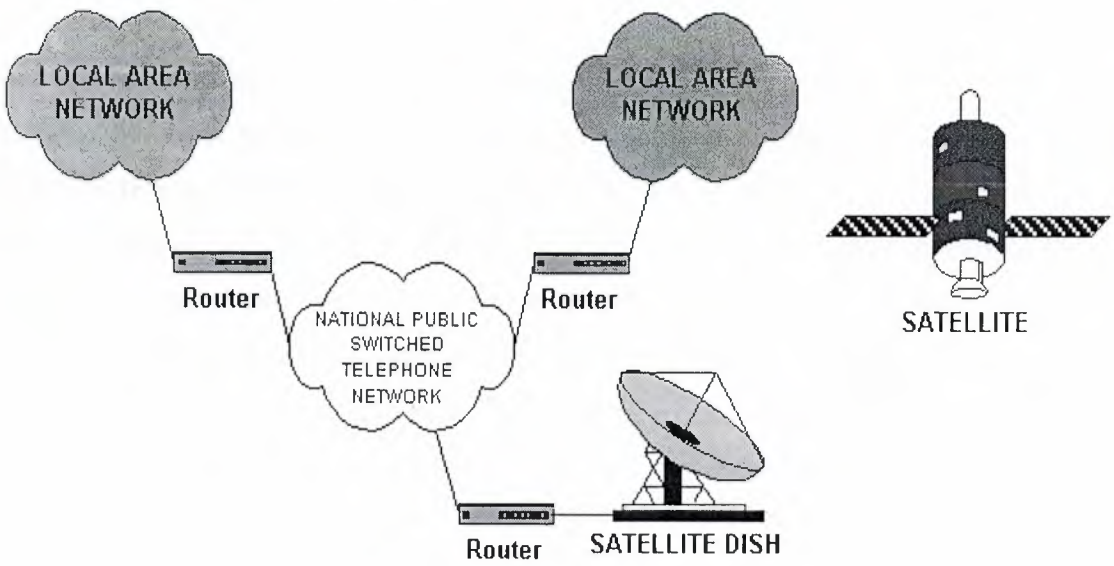


Figure 7 Interconnection of two LANs

1.6 Major Components of LANs

Servers.

Client / Workstation.

Media.

Shared Data.

Shared Printers and other peripherals.

Network Interface Card.

Hubs / Concentrator.

Repeaters, Bridges, Routers, Brouters, Gateways

1.7 Types of Local Area Networks

LANs are usually further divided into two major types

1.7.1 Peer-to-Peer:

A peer-to-peer network is one in which two or more PCs share files and access to devices such as printers without requiring separate server computer or server software. Where is a communications model in which each party has the same capabilities and either party can initiate a communication session and all devices support roughly equivalent capabilities.

1.7.2 Client-Server:

Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request. Although the client/server idea can be used by programs within a single computer, it is a more important idea in a network. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations. Computer transactions using the client/server model are very common. For example, to check your bank account from your computer, a client program in your computer forwards your request to a server program at the bank.

1.8 Local Area Networks Connectivity Devices

1.8.1 Repeaters

A network device used to regenerate or replicate a signal. Repeaters are used in transmission systems to regenerate analog or digital signals distorted by transmission

loss. Analog repeaters frequently can only amplify the signal while digital repeaters can reconstruct a signal to near its original quality.

1.8.2 Bridges

A device that connects two local-area networks (LANs), or two segments of the same LAN that use the same protocol, such as Ethernet or Token-Ring.

1.8.3 Routers

A device that forwards data packets along networks . A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect.

1.8.4 Brouters

A brouter has the best features of both routers and bridges in that it can be configured to pass the unroutable protocols by imitating a bridge, while not passing broadcast storms by acting as a router for other protocols

1.8.5 Gateways

1) A node on a network that serves as an entrance to another network. In enterprises, the gateway is the computer that routes the traffic from a workstation to the outside network that is serving the Web pages. In homes, the gateway is the ISP that connects the user to the internet.

In enterprises, the gateway node often acts as a proxy server and a firewall. The gateway is also associated with both a router, which use headers and forwarding tables to determine where packets are sent, and a switch, which provides the actual path for the packet in and out of the gateway.

(2) A computer system located on earth that switches data signals and voice signals between satellites and terrestrial networks.

(3) An earlier term for router, though now obsolete in this sense as router is commonly used.

1.9 Local Area Networks (LAN) in the work place and its advantages

Network allows more efficient management of resources. For example, multiple users can share a single top quality printer, rather than putting lesser quality printers on individual desktops. Also network software licenses can be less costly than separate, stand alone licenses for the same number of users.Network helps keep information reliable and up-to-date. A well managed, centralized data storage system allows

multiple users to access data from different locations, and limit access to data while it is being processed.

Network helps speeds up data sharing. Transferring files across a network is almost always faster than other, non-network means of sharing files.

Networks help business service their clients more effectively. Remote access to centralized data allows employees to service clients in the field, and clients to communicate directly to suppliers.

Speed: Networks provide a very rapid method for sharing and transferring files. Without a network, files are shared by copying them to floppy disks, then carrying or sending the disks from one computer to another. This method of transferring files is very time-consuming.

Security: Files and programs on a network can be designated as "copy inhibit," so that you do not have to worry about illegal copying of programs. Also, passwords can be established for specific directories to restrict access to authorized users.

Centralized Software Management: One of the greatest benefits of installing a local area network is the fact that all of the software can be loaded on one computer (the file server). This eliminates that need to spend time and energy installing updates and tracking files on independent computers throughout the building.

Electronic Mail: The presence of a network provides the hardware necessary to install an e-mail system. E-mail aids in personal and professional communication for all personnel, and it facilitates the dissemination of general information to the entire school staff. Electronic mail on a LAN can enable students to communicate with teachers and peers at their own school. If the LAN is connected to the Internet, people can communicate with others throughout the world. Network allows workgroups to communicate more effectively. Electronic mail and messaging is a staple of most network systems, in addition to scheduling systems, project monitoring, on-line conferencing and groupware, all of which help work teams be more productive.

Workgroup Computing: Workgroup software (such as Microsoft BackOffice) allows many users to work on a document or project concurrently. For example, educators located at various schools within a county could simultaneously contribute their ideas about new curriculum standards to the same document and spreadsheets.

1.10 Emerging Technology, Wireless Network

Wireless technology enhances the reach and mobility of computers or other network devices. Most agree that wireless networks and services represent the future of computer networking and the Internet

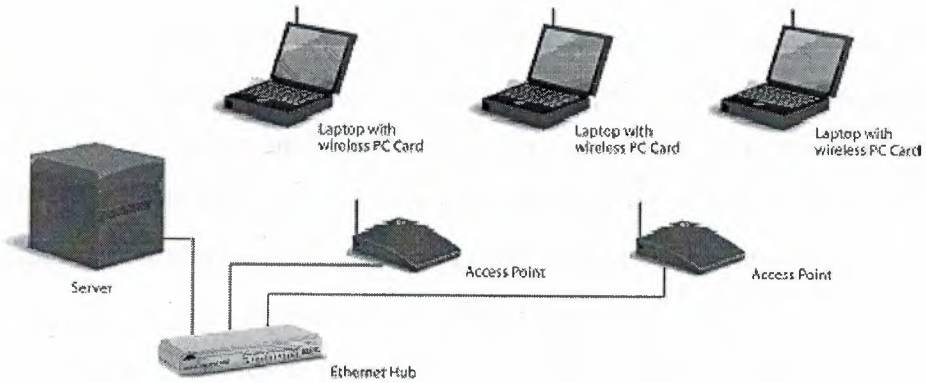


Figure 8 Wireless Network

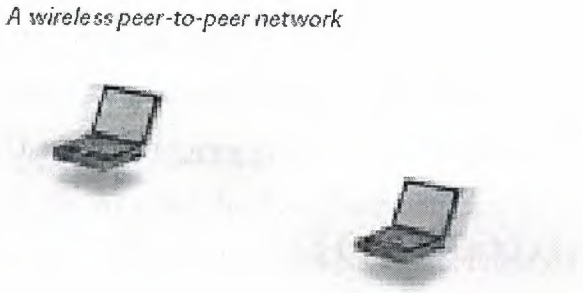


Figure 9 Wireless Peer-to-Peer Network

2. LAN TOPOLOGIES AND REFERENCE MODELS

2.1 Topologies

Geometric arrangement of devices on the network is called topology. Topology is a term used to describe the way in which computers are connected. It refers to the shape of the network. Two networks have the same topology if the connection configuration is the same, although the networks may differ in physical interconnections, distances between nodes, transmission rates, and/or signal types. Different network topologies offer different advantages and disadvantages in cost, complexity, and robustness. The first two differences are self-explanatory and the robustness of a network is its ability to continue functioning even if damage occurs to part of the network. There are two types of topology: physical and logical. The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Logical topology is the method used to pass the information between workstations.

2.2 Physical Topologies

The physical layout of devices on a network. Every LAN has a topology, or the way that the devices on a network are arranged and how they communicate with each other. The way that the workstations are connected to the network through the actual cables that transmit data -- the physical structure of the network -- is called the physical topology. The logical topology, in contrast, is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices.

There are six ways of connecting computers on a network. These physical topologies are categorized into the following basic type

2.2.1 Linear Bus Topology

Linear Bus

A linear bus topology consists of a main run of cable with a terminator at each end (See fig. 1). All nodes (file server, workstations, and peripherals) are connected to the linear cable. Ethernet and LocalTalk networks use a linear bus topology.

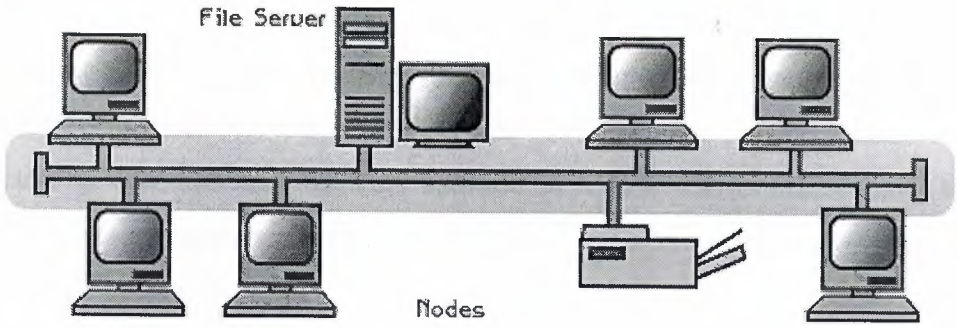


Figure 1 Linear Bus topology

Advantages of a Linear Bus Topology

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages of a Linear Bus Topology

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.

2.2.2 Ring Topology

This layout is similar to the linear bus, except that the nodes are connected in a circle using cable segments. In this layout, each node is physically connected only to two others. Each node passed information along to the next, until it arrives at its intended destination effectively either "clockwise" or "counterclockwise".All devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it. Ring topology is an active topology because each computer repeats (boosts) the signal before passing it on to the next computer. Messages proceed from node to node in one direction only. Should a node fail on the network, data can no longer be passed around the ring unless the failed node is either physically or electronically bypassed. Using bypass software, the network can withstand the failure of a workstation by bypassing it and still be able to maintain the network's integrity.

One of the major issues in a ring topology is the need for ensuring all workstations have equal access to the network. Normally, the entire network has to be

brought down while a new node is added and cabling reattached. However, this particular problem can be overcome by initially setting up the network with additional connectors. These connectors enable you to add or remove. The addition of the connectors is accomplished with the addition of a multistation access unit (MAU). The MAU is a wiring concentrator which allows workstations to be either inserted or bypassed on the ring.

The most common example of the simple ring architecture is Token Ring. SONET is based on double ring architectures. Both Token Ring/IEEE 802.5 and FDDI networks implement a ring topology In Token Ring, each device has an upstream and a downstream neighbor. If one device wants to send a packet to another device on the same ring, it sends that packet to its downstream neighbor, who forwards it to its downstream neighbor, and so on until it reaches the destination. First passes data to second, second passes data to third, and so on. In practice, there is a short connector cable from the computer to the ring. There is no central controlling computer. Each computer on the ring can communicate with any other in the ring with specifically addressed messages. Ring configuration is called broadcast topology. Only one node can broadcast at a time i.e. needs a Protocol. Rings are found in some office buildings or school campuses. If there is a line break, or if you are adding or removing a device anywhere in the ring this will bring down the network. In an effort to provide a solution to this problem, some network implementations (such as FDDI) support the use of a double-ring. As in new ring technology, if the primary ring breaks, or a device fails, the secondary ring can be used as a backup. Figure 2. and 3 show the ring topologies.

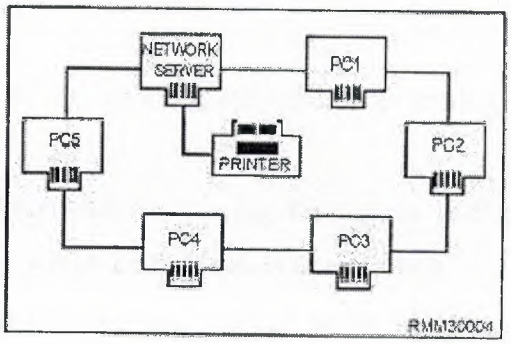


Figure 2 Ring Topology

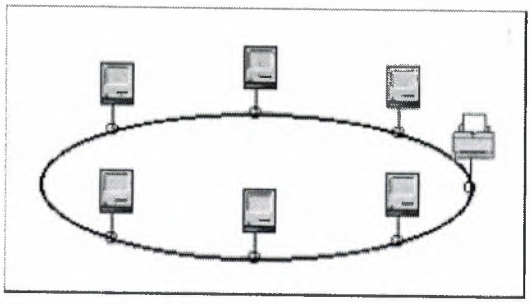


Figure 3 Ring Topology

- Advantages

1) The chief advantage over a bus is that if a break occurs in the ring, the machines will still be able to communicate by going to other way around the ring.

2) Equal access.

3) Very high transmission rates are possible.

4) Transmission of messages around the ring is relatively simple, traveling in one direction only.

5) No dependence on a central computer or file server as each node controls transmissions to and from itself.

6) Each node in the network is able to purify and amplify the data signal before sending it to the next node. Therefore, ring topology introduces less signal loss as data traveling along the path.

7) Ring-topology network is often used to cover a larger geographic location where implementation of star topology is difficult.

- Disadvantages

1) Unfortunately, the difficulty and cost of bringing both ends of the network together and wiring a ring topology usually outweigh the advantages of using a ring topology.

2) Difficult to troubleshoot, network changes affect many users, failure affects many users.

3) A failure in any cable or device breaks the loop and can take down the entire network.

4) One of the major disadvantages of ring topologies is the extreme difficulty of adding new workstations while the network is in operation.

5) Another drawback of ring topology is that users may access the data circulating around the ring when it passes through his or her computer.

6) Break anywhere in the ring will cause network communications to stop. A backup signal path may be implemented in this case to prevent the network from going down.

2.2.3 Star Topology

All devices are connected to a central hub(also called a multiport repeater or concentrator that may be an actual hub or a switch) to each workstation. which rebroadcasts all transmissions received from any peripheral node to all peripheral nodes on the network, including the originating node. Star networks are relatively easy to install and manage, but bottlenecks can occur because all data must pass through the hub. Nodes communicate across the network by passing data through the hub. Multiple hubs may be used to increase the number of computers connected to the network. For a star topology, either unshielded, twisted pair (UTP) wire or shielded twisted pair (STP) wire is used. The price of STP wire is much higher than that of UTP wire. To save costs, most network engineers use UTP cables for the network. However, if the distance between the hub and the node exceeds 110m, STP wire has to be used. As each computer connects to a hub using a single cable, a star-topology network uses more cable than does a bus-topology network. The hub is also an additional cost. Despite the higher costs of the hub and additional wiring, star topology has become the most popular network topology. Figure 4 shows simple star topology

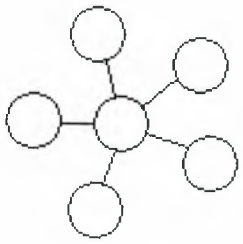


Figure 4. Simple Star Topology

Figure 5. shows star topology in more detail

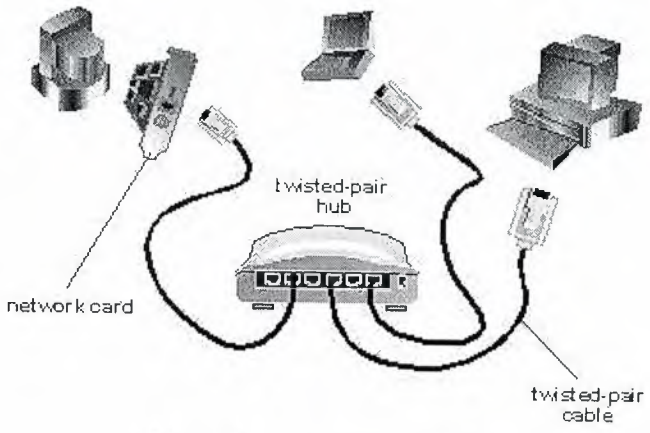


Figure 5 Detailed Star Topology

In practice, most Ethernet and Token Ring LANs are implemented in a star topology. In one option for a star topology, the central device aggregates the traffic from every device and broadcasts it back out to all other devices, letting them decide for themselves packet by packet what they should pay attention to. This is called a hub. Alternatively, the central device could act as a switch and selectively send traffic only where it is intended to go. The star topology is often called hub and spoke, as an analogy to a bicycle wheel. This term can be misleading because sometimes the hub is a hub and sometimes it's a switch of some kind. Most modern LANs are built as stars, regardless of their underlying technology. While expansion is fairly easy on a bus network, it is even easier on a large star network. Most hubs have the ability to be stacked. Stacking is linking multiple hubs together to provide more available connection spots. For example, if I had a 5-port (5 open connection spots) hub, and had all of the connections filled, I would want to expand by stacking. So, I would plug in a cable into the hub's uplink port and connect it to another empty 5-port hub. I would then have another 5 empty ports to work with. Computers connecting to a hub typically use a flexible cabling called 10BaseT, also known as "twisted pair" due to it's internal wiring configuration. At the end of each 10BaseT cable is an RJ-45 connector that bares a resemblance to a telephone connector. Don't bother attempting to plug an RJ-45 connector into a standard phone jack...it will not fit. A standard telephone uses an RJ-11 connector, which is smaller than an RJ-45 connector.

In Figure 6 practical implement of star topology is shown.

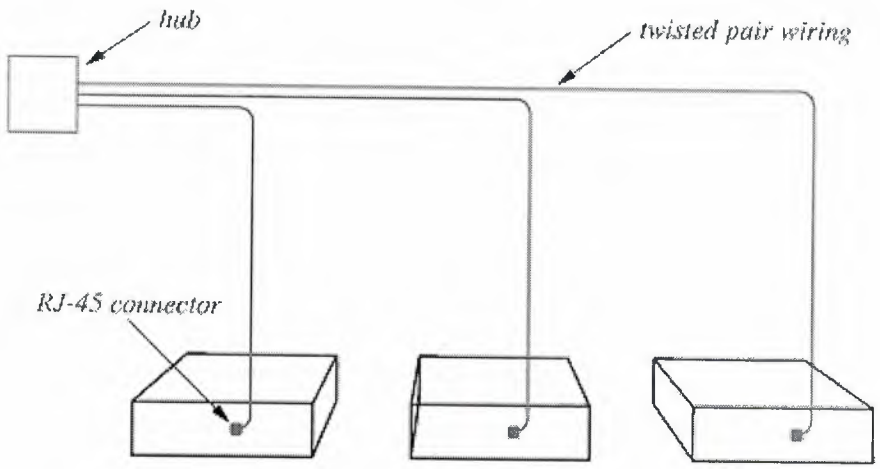


Figure 6. Star Topology in Practice

- Advantages

1) The main advantage is that a communication breakdown between any computer and the hub does not affect any other node on the network. Figure 2.9 shows connection of hub to nodes

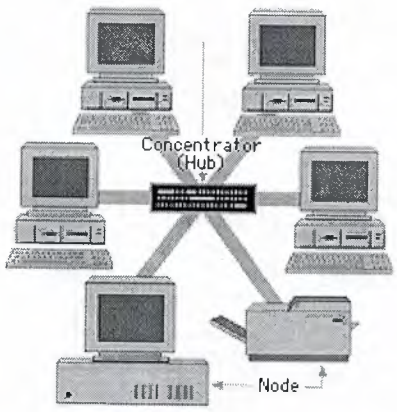


Figure 7 HUB is shown in the Star Topology

2) In addition, data travel through the hub during transmission, which enables the network administrator to monitor the status of all connected nodes

3) Moreover, the largest number of hops from any source computer to the destination computer is only two.

4) Its certainly easier to upgrade a network by upgrading only the device in the closet, without having to change the expensive cabling to every desk. No disruptions to the network when connecting or removing devices.

5) Its also much easier to make fast switching equipment in a small self-contained box than it would be to distribute the networking technology throughout the work area.

6) The prevalence of star topology networks has made it possible to build general-purpose structured cable plants. The cable plant is the set of cables and patch panels that connect all user workspaces to the aggregation point at the center of the star.

7) It is fairly easy to pinpoint a problem on a small star network. For example, if all the computers on the network can't communicate, one can most likely pinpoint the problem to hub failure.

8) If one computer goes offline, it does not halt network communications like a bus network would. All other machines connected to the hub can still communicate.

9) Another advantage of star topology is that the network administrator can give selected nodes a higher priority status than others. The central computer/hub looks for signals from these higher priority workstations before recognizing other nodes.

10) Hard disk can be shared by all users on a file basis. Figure 8 clearly defines the share of hard disk by other users.

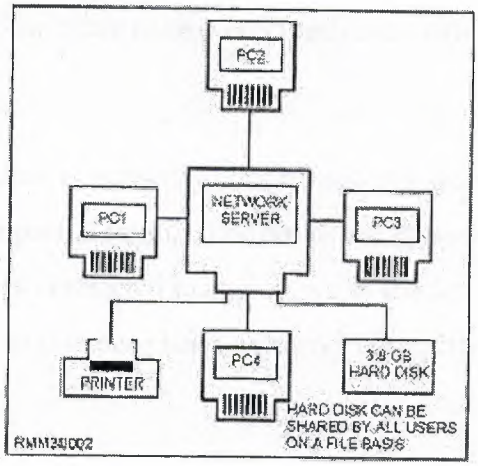


Figure 8 Hard Disk Sharing

- Disadvantages

1) The weakness of the star topology is that the whole network goes down if the hub breaks. There are many strategies for reducing this risk, however. The selection and implementation of these strategies are central to a good network design. This is like if you were to burn down the phone company's central office, then anyone connected to it wouldn't be able to make any phone calls.

2) All nodes receive the same signal therefore dividing bandwidth; max computers is 1,024 on a LAN; max UTP length is 100 meters (approx 330 ft); distance between computers is 2.5 meters.

3) The failure of a transmission line, i.e., channel, linking any peripheral node to the central node will result in the isolation of that peripheral node from all others.

4) More expensive than linear bus topologies because of the cost of the concentrator

2.2.4 Mesh Topology

There are two types of mesh topologies: full mesh and partial mesh.

Full mesh topology occurs when every node has a circuit connecting it to every other node in a network. Full mesh is very expensive to implement but yields the greatest amount of redundancy, so in the event that one of those nodes fails, network traffic can be directed to any of the other nodes. Full mesh is usually reserved for backbone networks.

Partial mesh topology is less expensive to implement and yields less redundancy than full mesh topology. With partial mesh, some nodes are organized in a full mesh scheme but others are only connected to one or two in the network. Partial mesh topology is commonly found in peripheral networks connected to a full meshed backbone.

Mesh network is a local area network (LAN) that employs one of two connection arrangements, full mesh topology or partial mesh topology. In the full mesh topology, each node (workstation or other device) is connected directly to each of the others. In the partial mesh topology, some nodes are connected to all the others, but some of the nodes are connected only to those other nodes with which they exchange the most data.

The illustration shows a full mesh network with five nodes. Each node is shown as a sphere, and connections are shown as straight lines. The connections can be wired or wireless.

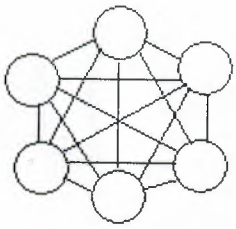


Figure 9 Simple Mesh Topology

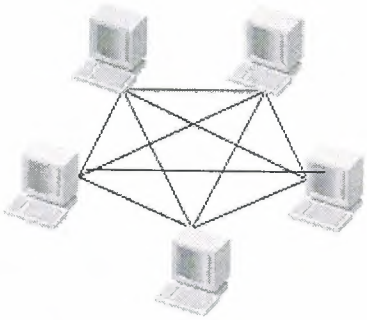


Figure 10 Mesh Topolog

Advantages

1) Mesh topology helps find the quickest route on the network.

