NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

LOCAL AREA NETWORKS

Graduation Project
COM- 400

Student: Azhar Ali Awan (992292)

Supervisor: Dr. Jamal Fathi

Nicosia-2002

ACKNOWLEDGEMENTS

Foremost I would like to pay my special thanks to my parents, who helped me on every phase of my life. They boosted me up about my studies as well as my life. I am very much thankful and grateful to my mother whose prayers and love for me has encouraged me so make this day come true. It is only because of them that today I am capable of completing my degree.

Secondly I would like to thank to my supervisor Dr. Jamal Fathi, without whom this project would have not been possible, whose words of encouragement kept us doing my project. His faith in my work and me and his invaluable knowledge for the project has made me taking keen interest in my project. He is an excellent teacher and advisor.

I would also like to thank my all friends and housemate who helped me so much in doing my project. They encouraged me a lot in completing my project, as it is not single man's work. I want to thank them as they contributed their time and provided me with very helpful suggestions.

CONTENTS

ABSTRACT

A Network is a group of computers and other devices that connected to each other. The most common types of Networks are LAN, MAN and WAN. 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 by ISO, hold communication between different devices. Some special softwares are installed on the communicating devices on the LAN, which help and facilitate in communication.

1. LOCAL AREA NETWORKS IN WORKPLACE

1.1 Overview

A network is a group of computers, printers, and other devices that are connected together with cables. Information travels over the cables, allowing network users to exchange documents & data with each other, print to the same printers, and generally share any hardware or software that is connected to the network. Each computer, printer, or other peripheral device that is connected to the network is called a node. Networks can have tens, thousands, or even millions of nodes. In the simplest terms, a network consists of two or more computers that are connected together to share information. Principal components of a computer network:

- Computers (processing nodes or hosts)
- Data communication system (transmission media, communication processors, modems, routers, bridges, radio systems, satellites, switches, etc)

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 1.1 shows the network connectivity of the world.

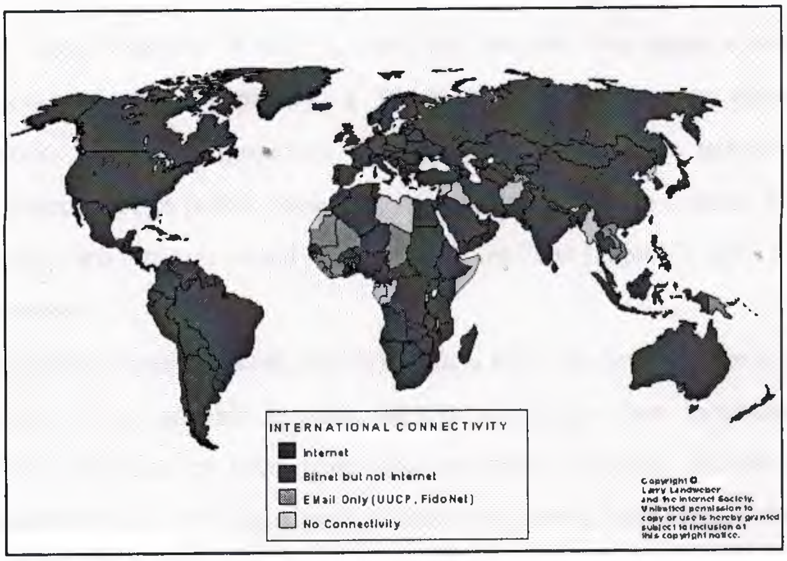


Figure 1.1 Computer Network Connectivity of the World

1.3 Goals of Computer Networks

1. Resource sharing and accessing them independently of their location.
2. Providing a universal environment for transmission of all kinds of information: data, speech, video, etc.
3. Supporting high reliability of accessing resources.
4. Distribution of loads according to the requirements very fast main frames, minis, PCs, etc.

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 1.2 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.

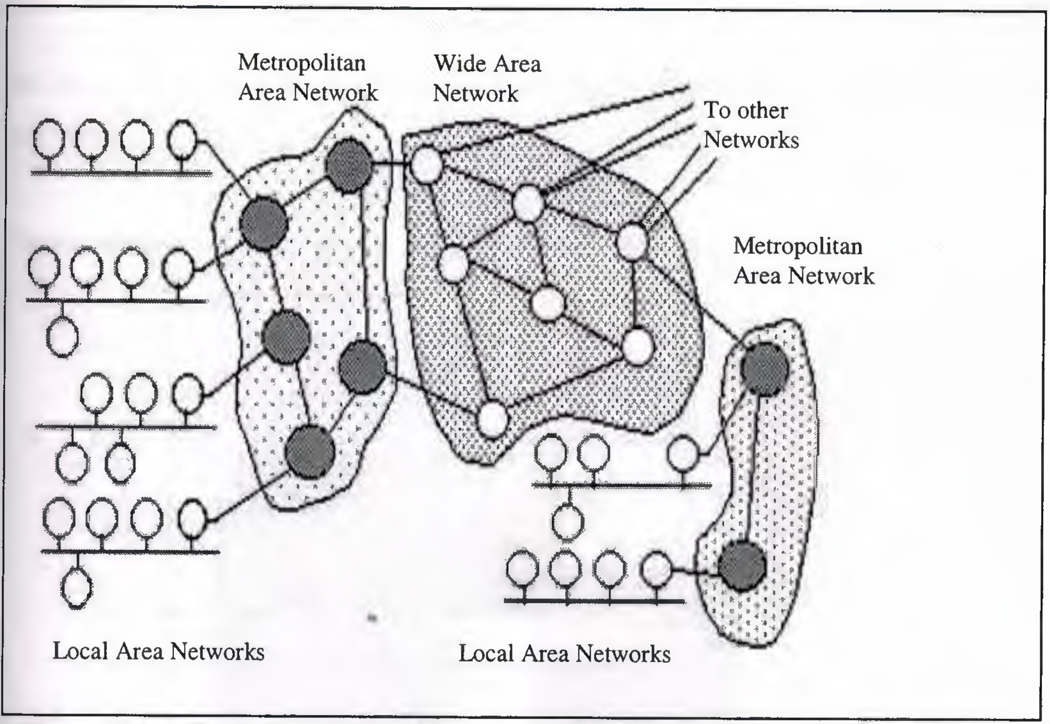


Figure 1.2 A Typical use of MANs to provide shared access to a Wide Area Network

Computer networks are used according to specified location and distance. In table 1.1 it is shown that which technology can be applied to the specific location and specific distance.

Table 1.1 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 1.3 a chart is shown which specifies the distances and speeds of different networks.

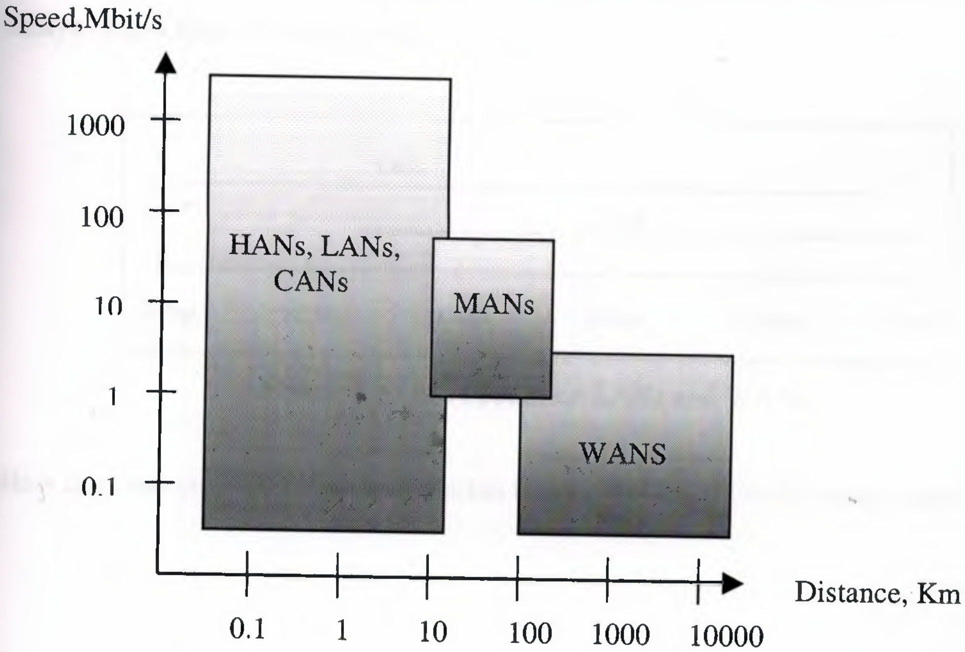


Figure 1.3 Distances and Speeds of the Different Networks

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 1.4. They have very small delays of less than 10 milliseconds.

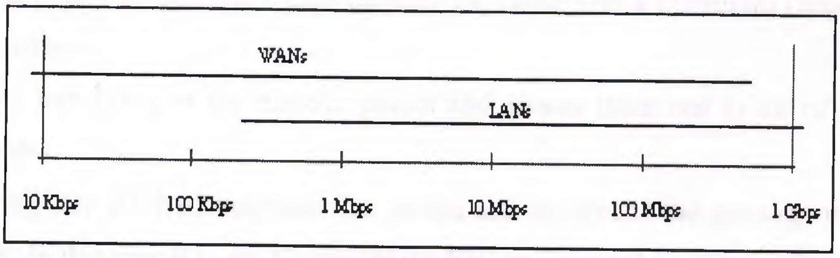


Figure 1.4 Data Speeds on LANs and WANs

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

The figure 1.5 shows and explains a simple network.

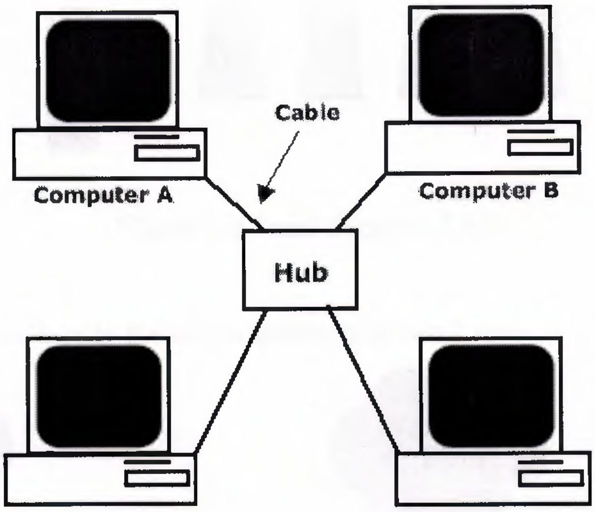


Figure 1.5 Simple Network

If Computer A wants to send a file to Computer B, the following would take place:

1. 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.
2. The pulses of electricity pass through the cable with a minimum (hopefully) of resistance.
3. The hub takes in the electric pulses and shoots them out to all of the other cables.
4. 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. etc.

Figure 1.6 shows small Ethernet local area network.

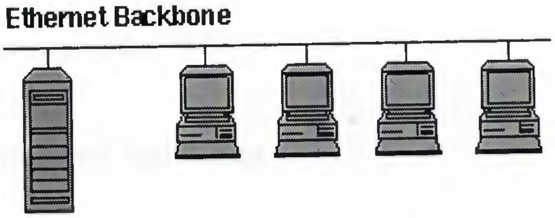


Figure 1.6 Small Ethernet LAN

The figure 1.7 shows briefly the interconnection of two LANs

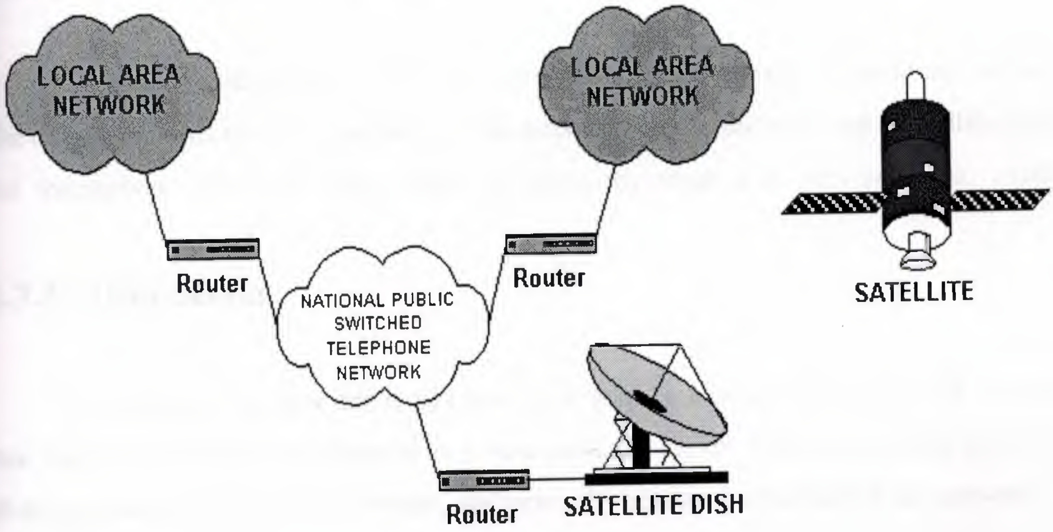


Figure 1.7 Interconnection of two LANs

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

- Physical connectors.
- Protocols.
- Network operating system (NOS).

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 doesn't have any dedicated servers or hierarchy among the computers. All of the computers on the network handle security and administration for themselves. The users must make the decisions about who gets access to what.

1.7.2 Client-Server

A client-server network works the same way as a peer-to-peer network except that there is at least one computer that is dedicated as a server. The server stores files for sharing, controls access to the printer, and generally acts as the dictator of the network.

1.8 Local Area Networks Connectivity Devices

1.8.1 Repeaters

Boost signal in order to allow a signal to travel farther and prevent attenuation. Attenuation is the degradation of a signal as it travels farther from its origination. Repeaters do not filter packets and will forward broadcasts. Both segments must use the same access method, meaning that you can't connect a token ring segment to an Ethernet segment. Repeaters will connect different cable types.

1.8.2 Bridges

Functions the same as a repeater, but can also divide a network in order to reduce traffic problems. A bridge can also connect unlike network segments (i.e. token ring and Ethernet). Bridges create routing tables based on the source address. If the bridge can't find the source address it will forward the packets to all segments.

1.8.3 Routers

A router will do everything that a bridge will do and more. Routers are used in complex networks because they do not pass broadcast traffic. A router will determine the most efficient path for a packet to take and send packets around failed segments. Unroutable protocols can't be forwarded.

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

Often used as a connection to a mainframe or the internet. Gateways enable communications between different protocols, data types and environments. This is achieved via protocol conversion, whereby the gateway strips the protocol stack off of the packet and adds the appropriate stack for the other side.

1.9 Local Area Networks (LAN) in the Workplace 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 Networks

Wireless networking refers to hardware and software combinations that enable two or more appliances to share data with each other without direct cable connections. Thus, in its widest sense, wireless networking includes cell and satellite phones, pagers, two-way radios, wireless LANs and modems, and Global Positioning Systems (GPS). Wireless LANs enable client computers and the server to communicate with one another without direct cable connections. Figure 1.8 and 1.9 shows the wireless network.

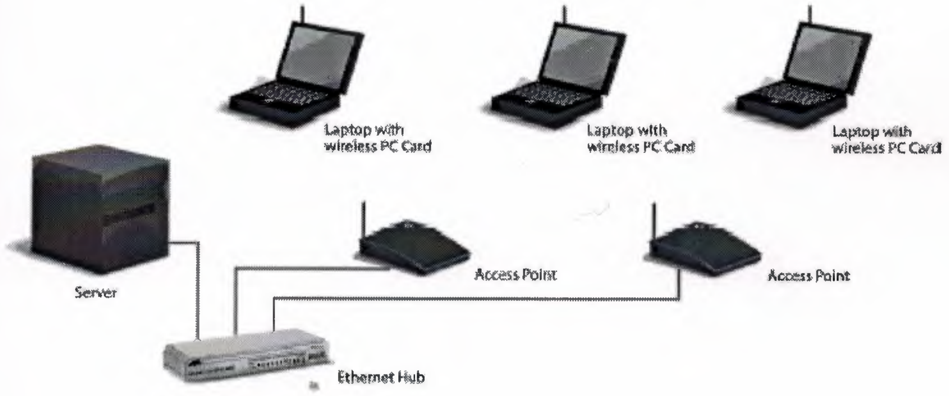

Laptop with wireless PC Card
Laptop with wireless PC Card
Laptop with wireless PC Card
Server
Access Point
Access Point
Ethernet Hub

Figure 1.8 Wireless Network

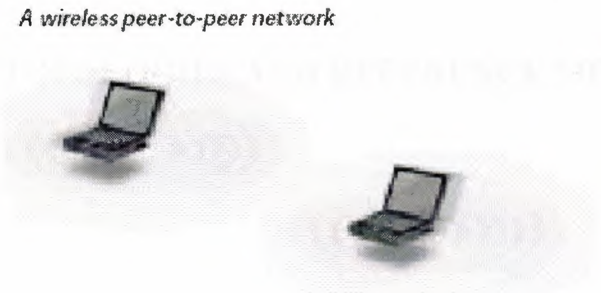


Figure 1.9 Wireless Peer-to-Peer Network

Now a days, we need Local Area Networks. We can have Local Area Networks in any offices and we can share information between desktops very easily. In order to make communication from component to another ISO (International Standards Organization) has defined a reference model known as OSI reference model, which helps in communication and we need some geometric arrangement for placing components called topologies which are explained in detail in the next chapter.

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

Network physical topologies are categorized into the following basic types:

2.2.1 Linear Bus Topology

This is the simplest and most common method of networking computers. The bus is a passive topology. It consists of a single cable called a trunk (also backbone or segment) that all nodes (file server, workstations, and peripherals) in a single line. It is also referred as broad cast topology. Another name for bus topology is a backbone arrangement because every computer or device is connected to a single cable. Ethernet and LocalTalk networks can use a linear bus topology. Most bus topologies use coaxial cables. This type of network is usually peer to peer and uses Thinnet (10base2) cabling. It is configured by connecting a "T-connector (also called British Naval Connector)"to the network adapter and then connecting cables to the T-connectors on the computers on the right and left. All ends of the cable must be terminated, that is plugged into a device such as a computer or terminator. At both ends of the chain the network must be terminated with a 50 ohm impedance terminator. . These networks are usually the easiest to put together for a small classroom or lab network but become unwieldy for larger networks. Figure 2.1 shows the simple linear bus topology.

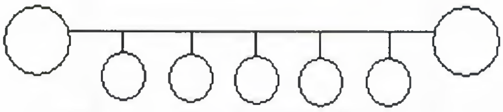


Figure 2.1 Simplified Linear Bus Topology

Figure 2.2 describes in detail about the bus topology

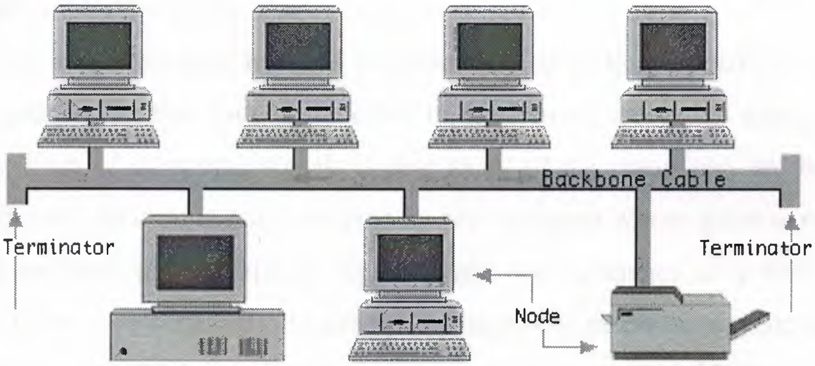


Figure 2.2 Linear Bus Topology

Figure 2.3 shows Bus topology..

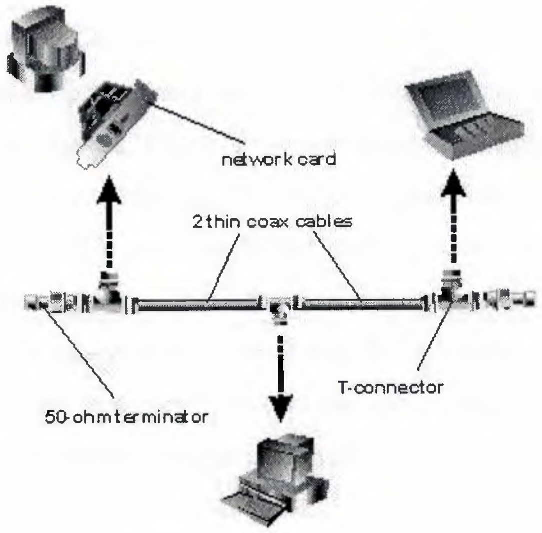


Figure 2.3 Bus Topology

- Communication on the Bus

Computer on a bus topology network communicate by addressing data to a particular computer and putting that data on the cable in the form of electronic signals. Network data in the form of electronic signals is sent to all of the computers on the network; however, the information is only accepted by the computer whose address matches the address is encoded in the original signal. Only one computer at a time can send messages. There is no standard measure for the impact of numbers of computers on any given network. On a bus, any device can communicate directly with any other device and all devices see these messages. This is called a "unicast". This odd word, "unicast," comes from the word "broadcast." A broadcast is sent to everybody; similarly, any device can send a single signal intended for all other devices on the wire. This is a "broadcast." A "mulitcast" is sent to several recipients, and a "unicast" is sent to just one recipient. To get point-to-point unicast communication going, however, there has to be some sort of address that identifies each device uniquely. This is called the MAC address. There also has to be some sort of mechanism to ensure that all devices don't try to transmit at the same time.

To transmit data between nodes. All the computers "listen" to the network all the time. Transmitting computer "listens" to see if it is in use. If not busy, transmitting computer sends a packet. All computers "see" the packet, but they only read it if addressed to them. If a collision is detected the transmitting computers wait a random time, and then tries again. Because only one node can broadcast at a time it needs a Protocol. As we know that the data, or electronic signal, is sent to the entire network, it will travel from one end of the cable to the other. If the signal were allowed to continue uninterrupted, it would keep bouncing back and fourth along the cable and prevent other computers from sending signals. Therefore signals must be stopped after it has a chance to reach the proper destination address. To stop the signal from bouncing, a component called a terminator is placed at each end of the cable to absorb free signals. Absorbing the free signal clears the signals so that other computers can send data. Every cable end on the network must be plugged into something. For example, a cable end could be plugged into computer or connector to extend the cable length. Any open cable ends-ends not plugged into something-must be terminated to prevent signal bounce.

- Advantages

1) Cheap, simple to set up.
2) Good for small networks.
3) Easy to connect a computer or peripheral to a linear bus.
4) Requires less cable length than a star topology.

- Disadvantages

1) A bus is costly to maintain.
2) If two computers try to transmit at the same time, a collision occurs.
3) Excess network traffic, a failure may affect many users, Problems are difficult to troubleshoot.
4) A disadvantage of the bus topology is that generally there must be a minimum distance between workstations to avoid signal interference.
5) Another disadvantage is that nodes must contend with each other for the use of the bus.
6) Simultaneous transmissions by more than one node are not permitted. This problem, however, can be solved by using one of several types of systems designed to control access to the bus.
7) Difficult to identify the problem if the entire network shuts down. Difficult to locate where the break in the cable is or which machine is causing the fault; a bus is also not

recommended when one device fails the rest of the LAN fails. This is referred as network being "down". The computers will still be able to function as stand-alone computers, but as long as the segment is broken they will not be able to communicate with each other.

8) Because only one computer at a time can send data on a bus network, network performance is affected by the number of computers attached to the bus. The more computers on the bus, the more computers there will be awaiting to put data on the bus, and the slower the network.

9) Terminators are required at both ends of the backbone cable.

10) Not meant to be used as a stand-alone solution in a large building.

11) The other problem that often develops in bus architectures is loss of one of the bus termination devices. In the case of 10Base2, this termination was a small electrical resister that cancelled echoes from the open end of the wire. If this terminator was damaged or removed, then every signal sent down the wire was met by a reflected signal. The result was noise and a seriously degraded performance.Both of these problems are avoided partially by using a central concentrator device such as a hub or a switch. In fact, new Ethernet segments are usually deployed by using such a device.

12) If one side holds the router that allows devices on the segment to get off, then the devices on the other side are effectively stranded. More serious problems can result if routers are on both sides of the break.

13) There is no easy way for the network administrator to run diagnostics on the entire network. Finally, the bus network can be easily compromised by an unauthorized network user, since all messages are sent along a common data highway. For this reason, it is difficult to maintain network security.

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 2.4 and 2.5 show the ring topologies.

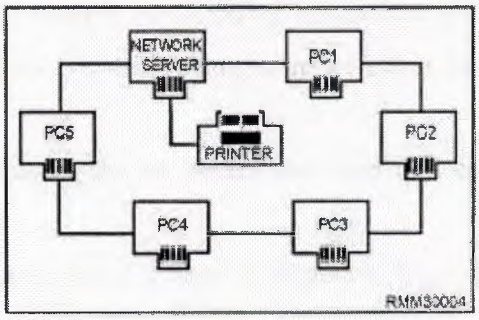


Figure 2.4 Ring Topology

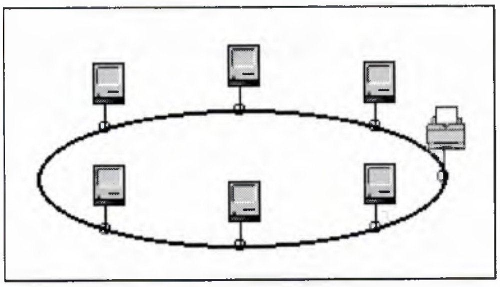


Figure 2.5 Ring Topology

- 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 2.6 shows simple star topology

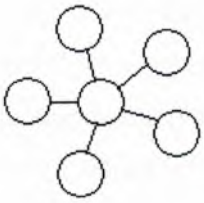


Figure 2.6 Simple Star Topology

Figure 2.7 shows star topology in more detail

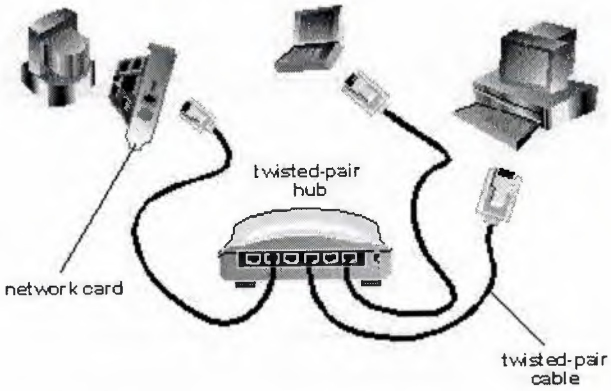


Figure 2.7 Detailed Star Topology

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 2.8 practical implement of star topology is shown.

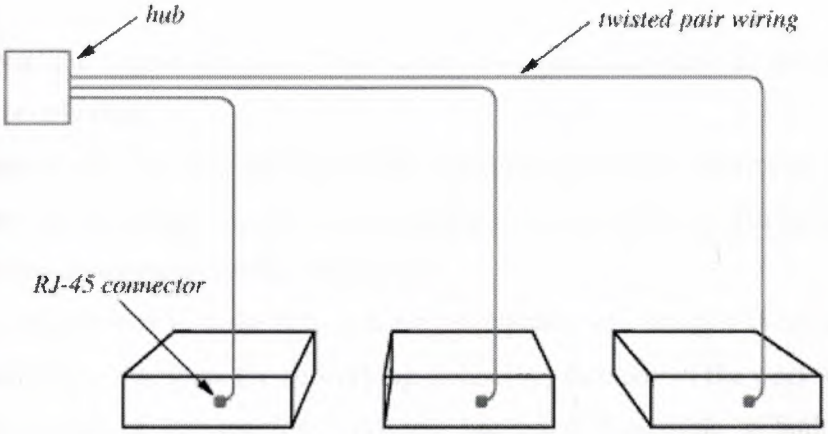


Figure 2.8 Star Topology in Practice

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

Figure 2.9 shows connection of hub to nodes

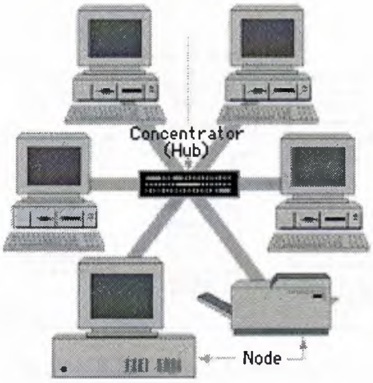


Figure 2.9 HUB is shown in the Star Topology

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 2.10 clearly defines the share of hard disk by other users.

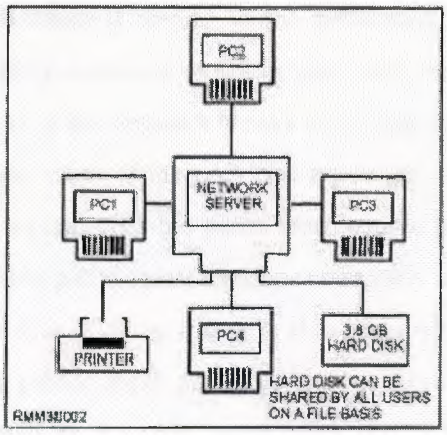


Figure 2.10 Hard Disk Sharing

- 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 concentrators.

2.2.4 Mesh Topology

A network topology in which there are at least two nodes with two or more paths between them. A meshed network can be either fully meshed or partially meshed. In a fully meshed network, every device is connected directly to every other device with no intervening devices. A partial mesh, on the other hand, has each device directly connected to several, but not necessarily all of the other devices. Fully connected mesh topology is also known as just fully connected topology. Mesh topologies use routers to determine the best path.

It is called mesh because it blends all the previously described methods into a single network that basically connects every device with each other. This method is complicated, but if any part of the network breaks down, the data can find other paths to reach its destination. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. (Recall that in a ring, although two cable paths exist, messages can only travel in one direction.) In addition to LANs some WANs, like the Internet, also employ mesh routing.

Clearly, defining a partial mesh precisely is a bit more difficult. Essentially, any network could be described as a partial mesh with this definition. Usually, a mesh describes a network of multiple point-to-point connections that can each send and receive in either direction. This definition excludes descriptions of both the ring and bus topologies because the ring circulates data in only one direction and the bus is not point-to-point. Figure 2.11 and 2.12 shows simple mesh topology.

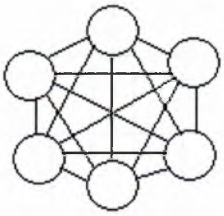


Figure 2.11 Simple Mesh Topology

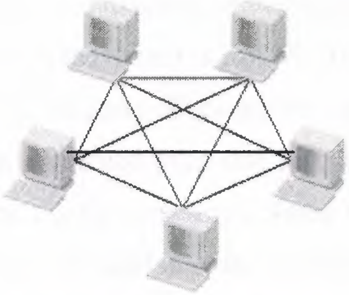


Figure 2.12 Mesh Topology

Since a mesh has every device connected to every other device with nothing in between, the latency on this sort of network is extremely low. Mesh networks aren't used because mesh networks are not very efficient.

Consider a fully meshed network with *N* devices. Each device has to have (*N*-1) connections to get to every other device. Counting all connections, the first device has (*N*-1) links. The second device also has (*N*-1) links, but the one back to the first device has already been counted, so that leaves (*N*-2). Similarly there are (*N*-3) new links for the third device, all the way down to (*N*-*N* = 0) for the last device (because all of its links were already counted). The easiest way to see how to add these devices up is to write it in a matrix, as shown in Table 2.1.

Table 2.1 Connections in a Mesh Network

	1	**2**	**3**	**4**	**...**	**N**
1	x	1	1	1		1
2		x	1	1		1
3			x	1		1
4				x		1
...					...	...
N						x

An "x" runs all the way down the diagonal of the matrix because no device talks to itself. The total number of boxes in the matrix is just *N2*. The number of entries along the diagonal is *N*, so there are (*N2-N*) links. But only the upper half of the matrix is important because each link is only counted once (the link from a →b is included, but not b →a, because that would be double counting). Since there is exactly the same number above the diagonal as below, the total number of links is just *N*(*N*-1)/2.

Making a fully meshed network with 5 devices requires 5(5-1)/2 = 10 links. That doesn’t sound so bad, but what happens if this number is increased to 10 devices? 10(9)/2 = 45 links. By the time you get to a small office LAN with 100 devices, you need 100(99)/2 = 4950 links.

Furthermore, if each of these links is a physical connection, then each of the 100 devices in that small office LAN needs 99 interfaces. It is possible to make all those links virtual--for example, with an ATM network. But doing so just moves the problem and makes it a resource issue on the ATM switching infrastructure, which has to keep track of every virtual circuit.

Figure 2.13 shows the practical connections in mesh topology.

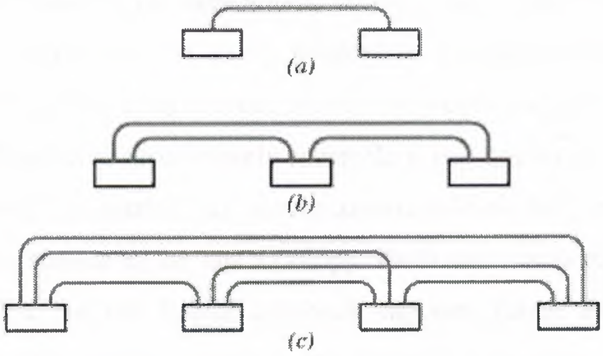


Figure 2.13 Mesh topology in practice

- 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 topologies integrate multiple star topologies together onto a bus. The distributed star or tree topology can provide many of the advantages of the bus and the star topologies. It connects workstations to a central point, called a hub. This hub can support several workstations or hubs which, in turn, can support other workstations. Distributed star topologies can be easily adapted to the physical arrangement of the facility site. If the site has a high concentration of workstations in a given area, the system can be configured to more closely resemble a star topology. If the workstations are widely dispersed, the system can use inexpensive hubs with long runs of shared cable between hubs, similar to the bus topology. Each hub functions as the "root" of a tree of devices. This bus/star hybrid approach supports future expandability of the network much better than a bus (limited in the number of devices due to the broadcast traffic it generates) or a star (limited by the number of hub ports) alone. It is a hybrid topology. Individual peripheral nodes are required to transmit to and receive from one other node only, toward a central node, and are not required to act as repeaters or regenerators. Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs. Figure 2.14 shows the simple tree topology.

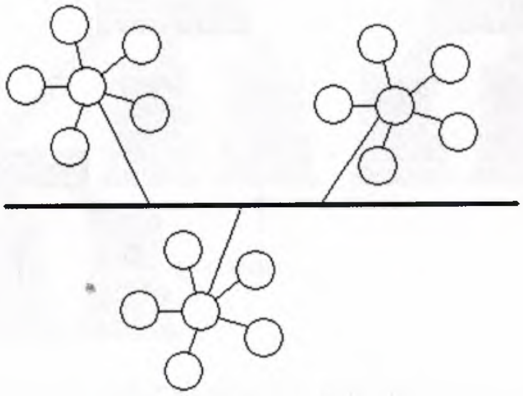


Figure 2.14 Simple Tree Topology

Figure 2.15 shows star topology in detail.

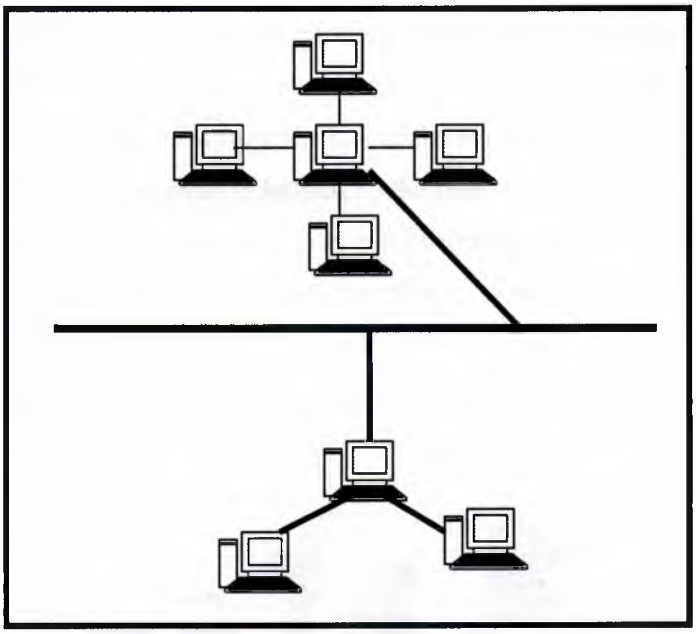


Figure 2.15 Tree (distributed star) Network Topology

In figure 2.16 Tree topology consisting of bus and star topologies is shown.

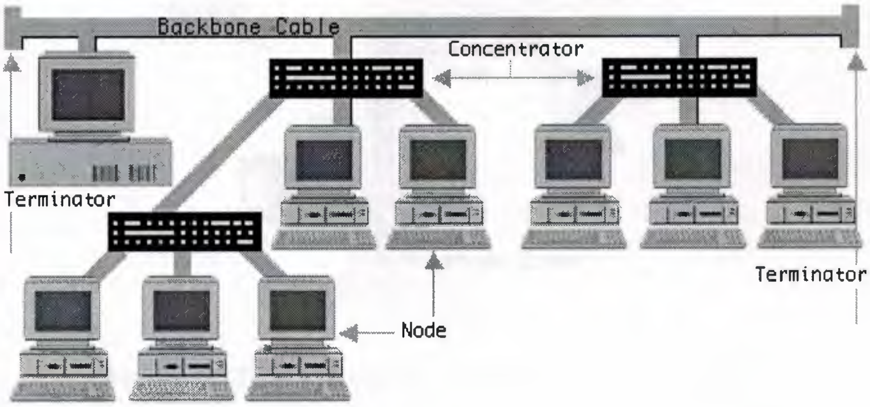


Figure 2.16 Tree Topology using Bus and Star Network Topologies

- 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.