2) It provides redundancy, in the event of a link failure, meshed networks enable data to be routed through any other site connected to the network.

Disadvantages

1) Because each device has a point-to-point connection to every other device, mesh topologies are the most expensive and difficult to maintain.

2) The other reason why meshed networks are not particularly efficient is that not every device needs to talk to every other device all of the time. So, in fact, most of those links will be idle most of the time.

3) Meshed topology is not very practical for anything but very small networks..

2.2.5 Tree Topology

tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable (See

fig. 11). Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.

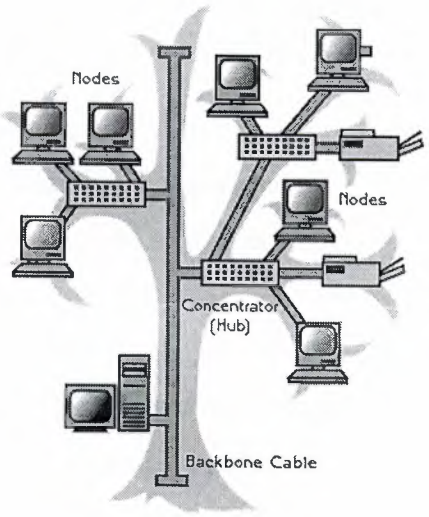


Fig 11 Tree topology

Advantages of a Tree Topology

Point-to-point wiring for individual segments.

Supported by several hardware and software venders.

Disadvantages of a Tree Topology

Overall length of each segment is limited by the type of cabling used.

If the backbone line breaks, the entire segment goes down.

More difficult to configure and wire than other topologies.

5-4-3 Rule

A consideration in setting up a tree topology using Ethernet protocol is the 5-4-3 rule. One aspect of the Ethernet protocol requires that a signal sent out on the network cable reach every part of the network within a specified length of time. Each concentrator or repeater that a signal goes through adds a small amount of time. This leads to the rule that between any two nodes on the network there can only be a maximum of 5 segments, connected through 4 repeaters/concentrators. In addition, only 3 of the segments may be populated (trunk) segments if they are made of coaxial cable. A populated segment is one which has one or more nodes attached to it . In Figure 4, the 5-4-3 rule is adhered to. The furthest two nodes on the network have 4 segments and 3 repeaters/concentrators between them.

This rule does not apply to other network protocols or Ethernet networks where all fiber optic cabling or a combination of a fiber backbone with UTP cabling is used. If there is a combination of fiber optic backbone and UTP cabling, the rule is simply translated to 7-6-5 rule.

- Advantages

1) Point-to-point wiring for individual segments

2) Supported by several hardware and software venders

- Disadvantages

1) As in the conventional star network, individual nodes may thus still be isolated from the network by a single-point failure of a transmission path to the node.

2) A single-point failure of a transmission path within a distributed node will result in partitioning two or more stations from the rest of the network.

3) Overall length of each segment is limited by the type of cabling used.

4) More difficult to configure and wire than other topologies.

5) If the backbone line breaks, the entire segment goes down.

2.2.6 Hybrid Topology

A combination of any two or more network topologies.It is also known as varaitaions of different topologies.Instances can occur where two basic network topologies, when connected together, can still retain the basic network character, and therefore not be a hybrid network. For example, a tree network connected to a tree network is still a tree network. Therefore, a hybrid network accrues only when two basic networks are connected and the resulting network topology fails to meet one of the basic topology definitions. For example, two star networks connected together exhibit hybrid network topologies. A hybrid topology always accrues when two different basic network topologies are connected.

- Star Bus

The star bus is the combination of the bus and star topologies. In a star bus topology network linked together with linear bus trunks. If one computer goes down, it will not affect the rest of the network. The other computers will be able to continue communicate. If hub goes down, all computers on the hub are unable to communicate.

If a hub is linked to other hubs, those connections will be broken as well. Figure .12 shows the star bus network

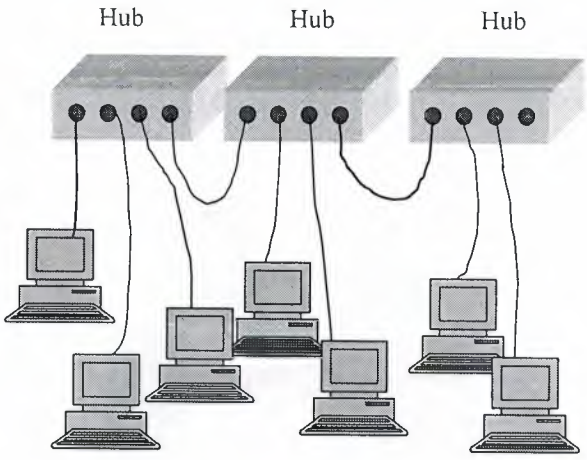


Figure 12. Star Bus Topology

Star Ring

The star ring (sometimes called star wired ring) appears similar to the star bus. Both the star ring and the star bus are centered in a hub which contains the actual ring or bus. The hubs in the star bus are connected by linear bus trunks, while the hubs in star ring are connected in a star pattern by main hub. Figure shows simple diagram of star ring network. Figure .13 describe about the star ring network

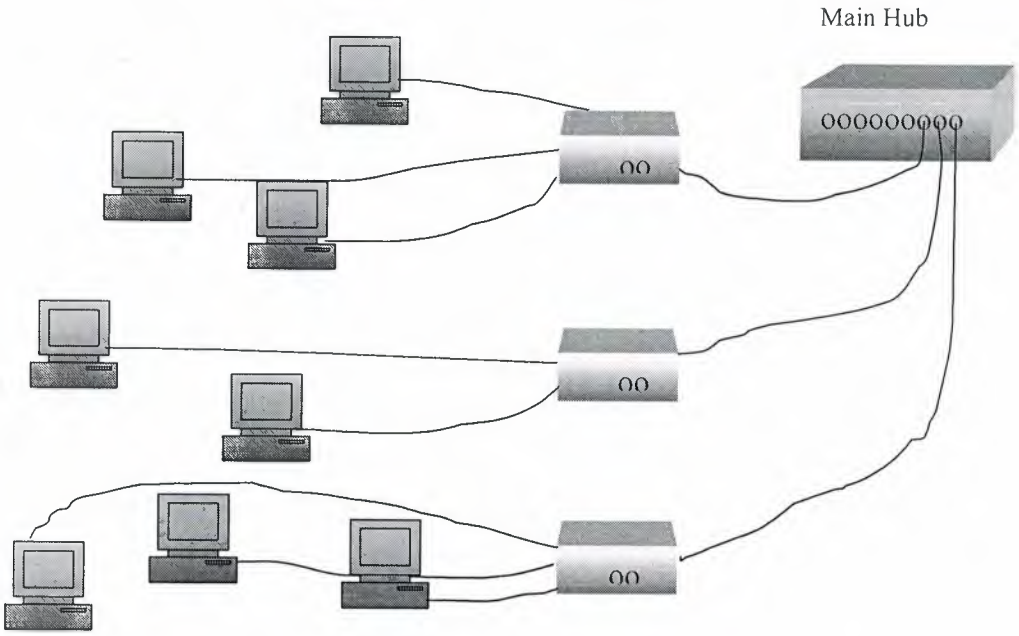


Figure 13 Star Ring Network

As the technology is advancing a star-wired ring topology may appear (externally) to be the same as a star topology. Internally, the MAU (multistation access unit) of a star-wired ring contains wiring that allows information to pass from one device to another in a circle or ring See figure .14 The Token Ring protocol uses a star-wired ring topology.

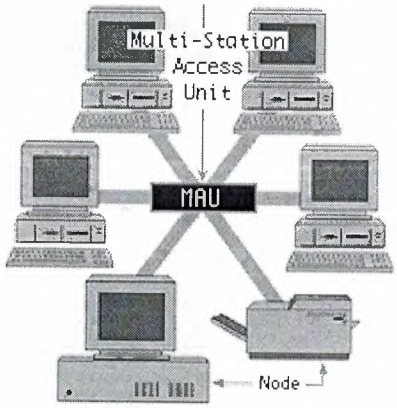


Figure 14 Star Ring Network

2.3 Logical Topologies

Logical topology is term used to describe a scheme used by the network's operating system to manage the flow of information between nodes. The operating system's communication scheme influences how person using the workstations visualize the way the computers are communicating with each other. Most operating systems use one of two basic kinds of logical topology:

2.3.1 Linear

This communication scheme functions like the linear bus topology and is common in Ethernet-based systems. Each node has a unique address, and the addresses are accessed sequentially. Information is passed up and down the list until the right destination address is found. Generates and sends the signal to all network devices. Figure .15 shows logical addresses correspond to the physical location of the computers

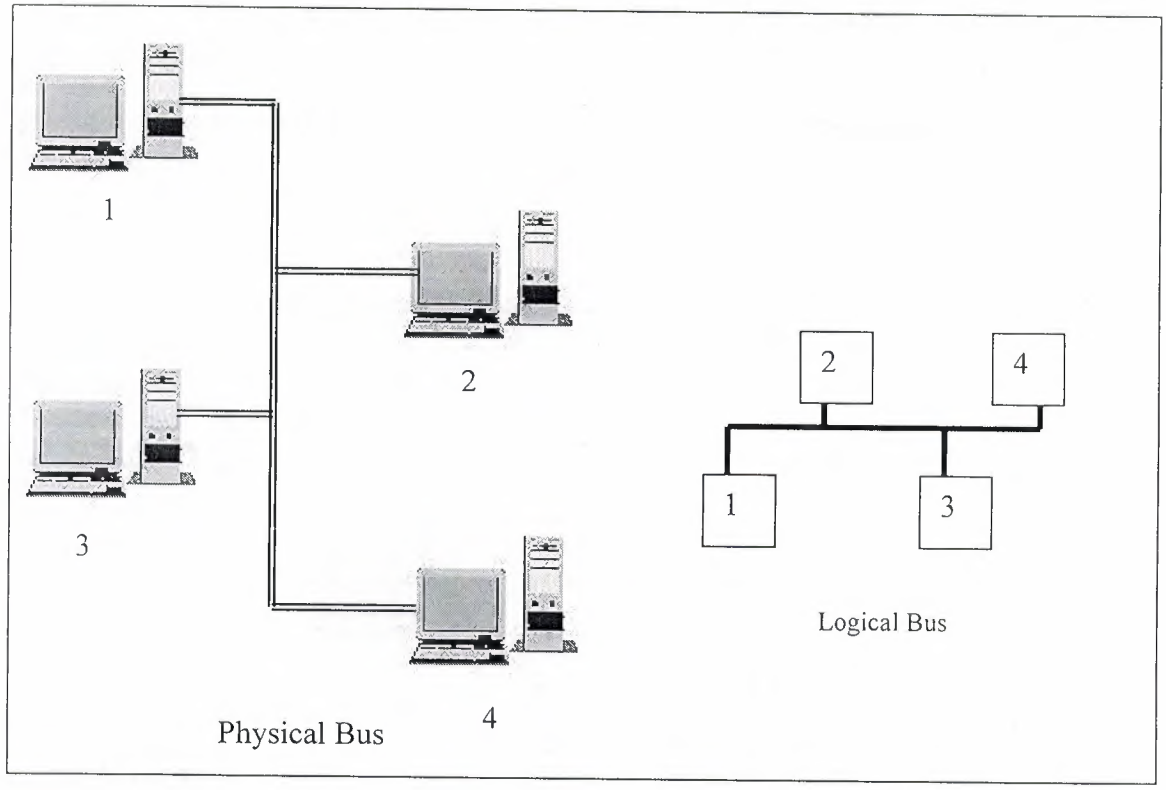


Figure 15 Physical and Logical Topologies

2.3.2 Token Ring

A type of computer network in which all the computers are arranged (schematically) in a circle. A token, which is a special bit pattern, travels around the circle. To send a message, a computer catches the token, attaches a message to it, and then lets it continue to travel around the network.

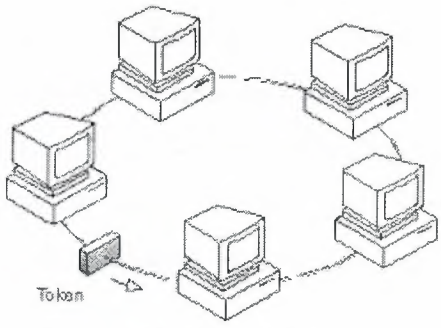


Figure 16 token

A type of CAM. Token passing uses a token, or series of bits, to grant a device permission to transmit over the network. Whichever device has the token can put data

into the network. When its transmission is complete, the device passes the token along to the next device in the topology. System rules in the protocol specifications mandate how long a device may keep the token, how long it can transmit for and how to generate a new token if there isn't one circulating. Also see contention and polling.

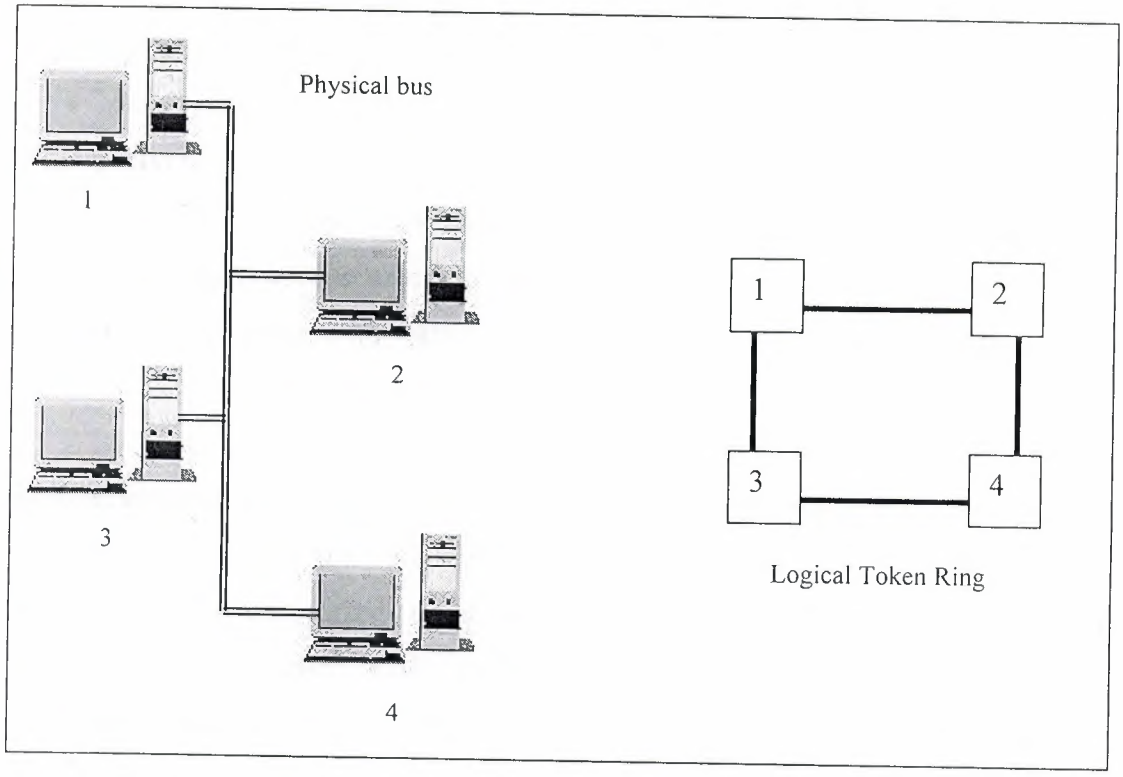


Figure 17 Physical Bus and Logical Token Ring

2.4 Considerations when Choosing Network Topologies

When we first set up the network, we need to choose the type of hardware, software and network operating systems to be used, and the physical and logical topologies. These choices are interdependent upon each other and together make up the network configuration. We can make these choices by weighing together these factors as:

- Cost

What is the most efficient system our business can afford? A linear bus network may be the least expensive way to install a network; we do not have to purchase concentrators.

- Speed: How fast system need to be?
- Environment: Are there environmental factors (for example, the presence of electrical fields) that influence the kind of hardware required?
- Size: How big will the network be? Will it require a dedicated file server or servers?
- Connectivity: Will other users (for example, field representatives using laptops computers) need to access the network from various remote locations?
- Future growth: With a star topology, expanding a network is easily done by adding another concentrator.

In some circumstances, our choices regarding certain kinds of hardware and standards will be constrained by other choices we've made. For example, if we elect ARCnet system, we must use wiring concentrators to make the network connections. These concentrators (also called hubs), are required by ARCnet to condition the electrical signal and thus maintain the electrical standards ARCnet needs in order to work.

We will find that our decisions tend to revolve around money: the cost of the number of nodes on the network, distances involved, and whatever future plans we envision for our business.

For an information management standpoint, nearly every business has certain unique characteristics. Each business must take the time to design the suitable information management system. An experienced network design consultant or responsible vendor can help us analyze business needs and explain our options in detail, showing which options are most suitable for particular business.

2.5 Data Communication Reference Models

Although each data communication protocol has its own operational reference model, all are contrasted to Open Systems Interconnect Reference Model (OSI-RM), TCP/IP reference model and the Institute of Electrical and Electronic Engineers (IEEE)

model. The OSI-RM is the basis for discussing the various elements of the data communication process. The IEEE model defines the operational specifications for transport layer protocols. Computer networking hardware and software vendors use definitions contained in reference models to ensure interoperability with other network elements. Most of the basic elements of network design and implementation can be accomplished without any detailed knowledge of the OSI-RM or protocols in general. Network troubleshooting and network security and management, however, are difficult without some understanding of the protocols in use and their interrelationships.

2.5.1 OSI Reference Model

The OSI, or Open System Interconnection, model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

Application(Layer 7)

This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer

Presentation(Layer 6)

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

Session(Layer 5)

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

Transport(Layer 4)

This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

Network(Layer 3)

This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

Data Link(Layer 2)

At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sublayers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

Physical(Layer1)

This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

2.5.1.1 Layer 7: Application

Though it is called the Application layer, it does not necessarily mean the applications that you and I interact with when we use a computer. The Application layer deals with printing, file transfer, remote terminal services, and directory browsing. Some user applications exist directly at the Application layer, such as Telnet and FTP. Other user applications have Application layer functions built into them. A word processing program that can print to a network printer has Application layer functions built into

it. Watching the status bar of your web browser is a good place to see Application layer functions at work. All application programs are included at this layer (including ones that do not require any communication services), and each application must employ its own protocol to communicate with the Lower-Layer Protocols (LLPs). Basic file and print services also fall into the application layer.

Layer 7 services are the places where the application communicates with the user in terms of actual (human) meaningful input and output data. The following standards govern data between the user application and network:

- ISO-X.500 Directory Services
  X.400 Message handling (e-mail) services
  Virtual Terminal Protocol (VTP)
- TCP/IP-Telnet virtual terminal service
  Simple Mail Transfer Protocol (STMP)
  Domain Name Service (DNS)
  Berkeley Remote Commands
  Sun's Network File System
  CMU's Andrew File System
- AppleTalk-AppleShare Print Service
- IPX-Netware Core Protocol
  NetWare Shell (NetX)

2.5.1.2 Layer 6: Presentation:

The primary job of the Presentation layer is that of translator. It takes care of translating ACSII into EBCIDIC, and vice versa; compression, decompression; encryption and decryption. Essentially, the Presentation layer works to transform data into the form that the Application layer can accept. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer. This layer addresses the problems of data representation as it appears to the user. Data syntax, character sets, and data formatting also fall under Layer 6. Layer 6 also provides the means for the various Layer 7 services to exchange information in an encoding scheme. Almost all systems use the ASCII encoding scheme to present data so it can be transmitted in a computer-

independent form. This way, computers of various types can exchange information with one another. Overall, Layer 6 presents data in a common and universally acceptable form that can be transported and exchanged without concern for the terminal used for displaying the data. One would see MIDI files and JPG files in the presentation layer. JPEG, is standard method of presenting files on the Internet.

Protocols associated with this layer are the following:

- ISO- Connection-oriented presentation protocol
- TCP/IP- Network Virtual Terminal
- AppleTalk- AppleTalk Filing Protocol

  Adobe PostScript
- IPX- Netware File Service Protocol (NFSP)
- Server Message Block (SMB)

2.5.1.2 Layer 5: Session

The bottom four layers -- Physical, Data Link, Network, and Transport -- all look "down" toward the bottom of the network. Their focus is on getting the job of moving data from point A to point B done. The Session layer, in a sense, looks up toward the top layers. Session is responsible for regulating the flow of information between applications. It synchronizes their communication, and takes care of such things as security and handling errors outside the scope of network communications (such as a server with a full disk drive, or a tape that needs to be mounted).

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination. Layer 5 manages the exchange of data between application processes. Session interposes communication, flow control, and error checking services. Most network operating systems (AppleTalk, Novell Netware and Microsoft Networking) provide service activities at this level. The variety of protocols used to provide session services are as follows:

- ISO- Connection-oriented session protocol
- TCP/IP- Berkeley socket service

  System V stream service

- AppleTalk-AppleTalk Data Stream Protocol (ADSP)
  AppleTalk Session Protocol (ASP)
  Printer Access Protocol (PAP)
  Zone Information Protocol (ZIP)
- IPX- NetBIOS

2.5.1.3 Layer 4: Transport

This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer. Layer 5 checks data for integrity and keeps application program apprised of the communication process, but layer 4 is concerned with end-to-end data transport. This transport can be managed as either connection-oriented or connectionless. Connection-oriented data transmission is needed for reliable end-to-end, sequenced delivery. Because the data loss might occur because of LLP delivery problems, a variety of services are needed to address such a condition.

A connection-oriented transport must be able to perform the following data handling services:

- Multiplexing- A connection-oriented transport service must be able to move the data in and out of the Layer 3 carrier.
- Segmenting- Data, in most cases, needs to be transmitted in several units. Segmenting is the process of breaking the data into segments and reassembling it at the remote end.
- Blocking- Some data segments are small enough to be moved in one data unit. Blocking is the process of putting multiple data segments into a single data unit and extracting them at the remote end.
- Concatenating- This is the process of putting multiple data units into a single Layer 3 carrier and extracting them at the remote end.
- Error detection and error recovery- The transport service must have a way of detecting if the data has become damaged during the layer 3 carrying process and have the means to resend it.
- Flow control- The transport must be able to regulate itself as to the number of data units it passes to the adjacent layers.

- Expedite data transfer- The transport layer needs to be able to provide for special delivery service for certain data units and override normal flow control conditions.

Some connections-oriented transport protocols are following:

- ISO- Transport Protocol Class 4 (TP4)
- TCP/IP- Transmission Control Protocol (TCP)

A connectionless transport protocol is also known as datagram, transport. Connectionless transport has no requirement for data sequencing, data integrity checking, or loss due to LLP delivery problems. Connectionless transport is used when fast delivery of unimportant data is required, for things like domain name service lookups or voice and video transport. The main requirement for this transport mechanism is consistent data delivery speed, but a slow, consistent stream is preferred over a fast, intermittent one.

Common connectionless transport protocols are the following:

- ISO-Transport Protocol class 0 (TP0)
- TCP/IP- User Datagram Protocol (UDP)
- AppleTalk- AppleTalk Transaction Protocol (ATP)
  Routing Table Maintenance Protocol (RTMP)
  AppleTalk Echo Protocol (AEP)
  Name Binding Protocol (NBP)
- IPX- Service Advertisement Protocol (SAP)

2.5.1.4 Network

The network layer is where the actual delivery of the transport data units takes place. The network layer provides the delivery addressing services needed to move the transport data units from host to host. This is accomplished by sequencing the data into data packets and adding a delivery information header with the source and destination addresses and any additional sequencing information. This packet data is known as datagram.

Layer 3 is also responsible for delivery of the datagrams, requiring some kind of routing service. Under the OSI-RM, activity of datagram is seen as two processes: routing and forwarding. Routing is the process of seeking and finding network information. Forwarding is the actual process of using the routing information to move data from host to host. In OSI environment, there are two type of network layer transport services:

- Connectionless service handled by connectionless network (CLNP)
- Connection-oriented service handled by CONS X_25 (connection-oriented network service over X.25)

2.5.1.5 Data Link

The Data Link layer performs several tasks. It compiles the stream of ones and zeros coming from the Physical layer into bytes, and then into frames -- units of information that have a logical meaning. Data Link can add its own header to the information it passes down to the Physical layer. Information in the header usually includes the destination and source addresses of the frame. Eg. to Computer 12, from computer 15. Data Link is sometimes said to perform error correction. In truth this is really more error detection and simple rejecting of corrupted frames. Layer two also performs flow control.