Figure 2.17 shows the back bone cable in the tree topology

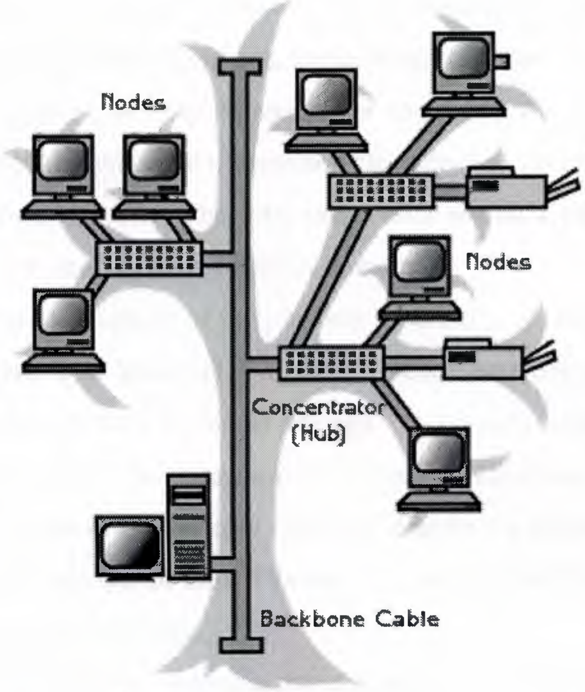


Figure 2.17 Tree Topology Showing Back Bone Cable

- 5-4-3-2-1 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 2.16, 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.

Further explained the 5-4-3-2-1 rule embodies a simple recipe for network design. It may not be easy to find examples in practice, but this rule neatly ties together several important elements of design theory.

To understand this rule, it's first necessary to understand the concepts of collision domains and propagation delay. Collision domains are portions of a network. When a network packet is transmitted over Ethernet, for example, it is possible for another packet from a different source to be transmitted close enough in time to the first packet to cause a collision on the wire. The total range over which a packet can travel and potentially collide with another is its collision domain.

Propagation delays are a property of the physical medium (*e.g.*, Ethernet). Propagation delays help determine how much of a time difference between the sending of two packets on a collision domain is "close enough" to actually cause a collision. The greater the propagation delay, the increased likelihood of collisions.

The 5-4-3-2-1 rule limits the range of a collision domain by limiting the propagation delay to a "reasonable" amount of time. The rule breaks down as follows:

5 - the number of network segments

4 - the number of repeaters needed to join the segments into one collision domain

3 - the number of network segments that have active (transmitting) devices attached

2 - the number of segments that do not have active devices attached

1 - the number of collision domains

Because the last two elements of the recipe follow naturally from the others, this rule is sometimes also known as the "5-4-3" rule for short.

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 2.18 shows the star bus network

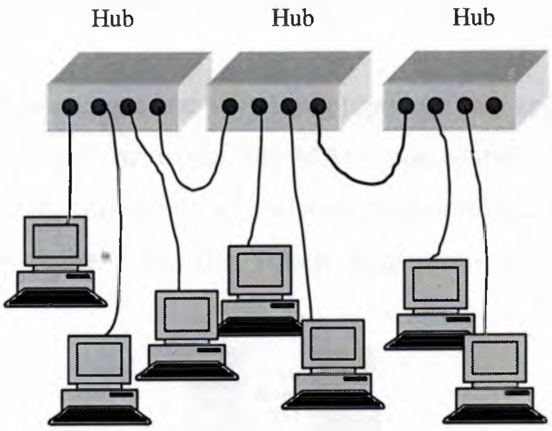


Figure 2.18 Star Bus Topology

- 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 2.19 describe about the star ring network

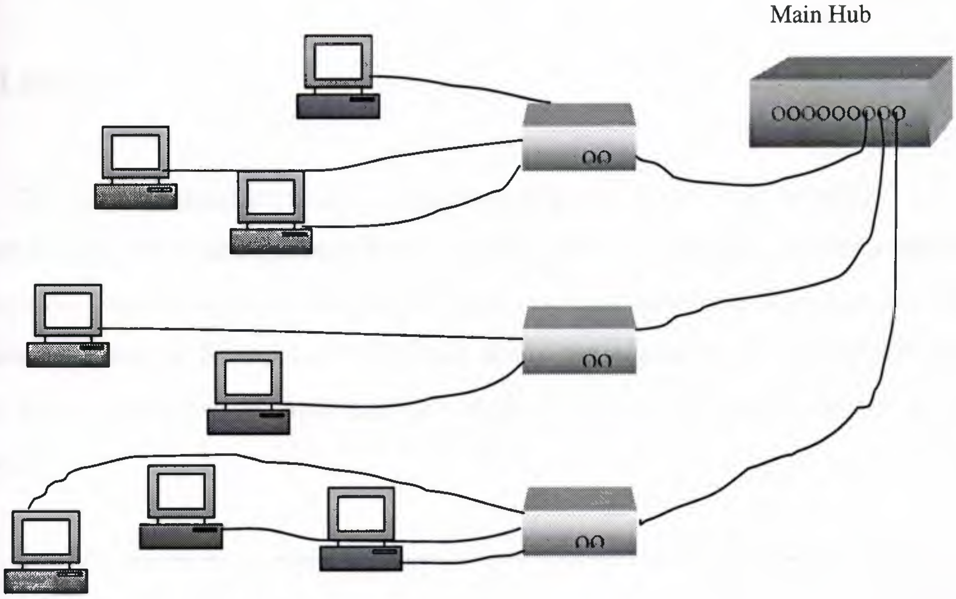


Figure 2.19 Star Ring Network

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 2.20. The Token Ring protocol uses a star-wired ring topology.

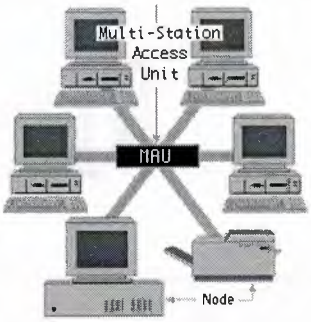


Figure 2.20 Star Ring Network

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 2.21 shows logical addresses correspond to the physical location of the computers.

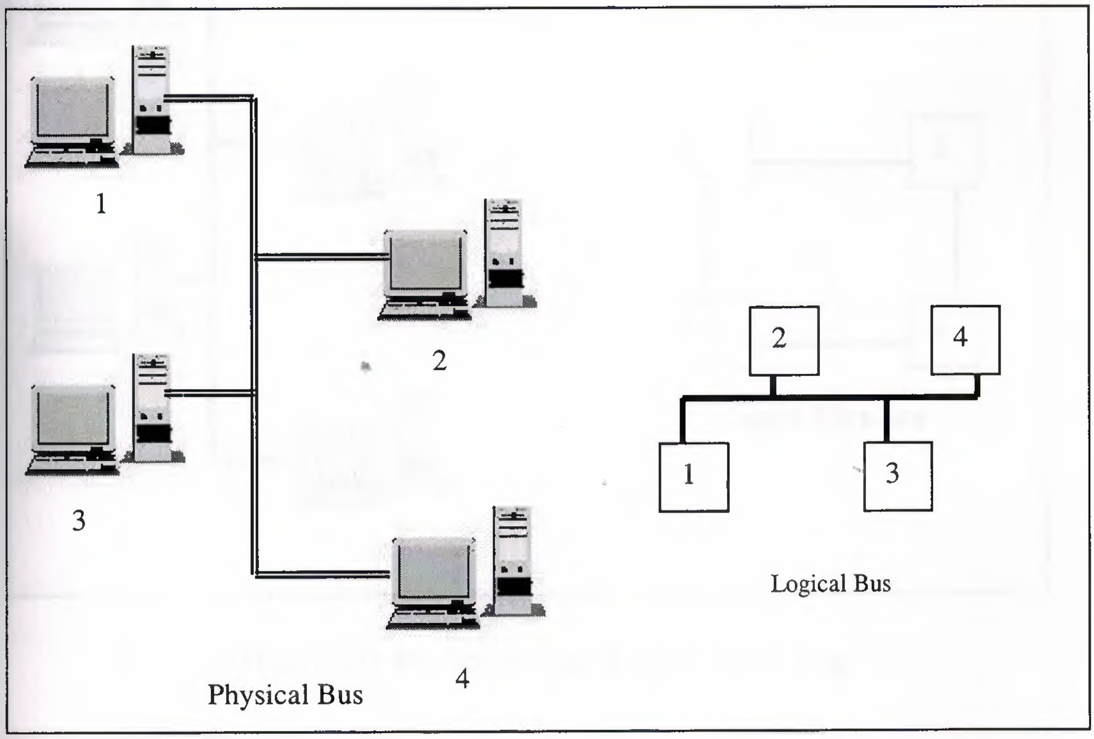


Figure 2.21 Physical and Logical Topologies

2.3.2 Token Ring

This scheme can be found on both linear bus and ring topologies. Each node has a unique address, and the addresses are accessed in a circular fashion. Notice that in a circular fashion. Notice that there isn't necessarily a correspondence between the logical addresses and the physical location of the computers relative to each other.

To transmit data between two computers:

- transmitting computer waits for the token to come round
- transmitting computer "captures" the token, and appends its packet to it
- the receiving computer reads the packet, and sets a bit to inform the transmitting computer that it has received the packet
- the transmitting computer receives the read packet, and erases the data

Figure 2.22 describes do not have the same correspondence to the linear bus layout

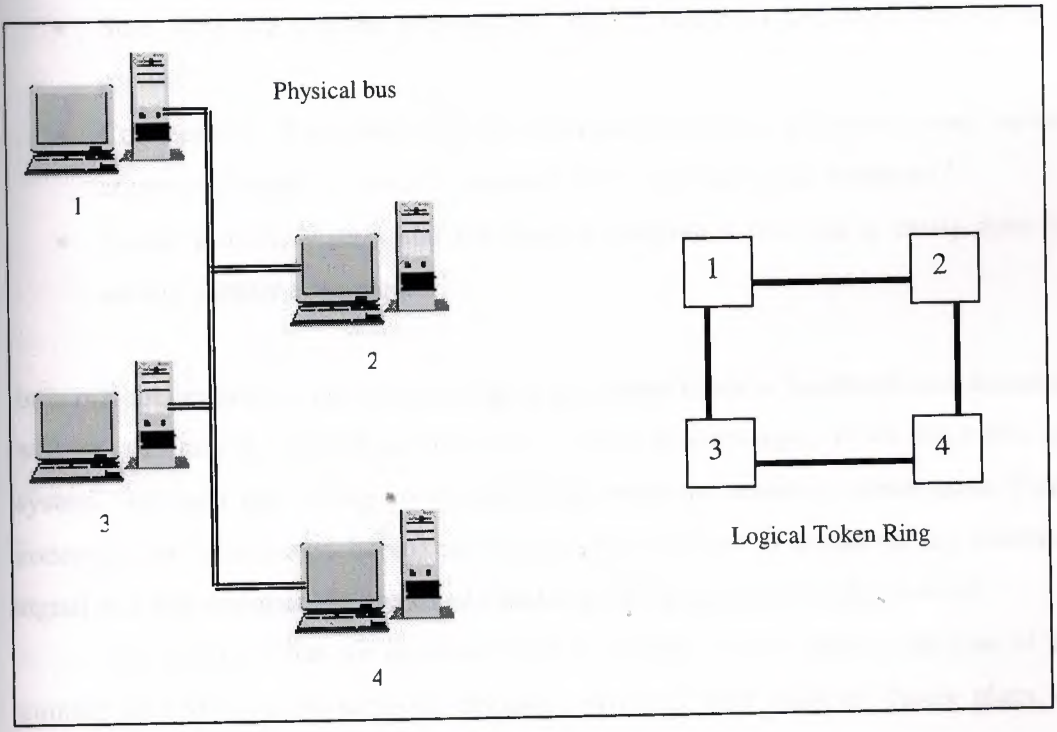


Figure 2.22 Physical Bus and Logical Token Ring

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-RM effort began in 1977 as a series of articles on development of a standard reference model for networking. In 1978, the OSI-RM was defined as a standard by the International Standards Organization (ISO). Standards for how products and protocols should operate were specified so that the services at each layer could function with adjoining layers. The lower three layers address host-to-host communication functions, and the upper four layers host-to-application communication functions. The protocols associated with the OSI-RM are known as the ISO protocol suite. The OSI-RM has seven layers. The OSI-RM is known as X.200 in the ISO universe. The principals that were applied to arrive at the seven layers are follows:

1) A layer should be created where a different level of abstraction is needed.
2) Each layer should perform a well defined function.
3) The function of each layer should be chosen with an eye toward defining internationally standardized protocols.

4) The layer boundaries should be chosen to minimize the information flow across the interfaces.

5) The number of layers large enough that distinct functions need not thrown together in the same layer out of same layer out of necessity, and small enough that the architecture does not become unwieldy.

The OSI-RM model is shown in the figure 2.23

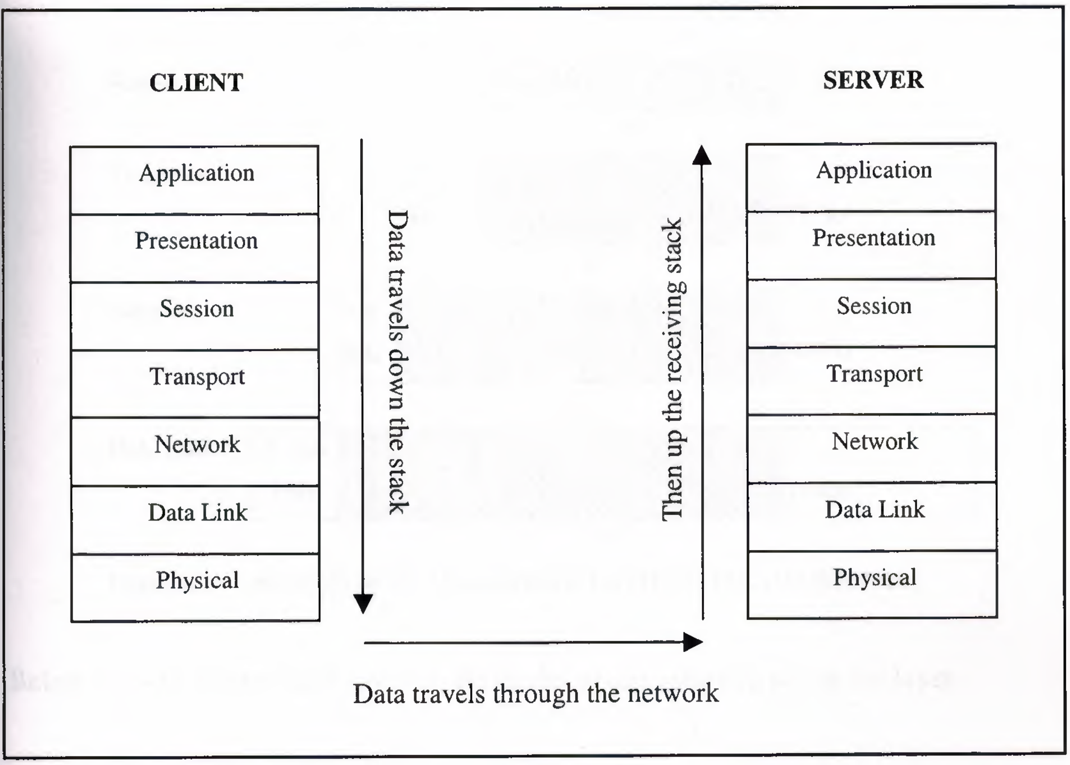
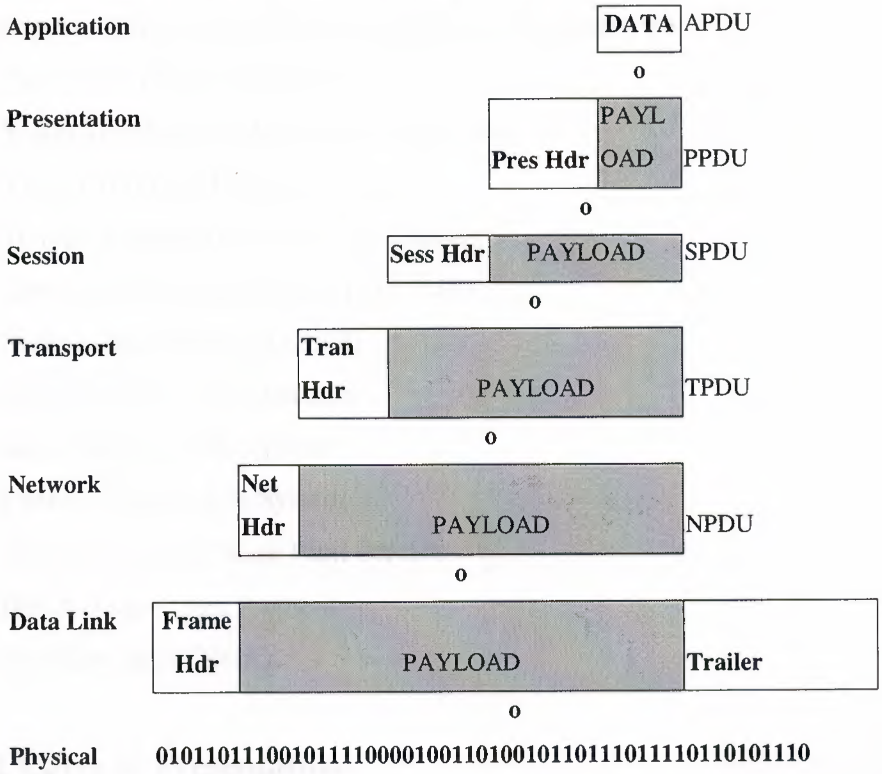

CLIENT
SERVER
Application
Presentation
Session
Transport
Network
Data Link
Physical
Data travels down the stack
Then up the receiving stack
Data travels through the network

Figure 2.23 OSI Reference Model

Each layer contains a Protocol Data Unit (PDU) and a Service Data Unit (SDU). PDUs are used for peer-to-peer conversations. SDUs are headers used by each layer to define what services are provided to the higher layer. Higher layer PDUs are encapsulated in lower layer PDUs. Encapsulation is the addition of lower layer headers to upper layer PDUs to form a lower layer PDU. Application data, Application PDU (APDU) is delivered to the Presentation layer. A Presentation header is applied and the Presentation PDU (PPDU) is created. This PPDU is passed to the Session layer, a Session header is applied and a Session PDU is created. The SPDU is passed to the Transport Layer, attach the Transport Header with pointer, i.e. Port, and a segment is created. Etc...Table 2.2 shows how higher layer PDUs are encapsulated in lower layer PDUs.

Table 2.2 Encapsulation of Higher Layer into Lower Layer



Below we will discuss each layer of the model in turn, starting top of the layer.

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.

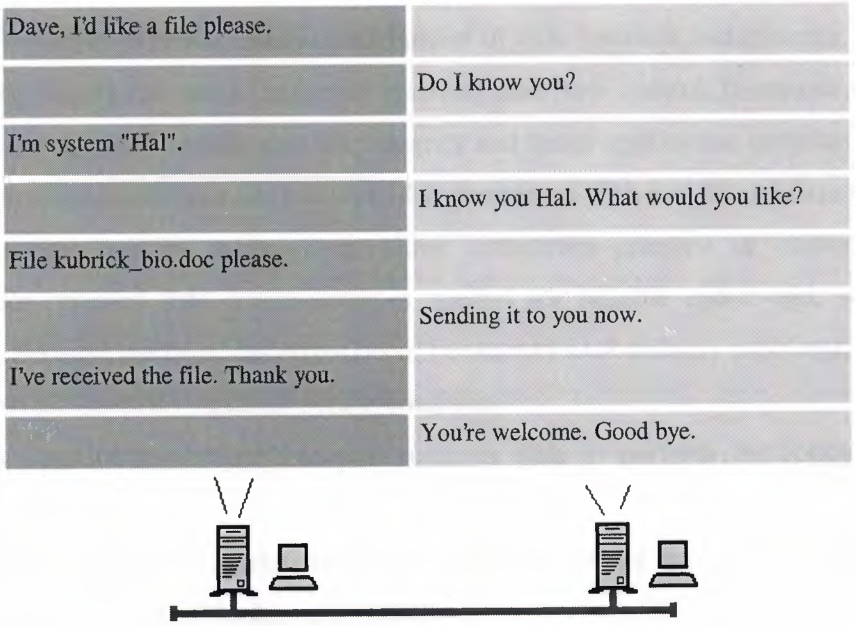
Protocols associated with this layer are the following:

- 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)

2.5.1.3 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). To understand communication between computers we have to look at the figure 2.24.

The figure 2.24 below shows the role the Session layer plays in coordinating upper level communication.



Dave, I'd like a file please.	
	Do I know you?
I'm system "Hal".	
	I know you Hal. What would you like?
File kubrick_bio.doc please.	
	Sending it to you now.
I've received the file. Thank you.	
	You're welcome. Good bye.

Figure 2.24 Role of Session Layer

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

2.5.1.4 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 (TPO)
- 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)

2.5.1.5 Layer 3: 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)

2.5.1.6 Layer 2: 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.

2.5.1.7 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.

2.5.2 The TCP/IP Reference Model

Here we will discuss the reference model used in the grandparent of all computer networks, the APRANET, and its successor, the world wide internet. The APRANET was a research network sponsored by the DoD (U.S. Department of Defense). It eventually connected hundred of universities and government installations using leased telephone lines. When satellite and radio networks were added later, the existing protocols had trouble internetworking with them, so new reference architecture was needed. Thus the ability to connect multiple networks together in a seamless way was one of the major design goals from the very beginning. This architecture was later became known as TCP/IP Reference Model, after its two primary protocols. It was first defined in (Cerf and Kahn, 1974). A later perspective is given in (Leiner et al.,1985). The design philosophy behind the model is discussed in (Clark, 1988).

The TCP/IP model does not exactly match the OSI model. There is no universal agreement regarding how to describe TCP/IP with a layered model but it is generally agreed that there are fewer levels than the seven layers of the OSI model. Most descriptions present from three to five layers. Figure 2.25 shows TCP/IP reference versus OSI reference model.

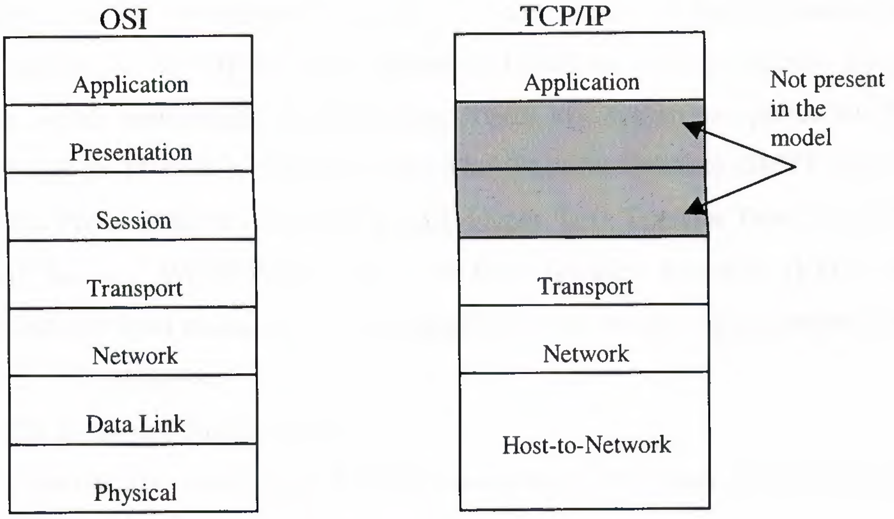


Figure 2.25 The TCP/IP reference model

Figure 2.26 shows the TCP/IP protocol family

Hyper Text Transfer Protocol (HTTP)	Simple Network Management Protocol (SNMP)	NFS XDR RPC	File Transfer Protocol (FTP)	Simple Mail Transfer Protocol (SMTP)	X Windows	Telnet Protocol (TELNET)	Layers 5 to 7
User Datagram Protocol (UDP)			Transmission Control Protocol (TCP)				Layer 4
Internet Protocol (IP) Internet Message Control Protocol (ICMP) Gateway-to-Gateway Protocols (EGP, IGP, RIP, OSPF)							Layer 3
No special TCP/IP Protocols provided In the LAN area Ethernet is predominantly used							Layers 1 & 2

Figure 2.26 TCP/IP Protocol Family

In this technical reference document the layers of the TCP/IP model are defined as follows:

- The Application Layer

  In TCP/IP the Application Layer also includes the OSI Presentation Layer and Session Layer. In this document an application is any process that occurs above the Transport Layer. This includes all of the processes that involve user interaction. The application determines the presentation of the data and controls the session. In TCP/IP the terms **socket** and **port** are used to describe the path over which applications communicate. There are numerous application level protocols in TCP/IP, including Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) used for e-mail, Hyper Text Transfer Protocol (HTTP) used for the World-Wide-Web, and File Transfer Protocol (FTP). Most application level protocols are associated with one or more port number. Some are described below.

1. PPP Point-to-Point Protocol -

A protocol for creating a TCP/IP connection over both synchronous and asynchronous systems. PPP provides connections for host to network or between two routers, It also has a security mechanism. PPP is well known as a protocol for connections over regular telephone lines using modems on both ends. This protocol is widely used for connecting personal computers to the internet.

2. SLIP Serial Line Internet Protocol -

A point-to-point protocol to use over a serial connection, a predecessor of PPP. There is also an advanced version of this protocol known as CSLIP (compressed serial line internet protocol) which reduce overhead on a SLIP connection by sending just a header information when possible, thus increasing packet throughput.

3. FTP File Transfer Protocol -

FTP enables transferring of text and binary files over TCP connection. FTP allows to transfer files according to a strict mechanism of ownership and access restrictions. It is one of the most commonly used protocols over the internet now days.

4. Telnet

Telnet is a terminal emulation protocol, defined in RFC854, for use over a TCP connection. It enables users to login to remote hosts and use their resources from the local host.

5. SMTP Simple Mail Transfer Protocol -

This protocol is dedicated for sending EMail messages originated on a local host, over a TCP connection, to a remote server. SMTP defines a set of rules which allows two programs to send and receive mail over the network. The protocol defines the data structure that would be delivered with information regarding the sender, the recipient (or several recipients) and, of course, the mail's body.

6. HTTP Hyper Text Transport Protocol -

A protocol used to transfer hypertext pages across the World Wide Web.

7. SNMP Simple Network Management Protocol -

A simple protocol that defines messages related to network management. Through the use of SNMP network devices such as routers can be configured by any host on the LAN.

8. ARPAddress Resolution Protocol -

In order to map an IP address into a hardware address the computer uses the ARP protocol which broadcast a request message that contains an IP address, to which the target computer replies with both the original IP address and the hardware address.

9. NNTP Network News Transport Protocol -

A protocol used to carry USENET posting between News clients and USENET servers.

- The Transport Layer

It is designed to allow peer entities on the source and destination hosts to carry on a conversation, the same as in the OSI transport layer. In TCP/IP there are two Transport Layer protocols. The first one, Transmission Control Protocol (TCP) guarantees that information is received as it was sent. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles the flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle. TCP uses the abstraction of ports (also referred to as sockets) to describe its transport scheme. These ports are used by hosts to establish virtual circuits (VCs) over which they can exchange upper layer protocol (ULP) data.

There are no rules for which ports are used to establish connections, but there are a set of "known" reserved ports that are used for services providing known application layer communication services. All ports under 1024 are reserved for server use. For example, the SMTP listens on TCP port 25, the telnet service listens on port 23, and HTTP, the protocol used for sending WWW data, listens on port 80. TCP establishes these client/server interapplication connections using a three-way handshake connection scheme. This process allows both sides to synchronize and establish the process endpoints. Figure 2.27 illustrates this connection process.

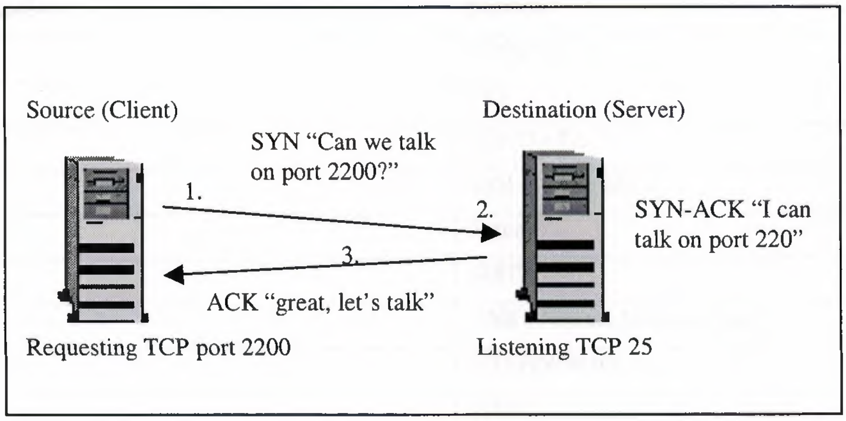


Figure 2.27 The TCP connection process

To setup a TCP connection, the client host sends a SYN (synchronization) packet to the application service port. The server host then sends a SYN and an ACK (acknowledgement) to the client's originating TCP port confirming that the connection is established. The client sends an ACK back to the server. Now the dedicated virtual circuit is established and full duplex data can take place. TCP keeps these processes organized by using the process endpoints to track the connections. The endpoint address is the process port number plus the IP address of the host that started the connection. In this example the process endpoint on server would be 192.160.33.20.2200 and the process endpoint on the client would be 90.16.44.8.25

The most common TCP service ports are listed in Table 2.3

Table 2.3 Common TCP Service Ports

Port Number	Service
1	TCPMUX
21	FTP
20	FTP-DATA
22	SSH (Secure Shell)
23	Telnet
25	SMTP
53	DNS (Domain Name Service)
80	HTTP(WWW)
139	WINS
119	NNTP (network News Transport Protocol)
110	POP3 (Post Office Protocol)
543	Klogin (Kerberos login)
544	Kshell (Kerberos Shell)
751	Kpasswd (Kerberos password)
750	Kerberos Server
512	Berkeley commands
513	Login
443	HTTPS secure WWW server
2105	Eklogin (encrypted Kerberos login)
2049	NFS (network File System)

The User Datagram Protocol (UDP) performs no end-to-end reliability checks. It is unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used one-shot, client-server type request reply queries and applications in which prompt delivery is more important than accurate deliver, such as speech or video. Like TCP, UDP has a set of reserved ports used for different application server exchange points.

The most commonly used ports are shown in Table 2.4

Table 2.4 Commonly used UDP Ports

Port Number	Service
49	TACACS authentication server
53	DNS (Domain Name service)
67	BOOTP server
68	BOOTP client
69	TFTP
137	NetBIOS name service
138	NetBIOS datagram service
123	NTP (network Time Protocol)
161	SNMP (Simple Network Management Protocol)
1645	RADIUS authentication server
1646	RADIUS accounting server
2049	NFS (Network File System)

- 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. All 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.

- 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 2.28 shows encapsulation.

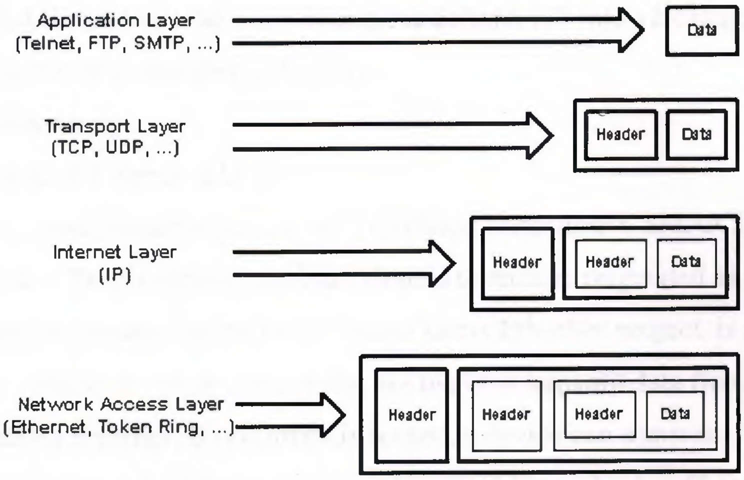


Figure 2.28 Encapsulation

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 2.29 shows IEEE 802 Project model (LAN reference model).

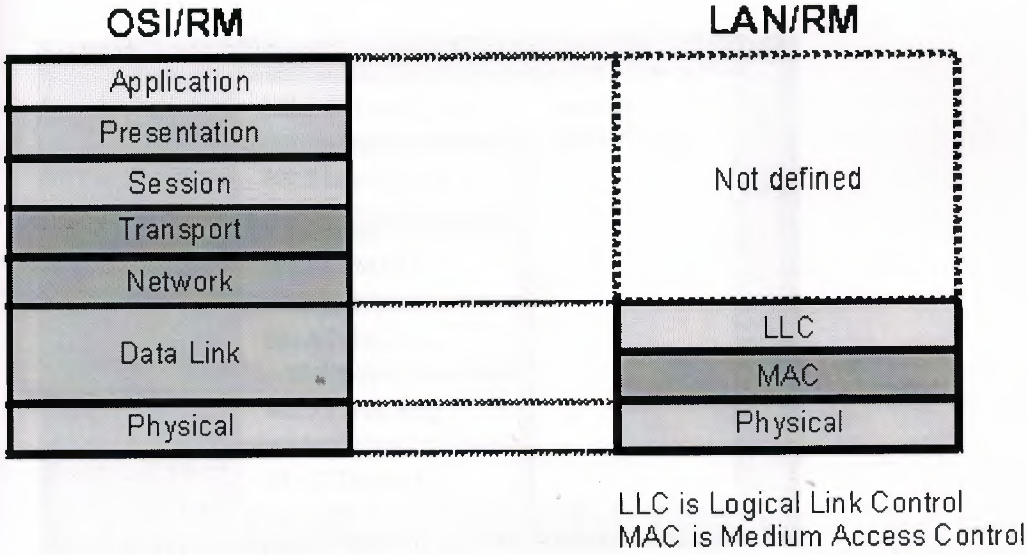


Figure 2.29 IEEE 802 /LAN Reference Model

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 Data link layer into two sub layers:

- Logical Link Control (LLC) – error and flow control

  The Logical Link Control sublayer manages data-link communication and defines the use of logical interface points, called service access points (SAPs). Other computers can refer to and use SAPs to transfer information from the Logical Link Control sublayer to the upper OSI layers. These standards are defined by 802.2.
- Media Access Control Sublayer – access control

  Media Access Control sublayer is the lower of two sublayers, providing shared access for the computers network adapter cards to the Physical layer. The Media Access Control layer communicates directly with the network adapter card and is responsible for delivering error-free data between two computers on the network.

Figure 2.30 below shows the IEEE 802 Logical Link Control and Media Access Control Standards.

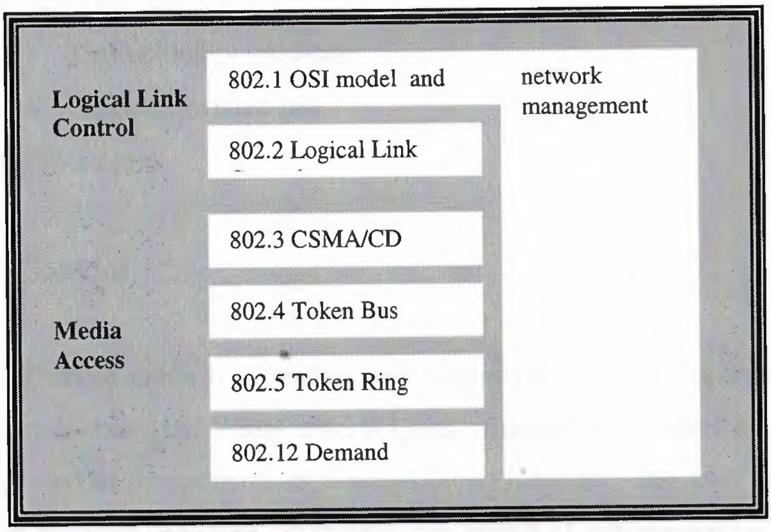


Figure 2.30 Project 802 Logical Link Control and Media Access Control Standards

Categories 802.3, 802.4, 802.5 and 802.12 define standards for both this sublayer and the OSI layer 1, the Physical layer.

3. LAN HARDWARE

3.1 LAN Cabling

The vast majority of networks today are connected by some sort of wire or cabling, cable is the medium that ordinarily connects network devices. Cable's ability to transmit encoded signals enables it to carry data from one place to another. These signals may be electrical as in copper cable or light pulses as in fiber-optic cable. There are variety of cable that can meet the varying needs and sizes of networks, from small to large.

Cabling can be confusing, Belden, a leading cable manufacturer, publishes a catalog that lists more than 2,200 types of cabling. Fortunately, only three major groups of cabling connect the majority of networks:

1) Coaxial
   - Thin (thinnet)
   - Thick (thicknet)
2) Twisted Pair
   - Unshielded twisted-pair
   - Shielded twisted-pair
3) Fiber-optic

3.1.1 Coaxial

Coaxial cable is a cabling type where two or more separate materials share a common central axis. While several types of networking cables could be identified as having coaxial components or constructions, there are only two cable types that can support network operation using only one strand of cabling with a shared axis. These are commonly accepted as the coaxial cables, and are divided into two main categories: thick and thin coaxial cable. Broadband transmission uses the same principles as cable TV and runs on coax. Broadband and cable TV take advantage of coax's ability to transmit many signals at the same time. Each signal is called a channel. Each channel travels along at a different frequency, so it does not interfere with other channels. Coax has a large bandwidth, which means it can handle plenty of traffic at high speeds. Other advantages include its relative immunity to electromagnetic interference (as compared to twisted-pair), its ability to carry signals over a significant distance, and its familiarity to many cable installers.