At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sublayers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. Data link is the facility that controls the transport of the upper layer protocol (ULP) data bits across the physical connection medium. ULP data is "enclosed" inside of a Layer 2 protocol "envelope," a frame, which is then transmitted Layer 2 has two data transport functions. MAC defines the logical representation of ULP data and access to transport medium. The second is link control (LC) or logical link control (LLC), The LLC layer controls frame synchronization, flow control and error checking. It acts as the interface between the Layer 3 protocol(s) and the MAC. Depending on Layer 2 protocol and its application (such as LAN use), the LC function is handled differently. The majorities

of LAN protocol utilize the Institute of Electrical and Electronic Engineers (IEEE) 802.2 LLC specification to perform this function. Advances in network speed, performance, reliability for the most part, all occur at the data link layer (Layer 2).

All transport control protocols are considered Layer 2. Some of the more common protocols are the following:

- IEEE 802.X Ethernet, Fast Ethernet, Gigabit Ethernet. The most common CSMA/CD baseband LAN protocol.
- ANSI X3t9.5 FDDI, Fiber Distributed Data Interface. A LAN/MAN redundant transport technology that runs over the fiber optic cable.
- ITU-T V.34 is the serial line standard used for modem transmission up to 28.8Kbps.
- ITU-T V.90 is the serial line standard that used for modem transmission up to 53.3Kbps. This is the standard that replaced USR's X2 and Lucent/Rockwell's Kflex proprietary standards.
- ITU-T V.35 is the standard used for synchronous communications between routers and public packet data network. The interface usually a Data Service Unit/Channel Service Unit (DSU/CSU), a device used to provide data conversion so the data can be sent over a digital telephone loop

2.5.1.6 Layer 1: Physical

This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level.

It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. The Physical layer defines functionality of the network hardware: what connectors are shaped like; how many pins they have;

what voltage (and for how long) defines a 1 or a 0; whether the media is copper wire, optical fibers, or open air.

This physical layer deals with specifications of the medium used to move bit data from point to point. All physical, electrical, mechanical aspects of the transmission media are addressed at Layer 1. Layer 1 and Layer 2 are also commonly looked at together because the physical layer standards are usually taken for granted.

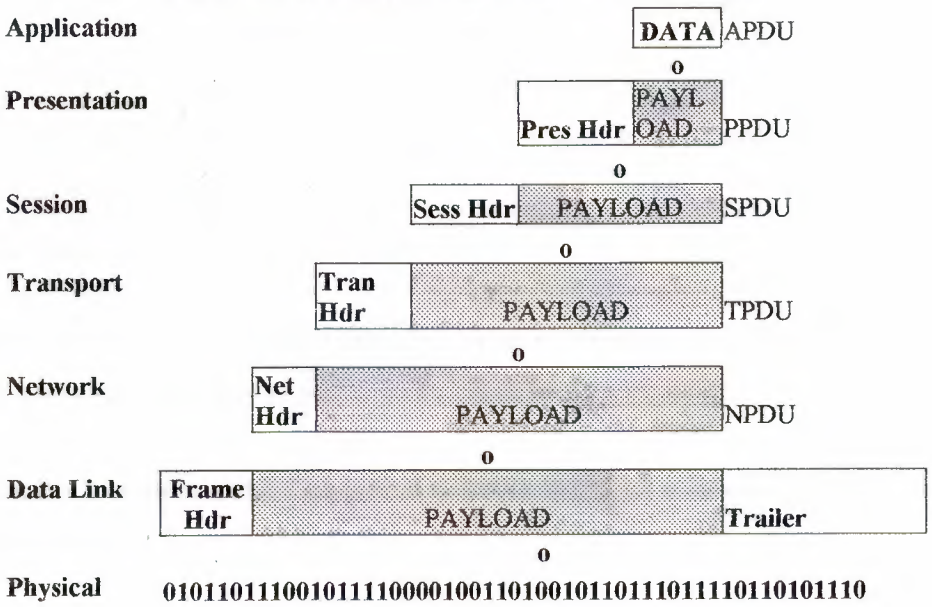
Do not fall into the trap of grouping them. The physical layer of the network is one of the most complex, and, next to configuration errors, the most common cause of problems found in networks. All physical media have the corresponding standards. When working with any medium, at least be aware of, the minimum operating specifications, such as connector type(s), maximum cable length, and any environmental installation requirements, that might interface with the performance of the transport or affect the operation of the other network/non-network equipment. Common physical layer standards are the following:

IEEE 10-BaseT – The cabling standard for using unshielded twisted-pair copper wire to transmit 802.3 Ethernet.

IEEE 100-BaseT – The cabling standard for using unshielded twisted-pair copper wire to transmit 802.3 Fast Ethernet.

EIA/TIA-232 – The standard used for unbalanced (async) circuits at speeds up to 64Kbps. This is commonly known as the RS-232 serial port standard. The actual serial port was based on the ITU-T V.24 standard that is no longer used.

Table 1. Encapsulation of Higher Layer into Lower Layer



The OSI-RM model is shown in the figure 18

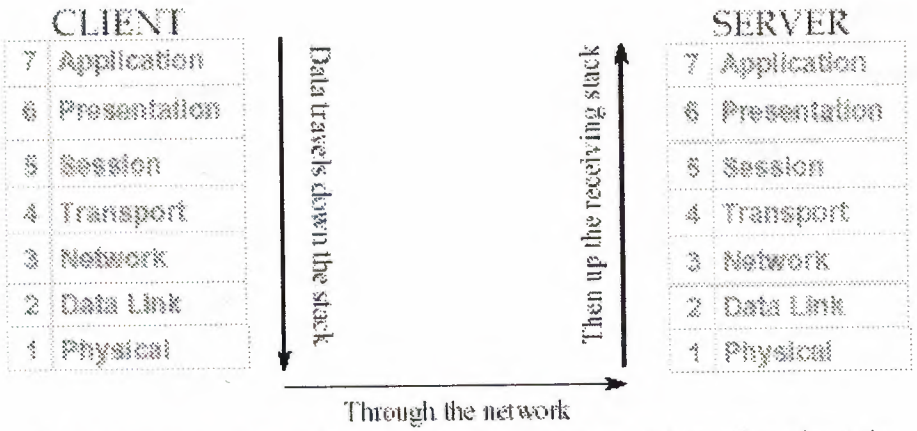


Figure 18 The OSI-RM model

2.5.2 The TCP/IP Reference Model

The TCP/IP reference model is the network model used in the current Internet architecture [19]. It has its origins back in the 1960's with the grandfather of the Internet, the ARPANET. This was a research network sponsored by the Department of Defense in the United States. The following were seen as major design goals:

- ability to connect multiple networks together seamlessly
- ability for connections to remain intact as long as the source and destination machines were functioning
- to be built on flexible architecture

The reference model was named after two of its main protocols, TCP (Transmission Control Protocol) [12] and IP (Internet Protocol).

They choose to build a packet-switched network based on a connectionless internetwork layer.

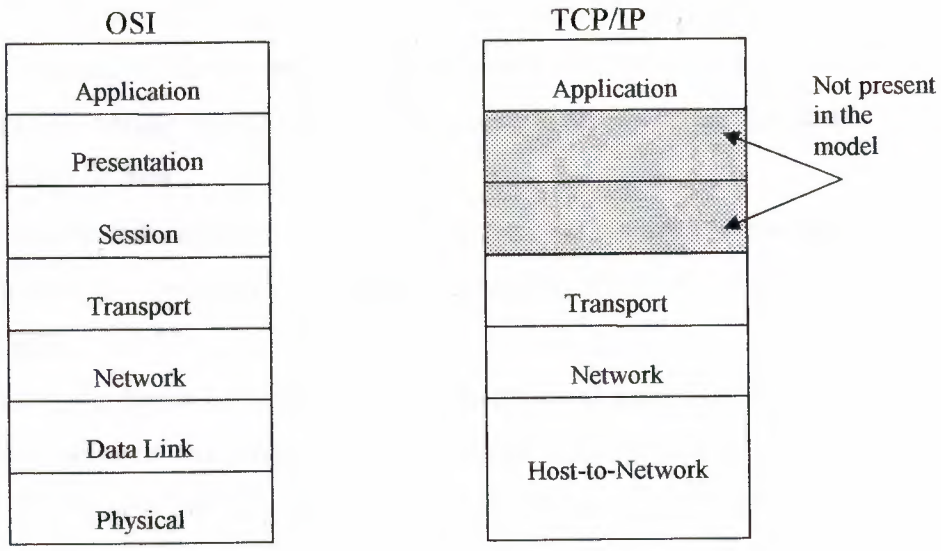


Figure 19 The TCP/IP reference model

A detailed description of the reference model is beyond the scope of this document and project. The basic idea of the networking system is to allow one application on a host computer to talk to another application on a different host computer.

The application forms its request, then passes the packet down to the lower layers, which add their own control information, either a header or a footer, onto the packet. Finally the packet reaches the physical layer and is transmitted through the cable onto the destination host. The packet then travels up through the different layers, with each layer reading, deciphering, and removing the header or footer that was attached by its counterpart on the originating computer. Finally the packet arrives at the application it was destined for. Even though technically each layer communicates with the layer above or below it, the process can be viewed as one layer talking to its partner on the host, as figure 19 shows.

2.5.2.1 The Application Layer

The original TCP/IP specification described a number of different applications that fit into the top layer of the protocol stack. These applications include Telnet, FTP, SMTP and DNS.

Telnet is a program that supports the TELNET [13] protocol over TCP. TELNET is a general two-way communication protocol that can be used to connect to another host and run applications on that host remotely.

FTP (File Transfer Protocol) [14] is a protocol that was originally designed to promote the sharing of files among computer users. It shields the user from the variations of file storage on different architectures and allows for a reliable and efficient transfer of data.
SMTP (Simple Mail Transport Protocol) [15] is the protocol used to transport electronic mail from one computer to another through a series of other computers along the route.
DNS [10] (Domain Name System) resolves the numerical address of a network node into its textual name or vice-versa. It would translate www.yahoo.com to 204.71.177.71 to allow the routing protocols to find the host that the packet is destined for.

2.5.2.2 The Transport Layer

The transport layer is the interface between the application layer and the complex hardware of the network. It is designed to allow peer entities on the source and destination hosts to carry on conversations.

Data may be user data or control data. Two modes are available, full-duplex and half duplex. In full-duplex operation, both sides can transmit and receive data simultaneously, whereas in half duplex, a side can only send or receive at one time.

Interaction between the transport layer and the layers immediately above and below are shown in figure 20. Any program running in the application layer has the ability to send a message using TCP or UDP, which are the two protocols defined for the transport layer. The application can communicate with the TCP or the UDP service, whichever it requires. Both the TCP and UDP communicate with the Internet Protocol in the internet layer. In all cases communication is a two way process. The applications can read and write to the transport layer. The diagram only shows two protocols in the transport layer. T/TCP will also reside in this layer between the other two protocols and function in the same manner.

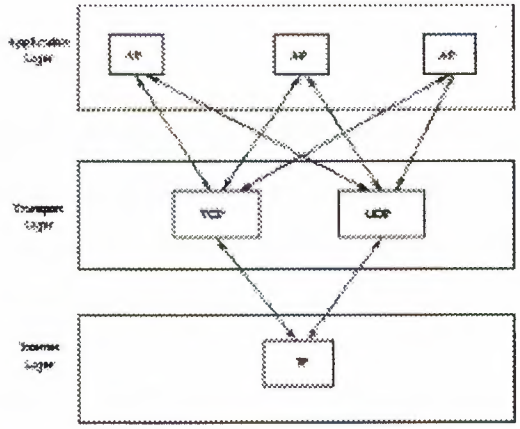


Figure 20: Interaction with Application, Transport and Internet Layers

A message to be sent originates in the application layer. This is then passed down onto the appropriate protocol in the transport layer. These protocols add a header to the message for the corresponding transport layer in the destination machine for purposes of reassembling the message. The segment is then passed onto the internet layer where the Internet Protocol adds a further header. Finally the segment is passed onto the physical layer, a header and a trailer are added at this stage.

2.5.2.3 The Network Layer

The job of the network layer is to inject packets into any network and have them travel independently to the destination. The layer defines IP (Internet Protocol) for its official packet format and protocol. Packet routing is a major job of this protocol.

- The Internet Layer

  In the OSI Reference Model the Network Layer isolates the upper layer protocols from the details of the underlying network and manages the connections across the network. The Internet Protocol (IP) is normally described as the TCP/IP Network Layer. Because of the Inter-Networking emphasis of TCP/IP this is commonly referred to as the Internet Layer.
  upper and lower layer communications travel through IP as they are passed through the TCP/IP protocol stack. In other words, internet layer defines an official packet format and protocol called IP. The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that TCP/IP internet layer is very similar to the OSI reference model.

2.5.2.4 The Host-to-Network Layer

The Host-to-Network layer interfaces the TCP/IP protocol stack to the physical network. The TCP/IP reference model does not specify in any great detail the operation of this layer, except that the host has to connect to the network using some protocol so it can send IP packets over it.

As it is not officially defined, it varies from implementation to implementation, with vendors supplying their own version.

- The Host-to-Network or Network Access Layer

  In TCP/IP the Data Link Layer and Physical Layer are normally grouped together. TCP/IP makes use of existing Data Link and Physical Layer standards rather than defining its own. Most RFCs that refer to the Data Link Layer describe how IP utilizes existing data link protocols such as Ethernet, Token Ring, FDDI, HSSI, and ATM. The characteristics of the hardware that carries the communication signal are typically defined by the Physical Layer. This describes attributes such as pin configurations, voltage levels, and cable requirements. Examples of Physical Layer standards are RS-232C, V.35, and IEEE 802.3.

The four layer structure of TCP/IP is built as information is passed down from applications to the physical network layer. When data is sent, each layer treats all of the information it receives from the layer above as data and adds control information to the front of that data. This control information is called a header, and the addition of a header is called encapsulation. When data is received, the opposite procedure takes place as each layer removes its header before passing the data to the layer above. The figure 21 shows encapsulation.

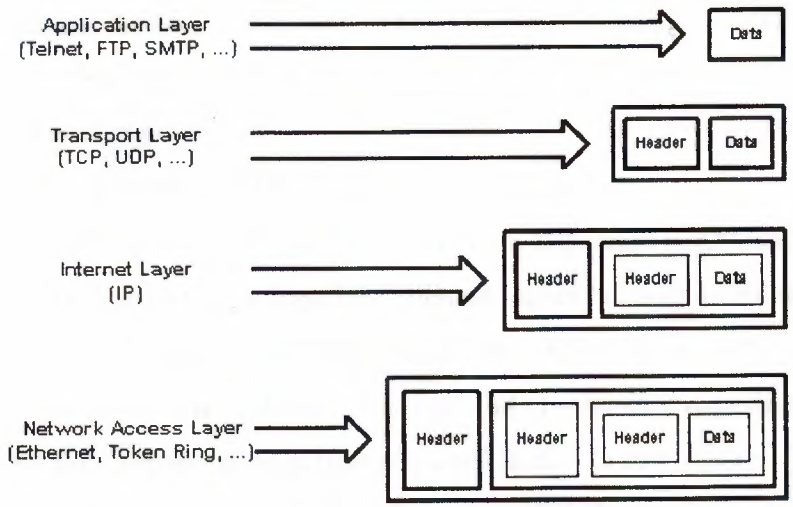


Figure 21. Encapsulation

2.5.3 The 802 Project Model

In the late 1970s, when LANs first began to emerge as a potential business tool, the IEEE realized that there was need to define certain LAN standards. To accomplish this task, the IEEE launched what became known as Project 802, named for the year and month it began (1980, February).

Although the published IEEE 802 standards actually predated the ISO standards, both were in development at roughly the same time and both shared information which resulted in two compatible models.

Project 802 defined network standards for the physical components of a network- the interface card and the cabling- which accounted for in the Physical and Data Link layers of the OSI model.

These standards, called the 802 specifications, have several areas of responsibility including:

- Network adapter cards.
- Wide area network components.
- Components used to create twisted-pair and coaxial cable networks.

The 802 specifications define the way network adapter cards access and transfer data over physical media. This includes connecting, maintaining and disconnecting network devices.

The LAN standards the 802 committees defined fall into 12 categories which can be identified by their number as follows:

802.1 Internetworking

802.2 Logical Link Control (LLC)

802.3 Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) LAN (Ethernet). This is a broadcast bus-oriented technique originated as a commercial product by the Digital/Intel/Xerox EtherNet project. is a network access method in which devices that are ready to transmit data first check the channel for a carrier. If no carrier is sensed, a device can transmit. If two devices transmit at once, a collision occurs and each computer backs off and waits a random amount of time before attempting to retransmit. Before a computer sends data, it first listens to determine whether any other station is talking. If it detects no activity, it transmits the data. If collision occurs between data from 2 computers, each computer waits a random amount of time, then attempts to transmits again.

802.4 Token Bus LAN

The token passing bus scheme is here defined for a broadcast medium and uses a 'token' to regulate the transmission of information. Only the station that holds the token has permission to transmit.

802.5 Token Ring LAN

In this case the medium is set up as a sequential ring and data is passed around, again possession of the token grants a station permission to transmit into the ring. IBM has adopted the token ring technology for its current generation of LAN products.

802.6 Metropolitan Area Network

802.7 Broadband Technical Advisory Group

802.8 Fiber-Optic Technical Advisory Group

802.9 Integrated Voice/Data Networks

802.10 Network Security

802.11 Wireless Networks

802.12 Demand Priority Access LAN, 100BaseVG-AnyLAN

The bottom two OSI layers, Physical layer and the Data Link layer, define how multiple computers can simultaneously use the network without interfacing with each other.

The figure 22 shows IEEE 802 Project model (LAN reference model).

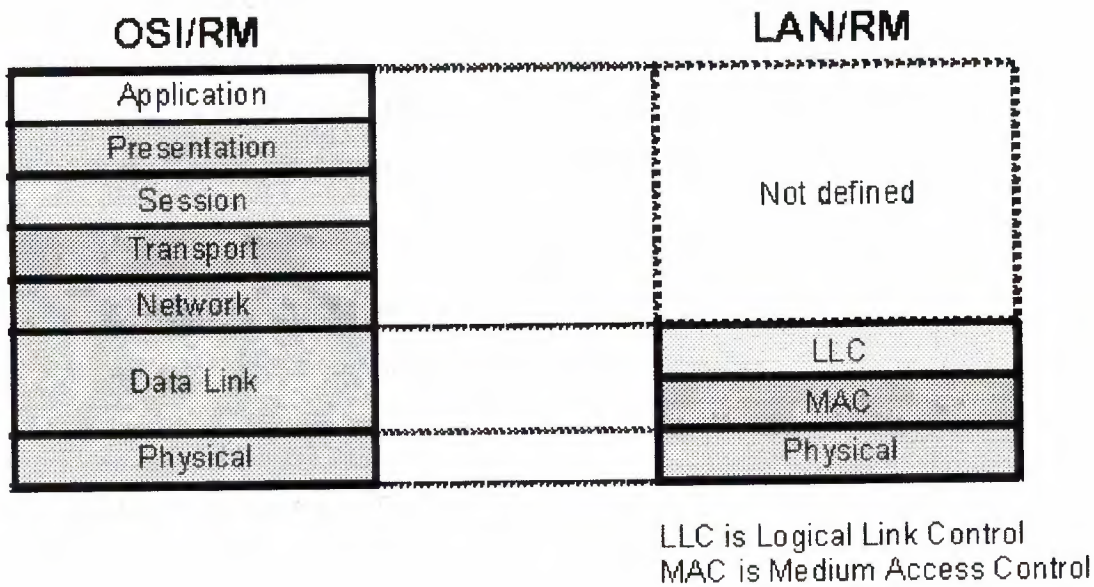


Figure 22 IEEE 802 /LAN Reference Model

The IEEE 802 project worked with the specifications in those two layers to create specifications which have defined the dominant LAN environments. The 802 standards committee decided that more detail was needed at the Data Link layer. They divided the

3. HARDWARE

3.1 Hardware

Cabling

The physical pathways that carry data within a LAN are called media. In most cases the medium is physical wiring, similar to the wiring that carries your telephone or cable TV signal, or glass strands known as fiber optic cable. Though more expensive and not yet as common, computer network signals can also be carried by wireless media.

All network media fit into the physical layer of the OSI model. This section will discuss some of the more common network media in use today:

- Unshielded Twisted Pair
- Shielded Twisted Pair
- Thick Coaxial Cable
- Thin Coaxial Cable
- Fiber Optic Cable
- Wireless Communications

General cabling considerations

Many cable types can be used for LANs. The cable employed depends on several factors including the network type, the network user locations, and the workstation connection budget. Often, networks include several different types of cable. For example, the network backbone may be fiber optic while the wiring from the hub to a wall outlet may be twisted pair. According to wiring standards, networks with multiple cable types are frowned upon; however, as long as distance limitations are respected and compatible hardware is used, there is no technical reason that prevents networks with multiple cable types from working.

Care must be taken to avoid introducing severe bends in a cable during installation. Crimping a cable can cause premature failure or diminish the performance of the cable. Sources of electromagnetic interference, such as ballasts in fluorescent light

fixtures and certain types of light switches must be considered when determining a cable path for copper cables. In theory, cables are protected from such interference by their shielding; however, wiring industry recommendations should be followed when running network cables around these "noisy" devices.

Exercise caution when running wires underneath carpeting. Carpeting has a very abrasive backing that will damage wiring in a very short period of time. Dirt and water ground into the carpeting will also significantly shorten the life of any cables underneath. Special wiring exists for under-the-carpet applications. Before running wiring underneath carpeting, make sure it's rated for that environment. Avoid running wiring under carpeting when at all possible because covered wiring will produce abnormal wear patterns in the carpet and can create a trip hazard as well as a fire hazard.

Use care when running wiring in an unprotected area, such as across a floor. Avoid running wiring near the natural walking pathway in a room or hallway. Tape cables down with a strong tape that will withstand foot traffic. Clearly mark cables that must be run in an open area and bundle them together to keep loose cords from becoming entangled with each other or with passersby. If wiring must be dropped from a ceiling, contain it in a "power pole." Likewise, contain wiring that must run down or across a wall in conduit or a cable trough.

Finally, when installing cables that travel between floors of a building, avoid damaging the firestop. A properly installed cable which spans multiple floors *will* burn in the presence of fire; however, fire will not spread to upper or lower floors by way of the cable run, because a cable run through a firestop is designed to prevent fires from spreading through it. In a building without such protection or where improper cable runs have breached the firestop, inter-story cables can spread fire freely! The same is true of cables in walls and ceilings. If cables must be installed between floors of a building, or in ceilings, walls or other concealed areas where *any* potential for fire exists, consult facilities personnel, local building inspectors or the fire department for guidance before installing any wires.

3.1.1 Unshielded twisted pair

Most people are familiar with Unshielded Twisted Pair (UTP) cabling because it is the standard choice for home and office telephone systems. This cabling is also referred to as 10baseT, Category 3, 4, or 5 Ethernet wire, telephone cable, or silver satin.

UTP consists of two or four pairs of 26, 24 or 22 AWG unshielded copper solid or stranded wires. AWG (American Wire Gauge) is a measurement of the thickness of a wire. A lower gauge indicates a thicker wire. Each pair of wires is twisted together (hence the name twisted pair) to reduce the electrical interference with other pairs in the same cable. Typical UTP wraps all the pairs of wires in a polyvinyl chloride (PVC) or plenum-rated plastic jacket.

Generally when used with networking, UTP ends will be crimped to RJ-45 connectors. These are slightly wider than the connectors found on standard home telephone systems and are used primarily for business telephone applications and networking. RJ-45 connectors plug into RJ-45 ports on the back of network interface cards or networking devices such as hubs, the same way a modular telephone plugs into the wall in a home.

UTP comes in 5 categories or quality levels established by the Electronic Industry Association and the Telecommunications Industry Association consortium (EIA/TIA). Categories 1 and 2 are used primarily for telephone applications and limited networking applications such as Apple's Local Talk. Categories 3, 4 and 5 meet the standards needed for modern networking. For reasons discussed below, it is always advisable to spend a little more and get category 5 UTP wire.

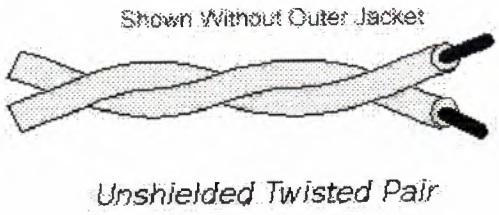
The primary measurement used to judge the quality and thus the category of Unshielded Twisted Pair cabling is the attenuation. Attenuation is the reduction in the power or clarity of signal passed over the cable due to dispersion from or absorption by the cable. This loss is measured in decibels (dB). In most cases, the measurement

of attenuation will be over a specific length of cable at a controlled temperature. In the case of UTP, the attenuation standard is measured over a kilometer at 20° Celsius.