Coax cable has four parts . The inner conductor is a solid metal wire surrounded by insulation. A thin, tubular piece of metal screen surrounds the insulation. Its axis of curvature coincides with that of the inner conductor, hence the name coaxial. Finally, an outer plastic cover surrounds the rest. Figure 3.1 shows the various parts of coaxial cable.

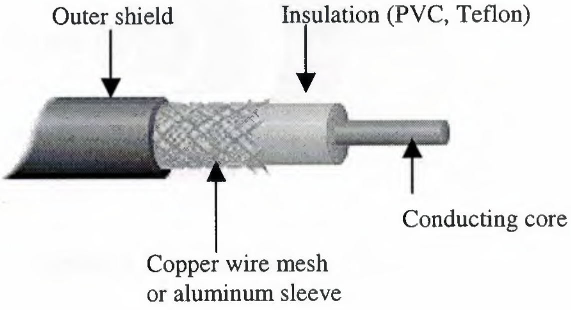


Figure 3.1 Coaxial Cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are: thick coaxial and thin coaxial.

3.1.1.1 Thick Coaxial (thicknet)

Thick coaxial is relatively rigid coaxial cable about 0.5 inch in diameter. Thick coaxial cable (also known as thick Ethernet cable, "thicknet," or 10BASE5 cable), is a cable constructed with a single solid core, which carries the network signals, and a series of layers of shielding and insulator material. The shielding of thick coaxial cable consists of four stages. The outermost shield is a braided metal screen. The second stage shield, working inward, is usually a metal foil, but in some brands of coaxial cable may be made up of a second screen. The third stage consists of a second braided shield followed by the fourth stage, a second foil shield. The various shields are separated by non-conductive insulator materials. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install. Figure 3.2 shows thick coaxial cable

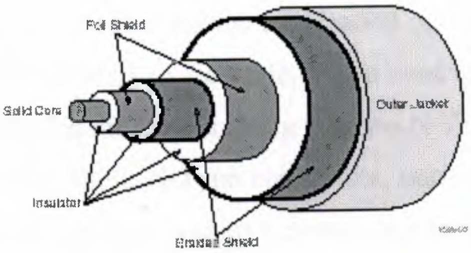


Figure 3.2 Thick Coaxial Cable

3.1.1.2 Thin Coaxial (thinet)

Thin coaxial is a flexible coaxial cable about 0.25 inch thick. Thin coaxial cable (also known as thin Ethernet cable, “thinnet,” “cheapernet,” RG-58 A/U, BNC or 10BASE2 cable) is a less shielded, and thus less expensive, type of coaxial cabling. Also used exclusively for Ethernet networks, thin coaxial cable is smaller, lighter, and more flexible than thick coaxial cable. The cable itself resembles (but is not identical to) television coaxial cable. Thin coaxial cable is made up of a single outer copper shield that may be braided or foil, a layer beneath that of non-conductive dielectric material, and a stranded center conductor. This shielding makes thin coaxial cable resistant to electromagnetic interference as the shielding of thick coaxial cable does, but does not provide the same extent of protection. Thin coaxial cable, due to its less extensive shielding capacity, can be run to a maximum length of 185 meters (606.7 ft).

Building Network Coax (BNC) connectors crimp onto a properly prepared cable end with a crimping tool. To prevent signal reflection on the cable, 50 Ohm terminators are used on unconnected cable ends. As with thick coaxial cable, thin coaxial cable allows multiple devices to connect to a single cable. Up to 30 transceivers may be connected to a single length of thin coaxial cable, spaced a minimum of 0.5 meter from one another. This minimum spacing requirement keeps the signals from one transceiver from interfering with the operation of others. The annular rings on the thin coaxial cable are placed 0.5 meter apart, and are a useful guide to transceiver placement.

Coaxial Cable Components

a) N-Type:

N-Type connectors are used for the termination of thick coaxial cables and also for the connection of transceivers to the cable. When used to provide a transceiver tap, the coaxial cable is broken at an Annular Ring and two N-Type connectors are attached to the resulting bare ends. These N-Type connectors, once in place, are screwed onto barrel housing. The barrel housing contains a center channel that the signals of the cable are passed across, and a pin or cable that contacts this center channel, providing access to and from the core of the coaxial cable. The pin that contacts the center channel is connected to the transceiver assembly and provides the path for Ethernet transmission and reception. Figure 3.3 shows the N-Type connector

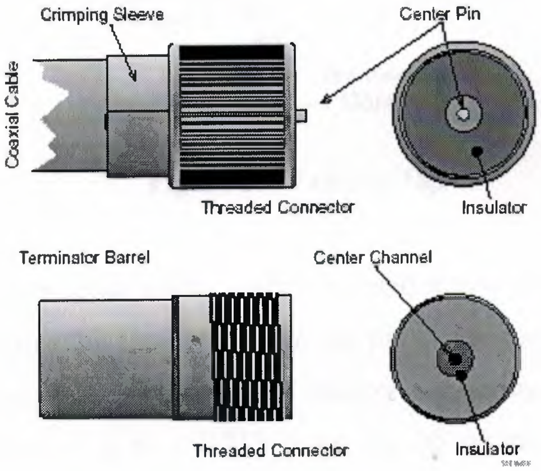


Figure 3.3 N-Type Connector and Terminator

b) Non-Intrusive:

Tapping a thick coaxial cable may be done without breaking the cable itself. The non-intrusive, or "vampire" tap, inserts a solid pin through the thick insulating material and shielding of the coaxial cable. The solid pin reaches in through the insulator to the core wire where signals pass through the cable. By contacting the core, the pin creates a tap. The signals travel through the pin to and from the core. Non-Intrusive taps are made up of saddles, which bind the connector assembly to the cable, and tap pins, which burrow through the insulator to the core wire. Non-Intrusive connector saddles are clamped to the cable to hold the assembly in place, and usually are either part of, or are easily connected to, an Ethernet transceiver assembly. Figure 3.4 shows vampire tap.

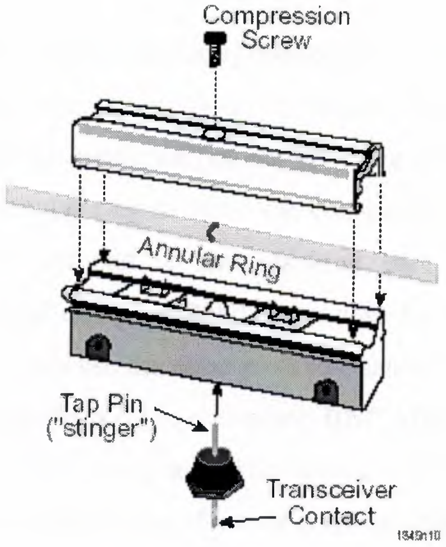


Figure 3.4 Vampire Tap

The non-intrusive tap's cable saddle is then inserted into a transceiver assembly. The contact pin, that carries the signal from the tap pin's connection to the coaxial cable core, makes a contact with a channel in the transceiver housing. The transceiver breaks the signal up and carries it to a DB15 connector, to which an AUI cable may be connected. Figure 3.5 describes the cable saddle and transceiver assembly.

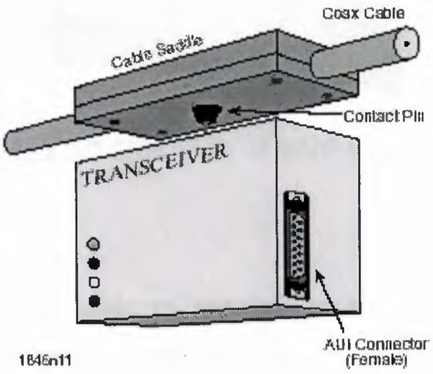


Figure 3.5 Cable Saddle and Transceiver Assembly

c) BNC:

The BNC (British Naval Connector) connector, used in 10BASE2 environments, is an intrusive connector much like the N-Type connector used with thick coaxial cable (described above). The BNC connector (shown in Figure 4-12) requires that the coaxial cable be broken at an annular ring to make the connection. Two BNC connectors are either screwed onto or crimped to the resulting bare ends. Cabletron Systems recommends the use of the crimp-on BNC connectors for more stable and consistent connections. BNC connectors use the same pin-and-channel system to provide a contact that is used in the thick coaxial N-Type connector. BNC Male connectors are attached to BNC female terminators or T-connectors. The outside metal housing of the BNC male connector has two guide channels that slip over corresponding locking key posts on the female BNC connector. When the outer housing is placed over the T-connector or terminator locking keys and turned, the connectors will snap securely into place. BNC connectors are shown in figure 3.6 and figure 3.7

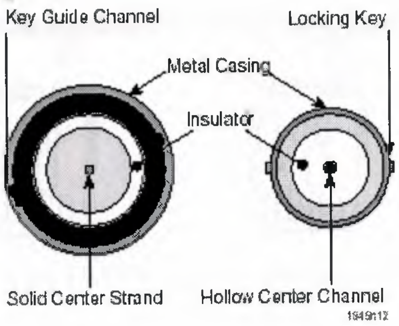


Figure 3.6 BNC Connectors

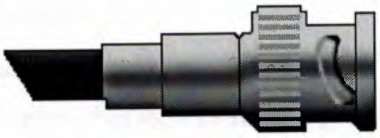


Figure 3.7 Side View of BNC Connector

d) T-Connector:

Connections from the cable to network nodes are typically made using T-connectors, which provide taps for additional runs of coaxial cable to workstations or network devices. T-connectors, as shown in Figure 3.8 and 3.9, below, provide three BNC connections, two of which attach to Male BNC connectors on the cable itself and one of which is used for connection to the Female BNC connection of a transceiver or Desktop Network Interface Card (DNI or NIC) on a workstation.

Figure 3.8 T-Connectors

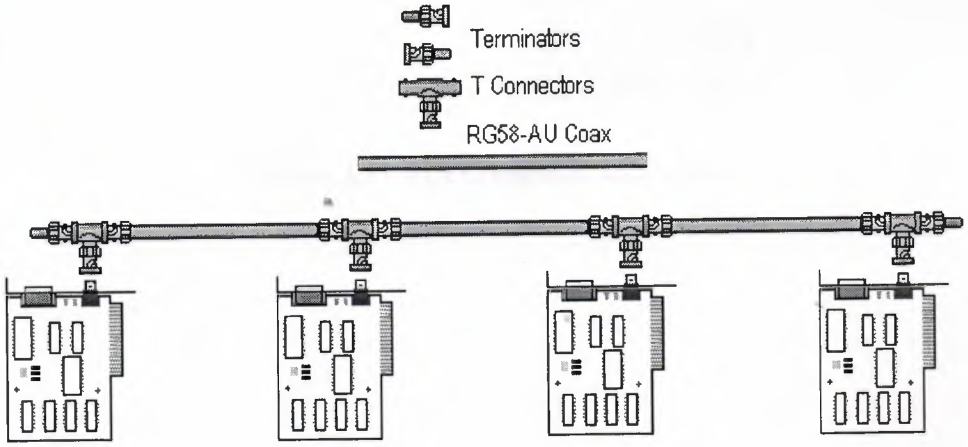


Figure 3.9 T-Connectors Implementation

e) AUI connectors (DB15 connectors):

10Base5 wire is connected not by BNC connectors but by AUI connectors. AUI connectors are a DB15 connector, that is, a D-shaped plug with 15 pins. These look just like RS-232 modem connectors, only about half as broad. These are common on equipment such as routers. Figure 3.10 and 3.11 shows AUI connectors

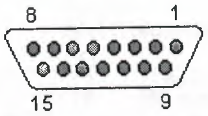


Figure 3.10 AUI Connector

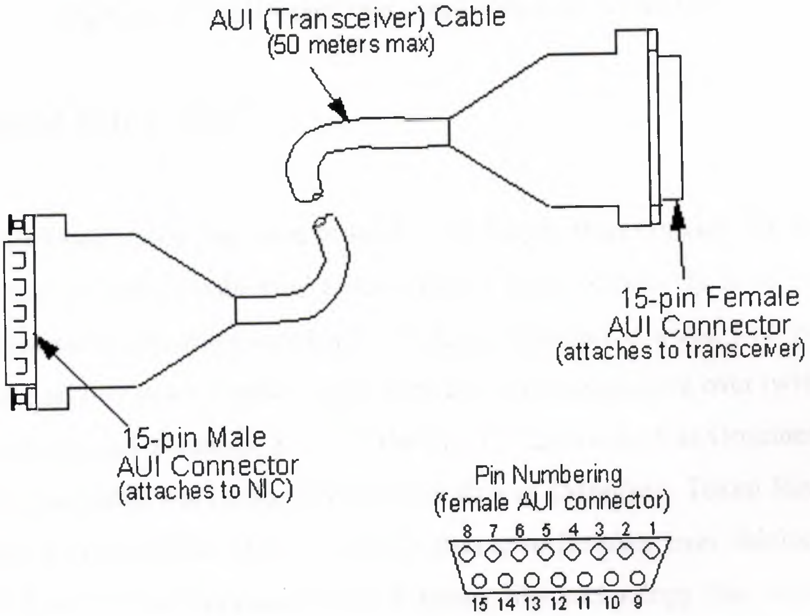


Figure 3.11 AUI Connector with Cable

In figure 3.12 AUI connector connected to Ethernet card.

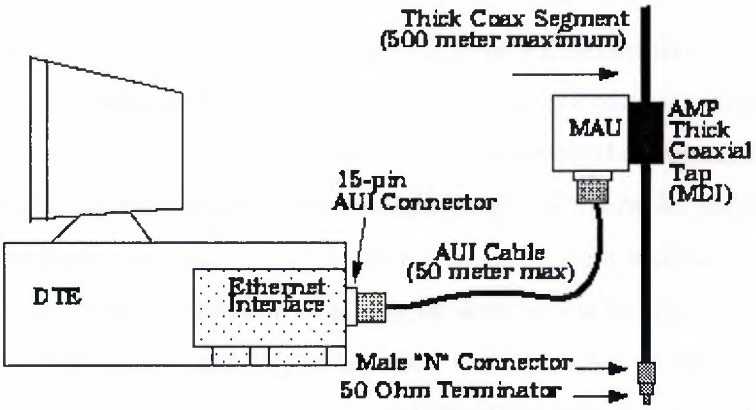


Figure 3.12 AUI Connector connected to Ethernet Card

3.1.2 Twisted Pair Cable

Twisted-pair cable has been around a lot longer than coaxial, but it has been carrying voice, not data. Unshielded twisted-pair is used extensively in the nationwide telephone system. Practically every home that has telephones is wired with twisted-pair cable. In the past few years, vendors have been able to transmit data over twisted-pair at reasonable speeds and distances. Some of the first PC LANs, such as Omninet or 10Net, used twisted-pair cable but could only transmit data at 1Mbit/sec. Token Ring, when it was introduced in 1984, was able to transmit data at 4Mbits/sec over shielded twisted-pair. In 1987, several vendors announced Ethernet-like technology that could transmit data over unshielded twisted-pair, but computers can only be about 300 feet apart, not the 2,000 feet allowed by thick coax. Recent developments in technology make it possible to run even 16Mbit/sec Token Ring and 100Mbit/sec FDDI traffic over unshielded twisted-pair.

Twisted-pair offers some significant benefits. It's lighter, thinner, more flexible, and easier to install than coax or fiber-optic cable. It's also inexpensive. It is therefore ideal in offices or work groups that are free of severe electromagnetic interference.

Although there are a variety of types of twisted-pair cable types, shielded (and unshielded are the two most important.

3.1.2.1 Unshielded Twisted pair (UTP)

Unshielded Twisted Pair cabling (referred to here as UTP, but also may be termed copper wire, 10BASE-T wire, Category 3, 4, or 5 Ethernet wire, telephone cable, or twisted pair without shielded or unshielded qualifier) is commonly made up of two, four, or 25 pairs of 22, 24, or 26 AWG unshielded copper solid or stranded wires. These pairs of wires are twisted together throughout the length of the cable, and are broken up into transmit and receive pairs. The UTP cable used in network installations is the same type of cable used in the installation of telephone lines within buildings. UTP cabling is differentiated by the quality category of the cable itself, which is an indicator of the type and quality of wire used and the number of times the wires are twisted around each other per foot. The categories range from Category 1 to Category 5, with Category 5 cabling being of the highest quality. Unshielded twisted pair is shown in figure 3.13

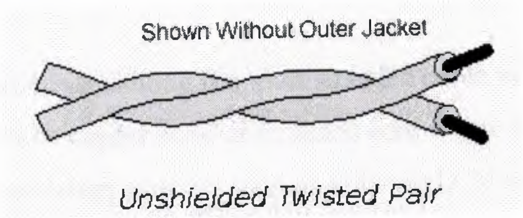


Figure 3.13 Unshielded Twisted Pair Cable

The wires that make up a length of UTP cable are numbered and color coded. These color codes allow the installer of the networking cable to determine which wires are connected to the pins of the RJ45 ports or patch panels. The numbering of the wires in EIA/TIA standard cables is based on the color of the insulating jacket that surrounds the core of each wire.

The standard five categories of UTP are:

- Category 1

  This refers to traditional UTP telephone cable which can carry voice but not data. Most telephone cable prior to 1983 was category one cable.

- Category 2

  This category certifies UTP cable for data transmission up to 4 Mbs (megabits per second). It consists of four twisted pairs.

- Category 3

This category certifies UTP cable for data transmission up to 10 Mbs. It consists of four twisted-pairs and four twists per second.

- Category 4

  This category certifies UTP cable for data transmission up to 16 Mbs. It consists of four twisted-pairs.

- Category 5

  This category certifies UTP cable for data transmission up to 100 Mbs. It consists of four twisted-pairs of copper wire.

Most telephones use a type of UTP. IN fact, one reason why UTP is so popular because many building are pre-wired for twisted-pair telephone systems. The potential problem in cabling is cross talk. Crosstalk is defined as the signals from one line getting mixed with signals from other line. UTP is particularly susceptible to cross talk.

3.1.2.2 Shielded Twisted pair (STP)

Shielded Twisted Pair cabling is a multistranded cable most often constructed of eight 26 AWG conductive copper solid or stranded core wires. Each wire is surrounded by a non-conductive insulating material such as Polyvinyl Chloride (PVC). These wires are twisted around one another in a specific arrangement to form pairs. The pairs are made up of associated wires - transmit wires are paired with transmit wires, receive wires are paired with receive wires. Each pair in the STP cable is then surrounded by a metallic foil shield that runs the length of the cable. Some types of STP incorporate an additional braided or foil shield that surrounds each of the shielded pairs in the cable. The overall cable is wrapped in an insulating jacket which covers the shields and holds the wires together. Figure 3.14 shows shielded twisted pair cable

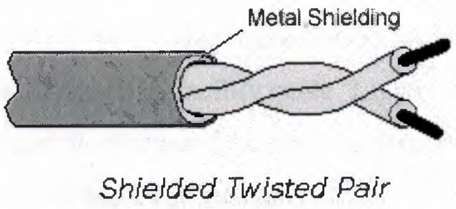


Figure 3.14 Shielded Twisted Pair Cable

Twisting the pairs together throughout the cable helps to reduce the effects of externally-induced electrical noise on the signals that pass through the cable. In each pair, one wire carries the normal network signal, while its associated wire carries a copy of the transmission that has been inverted. The twisting of associated pairs helps to reduce the interference of the other strands of wire throughout the cable. This is due to the method of transmission used with twisted pair transmissions. STP cabling is available in several different arrangements and construction styles, called Types. The type definitions are based on IBM cabling system. STP cabling that may be used in Token Ring environments falls into four types Type 1, Type 2, Type 6, and Type 9.

Type 1 STP consists of two pairs of solid 22 AWG copper strands. Each strand, approximately 0.02 inches thick, is surrounded by a layer of insulation. The characteristics of the insulation is determined by the fire resistance construction of the cable (plenum cable is thicker and made with slightly different material than normal PVC cabling).The individual wires are twisted into pairs. The pairs that are formed by this twisting are then surrounded by a mylar foil shield. These shielded pairs are then laid alongside one another in an overall braided metal shield. The shield containing the twisted pairs is then surrounded by a tight outer covering. Type 1 STP is heavy and rather inflexible, but provides excellent resistance to interference and noise due to its construction characteristics. Type 1 STP is most commonly used as a facility cabling, while more flexible cabling is used for jumper cables and patch panel connections.

IBM Type 2 cable is constructed in much the same fashion as Type 1 cable. The two central shielded pairs and the overall braided shield which surrounds them are constructed of the same materials, and then two additional pairs of AWG 22 insulated solid copper wires are laid outside the braided shield before the whole cable is surrounded by the tight outer covering. These outer wires may be used to carry telephone traffic, as the shields surrounding the inner, network wires is intended to eliminate the interference that might otherwise occur between the inner and outer pairs. The added pairs of wire in a Type 2 cable make it even less flexible than Type 1 cable. For this reason, it is typically used as facility cable. Lighter-gauge, more flexible cable types, such as Types 6 and 9, discussed below, are frequently used as patch cables between networking hardware and Type 2 cable.

Type 6 cable uses the same dual-shielded construction that Type 1 and Type 2 cable use, but the materials used in the construction are of a narrower gauge. The wires that make up the twisted pairs in a Type 6 cable are constructed of 26 AWG stranded conductors. The construction materials used in Type 6 cabling make it a much more flexible form of STP, but greatly reduce the cable's ability to carry network signals over long distances. Type 6 cable is intended for use as jumper or patch panel cabling only.

Type 9 cable is similar in construction to Type 6 cable, and is intended to be used for the same purposes. The center strands of a Type 9 cable are made of either solid or stranded 26 AWG conductors.

Twisted Pair Component Components

a) RJ45:

The RJ45 connector is a modular, plastic connector that is often used in UTP cable installations. It is similar to RJ-11 telephone connector. Although they look alike at first glance, there are crucial differences between them. The RJ45 is a keyed connector, designed to be plugged into an RJ45 port only in the correct alignment. The connector is a plastic housing that is crimped onto a length of UTP cable using a custom RJ45 die tool. The connector housing is often transparent, and consists of a main body, the contact blades or "pins," the raised key, and a locking clip and arm. Figure 3.15 shows RJ-45 connector

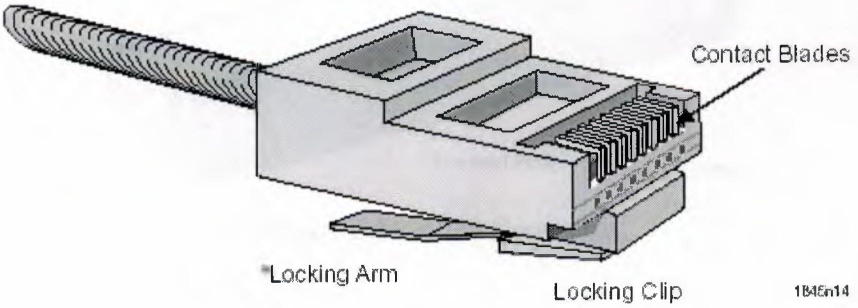


Figure 3.15 RJ-45 Connector

The locking clip, part of the raised key assembly, secures the connector in place after a connection is made. When the RJ45 connector is inserted into a port, the locking clip is pressed down and snaps up into place. A thin arm, attached to the locking clip, allows the clip to be lowered to release the connector from the port.

b) RJ21 (Telco):

The RJ21 or "Telco" connector is another standard 10BASE-T connector type. The RJ21 connector is a D-shaped metal or plastic housing that is wired and crimped to a UTP cable made up of 50 wires, a 25-pair cable. The RJ21 connector can only be plugged into an RJ21 port. The connector itself is sizable, and the cables that it connects to are often quite heavy, so the RJ21 relies on a tight fit and good cable management practices to keep itself in the port. Some devices may also incorporate a securing strap that wraps over the back of the connector and holds it tight to the port. The RJ21 is used in locations where 25-pair cable is being run either to stations or to an intermediary cable management device such as a patch panel or punchdown block. Due to the bulk of the 25-pair cable and the desirability of keeping the wires within the insulating jacket as much as possible, 25-pair cable is rarely run directly to Ethernet stations. The RJ21 connector, when used in a 10BASE-T environment, must use the EIA/TIA 568A pinout scheme. RJ-21 connector is shown in figure 3.16

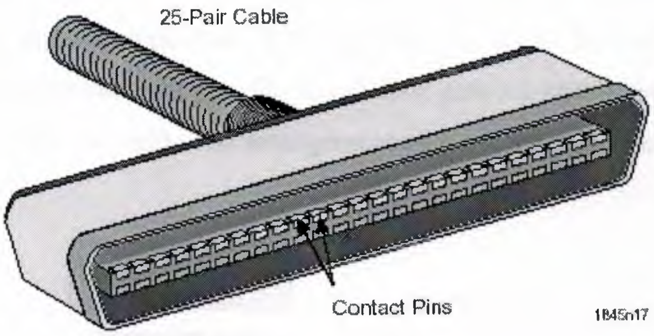


Figure 3.16 RJ-21 Connector

c) Medium Interface Connector (MIC):

The Medium Interface Connector is a genderless connector that is designed to be used with IBM Type 6 and Type 9 STP cabling. The MIC connector may also be used on Type 1 or Type 3 STP cabling. The design of the MIC connector allows it to be properly and securely connected to any other Token Ring MIC connector. It is made up of a plastic outer shell and four gold-plated contacts arranged in two rows of two each, as shown in Figure 3.17

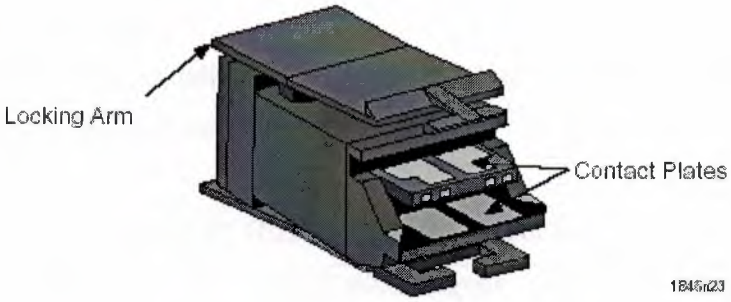


Figure 3.17 Medium Interface Connector

d) DB9:

The DB9 connector is a smaller standard connector for IEEE 802.5 networking applications, typically used for desktop and networking hardware connections. It is used in locations where a sturdy connection to STP cabling is required, but the use of MIC connectors is either impossible or undesirable. The DB9 cabling is usable on all types of STP cabling, but is most commonly found on jumper cabling such as IBM Types 6 and 9. The DB9 connector is a metal or composite shell with nine pins or channels at the end of the connector, arranged in two staggered rows. The pins are numbered from one to nine, beginning with the upper row of five pins or channels, that are numbered one to five, starting from the far right pin. The lower four pins are numbered from six to nine, beginning also at the far right. The arrangement of pins in the DB9 connector is shown in figure 3.18.

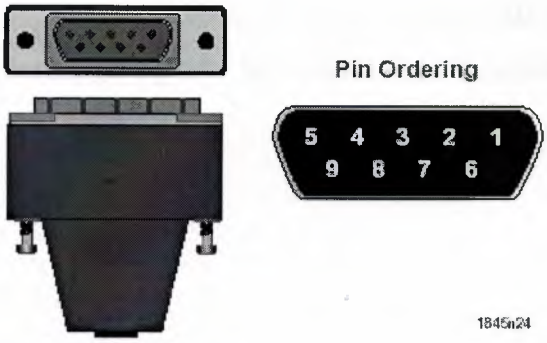


Figure 3.18 DB9 Connector

The male DB9 connector housing, or shell, also incorporates two securing screws. These screws are used to secure the DB9 connector to a female DB9 connector and hold it in place. The screws of a DB9 connector should always be used to ensure a solid connection between two connectors, otherwise, disconnection of the cable or damage to the connectors may result.

The connection of individual wires of a UTP cable to the pins of an IEEE 802.5 compliant RJ45 connector are given in Table 3.1

Table 3.1 IEEE 802.5 RJ45 Pinout for UTP

Wire Color	**IEEE 802.5 Signal**	**RJ45 Pinout**
White/Orange	TX-	3
Blue	RX+	4
White/Blue	RX-	5
Orange	TX+	6

3.1.3 Fiber Optic Cable

A technology that uses glass (or plastic) threads (fibers) to transmit data. A fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves.

Fiber optics has several advantages over traditional metal communications lines:

- Fiber optic cables have a much greater bandwidth than metal cables. This means that they can carry more data.
- Fiber optic cables are less susceptible than metal cables to interference.
- Fiber optic cables are much thinner and lighter than metal wires.
- Data can be transmitted digitally (the natural form for computer data) rather than analogically

Fiber optic cable is shown in figure 3.19

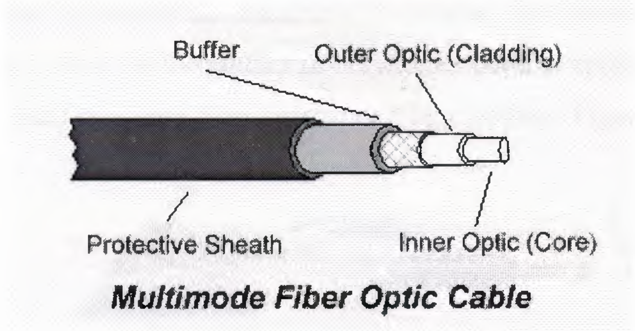


Figure 3.19 Fiber Optic Cable

Fiber cable consists of the following:

- Core - Thin glass center of the fiber where the light travels
- Cladding - Outer optical material surrounding the core that reflects the light back into the core
- Buffer coating - Plastic coating that protects the fiber from damage and moisture

Fiber-optics has been touted as the answer to all the problems of copper cable. It can carry voice, video, and data. It has enormous bandwidth and can carry signals for extremely long distances. Because it uses light pulses, not electricity to carry data, it is immune to electromagnetic interference. It is also more secure than copper cable, because an intruder cannot eavesdrop on the signals, but must physically tap into the cable. To get at the information inside, a device must be attached, and the light level will subsequently decrease.

Despite its many advantages, fiber-optic's deployment in the LAN has been slow. According to Dataquest figures, by 1993, fiber-optics held only 1.4 percent of the LAN market. Cable installer's experience and fiber's high cost is holding back its widespread installation. Very simply, installing fiber-optic cable is very difficult. Splicing fiber-optic cables together is even more difficult. Putting connectors on the fiber-optic cable is also harder than for copper cable. The expense of diagnostic tools is another problem. Time domain reflectometers, ohmmeters, voltmeters, and oscilloscopes can be easily connected to any type of copper cable. But such tools must be specifically designed or adapted for fiber-optics use.

Fiber-optics has enjoyed its greatest success as a backbone medium for connecting sub-networks. Its properties make it ideal for the heavy traffic, hostile environments, and great distances that characterize backbone networks. Its immunity to electrical interference makes it ideal for the factory floor, another popular application.

Fiber-optic cable itself is a core fiber surrounded by cladding. Figure 3.20 shows new fiber optic cable.

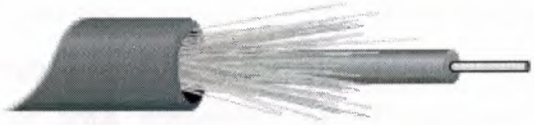


Figure 3.20 New Fiber Optic Cable

A protective covering surrounds both. LEDs or light emitting diodes send the signals down the cable. A detector receives the signals and converts them back to the electrical impulses that computers can understand. While the bits are encoded into light in a number of ways, the most popular method is to vary the intensity of the light.

Fiber-optic cable can be multimode or single-mode. In single-mode cable, the light travels straight down the fiber, which means data can travel greater distances. But since single-mode cable has a larger diameter than multimode cable, it is harder (more expensive) to manufacture. In multimode cable, the light bounces off the cable's walls as it travels down, which causes the signals to weaken sooner, and therefore data cannot travel great distances. Single-mode cable is most often used in the nationwide telephone system, and multimode cable is most often used in LANs, since data is not required to travel across the country.

Standards for fiber-optic LANs have been developed. ANSI's Fiber Distributed Data Interface (FDDI) describes a network that can transmit data at 100Mbits/sec. It also specifies a dual, counter-rotating ring, which makes it fault tolerant. The IEEE has also developed standards for fiber-optic Ethernet.

Imaging applications and the proliferation of networks will force installation of high capacity LANs. Fiber-optics has enormous potential. Its capacities are tremendous. When wiring a new building, the best strategy is to run fiber-optic backbones, with twisted-pair to the desktops.

Fiber Optic Components:

a) ST connector:

The 10BASE-FL standard and FOIRL specification for Ethernet networks define one style of connector as being acceptable for both multimode and single mode fiber optic cabling - the Straight-Tip or ST connector (note that ST connectors for single mode and multimode fiber optics are different in construction and are not to be used interchangeably). Designed by AT&T, the ST connector replaces the earlier Sub-Miniature Assembly or SMA connector. The ST connector is a keyed, locking connector that automatically aligns the center strands of the fiber optic cabling with the transmission or reception points of the network or cable management device it is connecting to. The ST connector is shown in figure 3.21

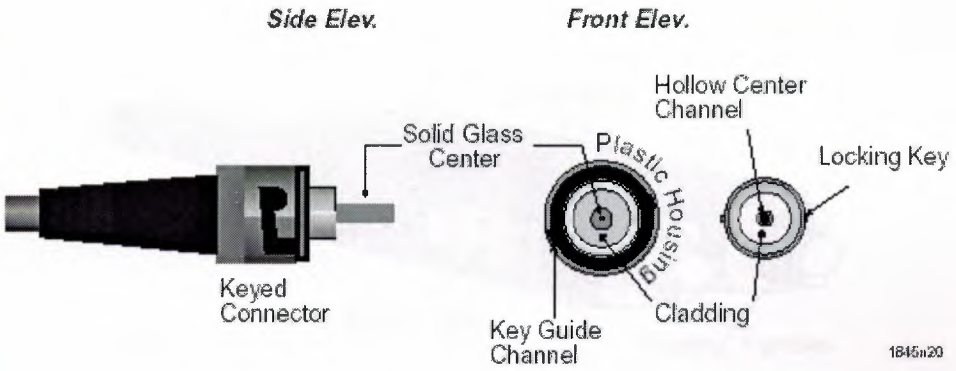


Figure 3.21 ST Connector

The key guide channels of the male ST connector allow the ST connector to only be connected to a female ST connector in the proper alignment. The alignment keys of the female ST connector ensure the proper rotation of the connector and, at the end of the channel, lock the male ST connector into place at the correct attitude. An integral spring helps to keep the ST connectors from being crushed together, damaging the fiber optic cables.

b) SC Connector:

The SC connector is a gendered connector that is recommended for use in Fast Ethernet networks that incorporate multimode fiber optics adhering to the 100BASE-FX specification. It consists of two plastic housings, the outer and inner. The inner housing fits loosely into the outer, and slides back and forth with a travel of approximately 2 mm (0.08 in).

The inner housing ends in two floating ferrules, which are very similar to the floating ferrules used in the FDDI MIC connector. The 100BASE-FX specification requires very precise alignment of the fiber optic strands in order to make an acceptable connection. In order to accomplish this, SC connectors and ports each incorporate “floating” ferrules that make the final connection between fibers. These floating ferrules are held in place relatively loosely. This arrangement allows the ferrules to move slightly when making a connection. This small amount of movement manages to accommodate the subtle differences in construction found from connector to connector and from port to port. The sides of the outer housing are open, allowing the inner housing to act as a latching mechanism when the connector is inserted properly in an SC port. SC connector is shown in figure 3.22

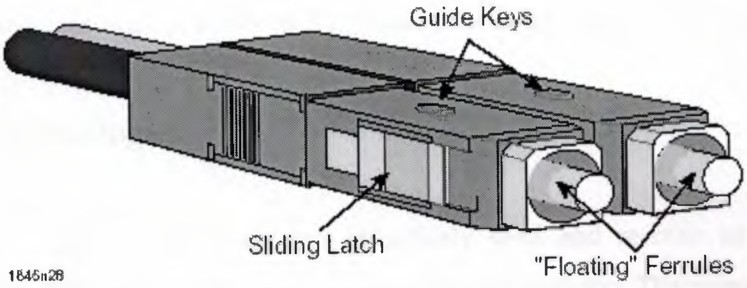


Figure 3.22 SC Connector

c) FDDI MIC:

The FDDI Media Interface Connector, not to be confused with the Token Ring Medium Interface Connector, is a gendered connector that is used with all fiber optic cabling for FDDI networks meeting the MMF-PMD and SMF-PMD standards. It consists of a plastic housing that separates the strands of a two-strand fiber optic cable and a set of ferrules that provide the physical point of connection for the fibers. Figure 3.23 describes the FDDI MIC.

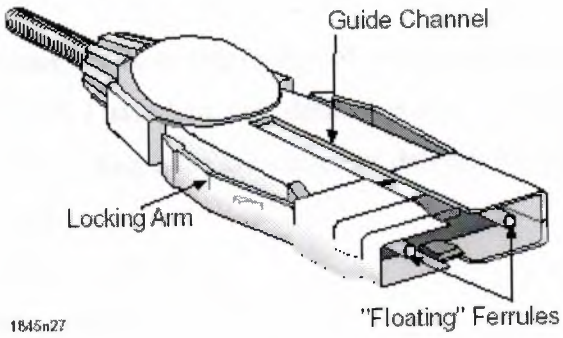


Figure 3.23 FDDI MIC

The MIC connector is designed to prevent the mis-connection of segments and devices. It is specifically constructed in an asymmetrical fashion that prevents the connection of transmit strands in the connector to the transmit devices of an FDDI device.