A lower attenuation level is also a good indicator that the cable is not experiencing crosstalk. Crosstalk exists when electrical interference takes place between the wires in a multi-stranded cable or with an outside source of interference.

Table 1 UTP category

UTP Category	Gauge Strands	Attenuation of a 10MHz signal at 20° C.
3	26, 24 or 22 AWG	> 98 dB / km
4	26, 24 or 22 AWG	> 72 dB / km
5	26, 24 or 22 AWG	> 65 dB / km



Fifure 1 unshielded twisted pair

How unshielded twisted pair wires work in a nutshell

Most network protocols over UTP require two pairs of wires. One pair is used to transmit data and the other pair is used to receive data. Within each pair, one wire contains a binary encoded electrical signal and the other wire an inverted copy of the signal. When a network interface card receives a signal, it decodes the signal packets as needed. The inverted signal is used as a checksum to ensure that the data were received properly.

Advantages of UTPUTP wiring is inexpensive and easy to work with. Because of the narrow gauge of the wires and the lack of shielding, UTP is very flexible and can fit in otherwise full conduits.

Since UTP has been a standard for telephone operation, many people are familiar with it and have worked with it. Many telephone installers are cross-trained in the installation of UTP networks.

When rewiring an organization's telephone system or installing wiring in a new facility, it is marginally inexpensive to run extra UTP cables in the same conduits. This will allow network expansion for years to come, since the wiring will already be in place.

Disadvantages of UTP

Because UTP is unshielded, it is prone to interference. This is especially true when it is run in a conduit with high frequency systems such as antenna wire or when the cable is exposed to high temperatures.

Networking protocols over UTP

- 10baseT
- 100baseTX and 100baseT4
- Token Ring
- CDDI

Twisted-Pair Ethernet or 10baseT is one of the most common networking protocols available. A logical bus topology, based on the IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Ethernet standard, 10baseT is implemented on a physical star topology using 10baseT hubs.

10baseT Ethernet transmits data at 10Mbps.

10baseT has become the lowest cost networking solution for multiple workstations available.

10baseT networks have two disadvantages. No single cable length can be over 100 meters in length. Only four hubs can be connected sequentially. Using multiple segments and repeaters, both of these drawbacks can be overcome.

Fast Ethernet over UTP is known as either 100baseTX or 100baseT4. Both of these are 100 Mbps logical bus Ethernet topologies over a Unshielded Twisted Pair physical star topology network.

The primary difference between 100baseTX and 100baseT4 is that 10baseTX uses only two pairs of category 5 UTP cable. 100baseT4 uses four pair of category 3, 4 or 5 UTP cable. The additional two pair are used for redundancy.

Since fast Ethernet uses identical protocols to 10baseT, it is fully compatible with 10baseT networks. A 100baseT hub can communicate (at 10 Mbps speeds) with 10baseT NICs and Hubs.

Though fast Ethernet is rapidly growing in popularity, hubs and NICs for 100baseTX and 100baseT4 cost approximately four to five times more than comparable equipment for a 10baseT network.

Token Ring is an IBM development using either Shielded Twisted Pair (discussed below) or UTP in a physical star environment to implement a logical ring network topology. Token Ring networks can work with either Shielded Twisted Pair (STP - described later) or Category 3, 4, or 5 Unshielded Twisted Pair. When using UTP with Token Ring, the distance the ring can travel and in the number of workstations that can be connected to the ring are limited. Token ring can operate at 4 Mbps or 16 Mbps. With 16 Mbps, a single wiring segment is limited to a maximum distance of 60 meters. Using UTP wiring will also limit a Token Ring to 72 connected workstations on the ring.

The main disadvantage to Token Ring is its dominance by IBM. IBM owns the license to most Token Ring patents and therefore controls the majority of the Token Ring market. As a result, prices for Token Ring network components are relatively high.

CDDI is a UTP implementation of the Fiber Distributed Data Interface (FDDI) standard. This implements a redundant physical and logical ring topology using four pair category 5 UTP. Due to the high cost of CDDI elements and the downward compatibility of Fast Ethernet, CDDI has a very small market share of networking protocols

3.1.2 Shielded twisted pair

Shielded Twisted Pair cabling (STP) is similar to Unshielded Twisted Pair in its operation and design. Shielded Twisted Pair consists of up to eight solid or stranded copper wires. These wires are insulated by a non-conductive material such as polyvinyl chloride (PVC) and then twisted around each other to form pairs. Each pair is then individually wrapped in a metallic shield that prevents interference from other pairs in the cable.

IBM developed the standards for STP wire specifically for token ring applications. Though there are several "types" of STP, as categorized by IBM, most network applications will be either Type-1 or Type-2.

The types of STP wiring are determined by the number of pairs included in the cable and gauge of the wires within the pairs. Type-1 STP is the most common type of STP Type 1 STP cable include two shielded pairs of 22 AWG solid copper wires. It is often used for long runs of cable within walls. The distance limitations and other specifications are the same as for UTP.

Type-2 STP is similar to Type 1 STP, except Type-2 wiring contains two solid shielded pairs of wires and four solid unshielded pairs of wires. The unshielded pairs are 24 gauge and are normally used for voice. Like Type 1, it is normally run in building walls.There are two other types of STP cables, Type 6 and Type 9. These STP cables use 26 gauge wire and were designed for very short runs. They are used only as jumper cables for patch panels and similar applications.

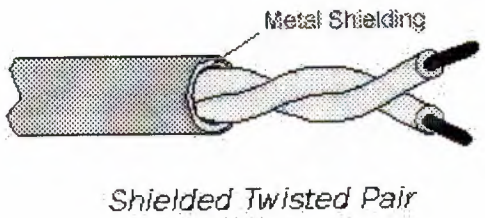


Figure 2 Shielded Twisted Pair

3.1.3 Thick coaxial cable

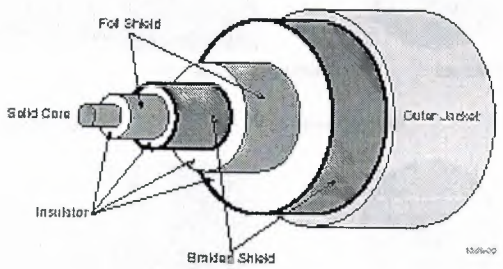
10base5 Ethernet is also known as **thick Ethernet** or **thicknet**. 10base5 runs on a thick coaxial cable. When using 10base5, a logical bus network is implemented over a physical bus.

The coaxial cable used in thick Ethernet is manufactured with a single copper core, which acts as the conductor and transmits the network data. Surrounding this core are several layers of shielding and insulating materials. Because of this insulation the cable is usually very thick (typically at least .0405 inch in diameter), the flexibility of the cable is severely limited.

Thick Ethernet cable has a core gauge of 12AWG and **impedance** of 50W. Impedance is measurement of the cables resistance to transmission of electrical current and is measured in Ohms. The symbol W is used to indicate Ohms.

Thick Ethernet has a limit of 500 meters between repeaters and supports a maximum of 100 network devices per unrepeated segment. Minimum distance between stations on an unrepeated segment is 2.5 meters.

10base5 was originally designed for use with mainframes and mini-computers. Because it is difficult to work with, its use is almost exclusively limited to network backbones.



Thick Coaxial Cable

Figure 3 Thick Coaxial Cable

3.1.4 Thin coaxial cable

The most common form of thin coaxial cable in networking is known as **10base2**. 10base2 networking cable is also known as **thin-net, thin Ethernet,** or **Cheapernet.** When using 10base2, a logical bus network is implemented over a physical bus.

The coaxial cable used in thin Ethernet is manufactured with a single copper core that acts as the conductor and transmits the network data. Surrounding this core is a layer of shielding and insulating material. Because the cable has less shielding, it is much more flexible than thick Ethernet. Thin Ethernet cable has impedance of 50W and a core gauge of 20 AWG.

The ends of 10base2 cables must be terminated with BNC connectors. Thin Ethernet has a limit of 185 meters between repeaters and supports a maximum of 30 network devices per unrepeated segment. Minimum distance between stations on an unrepeated segment is .5 meters.

Because of its flexibility and ease of use, thin Ethernet is very popular in areas where a physical bus topology is warranted. 10base2 is often run through walls, ceilings, or in the open.

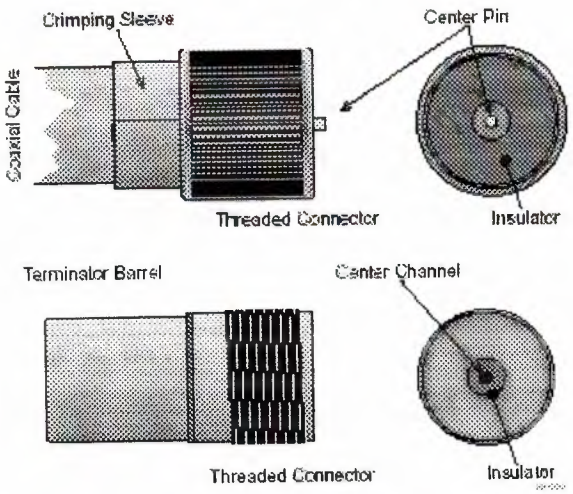


Figure 4 N-Type Connector and Terminator

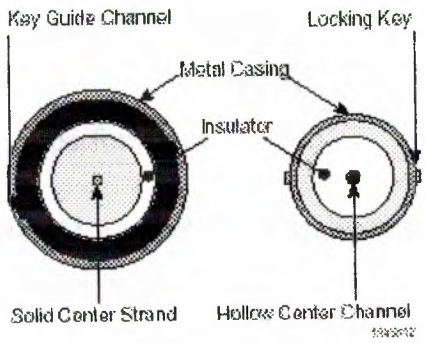


Figure 5 BNC Connectors

3.1.5 Fiber optic cable

Fiber optic cable is a glass or plastic cable that uses light as a transmission method. It is free from electrical interference and has a very low rate of signal degradation. Fiber optic cable is very high performance and may traverse long distances.

Fiber optic cable comes in two basic forms: single-mode and multi-mode. Single mode fiber is smaller than multimode fiber in terms of core diameter, and uses a laser beam as a light source. Light from a laser is of a uniform wavelength. It can be used over long distances because the light signal does not degrade over distance. Single mode fiber is usually used in WAN applications. It is also used for cable TV.

Multimode fiber is often used in LAN applications. It consists of several strands of fiber bundled together to make one carrier. It uses LEDs as a light source. LEDs produce light of different wavelengths, so the information carrying capacity of multimode fiber is diminished. Typically, single mode fiber can carry signals of 60 km without amplification, while multimode fiber is limited to distances less than 2 km.

The space between the fiber and the cladding (or outer shell) is filled with either a weave of threads and plastic or a gel. The former gives the fiber a smaller bending

radius, while a gel-filled cable has a larger bending radius. This characteristic makes the weave-filled cable a better choice for tight locations.

Regardless of how the fiber is insulated, care must be taken not to exceed the bending radius recommendations of the fiber. Severe bends or crimps in the cable will damage the fiber and result in a loss of performance.

Fiber can be used in a variety of LAN architectures. Several fiber cabling standards for Token Ring and Ethernet exist. Special cabling standards have been written for fiber backbones, individual devices linked together with fiber, and network devices connected to passive hubs. These standards allow efficient distribution of the network to these devices, and in many cases allow designers to exceed the distance and device limits imposed by traditional copper-based cabling.

In many networks, fiber is used as a backbone to distribute the network, while the last mile wiring is still some type of copper. In others, the network may be completely wired with fiber. A strictly fiber-based network is significantly more expensive than the traditional network and is normally reserved for special applications.

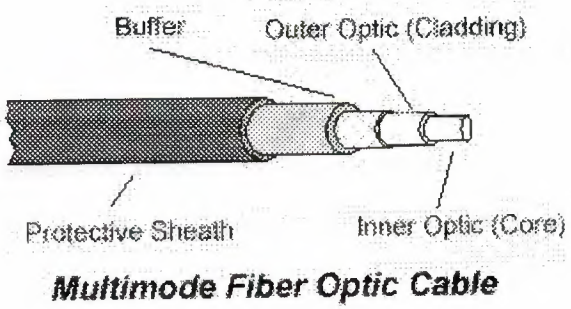


Figure 6 Multimode Fiber optic cable

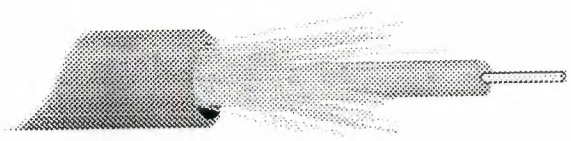


Figure 7 New Fiber Optic Cable

3.1.6 Wireless

Connecting one or several computers via radio waves is a practical alternative when the building you are located in does not allow for convenient cable runs. These might include historic buildings that cannot be altered, buildings with poured cement walls, and with buildings with asbestos that should not be disturbed.

The most common form of wireless networking for a LAN is wireless Ethernet. The Institute for Electrical and Electronic Engineers has adopted a standard for wireless Ethernet. All wireless Ethernet network component manufacturers now subscribe to the IEEE 802.11 standard.

A wireless Ethernet network consists of three main parts. An **access point,** a **station adapter** and **antennas**. An access point is a device that attaches to your conventional 10baseT Ethernet network and broadcasts the network signal via radio waves. A station adapter connects to the 10baseT Network Interface Card on the back of any workstation to allow it to receive networking signals transmitted by the access points. Antennas allow the network signal to be distributed over long distances. Ethernet bridges are also available that allow two physically separate Ethernet LANs to be bridged together via radio waves.

Wireless Ethernet has a range of up to 1000 meters in ideal conditions. Up to 15 access points can be connected within a 1000-meter range of one another. Wireless Ethernet transmits at speeds of 3Mbps. By using a frequency hopping spread spectrum, wireless Ethernet can avoid most radio interference. There are two types of spread spectrum radio systems currently available for wireless Ethernet.

- Direct Sequencing sends data redundantly over a 20MHz bandwidth. Because the receivers know the encoded pattern used to spread the spectrum, a level of security can be maintained.
- Frequency-Hopping wireless Ethernet broadcasts in 400ms bursts over 78 different 1 MHz channels. If data are lost due to interference, the transmitting station can detect this and retransmit.

The major drawback to wireless Ethernet technology has always been the cost. With the adoption of IEEE wireless Ethernet standards, however, the cost of wireless networking has dropped considerably. Users accustomed to 10Mbps speeds of 10baseT Ethernet may find the 3Mbps wireless speeds unacceptably slow.

Network media connectors

The connectors used to attach network media to the networking devices are also considered part of the physical layer of a network. The connectors you use on your network are specific to the cable you've chosen. Your network hardware, regardless of what level it falls into in your model, was designed to work with these connectors. Some common connectors you will find in networks include:

Registered jack (RJ)

Commonly, we refer to the modular jacks we work with as "RJ11" or "RJ45" jacks; however, these are technically misnomers. The jacks themselves are called 6-position, 8-position and 8-position-keyed modular jacks. There is also a 6-position modified modular jack (MMJ) developed originally by Digital Equipment Corp. to prevent its equipment from accidentally being plugged into the standard phone system. The Modified Modular Jack works in conjunction with the Modified Modular Plug (MMP).

The "RJ" part of the description actually describes the wiring configuration inside the jack. For example, the six-position modular jack can be wired as an RJ11C, RJ14C, or an RJ25C cable. These cable designations represent 1-pair wiring standards for single line telephones, modems, answering and fax machines, 2-pair wiring standards for 2-line phones and answering machines and 3-pair wiring standards for 3-line phones and answering machines respectively. Likewise, the 8-position modular jack can support a variety of wiring configurations for data applications. These wiring conventions are explicitly spelled out by the Universal Service Ordering Codes (USOC). The USOCs were originally developed by AT&T in the early 1970s and were later partially adopted by the FCC.

RJ11

The "RJ11" jack is the familiar modular phone connector that we've all seen and used. The RJ11 jack accommodates three pairs of Unshielded Twisted Pair cabling. It is possible to insert this 6-position jack into the wall plug designed for the 8-position jack, however this is not recommended, as doing so will damage the outside contacts (pins 1 and 8) on the wall plug.

RJ45

The RJ45 jack is typically used with 10-Base-T cabling. It accommodates four pairs of UTP and is used for data applications. Ethernet and Token Ring networks can use these connectors, as can ISDN, FDDI, ATM, 100VG-AnyLAN, and Fast Ethernet networks.

NOTE

Although the jacks are the same, the wiring configurations for each of these applications are different and therefore incompatible with each other!

BNC

BNC stands for Bayonet Neill-Concelman connector. It is widely used on television equipment (75W) and 10Base2 networks (50W). The BNC connector is a twist-lock connector used with coaxial cable. The standard BNC connector does not offer adequate strain relief for the cable itself, so the cable is subject to frequent failure at the point where it attaches to the connector. Special 90° BNC connectors are often used to relieve this strain.

Fiber

There are several different types of fiber connectors, including:

ST--This keyed, bayonet-style (twist-lock) connector is widely used.

SC--The SC connector, used internationally, is a snap-lock connector with a duplex connection, one each for transmit and receive.

Other--Other connectors in the fiber arena include SMA connectors, which are rapidly becoming obsolete, and proprietary and specialized connectors that are not as widely used.

Repeaters

Repeaters work at the physical level. They are not intelligent work, which means that they do not perform switching or routing functions. A repeater's main task is to boost the signal it receives from one segment of a network for transmission on a different segment.Generally, a repeater is used to extend a segment of a network. By design,

network segment lengths are limited by the attenuation (signal degradation) characteristics of the network wiring. Over distance, electrical signals lose voltage and change shape due to attenuation.

Because network signals are discrete, devices that interpret them must be able to clearly distinguish the patterns these signals are creating. In other words, network devices must be able to tell whether they're dealing with 1's or 0's. A repeater, therefore, will take a signal that has been attenuated and boost the signal back up to the proper voltage level and reshape the signal so that it looks like it did when it left the device that created it.

Hubs

Hubs work at the data link layer, acting as a breakout box for signals they receive. A hub is a common wiring point for a star topology. Some terminology is associated with hubs. The terms passive and active are associated with ArcNet networks. Passive hubs simply split the signal they receive. These hubs actually degrade the signal as they split it. Active hubs have the capacity to regenerate the signal before sending it out, acting somewhat like a repeater.

Other hubs are described as intelligent and are associated with architectures like Ethernet. An intelligent hub monitors each device connected to it, looking for faults. When a fault is detected, the intelligent hub responds by turning off the misbehaving port so that one device cannot monopolize the network resources. Likewise, intelligent hubs make it easy to add, remove and change components attached to the network.

Another term that is associated with hubs is management. Some hubs are manageable, which means that through software, a user can monitor and control the behavior of a hub, or individual ports on a hub. Depending on its level of sophistication, it may also be able to perform switching and other higher-layer functions. This breed of hub doesn't fit very neatly into the physical layer of the OSI model. Given their basic functions, however, hubs work at the physical layer.

Bridges

Generally speaking, bridges can be used to connect the same or similar segments of a LAN or whole networks. Bridges can be used strategically to isolate traffic on a network. A bridge examines packet headers to determine whether the packet needs to be passed to other segments attached to it. If a packet does not need to be passed along, the bridge will drop the packet, thereby reducing network traffic. Aside from

reducing traffic, there are other reasons to use bridges. A bridge can be used to extend the network without violating segment length limits.

There are different bridge sub-types.

Learning bridge

Also called a "transparent bridge." The learning bridge attempts to learn what addresses are on each segment connected to it in order to efficiently move traffic across the bridge. "Learning" requires that the bridge be outfitted with some capacity to maintain information about physical device addresses it encounters. Complex forwarding algorithms have been developed to assist in this process. A learning bridge can "learn" the topology of a network without human intervention and can maintain information it has learned, weeding out old information and adding new.

Remote bridge

Sometimes called a "half-bridge." The remote bridge is used to connect LAN segments to remote LANs, via some type of common carrier network. For example, a remote bridge In New York City would connect a LAN to a high-speed modem, a CSU/DSU (Channel Service Unit/Digital Service Unit) or some other WAN delivery mode. A second remote bridge would be similarly used to connect this LAN/WAN grouping to another LAN in Chicago. In this way, organizations with presence in more than one geographic location can form a single, relatively inexpensive network across an otherwise impractical distance.

When working with bridges in a network, you must take care that each network segment is connected to exactly one bridge. Segments that are connected to more than one bridge invite distaster in the form of a design error called a bridge loop.

To prevent bridge loops, a special algorithm called the "spanning tree" has been developed to help learning bridges on a network determine who they will and won't share information with. This ensures that information has exactly one pathway through the network.

NICs

A network interface card (NIC) must be installed in every host that wishes to connect to the network. The IP address of a computer is located on the NIC. The NIC interprets network signals for its host. On the newest computers, a network interface is often integrated into the main board.

Switches

A switch is electrically equivalent to a multisegment bridge or a group of bridges (depending on the size of the switch). In some respects, it acts like a concentrator, joining many (sometimes all) segments of a network into one location.

Although effort is made to avoid bridge loops, some switches don't use spanning tree algorithm. Thereforem loops can still be inadvertently designed with a switch/bridge combination. Switches should be carefully added to a network's design. Take extra care to avoid inadvertently designing a bridge loop into a switched network.

Transceivers

A transceiver performs the same function as a network card. Normally, a transceiver is external to the computer, while a NIC is internal. Transceivers isolate the host electrically from the network and detect collisions. Additionally, transceivers can act as adapters for devices that are designed to work with different network cabling.

Routers

In the most basic terms, routers perform routing functions. A router's job is to send packets created by higher layers of the network to their ultimate destination. Much of the work at this level involves discovering where a packet's ultimate destination may be.

Routers are designed to route at least one and sometimes many protocols. For example, a router that routes IP and IPX packets may be available for networks that have TCP/IP and Novell components.

Routers maintain large routing tables that hold information about where packets needed to be forwarded to reach a specific destination. Routers inside a LAN will probably know, or learn over time, where to send traffic destined for other points inside of the network. Most often, they will not learn about many (if any) destinations outside of your network. Instead, they will learn a few key points that will get outbound traffic one step closer to its eventual destination.

Internet routing is basically a forwarding system, where outbound packets are sent to larger, smarter routers that have a better chance of delivering packets than local routers do. In the reverse, inbound packets are forwarded to smaller, progressively more local routers that know specific details of networks connected to the Internet. A specific discussion of the protocols that happen at this layer follows.

Firewalls

Firewalls can take a variety of forms, from physical devices to software. A firewall will operate at either the Network Layer or at the Applications Layer. At the Network

Layer, the firewall is transparent to the user. That is to say that a user will not log into the firewall or give passwords to get through. This type of firewall will *not* be transparent when it refuses a user request!

A router, performing packet filtering examines incoming or outgoing packets and compares the packet requests to a list of rules it's been given that determine which requests are permitted and which requests are denied. Firewall rules can be tailored to allow or deny specific services like telnet, ftp, certain network requests, finger, whois, etc. Firewalls can be tailored to allow or deny most, if not all, Internet-based services. The more permissive your firewall is, the less effective it will be. For specifics on configuring a firewall to allow or deny a service, consult the firewall documentation or get specifics from the author or manufacturer of the permitted or denied service.

Software

In addition to hardware's importance in constructing a network, software plays a crucial role in the network's function.

Network operating systems

This section is not meant to cover network operating systems in depth, nor are the operating systems covered here the only systems available. Many networks consist of a variety of different computers and operating sytems. The task of a network operating system is to give all of these various components the tools they need to communicate directly with other hosts and resources on the network.

AppleShare IP

AppleShare IP 6.0 provides file, email, print, web and ftp services. AppleShare IP 6.0 supports file sharing for Windows 95 and Windows NT clients. It also supports Internet Mail Access Protocol (IMAPv4) for POP and SMTP mail servers.

TCP/IP print server support allows both Macintosh and Windows users to access printers on AppleShare IP 6.0 servers. AppleShare IP 6.0 supports plug-ins to permit customization of AppleShare's file, print and security capabilities.

AppleShare IP 6.0 requires a PowerPC G3, 604e, 604, 601 or 603e-based Power Macintosh computer or server; Mac OS 8.1 or later; Open Transport 1.3 or later; a minimum of 48MB of RAM with virtual memory; 64MB of RAM without virtual memory; 20MB of available hard disk space minimum; and a CD-ROM drive.