The sides of the FDDI MIC connector have built-in locking arms that snap the connector into place once it has been fully inserted and keep it from being pulled out.

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 Technologies/IEEE 802.3

The term Ethernet refers to the family of local-area network (LAN) products covered by the IEEE 802.3 standard that defines what is commonly known as the CSMA/CD protocol. Three data rates are currently defined for operation over optical fiber and twisted-pair cables:

- 10 Mbps—10Base-T Ethernet
- 100 Mbps—Fast Ethernet
- 1000 Mbps—Gigabit Ethernet

10-Gigabit Ethernet is under development and will likely be published as the IEEE 802.3ae supplement to the IEEE 802.3 base standard in late 2001 or early 2002.

Other technologies and protocols have been touted as likely replacements, but the market has spoken. Ethernet has survived as the major LAN technology (it is currently used for approximately 85 percent of the world's LAN-connected PCs and workstations) because its protocol has the following characteristics:

- Is easy to understand, implement, manage, and maintain
- Allows low-cost network implementations
- Provides extensive topological flexibility for network installation
- Guarantees successful interconnection and operation of standards-compliant products, regardless of manufacturer

The original Ethernet was developed as an experimental coaxial cable network in the 1970s by Xerox Corporation to operate with a data rate of 3 Mbps using a carrier sense multiple access collision detect (CSMA/CD) protocol for LANs with sporadic but occasionally heavy traffic requirements. Success with that project attracted early attention and led to the 1980 joint development of the 10-Mbps Ethernet Version 1.0 specification by the three-company consortium: Digital Equipment Corporation, Intel Corporation, and Xerox Corporation.

The original IEEE 802.3 standard was based on, and was very similar to, the Ethernet Version 1.0 specification. The draft standard was approved by the 802.3 working group in 1983 and was subsequently published as an official standard in 1985 (ANSI/IEEE Std. 802.3-1985). Since then, a number of supplements to the standard have been defined to take advantage of improvements in the technologies and to support additional network media and higher data rate capabilities, plus several new optional network access control features.

Throughout the rest of this chapter, the terms *Ethernet* and *802.3* will refer exclusively to network implementations compatible with the IEEE 802.3 standard.

Ethernet LANs consist of network nodes and interconnecting media. The network nodes fall into two major classes:

- Data terminal equipment (DTE)—Devices that are either the source or the destination of data frames. DTEs are typically devices such as PCs, workstations, file servers, or print servers that, as a group, are all often referred to as end stations.
- Data communication equipment (DCE)—Intermediate network devices that receive and forward frames across the network. DCEs may be either standalone devices such as repeaters, network switches, and routers, or communications interface units such as interface cards and modems.

Throughout this chapter, standalone intermediate network devices will be referred to as either intermediate nodes or *DCEs*. Network interface cards will be referred to as *NICs*.

The current Ethernet media options include two general types of copper cable: unshielded twisted-pair (UTP) and shielded twisted-pair (STP), plus several types of optical fiber cable.

Because Ethernet devices implement only the bottom two layers of the OSI protocol stack, they are typically implemented as network interface cards (NICs) that plug into the host device's motherboard. The different NICs are identified by a three-part product name that is based on the physical layer attributes.

The naming convention is a concatenation of three terms indicating the transmission rate, the transmission method, and the media type/signal encoding. For example, consider this:

- 10Base-T = 10 Mbps, baseband, over two twisted-pair cables
- 100Base-T2 = 100 Mbps, baseband, over two twisted-pair cables
- 100Base-T4 = 100 Mbps, baseband, over four-twisted pair cables
- 1000Base-LX = 100 Mbps, baseband, long wavelength over optical fiber cable

A question sometimes arises as to why the middle term always seems to be "Base." Early versions of the protocol also allowed for broadband transmission (for example, 10Broad), but broadband implementations were not successful in the marketplace. All current Ethernet implementations use baseband transmission

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.

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. Figure 9-1 summarizes IBM Token Ring network and IEEE 802.5 specifications

3.2.3 Fiber Distributed Data Interface (FDDI)

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.

Figure 3.24 shows the counter-rotating primary and secondary FDDI rings.

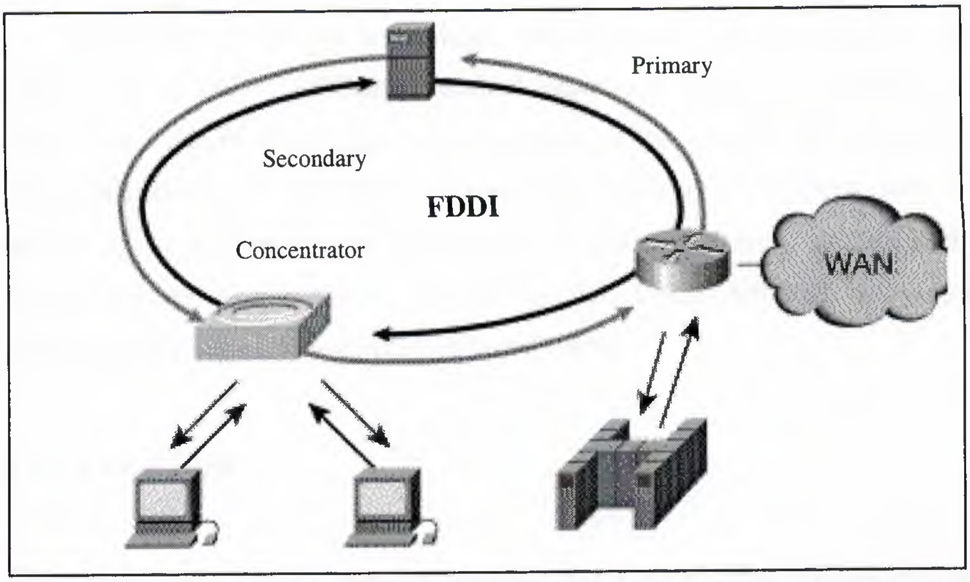


Figure 3.24 FDDI Uses Counter-Rotating Primary and Secondary Rings

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 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.

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

3.3 Characteristics of Ethernet, Token Ring, FDDI, ARCnet and LocalTalk Cables

In XBaseX classification 10BaseT, 100BaseT and 10Base2 are networking standards and there are others.

- The first number is an indication of the transmission speeds involved. It is listed in Mbps (Mega Bits per Second).
- The second portion designates Baseband or Broadband, how the data is sent across the cabling. In Baseband one signal takes up the entire bandwidth of the cable. This data is digital as shown in figure 3.25

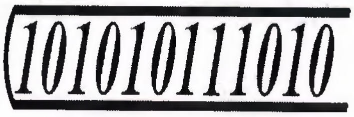


Figure 3.25 Digital Data

With Broadband, the total bandwidth of the cabling is divided and there will be many signals traveling through the cabling at a time. Broadband is analog. Broadband signals can travel father then Baseband as shown in figure 3.26.

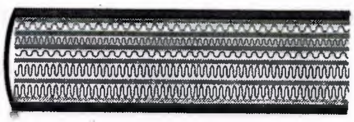
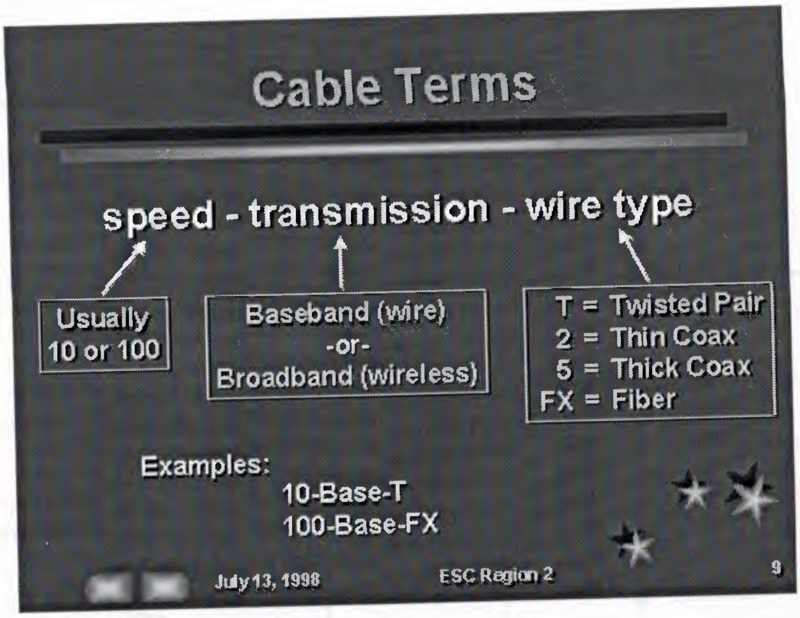


Figure 3.26 Broadband Signal

- The last portion is an indication of wire type and the approximate distances involved or the type of cabling.

Figure 3.27 defines the explanation of cable type specially *Ethernet.*



Cable Terms

speed - transmission - wire type

Usually
10 or 100

Baseband (wire)
-or-
Broadband (wireless)

T = Twisted Pair
2 = Thin Coax
5 = Thick Coax
FX = Fiber

Examples:
10-Base-T
100-Base-FX

July 13, 1998 ESC Region 2 9

Figure 3.27 Ethernet Cable Type Terms

With Ethernet 10Base2

- 255 devices cab be connected
- maximum length of a segment is 185 meters
- is usually standard industry RG-58 cable
    - has a solid copper center conductor
    - braided outer conductor
    - 50 ohm cable
    - requires termination at both ends of segment using 50 ohm terminator.
- Each computer connects to the computer with a T-Connector (BNC - British Naval Connector).

With Ethernet 10Base5

- is usually standard industry RG-8 or RG-11 cable
- maximum length of a segment is 500 meters
- 50 ohm cable
- requires termination at both ends of segment using 50 ohm terminator.

10Base5 wire is connected not by BNC connectors but by AUI connectors. AUI connectors are a DB15 connector, that is, a D-shaped plug with 15 pins. These look just like RS-232 modem connectors, only about half as broad. These are common on equipment such as routers.

Table 3.2 shows characteristics (e.g., speed, length, topology, cable type, etc.) of the 802.3 (Ethernet) standards:

Table 3.2 Characteristics of Ethernet

	Cable Type	**Maximum Length**	**Speed**	**Topology**
10Base-5	Coaxial (RG-8 or RG-11, Thicknet)	500 m	10 Mbps	Bus
10Base-2	Thin Coaxial (RG-58 A/U) thinet coax	185 m	10 Mbps	Bus
10Base-T	Category 3 or above unshielded twisted-pair (UTP)	100 m	10 Mbps	Star, using either simple repeater hubs or Ethernet switches
100Base-TX	Category 5 UTP	100 m	100 Mbps	Star, using either simple repeater hubs or Ethernet switches
100Base-FX	Fiber-optic	412 meters (Half-Duplex) 2000 m (full-duplex)	100 Mbps (200 Mb/s full-duplex mode)	Star (often only point-to-point)
1000Base-LX	Fiber-optic	440 m (multimode) 5000 m (singlemode)	1 Gbps	Star, using buffered distributor hub (or point-to-point)
1000Base-T	Category 5	100 m	1 Gbps	Star

The table 3.3 shows the characteristics of the Token Ring technology.

Table 3.3 Characteristic of Token Ring

Media	MAC Method	Signal Propagation Method	Speed	Topologies	Maximum Connections
Twisted-pair (various types) 10BaseT	Token passing	Forwarded from device to device (or port to port on a hub) in a closed loop	4 Mbps 16 Mbps	Ring Star-using Token Ring repeater hubs	255 nodes per segment

FDDI technologies characteristics are shown in the table 3.4

Table 3.4 FDDI Characteristics

Media	MAC Method	Signal Propagation Method	Speed	Topologies	Maximum Connections
Fiber-optic	Token passing	Forwarded from device to device (or port to port on a hub) in a closed loop	100 Mbps	Double ring Star	500 nodes

Here are some of the basic cabling specifications that can be found in a standard ARCnet network.

- Cable type is RG-62 A/U coaxial. This is an easy-to-handle, lightweight cable grade.
- The longest cable segment carrying an unamplified signal is 100 feet.
- The longest cable segment carrying an amplified signal is 2000 feet.
- The cable length along the entire network cannot be greater than 20,000 feet.
- Two passive hubs cannot be directly connected. In order to connect the two hubs do not amplify the signal, signal amplifying hub must be installed between them.
- Resistor cap must be installed on all unused connectors.

Cabling rules for LocalTalk are simple as well.

- The maximum total length of cable along the network is 1000 feet.

- The recommended maximum number of nodes is 32. Local Talk hardware supports up to 254 nodes, but with this many nodes, performance will be seriously degraded; therefore it is not recommended.

3.4 Cabling Considerations

Cabling depends on the needs of a particular site. The cabling purchased to set up a LAN for a small business has different requirements than those of a larger organization.

Some of the considerations which affect cabling price and performance include:

- Installation logistics

  How easy is the cable to install and work with? In small installations where distances are short and security isn't major issue, it does make sense to choose thick and expensive cable.
- Shielding

  The level of shielding required will be an added cost. Almost every network is using some form of shielding cable. The noisier the area in which cable is run, the more shielding is required.
- Crosstalk

  A corruption of the electrical signal transmitted through a Shielded or Unshielded Twisted Pair cable. Crosstalk refers to signals on one strand or set of strands affecting signals on another strand or set of strands. Inexpensive cabling has low resistance to outside electrical fields generated by power lines, motors and radio transmitters. This makes it susceptible to both noise and cross talk.
- Transmission speed

  Transmission rates are measured in megabits per second (Mbs). Thick cable transmits data faster than thin cable. Fiber-optic cable transmits data even faster, but fiber optic requires expertise to install and is relatively expensive.
- Cost

  Better cable which transmits data securely over long distances is more expensive than thin cable, which is easy to install and work with.

- Attenuation

  Attenuation is Loss of signal power (measured in decibels) due to transmission through a cable. Attenuation is dependent on the type, manufacture and installation quality of cabling, and is expressed in units of loss per length, most often dB/m (decibel per meter). If signal suffers too much attenuation, it will not understand by the receiving computer. Most networks have error checking systems that will generate a retransmission take time and slows down the network.

3.5 LAN Servers

The Server provides file storage space for users, Email services, and print queue services. The only thing that distinguishes a server from a workstation is the extra processing power, additional memory, large capacity hard drives, and "Server" version of Windows NT. A Server typically has one or two processors, over 150 Mb of RAM, and 6 to >12 GB of hard drive storage. A server is simply a computer that is running software that enables it to serve specific requests from clients. For example, you can have a file server that becomes a central storage place for your network, a print server that takes in print jobs and ships them off to a printer, as well as a multitude of other servers and server functions.

A server provides many benefits including:

- Optimization: server hardware is designed to quickly serve requests from clients
- Centralization: files are in one location for easy administration
- Security: multiple levels of permissions can prevent users from doing damage to files
- Redundancy and Back-up: data can be stored in redundant ways making for quick restore in case of problems

Any normal desktop computer could act as a server, but typically you want something much more robust. Standard server hardware includes:

- hot swappable drives to speed adding or replacing hard disks (used in RAID)
- the ability to support multiple processors
- support for larger amounts of RAM
- faster input and output

- fast network cards

Many servers can run multiple applications to serve a variety of needs. As the network grows, we will find uses for a variety specialized server applications. The following is just a brief introduction to the most common types of server applications . . .

3.5.1 File and Print Servers

File and print servers are typically combined on one server and perform as part of the network operating system. The file and printer servers manage the storage of data and the various printers on the network. These servers regulate and monitor access to these resources.

The three most popular are:

- Microsoft Windows NT 4
- Microsoft Windows 2000
- Novell Netware 6
- Microsoft Windows XP Professional
- LANtastic

3.5.2 Mail Servers

Mail servers manage local (within your network) and global (Internet-wide) electronic messaging. The mail server you choose should support the Internet standards such as POP3, and SMTP. Sometimes they even incorporate entire groupware solutions: managing calendars, contacts, group meeting scheduling, and other operations. There are many, many examples of mail servers, but the most popular are:

- Microsoft Exchange
- Eudora Mail Server

3.5.3 List Servers

While many mail servers offer the capability to serve an email listserv or mass email distribution, there are some servers that handle those tasks exclusively. Here are a few to look at:

- LISTSERV
  Lyris
- Arrow Mailing List Server

3.5.4 Fax Servers

Fax servers manage fax traffic in and out of the network, allowing multiple users to send and receive faxes without a fax machine.

Most of the popular email servers have fax servers that you can buy and integrate into your system, so look there first. One interesting note is that "Microsoft Small Business Server" (basically their BackOffice software for under 30 users) includes a fax server. However, they didn't include it in Windows 2000. Some other examples of standalone fax servers are:

- RelayFax
- FaxMaker

3.5.5 Web Servers

Web servers allow Internet users to attach to your server to view and maintain web pages. Web browsers such as Netscape and Internet Explorer request documents from the web server using standard protocols, and the web server retrieves the requested documents and forwards them on to the browsers. Web servers support a variety of technologies including CGI scripts, Active Server Pages, and secure connections to extend the power beyond the basic HTML code.

The two most popular web servers are:

- Apache (for "A patchy" web server)
- Microsoft Internet Information Services (IIS)

One interesting thing is that this field is primarily the domain of Linux and Unix (w/ Apache). However, Microsoft has been playing catch-up, and it is gathering support around its IIS product.

3.5.6 Database Servers or Database Management Systems (DBMS)

Though not exactly a server, DBMS systems allow multiple users to access the same database at the same time. While this functionality is typically built into database software (ex. Microsoft Access allows concurrent connections to its databases), a larger database or a database with many users may need a dedicated DBMS to serve all the requests. Examples of these include:

- Microsoft SQL Server
- IBM DB2
- Oracle's Database Management Products

3.5.7 Application Servers

Application servers have undergone many changes and have grown in both quantity and variety with the growth of the Internet. Basically, an application server acts as an intermediary to information. Here is a typical situation:

1. A client makes a request for information (often as a database request)
2. The application server passes that request on to the application
3. The application processes the request and sends the results to the application server that then returns the results to the client.
4. The client gets the results of their query without needing to download the whole database to his or her workstation.

In many usages, the application server works with a Web server and is called a Web application server. The web application server receives requests from a web page then returns the information in a new web page based on the results and uniquely created. The technology to do this typically involves the Common Gateway Interface (CGI), Microsoft's Active Server Pages (ASP), or Java Server Pages (JSP).

Examples of application servers include:

- Cold Fusion

3.5.8 Terminal Servers or Communication Server

Generally a terminal server refers to a piece of hardware that allows devices to be attached to the network without a need for network cards. PCs, "dumb" terminals supporting just a mouse and monitor, or printers can all be attached via standard ports, and can then be managed by the network administrator.