Lantastic

LANtastic 8.0 enables PCs on Windows NT® 4.0, Windows® 95/98, Windows 3.1 and DOS (no Macintosh support) to share files, corporate resources and e-mail. There is also an OS/2® upgrade package, which provides additional support for OS/2.
Lantastic 8.0 offers multi-level security for networked documents and resources.
Technical support options include fee-based priority telephone consulting; per-incident support; Web-based Knowledgebase; online message forums, technical notes, tips, product updates and utilities for download.
LANtastic 8.0 includes Netscape Navigator® 4.0 browser, EudoraTM Lite e-mail client and Forte Free Agent news reader.

Novell

NetWare 4.2 replaces intraNetWare and NetWare 4.11.
NetWare 4.2 includes:
NetWare 5 compatibility; IP and IPX protocol integration; most current version of NDS; IP and Z.E.N.works"-ready client software; A three-user demonstration copy of NetWare 5; the Z.E.N.works Starter Pack (allows centralized administration of Windows desktops and applications); five-user version of Oracle8; supports network access for remote employees; Netscape FastTrack Server for NetWare; Netscape Communicator; Multi-protocol Router (v3.2); Perl (v5.1) and NetBasic (v6) scripting tools; integrated with all reliability updates; Year 2000 compatible.

TCP/IP

Unlike a packaged network operating system, the TCP/IP protocol suite is the standard protocol suite that allows Internet access. Sometimes this collection of protocols is called a TCP/IP stack. All Internet-compatible NOS's include a TCP/IP suite.
TCP/IP software is normally included with UNIX installations. Most versions of the UNIX operating system (including the different distributions of Linux) have everything needed to use a UNIX computer as a network server or client.
Typically, UNIX installations include file, mail, and print services, as well as ftp, telnet, World Wide Web, DNS, and routing servers. For most of these services, client software is also included. Additionally, third-party products and revisions are available to add other functions to a UNIX computer, like remote authorization. Some third-party products are distributed free while others are distributed at some cost.
Commercial distributions of UNIX from by a particular company (e.g Sun, Silicon Graphics, HP, etc) offer upgrades for a fee.

Windows NT

Windows NT 4.0 provides traditional network services, web, ftp, DNS, POP mail and gopher servers. NT supports filesharing for DOS, Windows, UNIX and Macintosh, and includes TCP/IP protocols and NetBEUI protocols.

Optionally, Backoffice, a server suite, includes NT Server, firewall, cache, database, Internet mail, small business, legacy integration, intranet, remote authentication, and secure business servers, network resource prioritization and usage statistics tools, and a Web editing package.

Windows NT Server 4.0 requires either an Intel 486/33 or higher CPU, and 125 MB hard drive space, or a RISC processor compatible with NT and 160 MB of space. Additionally, 16 MB of memory, a CD-ROM and VGA video are required.

3.2 LAN Technologies

Each computer in a LAN can effectively send and receive any information addressed to it. This information is in the form of data 'packets'. The standards followed to regularize the transmission of packets, are called LAN standards. Usually LAN standards differ due to their media access technology and the physical transmission medium. Some popular technologies and standards are being covered in this article. The following are the most popular standards.

- Ethernet / IEEE 802.3
- Token Ring / IEEE 802.5
- FDDI (Fiber Distributed Data Interface)
- ARCnet
- LocalTalk (Macintosh Neworks)
- Wireless / IEEE 802.11b

3.2.1 Ethernet / IEEE 802.3

Ethernet is the least expensive high speed LAN alternative. Ethernet adapter cards for a PC range from $60 to $120. They transmit and receive data at speeds of 10 million bits per second through up to 300 feet of telephone wire to a "hub" device normally stacked in a wiring closet. The hub adds less than $50 to the cost of each desktop

connection. Data is transferred between wiring closets using either a heavy coax cable ("Thicknet") or fiber optic cable.

Most textbook treatments of Ethernet would concentrate on Thicknet coax, because that is the wiring arrangement used when Xerox invented the LAN. Today this is still used for medium-long distances where medium levels of reliability are needed. Fiber goes farther and has greater reliability, but a higher cost. To connect a number of workstations within the same room, a light duty coax cable called "Thinnet" is commonly used. These other media reflect an older view of workstation computers in a laboratory environment.

However, the PC and Macintosh have changed the geography of networking. Computers are now located on desktops, dorm rooms, and at home. Telephone wire is the clear choice (where possible) for the last hop from basement to desktop.

Drivers to support the PC Ethernet card come in four versions:

Access to the Internet under DOS can be provided using one of the Packet Driver programs. A collection of free drivers is available from various Internet servers.

Support for Novell clients under DOS can be packaged as a module called IPX.COM.

When Novell must share the Ethernet with other software, it supplies a proprietary interface called ODI. Because of the large market share controlled by Novell, ODI supports most adapter cards and is used by several other software vendors.

All the major companies (Microsoft, IBM, DEC, AT&amp T) and all the other operating systems (Windows for Workgroups, OS/2, NT, Chicago) use NDIS. Developed jointly by Microsoft and 3Com, NDIS also supports most adapter cards and is the native choice for Windows and OS/2 peer networks.

Through NDIS or ODI it is possible to support Novell IPX, IBM SNA, DECNET, Appletalk, TCP/IP (for the Internet), and NETBIOS all simultaneously. Of course, it takes a very large machine and an advanced operating system to squeeze all this software into memory.

This document is intended to explain the basic elements of the Ethernet to a PC user. It assumes that someone else will probably be purchasing the central equipment and installing the wire. To review details of the standards and restrictions on equipment and cable, consider the Ethernet Page at University of Texas.

Definitions and Standards

The early development of Ethernet was done by Xerox research. The name "Ethernet" was a registered trademark of Xerox Corporation. The technology was refined and a second generation called Ethernet II was widely used. Ethernet from this period is often called DIX after its corporate sponsors Digital, Intel, and Xerox. As the holder of the trademark, Xerox established and published the standards.

Obviously, no technology could become an international standard for all sorts of equipment if the rules were controlled by a single US corporation. The IEEE was assigned the task of developing formal international standards for all Local Area Network technology. It formed the "802" committee to look at Ethernet, Token Ring, Fiber Optic, and other LAN technology. The objective of the project was not just to standardize each LAN individually, but also to establish rules that would be global to all types of LANs so that data could easily move from Ethernet to Token Ring or Fiber Optics.

This larger view created conflicts with the existing practice under the old Xerox DIX system. The IEEE was careful to separate the new and old rules. It recognized that

there would be a period when old DIX messages and new IEEE 802 messages would have to coexist on the same LAN. It published a set of standards of which the most important are:

802.3 - Hardware standards for Ethernet cards and cables

802.5 - Hardware standards for Token Ring cards and cables

802.2 - The new message format for data on any LAN

The 802.3 standard further refined the electrical connection to the Ethernet. It was immediately adopted by all the hardware vendors. Today all cards and other devices conform to this standard.

However, the 802.2 standard would require a change to the network architecture of all existing Ethernet users. Apple had to change its Ethertalk, and did so when converting from Phase 1 to Phase 2 Appletalk. DEC had to change its DECNET. Novell added 802 as an option to its IPX, but it supports both DIX and 802 message formats at the same time.

The TCP/IP protocol used by the Internet refused to change. Internet standards are managed by the IETF group, and they decided to stick with the old DIX message format indefinitely. This produced a deadlock between two standards organizations that has not been resolved.

IBM waited until the 802 committee released its standards, then rigorously implemented the 802 rules for everything *except* TCP/IP where the IETF rules take precedence. This means that NETBEUI (the format for NETBIOS on the LAN) and SNA obey the 802 conventions.

So "Ethernet" suffers from too many standards. The old DIX rules for message format persist for some uses (Internet, DECNET, some Novell). The new 802 rules apply to other traffic (SNA, NETBEUI). The most pressing problem is to make sure that Novell clients and servers are configured to use the same frame format.

Access and Collisions

Ethernet uses a protocol called CSMACD. This stands for "Carrier Sense, Multiple Access, Collision Detect". The "Multiple Access" part means that every station is connected to a single copper wire (or a set of wires that are connected together to form a single data path). The "Carrier Sense" part says that before transmitting data, a station checks the wire to see if any other station is already sending something. If the LAN appears to be idle, then the station can begin to send data.

An Ethernet station sends data at a rate of 10 megabits per second. That bit allows 100 nanoseconds per bit. Light and electricity travel about one foot in a nanosecond.

Therefore, after the electric signal for the first bit has traveled about 100 feet down the wire, the station has begun to send the second bit. However, an Ethernet cable can run for hundreds of feet. If two stations are located, say, 250 feet apart on the same cable, and both begin transmitting at the same time, then they will be in the middle of the third bit before the signal from each reaches the other station.

This explains the need for the "Collision Detect" part. Two stations can begin to send data at the same time, and their signals will "collide" nanoseconds later. When such a collision occurs, the two stations stop transmitting, "back off", and try again later after a randomly chosen delay period.

While an Ethernet can be built using one common signal wire, such an arrangement is not flexible enough to wire most buildings. Unlike an ordinary telephone circuit, Ethernet wire cannot be just spliced together, connecting one copper wire to another. Ethernet requires a repeater. A repeater is a simple station that is connected to two wires. Any data that it receives on one wire it repeats bit-for-bit on the other wire. When collisions occur, it repeats the collision as well.

In common practice, repeaters are used to convert the Ethernet signal from one type of wire to another. In particular, when the connection to the desktop uses ordinary telephone wire, the hub back in the telephone closet contains a repeater for every phone circuit. Any data coming down any phone line is copied onto the main Ethernet

coax cable, and any data from the main cable is duplicated and transmitted down every phone line. The repeaters in the hub electrically isolate each phone circuit, which is necessary if a 10 megabit signal is going to be carried 300 feet on ordinary wire.

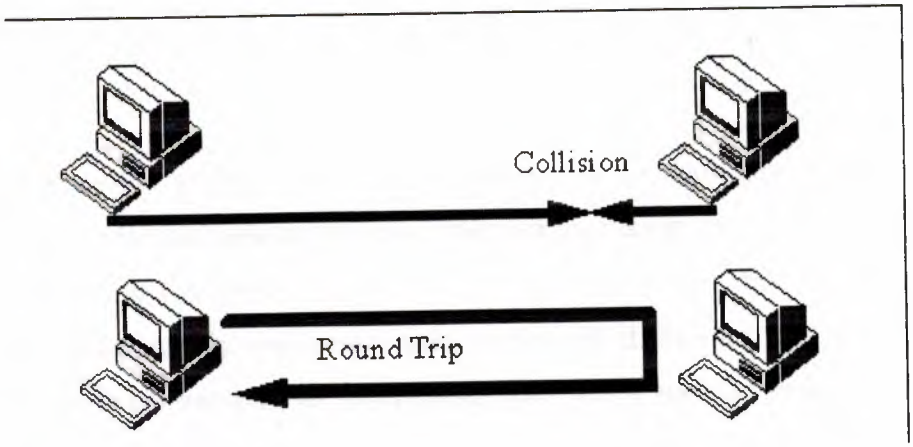


Figure 9 Collision

Every set of rules is best understood by characterizing its worst case. The worst case for Ethernet starts when a PC at the extreme end of one wire begins sending data. The electric signal passes down the wire through repeaters, and just before it gets to the last station at the other end of the LAN, that station (hearing nothing and thinking that the LAN is idle) begins to transmit its own data. A collision occurs. The second station recognizes this immediately, but the first station will not detect it until the collision signal retraces the first path all the way back through the LAN to its starting point.

Any system based on collision detect must control the time required for the worst round trip through the LAN. As the term "Ethernet" is commonly defined, this round trip is limited to 50 microseconds (millionths of a second). At a signaling speed of 10 million bits per second, this is enough time to transmit 500 bits. At 8 bits per byte, this is slightly less than 64 bytes.

To make sure that the collision is recognized, Ethernet requires that a station must continue transmitting until the 50 microsecond period has ended. If the station has less than 64 bytes of data to send, then it must pad the data by adding zeros at the end.

In simpler days, when Ethernet was dominated by heavy duty coax cable, it was possible to translate the 50 millisecond limit and other electrical restrictions into rules about cable length, number of stations, and number of repeaters. However, by adding new media (such as Fiber Optic cable) and smarter electronics, it becomes difficult to

state physical distance limits with precision. However those limits work out, they are ultimately reflections of the constraint on the worst case round trip.

It would be possible to define some other Ethernet-like collision system with a 40 microsecond or 60 microsecond period. Changing the period, the speed, and the minimum message size simply require a new standard and some alternate equipment. AT&amp T, for example, once promoted a system called "Starlan" that transmitted data a 1 megabit per second over older phone wire. Many such systems are possible, but the term "Ethernet" is generally reserved for a system that transmits 10 megabits per second with a round trip delay of 50 microseconds.

To extend the LAN farther than the 50 microsecond limit will permit, one needs a bridge or router. These terms are often confused:

A repeater receives and then immediately retransmits each bit. It has no memory and does not depend on any particular protocol. It duplicates everything, including the collisions.

A bridge receives the entire message into memory. If the message was damaged by a collision or noise, then it is discarded. If the bridge knows that the message was being sent between two stations on the same cable, then it discards it. Otherwise, the message is queued up and will be retransmitted on another Ethernet cable. The bridge has no address. Its actions are transparent to the client and server workstations.

A router acts as an agent to receive and forward messages. The router has an address and is known to the client or server machines. Typically, machines directly send messages to each other when they are on the same cable, and they send the router messages addressed to another zone, department, or subnetwork. Routing is a function specific to each protocol. For IPX, the Novell server can act as a router. For SNA, an

APPN Network Node does the routing. TCP/IP can be routed by dedicated devices, UNIX workstations, or OS/2 servers.

Problem Determination

In the classical "Thick Net" fat yellow Ethernet cable, a heavy copper wire is embedded in plastic and surrounded by a grounded metal shield. At each end of the cable, the central signal wire is connected to a resistor that in turn connects to the grounded shield. As was previously noted, each bit follows the previous bit at a distance of about 100 feet. The bits are represented by a wave of electrical voltage. The resistor at each end of the wire removes the signal cleanly from the wire. Without such a termination, some part of the voltage wave would hit the end of the wire and bounce back, causing confusion and perhaps appearing as a collision.

Ethernets fail in three common ways. A nail can be driven into the cable breaking the signal wire. A nail can be driven in touching the signal wire and shorting it to the external grounded metal shield. Finally, a station on the LAN can break down and start to generate a continuous stream of junk blocking everyone else from sending.

There is a specialized device that finds problems in an Ethernet LAN. It plugs into any attachment point in the cable, and sends out its own voltage pulse. The effect is similar to a sonar "ping." If the cable is broken, then there is no proper terminating resistor. The pulse will hit the loose end of the broken cable and will bounce back. The test device senses the echo, computes how long the round trip took, and then reports how far away the break is in the cable.

If the Ethernet cable is shorted out, a simple volt meter would determine that the proper resistor is missing from the signal and shield wires. Again, by sending out a pulse and timing the return, the test device can determine the distance to the problem.

Most of the thinking about Ethernet repair have been based on the original Thicknet media. However, modern Ethernet installation may not use any of this old coax cable. The connection to the desktop may be based on telephone wire between the PC and a

"hub" device. The hubs may stack up in a wiring closet and then be connected to other rooms using fiber optic cable.

Newer generations of "smart" hubs can perform part of the error detection and reporting function. For example, they could isolate a problem in the connection to a

particular desktop workstation and automatically isolate that unit from the rest of the network.

Ethernet presents a classic trade-off. The simplest equipment has a very low cost, but requires some technical expertise to locate and repair errors. More sophisticated equipment may be able to do automatic error detection and recovery, but at a higher price.

Frame Formats

A block of data transmitted on the Ethernet is called a "frame." The first 12 bytes of every frame contain the 6 byte destination address (the recipient) and a 6 byte source address (the sender). Each Ethernet adapter card comes with a unique factory installed address (the "universally administered address"). Use of this hardware address guarantees a unique identity to each card.

The PC software (in PROTOCOL.INI or NET.CFG) can be configured to substitute a different address number. When this option is used, it is called a "locally administered address." If the use of this feature is properly controlled, the address can contain information about the building, department, room, machine, wiring circuit, or owner's telephone number. When accurate, such information can speed problem determination.

The source address field of each frame must contain the unique address (universal or local) assigned to the sending card. The destination field can contain a "multicast" address representing a group of workstations with some common characteristic. A Novell client may broadcast a request to identify all Netware servers on the LAN, while a Microsoft or IBM client machine broadcasts a query to all machines supporting NETBIOS to find a particular server or domain.

In normal operation, an Ethernet adapter will receive only frames with a destination address that matches its unique address, or destination addresses that represent a multicast message. However, most Ethernet adapters can be set into "promiscuous" mode where they receive all frames that appear on the LAN. If this poses a security problem, a new generation of smart hub devices can filter out all frames with private destination addresses belonging to another station.

There are three common conventions for the format of the remainder of the frame:

...Ethernet II or DIX

...IEEE 802.3 and 802.2 ...SNAP

Ethernet II or DIX

Before the development of international standards, Xerox administered the Ethernet conventions. As each vendor developed a protocol, a two byte Type code was assigned by Xerox to identify it. Codes were given out to XNS (the Xerox own protocol), DECNET, IP, and Novell IPX. Since short Ethernet frames must be padded with zeros to a length of 64 bytes, each of these higher level protocols required either a larger minimum message size or an internal length field that can be used to distinguish data from padding.

Type field values of particular note include:

0x0600 XNS (Xerox)
0x0800 IP (the Internet protocol)
0x6003 DECNET

IEEE 802.3 and 802.2

The IEEE 802 committee was charged to develop protocols that could operate the same way across all LAN media. To allow collision detect, the 10 megabit Ethernet requires a minimum packet size of 64 bytes. Any shorter message must be padded with zeros. The requirement to pad messages is unique to Ethernet and does not apply to any other LAN media. In order for Ethernet to be interchangeable with other types of LANs, it would have to provide a length field to distinguish significant data from padding.

The DIX standard did not need a length field because the vendor protocols that used it (XNS, DECNET, IPX, IP) all had their own length fields. However, the 802 committee needed a standard that did not depend on the good behavior of other

programs. The 802.3 standard therefore replaced the two byte type field with a two byte length field.

Xerox had not assigned any important types to have a decimal value below 1500. Since the maximum size of a packet on Ethernet is 1500 bytes, there was no conflict or overlap between DIX and 802 standards. Any Ethernet packet with a type/length field less than 1500 is in 802.3 format (with a length) while any packet in which the field value is greater than 1500 must be in DIX format (with a type).

The 802 committee then created a new field to substitute for Type. The 802.2 header follows the 802.3 header (and also follows the comparable fields in a Token Ring, FDDI, or other types of LAN).

The 802.2 header is three bytes long for control packets or the kind of connectionless data sent by all the old DIX protocols. A four byte header is defined for connection oriented data, which refers primarily to SNA and NETBEUI. The first two bytes identify the SAP. Even with hindsight it is not clear exactly what the IEEE expected this field to be used for. In current use, the two SAP fields are set to 0x0404 for SNA and 0xF0F0 for NETBEUI.

SNAP .

The IEEE left all the other protocols in a confusing situation. They did not need any new services and did not benefit from the change. Furthermore, a one byte SAP could not substitute for the two byte type field. Yet 802.2 was an International Standard, and that has the force of law in many areas. The compromise was to create a special version of the 802.2 header that conformed to the standard but actually repackaged the old DIX conventions.

Under SNAP, the 802.2 header appears to be a datagram message (control field 0x03) between SAP ID 0xAA. The first five bytes of what 802.2 considers data are actually a subheader ending in the two byte DIX type value. Any of the old DIX protocols can convert their existing logic to legal 802 SNAP by simply moving the DIX type field back eight bytes from its original location.

3.2.2 Token Ring / IEEE 802.5

The Token Ring network was originally developed by IBM in the 1970s. It is still IBM's primary local-area network (LAN) technology. The related IEEE 802.5 specification is almost identical to and completely compatible with IBM's Token Ring network. In fact, the IEEE 802.5 specification was modeled after IBM Token Ring, and it continues to shadow IBM's Token Ring development. The term *Token Ring* generally is used to refer to both IBM's Token Ring network and IEEE 802.5 networks. This chapter addresses both Token Ring and IEEE 802.5.

Token Ring and IEEE 802.5 networks are basically compatible, although the specifications differ in minor ways. IBM's Token Ring network specifies a star, with all end stations attached to a device called a multistation access unit (MSAU). In contrast, IEEE 802.5 does not specify a topology, although virtually all IEEE 802.5 implementations are based on a star. Other differences exist, including media type (IEEE 802.5 does not specify a media type, although IBM Token Ring networks use twisted-pair wire) and routing information field size.The Figure summarizes IBM Token Ring network and IEEE 802.5 specifications.

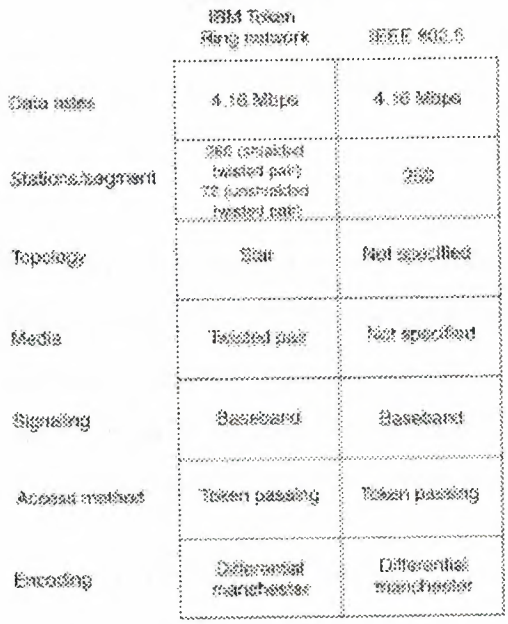


Figure 10 IBM Token Ring Network and IEEE 802.5 are Generally Compatible

Physical Connections

IBM Token Ring network stations are directly connected to MSAUs, which can be wired together to form one large ring (see the Figure below). Patch cables connect MSAUs to adjacent MSAUs, while lobe cables connect MSAUs to stations. MSAUs include bypass relays for removing stations from the ring.

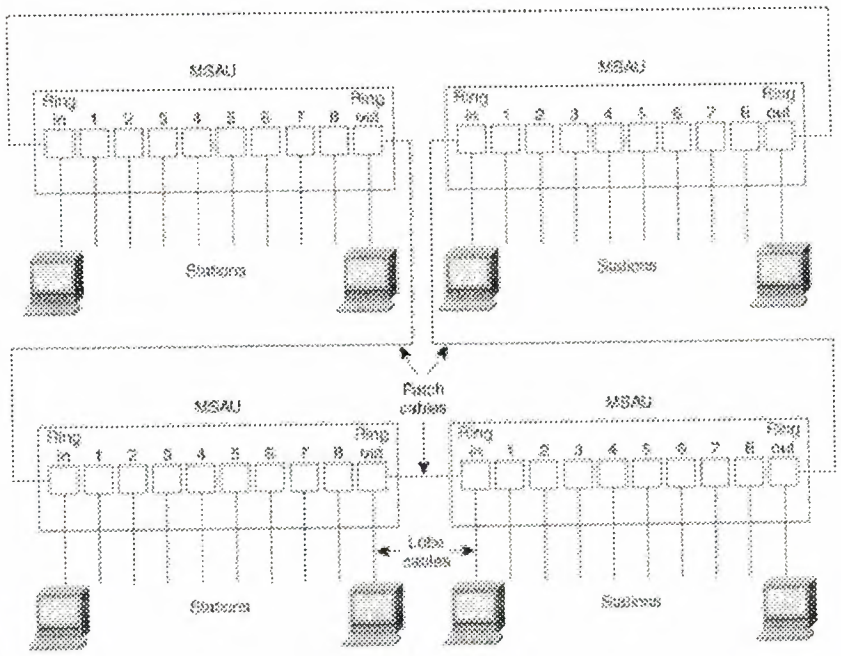


Figure 11 MSAUs Can Be Wired Together to Form One Large Ring in an IBM Token Ring Network

Token Ring Operation

Token Ring and IEEE 802.5 are two principal examples of token-passing networks (FDDI is the other). *Token-passing networks* move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time.

If a station possessing the token does have information to transmit, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. While the information frame is circling the ring, no token is on the network (unless the ring supports early token release), which means that other stations wanting to transmit must wait. Therefore, collisions cannot occur in Token

Ring networks. If early token release is supported, a new token can be released when frame transmission is complete.

The information frame circulates the ring until it reaches the intended destination station, which copies the information for further processing. The information frame continues to circle the ring and is finally removed when it reaches the sending station. The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination.

Unlike CSMA/CD networks (such as Ethernet), token-passing networks are deterministic, which means that it is possible to calculate the maximum time that will pass before any end station will be capable of transmitting. This feature and several reliability features, which are discussed in the section "Fault-Management Mechanisms," later in this chapter, make Token Ring networks ideal for applications in which delay must be predictable and robust network operation is important. Factory automation environments are examples of such applications.

Priority System

Token Ring networks use a sophisticated priority system that permits certain user-designated, high-priority stations to use the network more frequently. Token Ring frames have two fields that control priority: the priority field and the reservation field.

Only stations with a priority equal to or higher than the priority value contained in a token can seize that token. After the token is seized and changed to an information frame, only stations with a priority value higher than that of the transmitting station can reserve the token for the next pass around the network. When the next token is generated, it includes the higher priority of the reserving station. Stations that raise a token's priority level must reinstate the previous priority after their transmission is complete.

Fault-Management Mechanisms

Token Ring networks employ several mechanisms for detecting and compensating for network faults. For example, one station in the Token Ring network is selected to be the *active monitor*. This station, which potentially can be any station on the network,

acts as a centralized source of timing information for other ring stations and performs a variety of ring-maintenance functions. One of these functions is the removal of continuously circulating frames from the ring. When a sending device fails, its frame may continue to circle the ring. This can prevent other stations from transmitting their own frames and essentially can lock up the network. The active monitor can detect such frames, remove them from the ring, and generate a new token.

The IBM Token Ring network's star topology also contributes to overall network reliability. Because all information in a Token Ring network is seen by active MSAUs, these devices can be programmed to check for problems and selectively remove stations from the ring, if necessary.

A Token Ring algorithm called *beaconing* detects and tries to repair certain network faults. Whenever a station detects a serious problem with the network (such as a cable break), it sends a beacon frame, which defines a failure domain. This domain includes the station reporting the failure, its nearest active upstream neighbor (NAUN), and everything in between. Beaconing initiates a process called *autoreconfiguration*, in which nodes within the failure domain automatically perform diagnostics in an attempt to reconfigure the network around the failed areas. Physically, the MSAU can accomplish this through electrical reconfiguration.

Frame Format

Token Ring and IEEE 802.5 support two basic frame types: tokens and data/command frames. Tokens are 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter. Data/command frames vary in size, depending on the sizeof the Information field. Data frames carry information for upper-layer protocols,while command frames contain control information and have no data forupperlayerprotocols. Both formats are shown in Figure below.

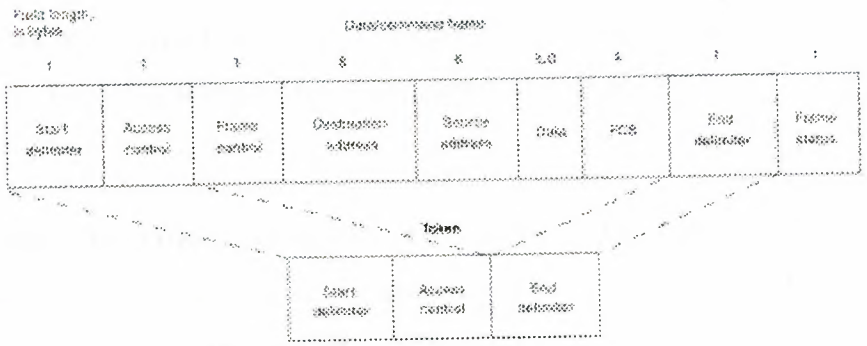


Figure 12 IEEE 802.5 and Token Ring Specify Tokens and Data/Command Frames

Token Frame Fields

The three token frame fields illustrated in Figure above are summarized in the descriptions that follow:

Start delimiter—Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.

Access-control byte—Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).

End delimiter—Signals the end of the token or data/command frame. This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Data/Command Frame Fields

Data/command frames have the same three fields as Token Frames, plus several others.

The Data/command frame fields illustrated in Figure 9-3 are described in the following summaries:

Start delimiter—Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.

Access-control byte—Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).

Frame-control bytes—Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.

Destination and source addresses—Consists of two 6-byte address fields that identify the destination and source station addresses.

Data—Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.

Frame-check sequence (FCS)—Is filed by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.

End Delimiter—Signals the end of the token or data/command frame. The end delimiter also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Frame Status—Is a 1-byte field terminating a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator

3.2.3 FDDI (Fiber Distributed Data Interface)

The *Fiber Distributed Data Interface (FDDI)* specifies a 100-Mbps token-passing, dual-ring LAN using fiber-optic cable. FDDI is frequently used as high-speed backbone technology because of its support for high bandwidth and greater distances than copper. It should be noted that relatively recently, a related copper specification, called Copper Distributed Data Interface (CDDI), has emerged to provide 100-Mbps

service over copper. CDDI is the implementation of FDDI protocols over twisted-pair copper wire. This chapter focuses mainly on FDDI specifications and operations, but it also provides a high-level overview of CDDI.

FDDI uses dual-ring architecture with traffic on each ring flowing in opposite directions (called counter-rotating). The dual rings consist of a primary and a secondary ring. During normal operation, the primary ring is used for data transmission, and the secondary ring remains idle. As will be discussed in detail later in this chapter, the primary purpose of the dual rings is to provide superior reliability and robustness. The Figure below shows the counter-rotating primary and secondary FDDI rings.

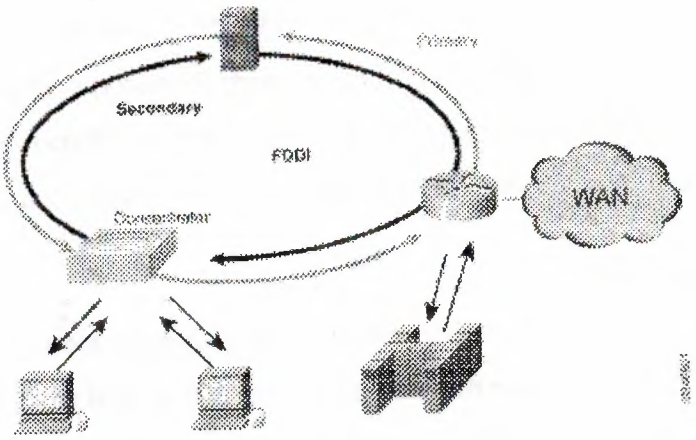


Figure 13 FDDI Uses Counter-Rotating Primary and Secondary Rings

Standards

FDDI was developed by the American National Standards Institute (ANSI) X3T9.5 standards committee in the mid-1980s. At the time, high-speed engineering workstations were beginning to tax the bandwidth of existing local-area networks (LANs) based on Ethernet and Token Ring. A new LAN media was needed that could easily support these workstations and their new distributed applications. At the same time, network reliability had become an increasingly important issue as system managers migrated mission-critical applications from large computers to networks.

FDDI was developed to fill these needs. After completing the FDDI specification, ANSI submitted FDDI to the International Organization for Standardization (ISO), which created an international version of FDDI that is completely compatible with the ANSI standard version.

FDDI Transmission Media

FDDI uses optical fiber as the primary transmission medium, but it also can run over copper cabling. As mentioned earlier, FDDI over copper is referred to as *Copper-Distributed Data Interface (CDDI)*. Optical fiber has several advantages over copper media. In particular, security, reliability, and performance all are enhanced with optical fiber media because fiber does not emit electrical signals. A physical medium that does emit electrical signals (copper) can be tapped and therefore would permit unauthorized access to the data that is transiting the medium. In addition, fiber is immune to electrical interference from radio frequency interference (RFI) and electromagnetic interference (EMI). Fiber historically has supported much higher bandwidth (throughput potential) than copper, although recent technological advances have made copper capable of transmitting at 100 Mbps. Finally, FDDI allows 2 km between stations using multimode fiber, and even longer distances using a single mode.

FDDI defines two types of optical fiber: single-mode and multimode. A *mode* is a ray of light that enters the fiber at a particular angle. *Multimode* fiber uses LED as the light-generating device, while *single-mode* fiber generally uses lasers.

Multimode fiber allows multiple modes of light to propagate through the fiber. Because these modes of light enter the fiber at different angles, they will arrive at the end of the fiber at different times. This characteristic is known as *modal dispersion*. Modal dispersion limits the bandwidth and distances that can be accomplished using

multimode fibers. For this reason, multimode fiber is generally used for connectivity within a building or a relatively geographically contained environment.

Single-mode fiber allows only one mode of light to propagate through the fiber. Because only a single mode of light is used, modal dispersion is not present with

single-mode fiber. Therefore, single-mode fiber is capable of delivering considerably higher performance connectivity over much larger distances, which is why it generally is used for connectivity between buildings and within environments that are more geographically dispersed.

The Figure depicts single-mode fiber using a laser light source and multimode fiber using a light emitting diode (LED) light source.

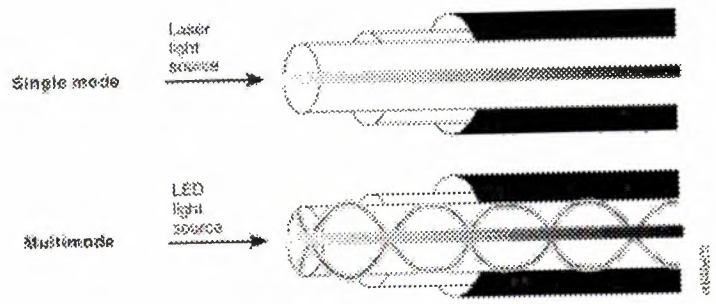


Figure 14 Light Sources Differ for Single-Mode and Multimode Fibers

FDDI Specifications

FDDI specifies the physical and media-access portions of the OSI reference model. FDDI is not actually a single specification, but it is a collection of four separate specifications, each with a specific function. Combined, these specifications have the capability to provide high-speed connectivity between upper-layer protocols such as TCP/IP and IPX, and media such as fiber-optic cabling.

FDDI's four specifications are the Media Access Control (MAC), Physical Layer Protocol (PHY), Physical-Medium Dependent (PMD), and Station Management (SMT) specifications. The MAC specification defines how the medium is accessed, including frame format, token handling, addressing, algorithms for calculating cyclic redundancy check (CRC) value, and error-recovery mechanisms. The PHY specification defines data encoding/decoding procedures, clocking requirements, and framing, among other functions. The PMD specification defines the characteristics of

the transmission medium, including fiber-optic links, power levels, bit-error rates, optical components, and connectors. The SMT specification defines FDDI station

configuration, ring configuration, and ring control features, including station insertion and removal, initialization, fault isolation and recovery, scheduling, and statistics collection.

FDDI is similar to IEEE 802.3 Ethernet and IEEE 802.5 Token Ring in its relationship with the OSI model. Its primary purpose is to provide connectivity between upper OSI layers of common protocols and the media used to connect network devices. The figure below illustrates the four FDDI specifications and their relationship to each other and to the IEEE-defined Logical Link Control (LLC) sublayer. The LLC sublayer is a component of Layer 2, the MAC layer, of the OSI reference model.

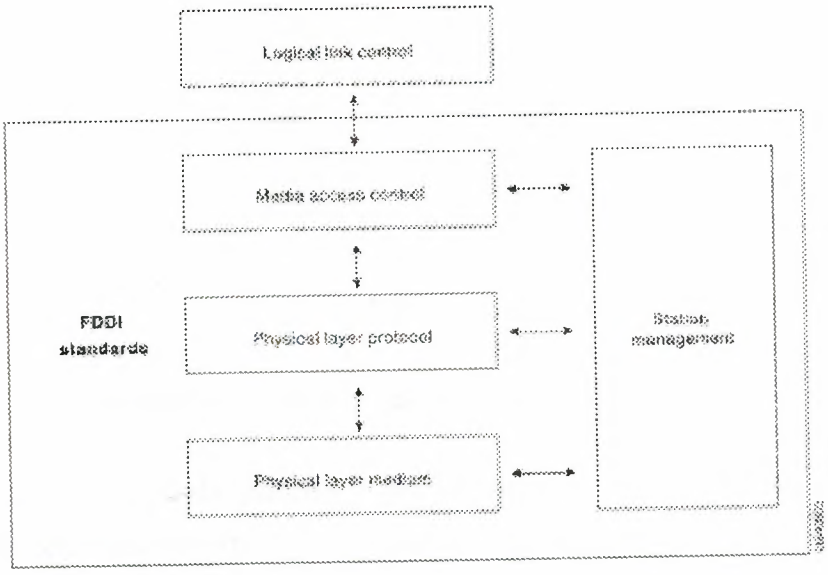


Figure 15 FDDI Specifications Map to the OSI Hierarchical Model

FDDI Station-Attachment Types

One of the unique characteristics of FDDI is that multiple ways actually exist by which to connect FDDI devices. FDDI defines four types of devices: single-attachment station (SAS), dual-attachment station (DAS), single-attached concentrator (SAC), and dual-attached concentrator (DAC).

An SAS attaches to only one ring (the primary) through a concentrator. One of the primary advantages of connecting devices with SAS attachments is that the devices

will not have any effect on the FDDI ring if they are disconnected or powered off. Concentrators will be covered in more detail in the following discussion.

Each FDDI DAS has two ports, designated A and B. These ports connect the DAS to the dual FDDI ring. Therefore, each port provides a connection for both the primary and the secondary rings. As you will see in the next section, devices using DAS connections will affect the rings if they are disconnected or powered off. The figure below shows FDDI DAS A and B ports with attachments to the primary and secondary rings.

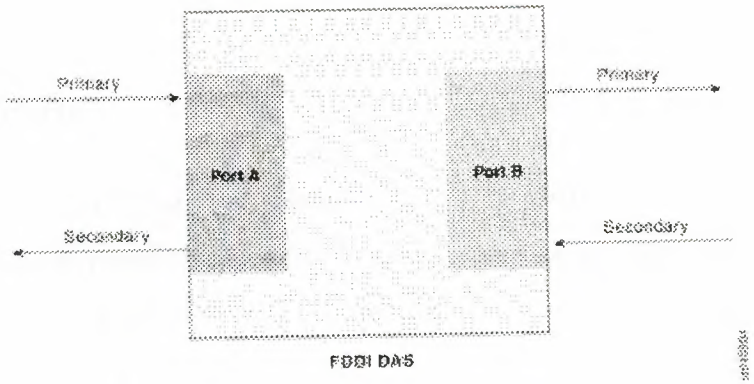


Figure 16 FDDI DAS Ports Attach to the Primary and Secondary Rings

An *FDDI concentrator* (also called a *dual-attachment concentrator [DAC]*) is the building block of an FDDI network. It attaches directly to both the primary and secondary rings and ensures that the failure or power-down of any SAS does not bring down the ring. This is particularly useful when PCs, or similar devices that are frequently powered on and off, connect to the ring. The figure below shows the ring attachments of an FDDI SAS, DAS, and concentrator.

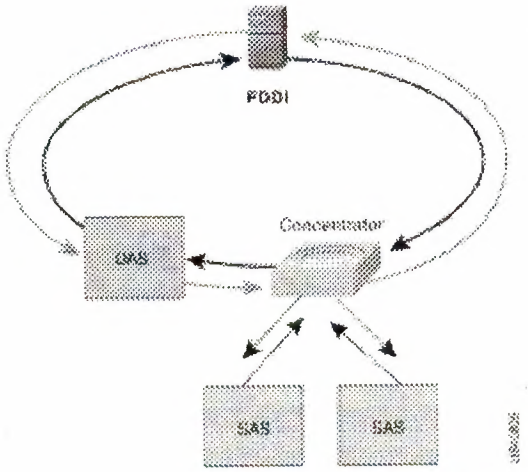


Figure 17 A Concentrator Attaches to Both the Primary and Secondary Rings

FDDI Fault Tolerance

FDDI provides a number of fault-tolerant features. In particular, FDDI's dual-ring environment, the implementation of the optical bypass switch, and dual-homing support make FDDI a resilient media technology.

Dual Ring

FDDI's primary fault-tolerant feature is the dual ring. If a station on the dual ring fails or is powered down, or if the cable is damaged, the dual ring is automatically wrapped (doubled back onto itself) into a single ring. When the ring is wrapped, the dual-ring topology becomes a single-ring topology. Data continues to be transmitted on the FDDI ring without performance impact during the wrap condition. Figure A and Figure B below illustrate the effect of a ring wrapping in FDDI.

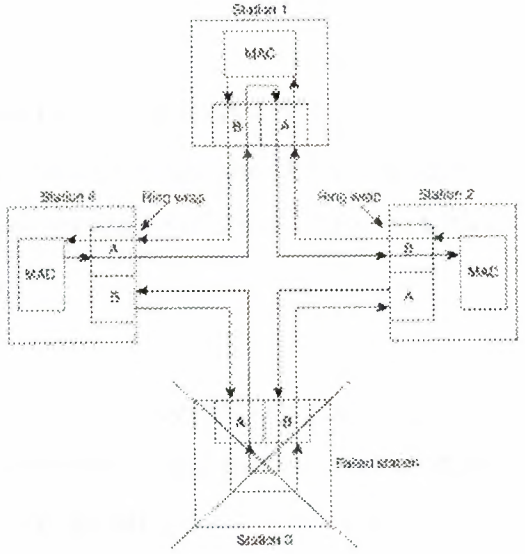


Figure 18 A: A Ring Recovers From A Station Failure by Wrapping

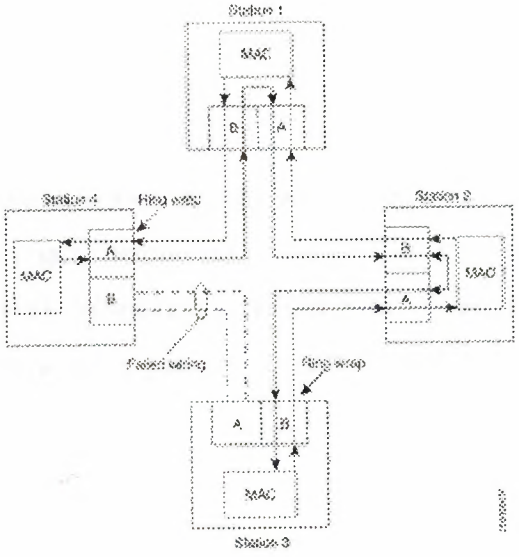


Figure18 B : Fault Wrap

When a single station fails, as shown in Figure A, devices on either side of the failed (or powered-down) station wrap, forming a single ring. Network operation continues for the remaining stations on the ring. When a cable failure occurs, as shown in

Figure B, devices on either side of the cable fault wrap. Network operation continues for all stations.

It should be noted that FDDI truly provides fault tolerance against a single failure only. When two or more failures occur, the FDDI ring segments into two or more independent rings that are incapable of communicating with each other.

Optical Bypass Switch

An *optical bypass switch* provides continuous dual-ring operation if a device on the dual ring fails. This is used both to prevent ring segmentation and to eliminate failed stations from the ring. The optical bypass switch performs this function using optical mirrors that pass light from the ring directly to the DAS device during normal operation. If a failure of the DAS device occurs, such as a power-off, the optical bypass switch will pass the light through itself by using internal mirrors and thereby will maintain the ring's integrity.

The benefit of this capability is that the ring will not enter a wrapped condition in case of a device failure.The Figure below shows the functionality of an optical bypass switch in an FDDI network. When using the OB, you will notice a tremendous digression of your network as the packets are sent through the OB unit.

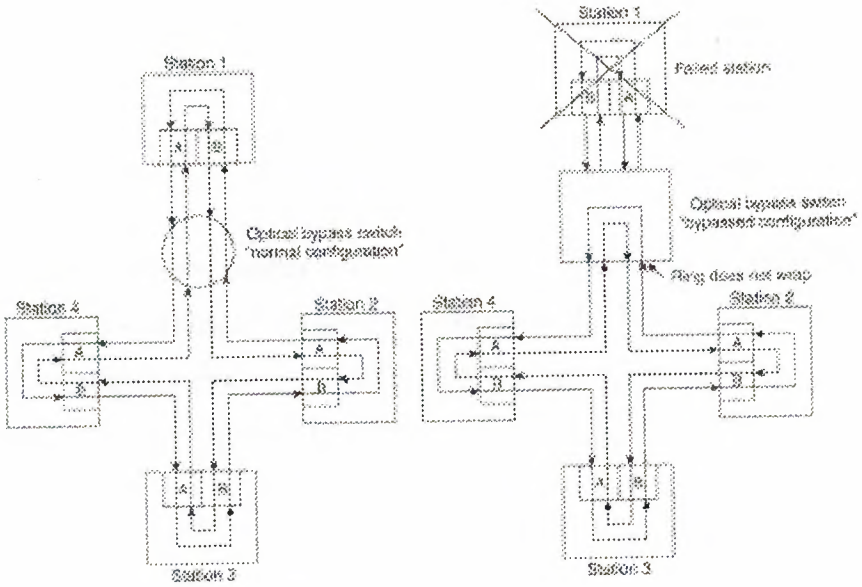


Figure 19: The Optical Bypass Switch Uses Internal Mirrors to Maintain a Network

Dual Homing

Critical devices, such as routers or mainframe hosts, can use a fault-tolerant technique called *dual homing* to provide additional redundancy and to help guarantee operation. In dual-homing situations, the critical device is attached to two concentrators. The Figure below shows a dual-homed configuration for devices such as file servers and routers.

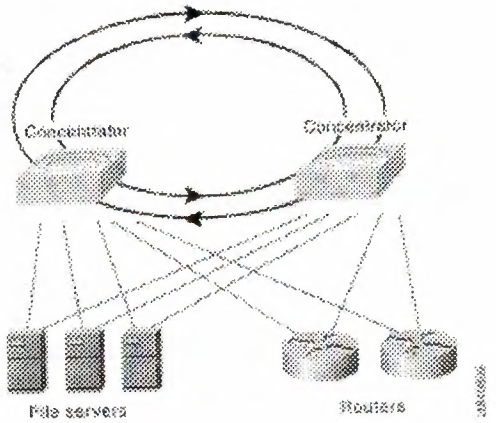


Figure 20 : A Dual-Homed Configuration Guarantees Operation

One pair of concentrator links is declared the active link; the other pair is declared passive. The passive link stays in backup mode until the primary link (or the

concentrator to which it is attached) is determined to have failed. When this occurs, the passive link automatically activates.

FDDI Frame Format

The FDDI frame format is similar to the format of a Token Ring frame. This is one of the areas in which FDDI borrows heavily from earlier LAN technologies, such as Token Ring. FDDI frames can be as large as 4,500 bytes. The figure shows the frame format of an FDDI data frame and token.

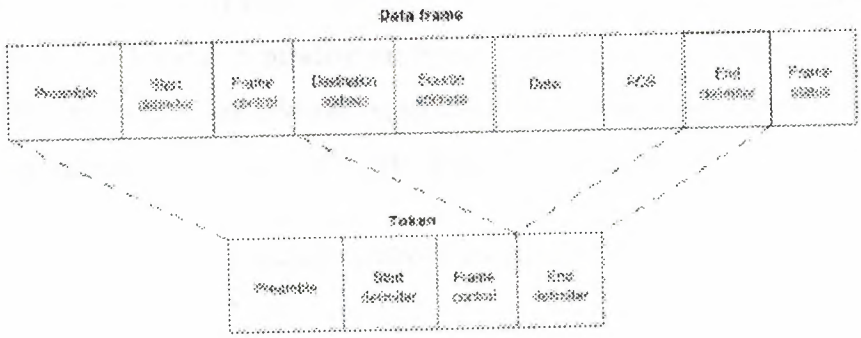


Figure 21 : The FDDI Frame Is Similar to That of a Token Ring Frame

FDDI Frame Fields

The following descriptions summarize the FDDI data frame and token fields illustrated in the figure above.

Preamble—Gives a unique sequence that prepares each station for an upcoming frame.

Start delimiter—Indicates the beginning of a frame by employing a signaling pattern that differentiates it from the rest of the frame.

Frame control—Indicates the size of the address fields and whether the frame contains asynchronous or synchronous data, among other control information.

Destination address—Contains a unicast (singular), multicast (group), or broadcast (every station) address. As with Ethernet and Token Ring addresses, FDDI destination addresses are 6 bytes long.

Source address—Identifies the single station that sent the frame. As with Ethernet and Token Ring addresses, FDDI source addresses are 6 bytes long.

Data—Contains either information destined for an upper-layer protocol or control information.

Frame check sequence (FCS)—Is filed by the source station with a calculated cyclic redundancy check value dependent on frame contents (as with Token Ring and Ethernet). The destination address recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.

End delimiter—Contains unique symbols; cannot be data symbols that indicate the end of the frame.

Frame status—Allows the source station to determine whether an error occurred; identifies whether the frame was recognized and copied by a receiving station.

Copper Distributed Data Interface

Copper Distributed Data Interface (CDDI) is the implementation of FDDI protocols over twisted-pair copper wire. Like FDDI, CDDI provides data rates of 100 Mbps and uses dual-ring architecture to provide redundancy. CDDI supports distances of about 100 meters from desktop to concentrator.

CDDI is defined by the ANSI X3T9.5 Committee. The CDDI standard is officially named the Twisted-Pair Physical Medium-Dependent (TP-PMD) standard. It is also referred to as the Twisted-Pair Distributed Data Interface (TP-DDI), consistent with

the term Fiber Distributed Data Interface (FDDI). CDDI is consistent with the physical and media-access control layers defined by the ANSI standard.

The ANSI standard recognizes only two types of cables for CDDI: shielded twisted pair (STP) and unshielded twisted pair (UTP). STP cabling has 150-ohm impedance and adheres to EIA/TIA 568 (IBM Type 1) specifications. UTP is data-grade cabling (Category 5) consisting of four unshielded pairs using tight-pair twists and specially developed insulating polymers in plastic jackets adhering to EIA/TIA 568B specifications.

The figure below illustrates the CDDI TP-PMD specification in relation to the remaining FDDI specifications.

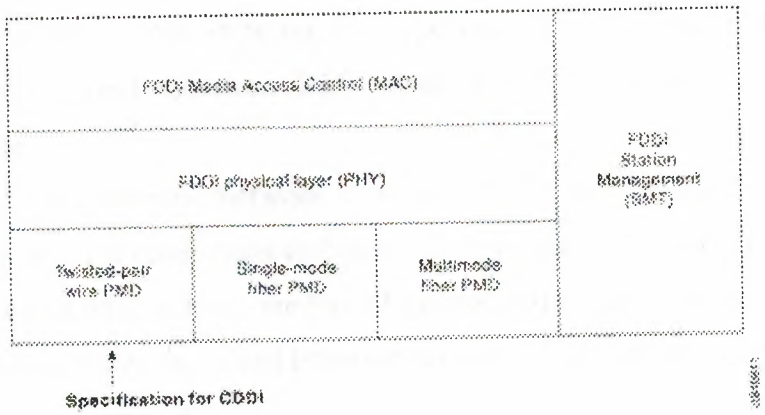


Figure 22: CDDI TP-PMD and FDDI Specifications Adhere to Different Standards

3.2.4 ARCnet

ARCnet is an older technology. ARCnet was first developed by Datapoint Corporation in 1977. ARCnet (Attached Resources Computing) utilizes coaxial or twisted pair cable in either a star or bus topology. It has a data transfer rate of 2.5 Mbps (Au, 1996). However, ARCNETPLUS provides signaling at 20 Mbps. ARCnet uses a media access protocol based on assigning numbers to each station, and stations broadcast when their numbers come up (Derfler, 1995). Although not as popular as Ethernet, some libraries have ARCnet-based LANs

3.2.5 LocalTalk

LocalTalk is not an industry standard, but it is a popular proprietary networking implementation developed by Apple. LocalTalk has a data transfer rate of 230 Kbps and uses shielded twisted pair cables in a bus topology. Apple specifies a 32 node per zone limit, and suggests a maximum total cable length of 1000 meters. LocalTalk uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA); this differs from CSMA/CD in that it employs a scheme to avoid collisions of data transmissions on the network as opposed to trying to correct them. (Breeding, 1992; Thomas, 1996). Many libraries use LocalTalk architecture, and many school media centers utilize LocalTalk as well.

3.2.6 Wireless Technologies 802.11b

802.11b is a wireless Ethernet technology operating at 11MB. 802.11b devices use Direct Sequence Spread Spectrum (DSSS) radio technology operating in the 2.4GHz frequency band.

An 802.11b wireless network consists of wireless NICs and access points. Access points act as wireless hubs to link multiple wireless NICs into a single subnet. Access points also have at least one fixed Ethernet port to allow the wireless network to be bridged to a traditional wired Ethernet network.. Wireless and wired devices can coexist on the same network.

802.11b devices can communicate across a maximum range of 50-300 feet from each other

4. NETWORK OPERATING SYSTEM AND PLANNING THE NETWORK

4.1 What is a Network Operating System (NOS)?

Unlike operating systems, such as OS/2, DOS, Windows 95, Windows 98, Windows ME that are designed for single users to control one computer, network operating systems (NOS) coordinate the activities of multiple computers across a network. The network operating system acts as a director to keep the network running smoothly.

The two major types of network operating systems are:

- Peer-to-Peer
- Client/Server

4.2 Peer-to-Peer Network Operating System

Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source. In a peer-to-peer network, all computers are considered equal; they all have the same abilities to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks. AppleShare and Windows for Workgroups are examples of programs that can function as peer-to-peer network operating systems. Figures 1 shows resources are shared equally.

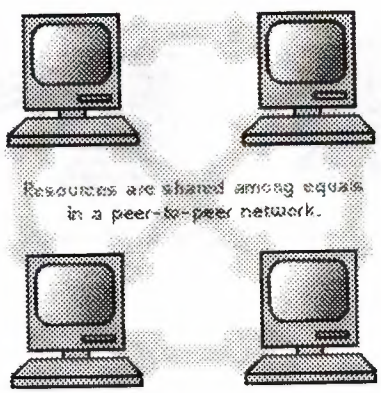


Figure 1 peer to peer network

Advantages of a peer-to-peer network:

- Less initial expense - No need for a dedicated server.
- Setup - An operating system (such as Windows 95, 98, ME etc) already in place may only need to be reconfigured for peer-to-peer operations.

Disadvantages of a peer-to-peer network:

- Decentralized - No central repository for files and applications.
- Security - Does not provide the security available on a client/server network

4.3 Client/Server Network Operating System

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers. The file servers become the heart of the system, providing access to resources and providing security. Individual workstations (clients) have access to the resources available on the file servers. The network operating system provides the mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical location. Novell Netware, Windows NT Server, Windows 2000 Server, Windows XP are examples of client/server network operating systems. Figure 2 shows how resources are controlled by the file server in a client/server network

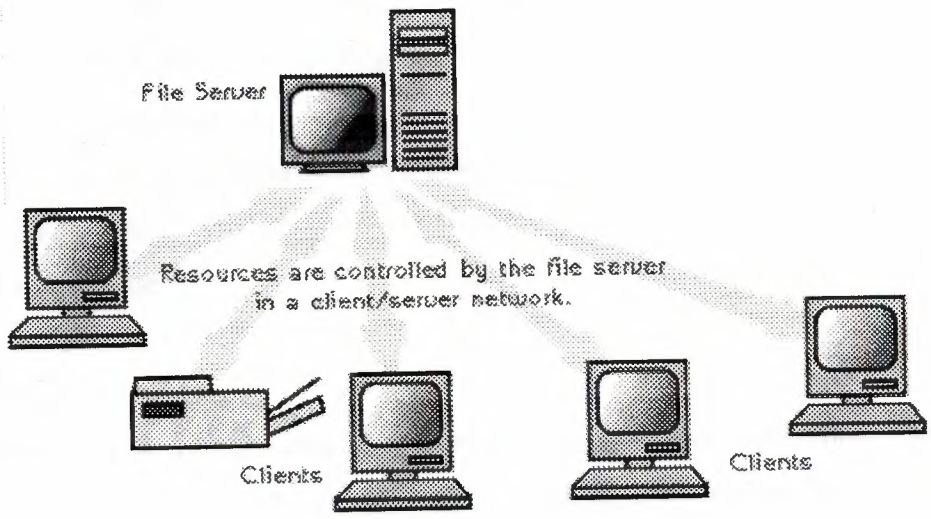


Figure 2 Client/Server Network

Advantages of a client/server network:

- Centralized - Resources and data security are controlled through the server.
- Scalability - Any or all elements can be replaced individually as needs increase.
- Flexibility - New technology can be easily integrated into system.
- Interoperability - All components (client/network/server) work together.
- Accessibility - Server can be accessed remotely and across multiple platforms.

Disadvantages of a client/server network:

- Expense - Requires initial investment in dedicated server.
- Maintenance - Large networks will require a staff to ensure efficient operation.
- Dependence - When server goes down, operations will cease across the network

4.4 Popular Network Operating Systems

The following list includes some of the more popular peer-to-peer and client/server network operating systems.

- AppleShare (Macintosh)
- LANtastic
- Linux
- Microsoft Windows NT Server
- Microsoft Windows 2000 Server
- Microsoft Windows XP Professional
- Novell Netware 6

Although I define all popular network operating systems but to be brief I will only discuss the installations of most secure, reliable and widely used network operating systems out of these.

4.4.1 Common Protocols

In networking and communications, the formal specification that defines the certain procedures to follow when to transmit and receive data. Protocols define the format, timing, sequence, and error checking used on the network. This section looks as some of the most commonly used protocols. They are:

- TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry standard suite of protocols providing communications in a heterogeneous environment. It was developed by Defense Advanced Research Projects Agency (DARPA). In addition, TCP/IP provides a routable enterprise networking protocol and access to the worldwide Internet and its resources.

It has become the standard protocol used for interoperability among many different types of computers. Almost all networks support TCP/IP ass a protocol. Because of its popularity, TCP/IP has become the de facto standard for internetworking. Historically, there are two primary disadvantages of TCP/IP: its size and speed. Its relatively a large protocol. Other protocols written specifically for TCP/IP suite include: STMP (simple mail transfer protocol e.g. E-mail), FTP (File Transfer Protocol i.e. for exchanging files among computers running TCP/IP), SNMP (simple network management protocol-Network management).

- NetBEUI and NetBIOS

NetBEUI is NetBIOS extended user interface. Originally, NetBIOS and NetBEUI were very tightly tied together, and considered one protocol. However several network vendors separated NetBIOS, the Session layer protocol, out so that it could be used with other routable transport protocols. NetBIOS (network basic input/output system) is an IBM session layer LAN interface that acts as an application interface to the network. It provides the tools for a program to establish a session with another program over the network It is very popular because so many application programs support it.

NetBEUI is a small, fast and efficient Transport layer protocol that is supplied with all Microsoft network products except Windows XP. It has been available since mid-1980s. Its advantages include its small stack size (important for MS-DOS based computers), its speed of data transfer on the network medium, and its compatibility with Microsoft products. The major disadvantage of NetBEUI it does not support routing. It is also limited to Microsoft-based networks.

- X.25

X.25 is a set of protocols incorporated in a packet switching network made up of switching services. It describes the electrical connections, the transmission protocol, error detection and correction, and other aspects of link. The switching services were originally established to connect remote terminals to main frame host systems.

- XNS

Xerox Network System (XNS) was developed by developed by Xerox for their Ethernet LANs. It became widely used in the 1980s, but has been slowly replaced by TCP/IP. It is a large, slow protocol, but produces more broadcasts, causing more traffic.

IPX/SPX and NWLink

Internetwork packet exchange/sequenced packet exchange is a protocol stack that is used in Novell networks. Like NetBEUI, it relatively small and fast protocol on a LAN. But, unlike NetBEUI, it does support routing. Microsoft provides NWLink as its version of IPX/SPX. It is a transport protocol and is routable.

- APPC

APPC (advanced program-to-program communication) is IBM's transport protocol developed as part of its systems network architecture (SNA). It was designed to enable application programs running on different computers to communicate and exchange data directly.

- AppleTalk

AppleTalk is a Apple Computer's (Macintosh) proprietary protocol stack designed to enable Apple Macintosh computers to share files and printers in a networked environment.

- OSI Protocol Suite

The OSI protocol suite is the complete protocol stack. Each protocol maps directly to a single layer of the OSI model. The OSI protocol suite includes routing and transport protocols, IEEE 802 series protocols, a Session layer protocol, a Presentation layer protocol, and several Application layer protocols designed to provide full networking functionality., including file access, printing, and terminal emulation.

- DECnet

DECnet is Digital Equipment Corporation's proprietary protocol stack. It is a set of hardware and software products that implement the Digital Network Architecture (DNA). It defines communication networks over Ethernet local area networks, fiber distributed data interface metropolitan area networks (FDDI MANs) and WANs that use private or public data transmission facilities. DECnet can also use TCP/IP and OSI protocols as well as its own protocols. It is a routable protocol.

4.4.2 AppleShare (Macintosh)

Apple Computers integrates networking services with its Macintosh operating system. Once Macintosh are up and running and cables are connected the, operating systems is ready to go. This operating system requires Macintosh machines. The integration of network services with the operating system is smooth and reliable. The most important feature of this operating system is the Publish/Subscribe system. Using this utility a user can "Publish" a message (make it available to other users on the network), and it will be instantly available to all "Subscribers" (those users who have opted for immediate display of "Published" messages). This makes for convenient sharing of up-to-the minute information.

4.4.3 LANtastic

LANtastic is classical operating system for peer-to-peer networks. It is manufactured by the Artisoft Corporation, which also manufactures network hardware. It advantages include ease of setup, relatively low memory requirements, good security for peer-to-peer system, and fairly low cost. LANtastic can run with minimal hardware any IBM compatible PC running Microsoft Windows preferable Windows NT or Windows 2000, standard Ethernet cards.

The LANtastic operating system is NetBIOS compatible meaning that it makes use of certain file and data-flow services belonging to underlying system, in order to manage its network operations.

4.4.4 Linux

Linux can be installed on UNIX based network systems. There are many developers of Linux operating system but the most popular developer is Red Hat Inc. Linux is case sensitive. In other words, a rose is not a ROSE is not a rOsE. It supports both type of installations GUI (Graphical User Interface) and text mode. These recommendations are based on an installation that only installs one language (such as English).

- Workstation

  A workstation installation, installing either GNOME (GNU Network Object model Environment. GNOME is part of the GNU project and part of the open source movement. GNOME is a Windows-like desktop system and is not dependent on any one window manager. The main objective of GNOME is to provide a user-friendly suite of applications and an easy-to-use desktop) or KDE

(K Desktop Environment. KDE is a network-transparent contemporary desktop environment for Linux and UNIX workstations) requires at least 1.5 GB of free space. Choosing both GNOME and KDE requires at least 1.8 GB of free disk space.

- Server

  A server installation requires 1.3 GB for a minimal installation without X (the graphical environment), at least 1.4 GB of free space if all components (package groups) other than X are installed, and at least 2.1 GB to install all packages including GNOME and KDE

- Laptop

  A laptop installation, when you choose to install GNOME or KDE, requires at least 1.5 GB of free space. If you choose both GNOME and KDE, you will need at least 1.8 GB of free disk space.

Linux install options include Workstation, Server, Laptop, Custom, and Upgrade. Red Hat Linux allows choosing the installation type that best fits needs of the network. Figure 3 shows the install screen of Red Hat Linux

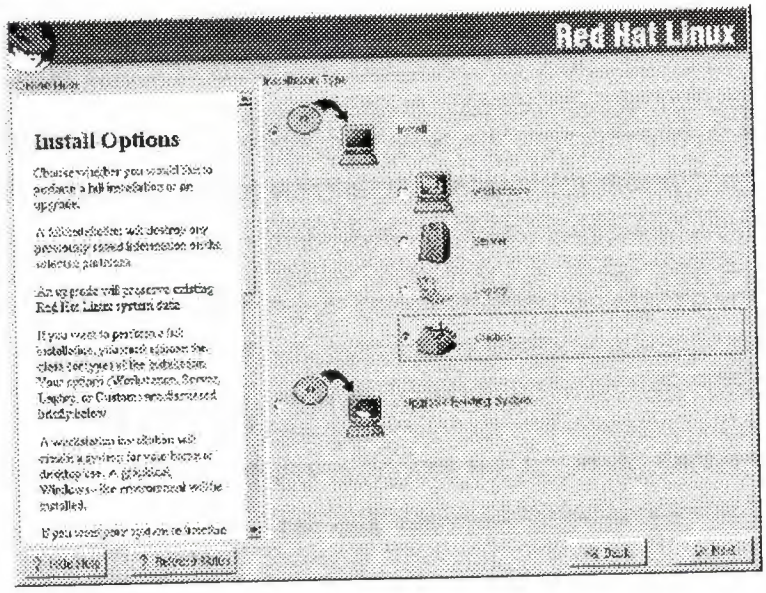


Figure 3 Red Hat Linux 7.3 Install Screen

4.4.5 Microsoft Windows NT Server

Windows NT server is Windows-based client server operating system developed by Microsoft Corporation. It provides high levels of security and robust performance. Windows NT server can run on file servers using Intel processors (at least an 80486 processor is recommended). It is designed to interact with its companion product,

Windows NT workstation, but it can interact with other platforms as well: MS-DOS (using LAN manager), OS/2, Windows 95, 98, ME. Windows NT server supports virtually all network adapter cards and cabling systems.

Protocols supported by Windows NT are NWLink (compatible with Novell IPX.SPX), NetBEUI, Data Control and TCP/IP Windows NT Server is fully integrated system. Installation on file server is automated; as simple as inserting and installation disk and booting the server. During installation, NT creates a special database called the "Registry" that we enter containing information about the server and clients who logged on. When installing Windows NT workstation, client software can be installed from the server or from other workstations. Client data is centralized in the NT system. Each client is given a user account, which gives users access to network services. The network administrator has centralized control over client accounts and can restrict access to specific services for security purposes. User accounts include information about user name, password, full name, logon hours, logon workstations, expiration date, user directory (private directory on server for user), logon script (a batch file of operating system commands that executes when users log on) and account type.

4.4.6 Window 2000 Server

Staying competitive in the new digital economy requires an advanced computer-based, client/server infrastructure that lowers costs and enables organization to adapt quickly to change. The Microsoft Windows 2000 platform — the combination of Windows 2000 Professional and Windows 2000 Server — can deliver the following benefits to organizations of all sizes:

- Lower total cost of ownership (TCO).
- A reliable platform for computing 24-hours-a-day, seven-days-a-week.
- A digital infrastructure that can accommodate rapid change.

The entire product family is designed to provide networking, application, communications, and Web services with increased manageability, reliability, availability, interoperability, scalability, and security. To accommodate the computing needs of organizations of all sizes, there are several Windows 2000 products available. The following sections introduce you to specific products that make up the Windows 2000 family.

Windows 2000 Server extends the application services established by Microsoft Windows NT Server version 4.0. By integrating application services such as Component Services, transaction and message queuing, and Extensible Markup Language (XML) support, Windows 2000 Server is an ideal platform for both independent software vendor solutions and custom line-of-business applications. It provides more security than Windows NT. It is simply more powerful and enhanced version on Windows NT. The most important Feature of Windows 2000 is Terminal Services and Mobile Devices. These features let user manage services from anywhere on the network. For example, if user receive a call about a network bandwidth issue while visiting a branch office, user can use a wireless handheld computer to access the network's centralized management tools, diagnose the issue, and work to resolve it.

4.4.6.1 Installation of Windows 2000 Server

These are the hardware requirements for the common infrastructure:

- Server(s): 1 Capable of running Windows 2000 Server. An Intel–processor-based server running Windows 2000 Server must have at least 64 megabytes (MB) of RAM. Microsoft recommends that the server have several gigabytes of disk storage. In addition, servers should be equipped with high-speed network interface cards
- Workstation(s): As Needed Capable of running Windows 2000 Server. Use a sufficient number of workstations to simulate a variety of workstation environments, including your organization's typical desktop, roaming user, mobile user, and any other configurations that may be appropriate. These computers must be capable of running Windows 2000 Professional. Microsoft recommends a minimum of 32 MB of RAM for Intel processor-based workstations. For best results, make sure that these computers have sufficient RAM and disk storage.
- Network Hub(s): As Needed A private network is recommended
- Network Interface Cards: As Needed
- Backup Device Optional: RS-232
- UPS: Optional To protect the servers
- Printer Optional: To print-out configuration information and other tests

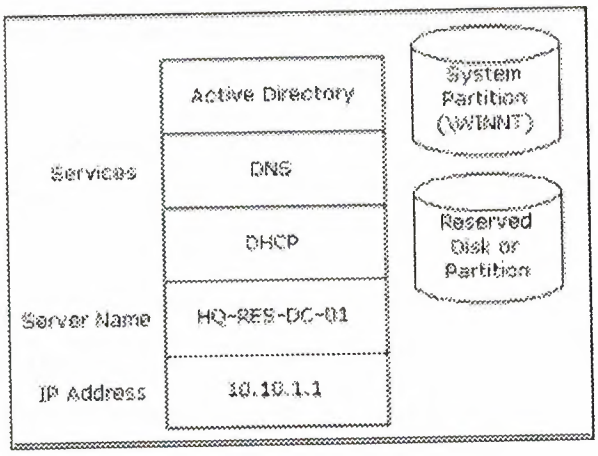


Figure 4 Server Configuration

To use a single server for the infrastructure, a server is needed with either two disk drives or a single disk drive with two partitions. The first disk or partition holds Windows 2000 and the other files for the common infrastructure, such as the Windows Installer packages and application source files.

Each disk or partition must hold several gigabytes of information, and each disk or partition must be formatted for the NTFS file system. The steps for creating partitions and formatting them are contained within this guide. This installation procedure starts with making boot disks. Start the installation after booting from these disks. Four formatted disks and the Windows 2000 Server CD.

Setup creates the disk partitions on the computer running Windows 2000 Server, formats the drive, and then copies installation files from the CD to the server.

1. Insert the Windows 2000 Server installation floppy disk number one.
2. Restart the computer. The Windows 2000 Server installation begins.
3. Insert the remaining three Windows 2000 Server installation disks as prompted by Windows 2000 Setup.
4. At the Welcome to Setup screen, press Enter.
5. Review and if acceptable, agree to the license agreement by pressing F8.
6. Follow the instructions to delete all existing disk partitions. The exact steps will differ based on the number and type of partitions already on the computer. Continue to delete partitions until all disk space is labeled as Unpartitioned space.

7. When all disk space is labeled as Unpartitioned space, press C to create a partition in the unpartitioned space.
8. If server has a single disk drive, split the available disk space in half to create two equal sized partitions. Delete the total space default value. Type the value of half your total disk space at the Create partition of size (in MB) prompt. Press Enter. (If your server has two disk drives, type the total size of the first drive at this prompt.)
9. After the New (Unformatted) partition is created, press Enter.
10. Select Format the partition using the NTFS file system (the default selection) and press "Enter". Remove the floppy disk from the drive.

Windows 2000 Setup formats the partition and then copies the files from the Windows 2000 Server CD to the hard drive. The computer restarts, and the Windows 2000 Installation Program continues.

This procedure continues the installation with the Windows 2000 Server Setup Wizard.

1. The Welcome to the Windows 2000 Setup Wizard appears, click Next. Windows 2000 then detects and installs devices. This can take several minutes, and during the process your screen may flicker.
2. In the Regional Settings dialog box, make changes required for your locale and click Next.
3. In the Personalize Your Software dialog, type name in the Name box and type organization name in the Organization box. Click Next.
4. Type the Product Key in the text boxes provided. Click Next.
5. In the Licensing Modes dialog box, select the appropriate licensing mode for your organization and click Next.
6. In the Computer Name and Administrator Password dialog box, type the new computer name HQ-RES-DC-01 in the computer name box and click Next.
7. In the Windows 2000 Components dialog box, click Next. Wait while networking components are installed. This takes a few minutes.
8. In the Date and Time Settings dialog, correct the current date and time if necessary and click Next.
9. In the Networking Settings dialog, make sure Typical Settings is selected and then click Next.

10. In the Workgroups or Computer Domain dialog box, No is selected by default, then click Next.

Windows 2000 Server Installation continues and configures the necessary components. This takes a few minutes.

11. When you reach the Completing the Windows 2000 Setup Wizard, remove the CD-ROM from the drive and click Finish.

The server restarts and the operating system loads from the hard drive.

Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS), and DCPromo (the command-line tool that creates DNS and Active Directory) can be installed manually or by using the Windows 2000 Configure Your Server Wizard. This guide uses the wizard; the manual procedures are not covered here.

1. Press Ctrl-Alt-Del and log on to the server as administrator. Leave the password blank.
2. When the Windows 2000 Configure Your Server page appears, select This is the only server in my network and click Next.
3. Click Next to configure the server as a domain controller and set up Active Directory, DHCP, and DNS.
4. On the What do you want to name your domain page, type organization name.
5. In the Domain name box, type "com". Click on the screen outside of the textbox to see the Preview of the Active Directory domain name. Click Next.

The figure 5 shows the Windows 2000 "Configure Your Server Wizard".

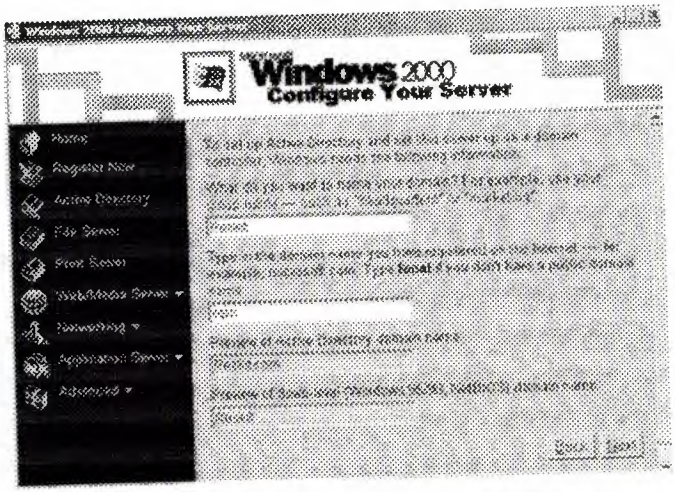


Figure 5 Configure Your Server Wizard

6. Click Next to run the wizard. When prompted, insert the Windows 2000 Server CD-ROM. When the wizard is finished, the machine reboots.

The Configure Your Server Wizard installs DNS and DHCP and configures DNS, DHCP, and Active Directory. The default values set by the wizard are shown in table 1.

DHCP Scope:	10.0.0.3-10.0.0.254
Preferred DNS Server:	127.0.0.1
IP address:	10.10.1.1
Subnet mask:	255.0.0.0

Table 1 Default Values Set by Wizard

Active Directory Sample Infrastructure:

The common infrastructure is based on the fictitious company name.

The company name e.g. Reskit has the DNS name reskit.com that was configured using the Configure Your Server Wizard in the preceding section. Figure 6 below illustrates the sample Active Directory structure.

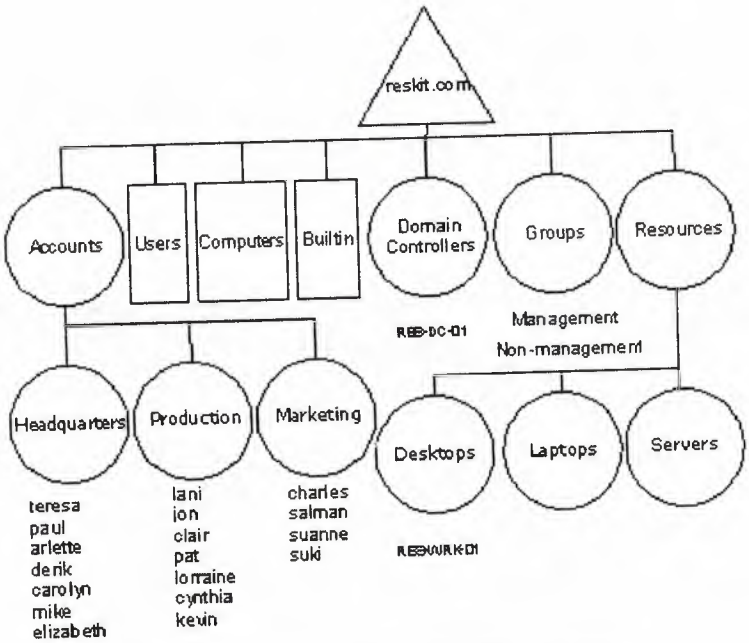


Figure 6 Sample Active Directory Structure

Of most interest here are the Domain (reskit.com), and the Accounts, Headquarters, Production, Marketing, Groups, Resources, Desktops, Laptops, and Servers organizational units (OUs). These are represented by circles in Figure 4.6. OUs exist for the delegation of administration and for the application of

Populating Active Directory:

This section describes how to manually create the OUs, Users, and Security Groups outlined in Appendix A of this document.

- To create Organizational Units and Groups

1. Click Start, point to Programs, then point to Administrative Tools, and click Active Directory Users and Computers.
2. Click the + next to Reskit.com to expand it. Click Reskit.com itself to show its contents in the right pane.
3. In the left pane, right-click Reskit.com, point to New, and click Organizational Unit.
4. Type Accounts in the name box, and click OK.
5. Repeat steps 3 and 4 to create the Groups and Resources OUs. These three OUs now show up in the right pane.
6. Click Accounts in the left pane. Its contents now display in the right pane (it is empty to start).
7. Right-click Accounts, point to New, and click Organizational Unit.
8. Type Headquarters, and click OK.
9. Repeat steps 6 and 7 to create the Production and Marketing OUs under Accounts. When you have finished, the OU structure should look like Figure 7 below:

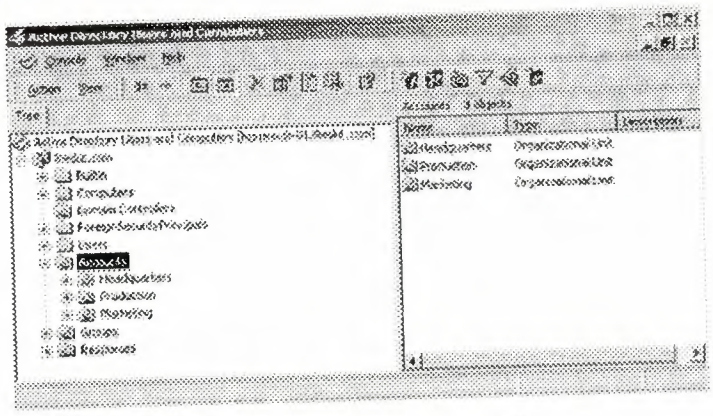


Figure 7 Create Organizational Units

10. In the same way, create Desktops, Laptops, and Servers under the Resources OU.
11. Create the two security groups by right-clicking Groups, then pointing to New, then clicking Group. The two groups to add are Management and Non-management. The settings for each group should be Global and Security. Click OK to create each group.

- To create User Accounts

1. In the left-hand screen, click the + next to the Accounts folder to expand it.
2. Click Headquarters (under Accounts) in the left-hand screen. Its contents now display in the right pane (it is empty at the beginning of this procedure).
3. Right-click Headquarters, point to New, and click User.
4. Type Teresa (for example) for the first name and Atkinson (for example) for the last name. (Note that the full name is automatically filled in at the full name box.)
5. Type Teresa for the User logon name. The window will look like Figure 8 below:

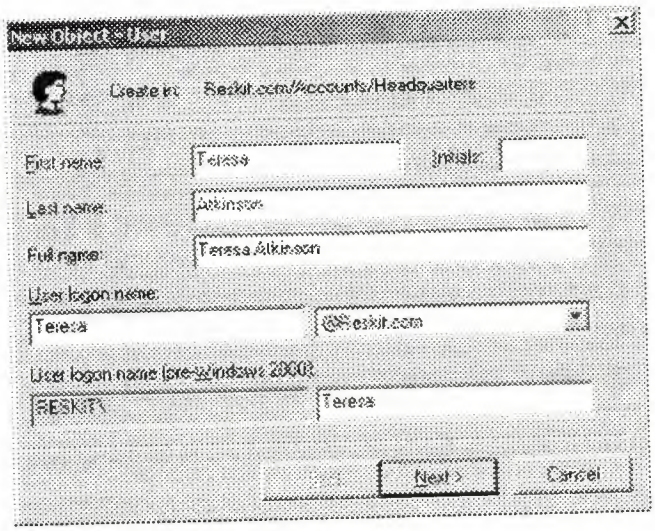


Figure 8 Adding a User

6. Click Next.
7. Click Next on the Password page to accept the defaults.
8. Click Finish. Teresa Atkinson now displays on the right-hand screen, as a user under Reskit.com/Accounts/Headquarters.

9. Repeat steps 2 through 7, adding the names listed in Appendix A for the Headquarters OU. When you are finished, the Headquarters OU.
10. Repeat steps 1 through 8 to create the users in the Production and Marketing OUs.

To add Users to Security Groups

1. In the left pane, click Groups.
2. In the right pane, double-click the group Management.
3. Click the Members tab and then click Add.
4. Select the users in the upper pane as shown in Figure 9 below by holding down the ctrl key while clicking each name; click Add to add them all at once. Their names will display in the bottom pane. Click OK to accept.

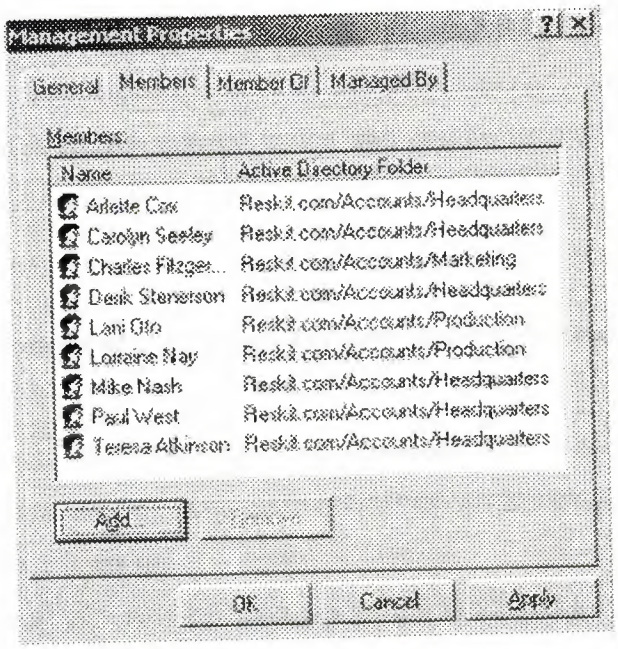


Figure 9 The members of the Management group are drawn from three OUs.

5. Repeat steps 2 through 4 to add members to the Non-management group.
6. Close the Active Directory Users and Computers snap-in.

We have finished installation of the Windows 2000 Server.

4.4.7 Window XP professional

Window XP is new operating system developed by Microsoft Corporation. Networking point of view Windows XP is designed for home or small business local area networking. Windows XP is the first Microsoft Windows system where Microsoft's own NetBEUI protocol is not supported. But NetBEUI can be installed on Windows XP but it is not recommended. The supported protocols are NWLink IPX/SPX and NetBIOS compatible protocols. Windows XP contains powerful new features designed to keep computer network running no matter what. Sophisticated protection software guards each computer's operating system, and also establishes a protective barrier, or firewall, that shields the entire network from outside hackers and viruses spread over the Internet. In Windows XP networking, TCP/IP is the preferred protocol.

To make a local area connection

- If a network adapter is installed, and have set up a home or small office network, you are connected to a local area network (LAN). You are also connected to a LAN if your Windows XP Professional computer is part of a corporate network. When you start your computer, your network adapter is detected and the local area connection automatically starts. Unlike other types of connections, the local area connection is created automatically, and you do not have to click the local area connection in order to start it.

Notes

- A local area connection is automatically created for each network adapter that is detected.
- If more than one network adapter is installed, you can eliminate possible confusion by immediately renaming each local area connection to reflect the network that it connects to.
- If your computer has one network adapter, but you need to connect to multiple LANs (for example, when traveling to a regional office), the network components for your local area connection need to be enabled or disabled each time you connect to a different LAN.
- If more than one network adapter is installed, you need to add or enable the network clients, services, and protocols that are required for each local area connection. The client, service, or protocol is added or enabled for all other network and dial-up connections.

4.4.7.1 Installation of Windows XP

1. First you must link your computers together by installing appropriate hardware in each and by joining the computers with wires or by means of wireless technology. Figure 10 shows the LAN connection

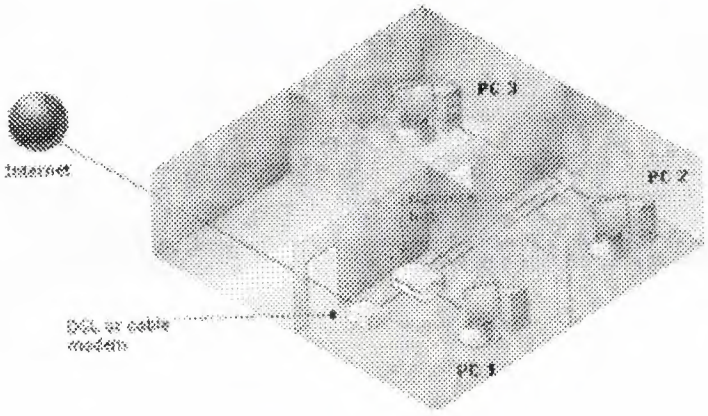


Figure 10 LAN Connection

2. One computer equipped with Windows XP and Internet access. This computer will serve as the network's central unit, or Internet Connection Sharing (ICS) host. It should be fastest, most capable machine.
3. One or more additional computers running Windows XP, Windows Millennium Edition, Windows 98 Second Edition, or Windows 98. These computers are called clients and will connect to the ICS host.
4. An individual network adapter for each computer
5. Windows 95, Windows 2000, Macintosh or UNIX/Linux computers can be included on network. However, these computers may require additional software to allow you to share folders or a printer. Consult the documentation that came with those computers.
6. Switch on all computers, printers and other peripherals.
7. Go to the ICS host computer and make sure it is connected to the Internet.
8. Run the Network Setup Wizard on the ICS host
9. To run the Network Setup Wizard on the ICS host, click Start -> Control Panel -> Network and Internet Connections -> Setup or Change Your Home or Small Office Network. Follow the instructions in each screen and press Next to continue Figure 11 shows the network set up wizard.

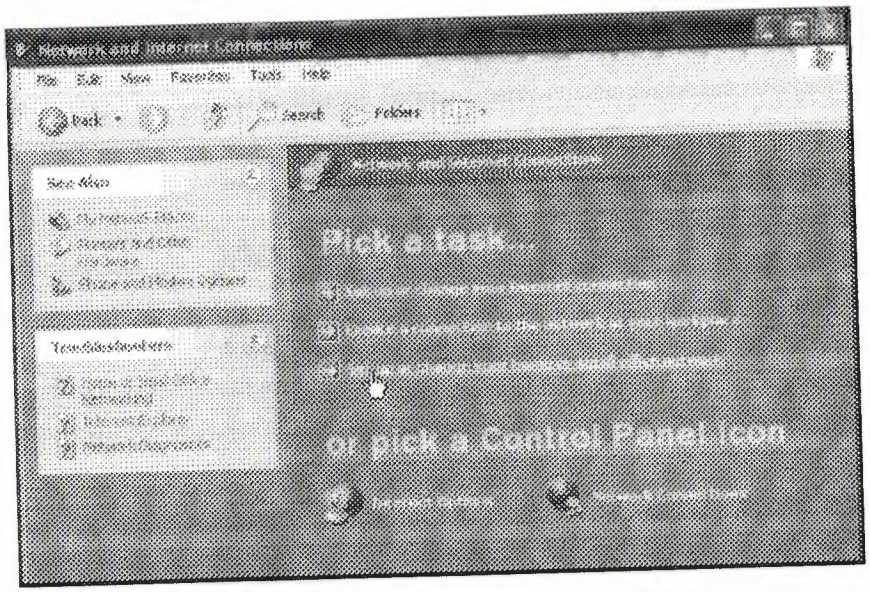


Figure 11 Windows XP Network Setup Wizard

The Network Setup Wizard will guide you through:

- Configuring network adaptors (NICs).
- Configuring computers to share a single Internet connection.
- Naming each computer. (Each computer requires a name to identify it on the network.)
- Sharing the Shared Files folder. Any files in this folder will be accessible to all computers on the network.
- Sharing printers.
- Installing the Internet Connection Firewall to guard you from online attacks.

10. Run the Network Setup Wizard on all computers

To do so:

- Insert the Windows XP CD in the first computer's drive.
- When the XP Welcome Menu appears, click Perform Additional Tasks.
- Click Setup Home or Small Office Networking and follow the prompts.
- Repeat steps 1 to 3 for each computer on your network.
- Make sure that an active Internet connection is maintained on host computer as you proceed through this process.

Using Network

Once network is up and running, other computers on the network can be easily accessed via My Network Places (click Start -> My Network Places) as shown in figure 12

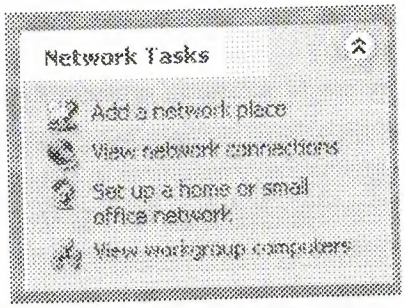


Figure 12 Network Tasks Window

4.4.8 Novell NetWare 6

2002 award winner NetWare is the large client/server system developed by the Novell Corporation. Currently more than half of the PC-based file server systems run using NetWare. The newest version on Novell NetWare is version 6. NetWare file system is propriety, and optimized for networking environment. It has many unique features that can improve a network overall performance, speed and reliability. Novell Native File Access Protocols let Macintosh, Windows, and UNIX workstations access and store files on NetWare servers without having to install any additional software—such as Novell Client software. The software is installed only on the NetWare server and provides "out of the box" network access. Just plug in the network cable, start the computer, and access to servers on the network. No more client configuration. No more client software. No more problems.

Minimum System Requirements

NetWare 6 has the following minimum system requirements:

- A server-class PC with a Pentium* II or AMD* K7 processor
- 256 MB of RAM
- A Super VGA display adapter
- A DOS partition of at least 200 MB and 200 MB available space
- 2 GB of available disk space outside the DOS partition for volume SYS:

- One network board
- A CD drive
- A USB, PS/2*, or serial mouse (recommended but not required)

4.4.8.1 Installing the Novell NetWare 6

To begin the installation, complete the following steps.

1. Insert the NetWare 6 Operating System CD, or log in to the network to access the installation files on the network.
2. At the CD drive or network drive prompt, enter INSTALL.

To select the type of installation and select regional settings, you must

- Select the language and accept the License Agreement
- Select the type of installation
- Specify server settings
- Select the regional settings
- Select the mouse and video type
- Follow the instructions

Naming the Server

The NetWare server name must be unique. The name can be between 2 and 47 alphanumeric characters and can contain underscores (_) and hyphens (-), but no spaces. The first character cannot be a period (.). Figure 13 shows the NetWare server properties window.

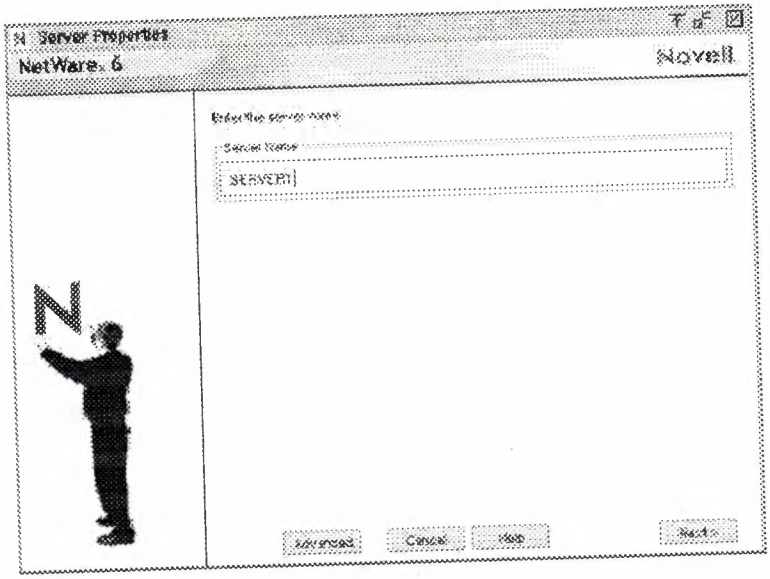


Figure 12 Novell NetWare Server Properties Window

Setting Up Domain Name Service:

The IP protocol identifies computers and systems by their assigned IP addresses, such as 123.45.56.89. Domain Name Service (DNS) allows a specific server on the network to maintain a list of simple, readable names that match IP addresses. Applications (or protocols) that require IP addresses rather than names can use a DNS server to translate from one form to another. Figure 13 shows the NetWare DNS window.

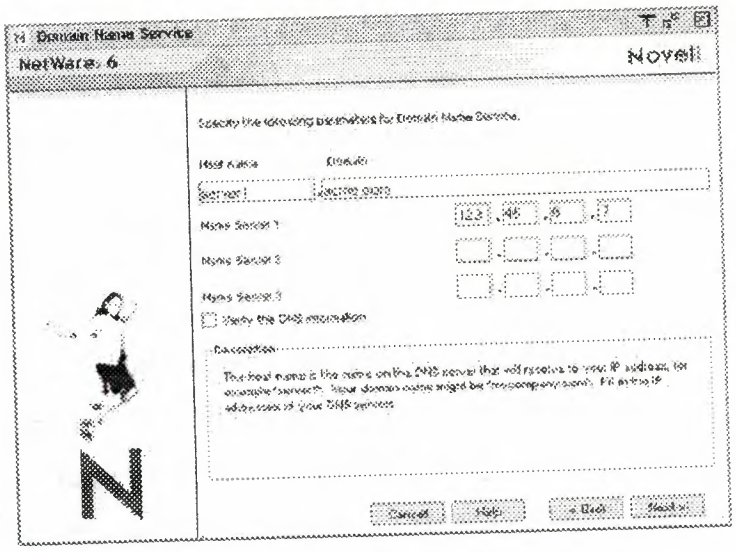


Figure 13 NetWare DNS window

4.5 Internet Access over LAN

There are various methods of connecting a LAN to the Internet Gateway, which are explained as below:

- Dial-up

  A common way of accessing Internet over LAN is the Dial-Up approach. In this method, a remote user gets to Internet as follows - Initially the remote user's PC is linked to the local gateway through an existing dialup line using modems, once the user has reached the local gateway, further routing up to Internet is taken care of, by the local gateway itself. The routing procedures are transparent to the end user

- Leased Line

  Leased line facility provides reliable, high speed services starting as low as 2.4kbps and ranging as high as 45 Mbps (T3 service). A leased line connection

is an affordable way to link two or more sites for a fixed monthly charge. Leased Lines can be either fiber optic or copper lines High capacity leased line service is an excellent way to provide data, voice and video links between sites. Leased line service provides a consistent amount of bandwidth for all your communication needs.

- ISDN

  Integrated Services digital Network (ISDN) is a digital telephone system. ISDN involves the digitization of telephone network so that voice, data, graphics, text, music, video and other source material can be provided to end users from a single end-user terminal over existing telephone wiring.

- VSAT Technology

  VSAT technology has emerged as a very useful, everyday application of modern telecommunications. VSAT stands for 'Very Small Aperture Terminal' and refers to 'receive/transmit' terminals installed at dispersed sites connecting to a central hub via satellite using small diameter antenna dishes (0.6 to 3.8 meter). VSAT technology represents a cost effective solution for users seeking an independent communications network connecting a large number of geographically dispersed sites. VSAT networks offer value-added satellite-based services capable of supporting the Internet, data, voice/fax etc. over LAN. Generally, these systems operate in the Ku-band and C-band frequencies

- Cable Modem

  The Internet Access over cable modem is a very new and fast emerging technology. A "Cable Modem" is a device that allows high speed data access via a cable TV (CATV) network. A cable modem will typically have two connections, one to the cable wall outlet and the other to the PC. This will enable the typical array of Internet services at speeds of 100 to 1000 times as fast as the telephone modem. The speed of cable modems range from 500 Kbps to 10 Mbps

4.6 Planning the Network

Every business has certain unique characteristics. The everyday logistics of running businesses are based on the careful planning of businesses. Same terminology is applied

when implementing local area networks. Planning process for network includes the following steps:

- The number of computers placed on the network.
- Site analysis
- Total budget for setting up LAN.
- Technology to be used
- Placing network equipment.
- Kind of cabling a LAN should have.
- Software needed for LAN
- Cost of network equipment, labor, computers, software and cables.
- Security

In addition to above considerations and after implementing the LAN the backup of whole data should be made.

CONCLUSION

This Project provides comprehensive information and guidelines for implementing the Local Area Network (LAN) in the work place. Local Area Networks are today's need. LAN is used to make communication between one device to another in an office connected on the LAN. It is easy to share information and data. And also reduces the cost of the storage device and also wastage of time. As one storage device in the server can be used to store information from any device attached to LAN. We can get up to date information from any device attached to LAN. Local Area Network is distinguished in to three kinds according to the size, transmission technology and topology. There are five basic types of topologies, which are implemented according to the cost, quality and reliability. There are some reference models, which describe the standard way of communications and protocols between the local area network. One main disadvantage of LAN is restrictness of small size, which has been solved by the WANs (Combination of more than two LANs). Now a days after seeing the advanced features of LAN every one uses a small Local Area Network to make communication between the terminals in an office or building.

REFERENCES

[1] Tanebaum Andrew S., Computer Networks, 1996

[2] Martin Michael J., Understanding the Network: A Practical Guide to Internetworking, Macmillan Computer publishing, USA, 2000

[3] Microsoft, Networking Essentials, Microsoft Corporation, Washington, 1996

[4] Mahler, Kevin. CCNA Training Guide. Indianapolis: New Riders, 1999.

[5] Cisco IOS Wide Area Networking Solutions. Indianapolis: Cisco Press, 1999.