However, Microsoft has co-opted this term and changed it to fit their purposes. A Microsoft Terminal Server is a program running on its Windows NT 4.0 operating system that provides the graphical user interface of the Windows desktop to user terminals that don't have this capability themselves. The latter include the relatively low-cost Net PCs or "thin clients" that some companies are purchasing as alternatives to the autonomous and more expensive PC with its own operating system and applications. In the past, Terminal Server required an entirely different operating system version, but Microsoft has expanded this capability to be a standard application in Windows 2000.

3.5.9 Proxy Servers

Proxy servers act as intermediaries between your network users and the wide world of the Internet. Proxy servers perform a number of functions:

- Masks your network users IP addresses
- Strengthens security by only allowing certain requests to come through and by providing virus protection
- Caches web page data for a given period of time to allow for more rapid access

Examples of proxy servers include:

- Microsoft Proxy Server
- Wingate

3.5.10 Conclusion

The preceding list is only an introduction to common server applications. With the amount of time and money thrown at the Internet, many types of servers are springing up to fill every conceivable need. Whether you need to start up an email list, or provide access to talk radio 24 hours a day, there is a server for you.

3.6 LAN Workstations

Workstations generally come with a large, high-resolution graphics screen, at least 64 MB (megabytes) of RAM, built-in network support. Most workstations also have a mass storage device such as a disk drive, but a special type of workstation, called a diskless workstation, comes without a disk drive. The most common operating systems for workstations are UNIX and Windows NT.

In terms of computing power, workstations lie between personal computers and minicomputers, although the line is fuzzy on both ends. High-end personal computers are equivalent to low-end workstations. And high-end workstations are equivalent to minicomputers.

Like personal computers, most workstations are single-user computers. However, workstations are typically linked together to form a local-area network, although they can also be used as stand-alone systems.

The leading manufacturers of workstations are Sun Microsystems, Hewlett-Packard Company, Silicon Graphics Incorporated, and Compaq.

In networking, workstation refers to any computer connected to a local-area network. It could be a workstation or a personal computer.

3.7 Network Interface Cards

A NIC translates data from the parallel data bus to the serial bit stream. The network interface card (NIC) provides the physical connection between the network and the computer workstation. Most NICs are internal, with the card fitting into an expansion slot inside the computer. Some computers, such as Mac Classics, use external boxes which are attached to a serial port or a SCSI port. Laptop computers can now be purchased with a network interface card built-in or with network cards that slip into a PCMCIA slot.

Network interface cards are a major factor in determining the speed and performance of a network. It is a good idea to use the fastest network card available for the type of workstation you are using.

The three most common network interface connections are Ethernet cards, LocalTalk connectors, and Token Ring cards. According to a International Data Corporation study, Ethernet is the most popular, followed by Token Ring and LocalTalk

Ethernet cards are usually purchased separately from a computer, although many computers (such as the Macintosh) now include an option for a pre-installed Ethernet card. Ethernet cards contain connections for either coaxial or twisted pair cables (or both) (See fig. 3.28). If it is designed for coaxial cable, the connection will be BNC. If it is designed for twisted pair, it will have a RJ-45 connection. Some Ethernet cards also contain an AUI connector. This can be used to attach coaxial, twisted pair, or fiber optics cable to an Ethernet card. When this method is used there is always an external transceiver attached to the workstation. Ethernet Network Interface Card is shown in figure 3.28

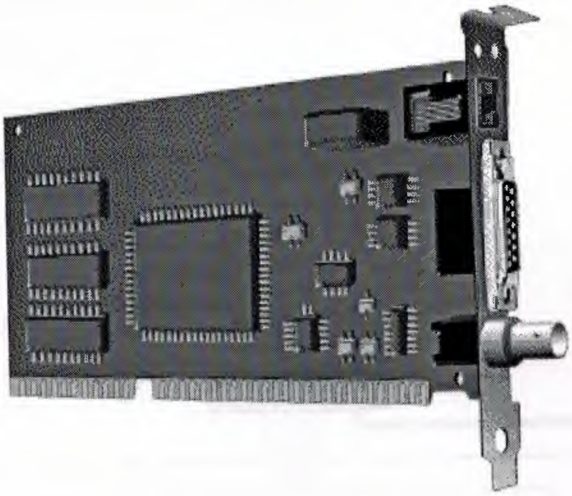


Figure 3.28 Ethernet card, from top to bottom: RJ-45, AUI, and BNC connectors

LocalTalk is Apple's built-in solution for networking Macintosh computers. It utilizes a special adapter box and a cable that plugs into the printer port of a Macintosh. A major disadvantage of LocalTalk is that it is slow in comparison to Ethernet. Most Ethernet connections operate at 10 Mbps (Megabits per second). In contrast, LocalTalk operates at only 230 Kbps (or .23 Mbps).

Token Ring network cards look similar to Ethernet cards. One visible difference is the type of connector on the back end of the card. Token Ring cards generally have a nine pin DIN type connector to attach the card to the network cable.

3.8 Hubs / Concentrators

A concentrator is a device that provides a central connection point for cables from workstations, servers, and peripherals. In a star topology, twisted-pair wire is run from each workstation to a central concentrator. Hubs are multislot concentrators into which can be plugged a number of multi-port cards to provide additional access as the network grows in size. Some concentrators are passive, that is they allow the signal to pass from one computer to another without any change. Most concentrators are active, that is they electrically amplify the signal as it moves from one device to another. Active concentrators are used like repeaters to extend the length of a network. Concentrators/Hubs are:

- Usually configured with 8, 12, or 24 RJ-45 ports
- Often used in a star or star-wired ring topology
- Sold with specialized software for port management

Hub is shown in figure 3.29

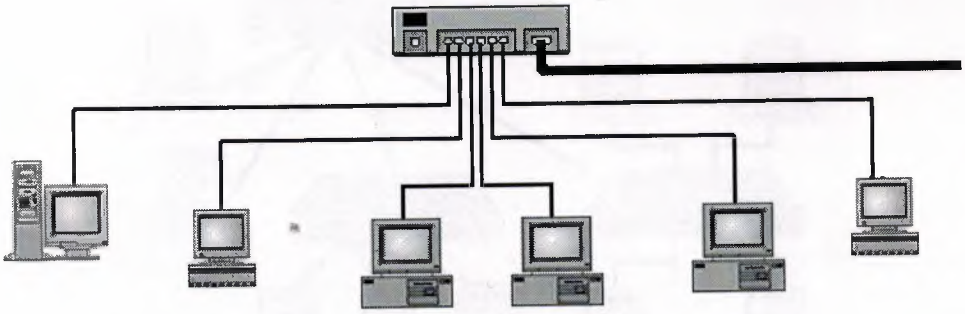


Figure 3.29 Hub

3.9 Switches

Switches allow you to avoid the congestion of a shared Ethernet network by permitting you to create individual segments. The improvement in network performance can be dramatic. In the figure below, the switch is being fed a 100Mbps signal. The switch is then creating four segmented networks, each with its own 10Mbps path. Net 3 and Net 4 are then connecting to a hub, creating two shared 10Mbps networks. Switches come in a variety of configurations.

Figure 3.30 shows a switch

Figure 3.30 Switch

Figure 3.31 shows a switch connected to hubs

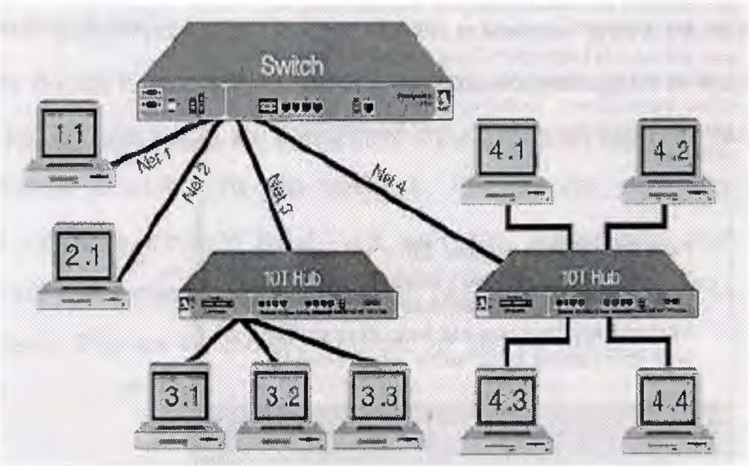


Figure 3.31 Switch connected to Hub

All this hardware which is used in the Local Area Network is controlled by some software. This software is installed on server/workstation by which all this hardware is connected.

4. NETWORK OPRATING SYSTEM AND PLANNING THE NETWORK

4.1 Overview

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 4.1 shows resources are shared equally.

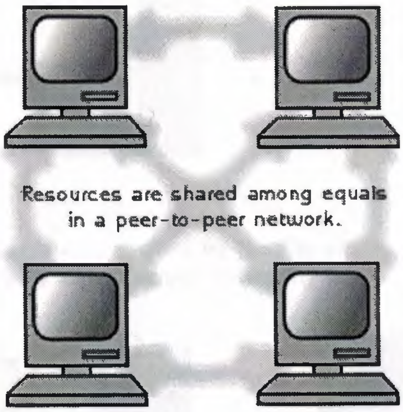


Figure 4.1 Peer-to-Peer Network

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 4.2 shows how resources are controlled by the file server in a client/server network

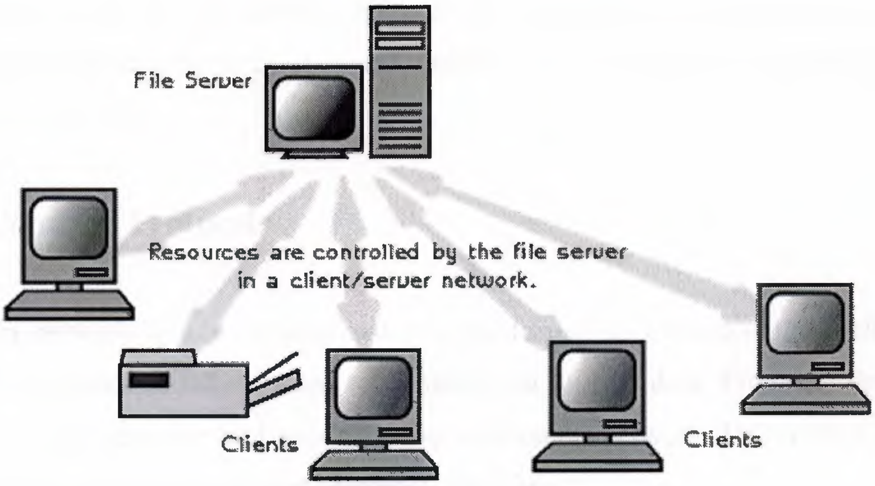

File Server
Resources are controlled by the file server in a client/server network.
Clients
Clients

Figure 4.2 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).

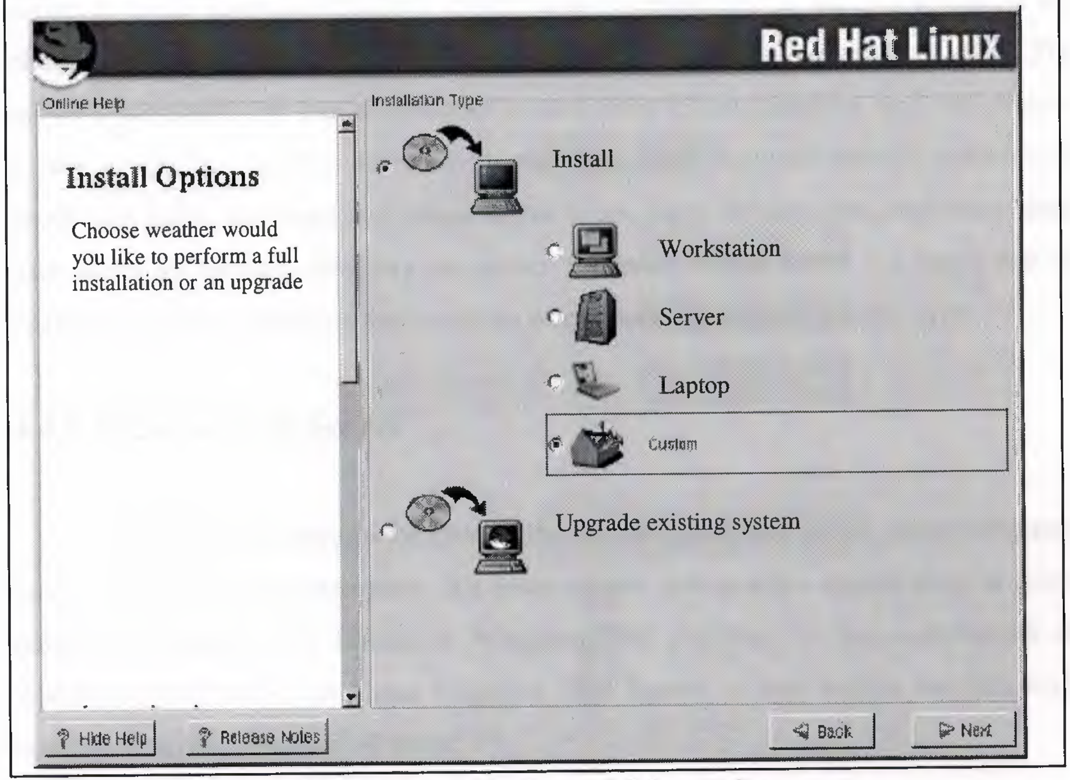
- Workstation

  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 4.3 shows the install screen of Red Hat Linux



Install Options

Choose weather would you like to perform a full installation or an upgrade

● Install

○ Workstation

○ Server

○ Laptop

● Custom

○ Upgrade existing system

Figure 4.3 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 4.4 below shows the basic server configuration.

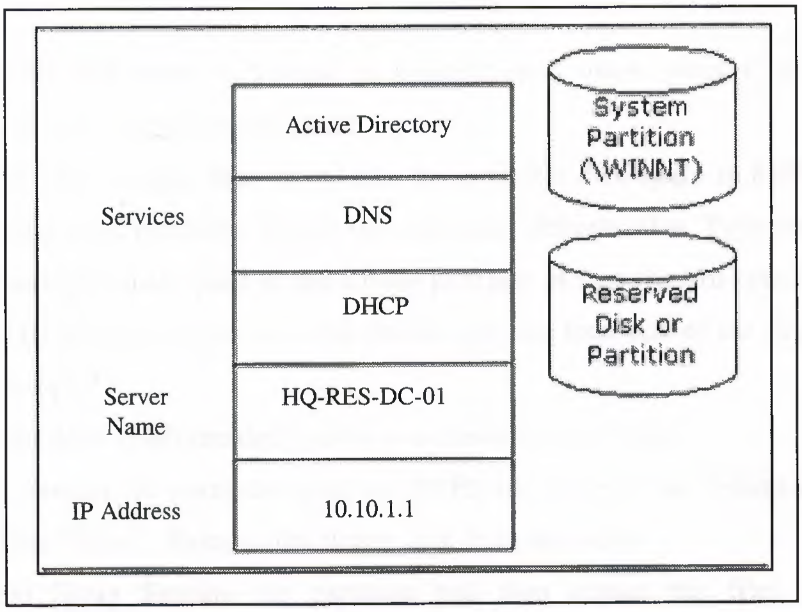


Figure 4.4 Server Configuration

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.

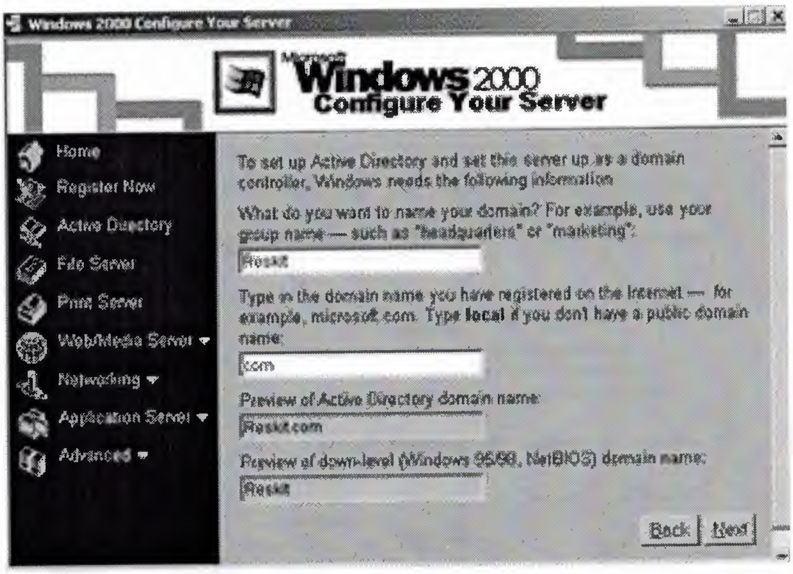
11. When you reach the Completing the Windows 2000 Setup Wizard, remove the CD-ROM from the drive and click Finish.

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 4.5 shows the Windows 2000 “Configure Your Server Wizard”.



To set up Active Directory and set this server up as a domain controller, Windows needs the following information

What do you want to name your domain? For example, use your group name — such as "headquarters" or "marketing":

Reskit

Type in the domain name you have registered on the Internet — for example, microsoft.com. Type **local** if you don't have a public domain name:

com

Preview of Active Directory domain name:

Reskit.com

Preview of down-level (Windows 95/98, NetBIOS) domain name:

Reskit

Figure 4.5 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 4.1.

Table 4.1 Default Values Set by Wizard

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

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 4.6 below illustrates the sample Active Directory structure.

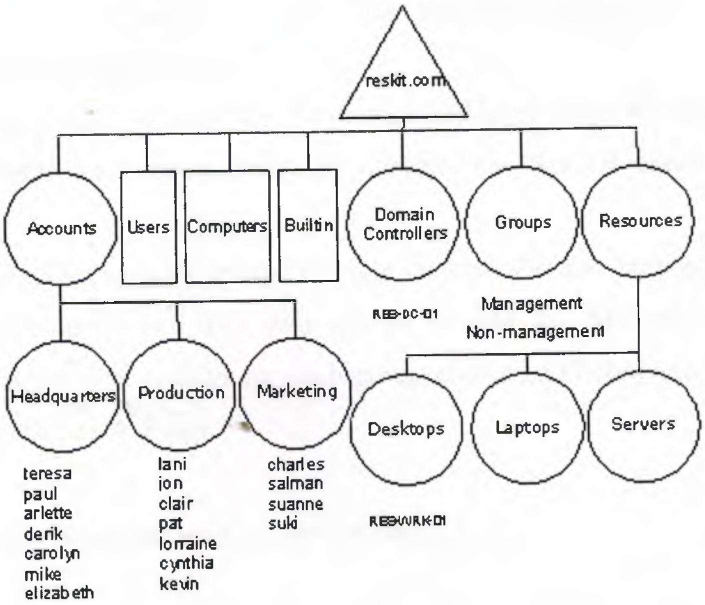


Figure 4.6 Sample Active Directory Structure

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.

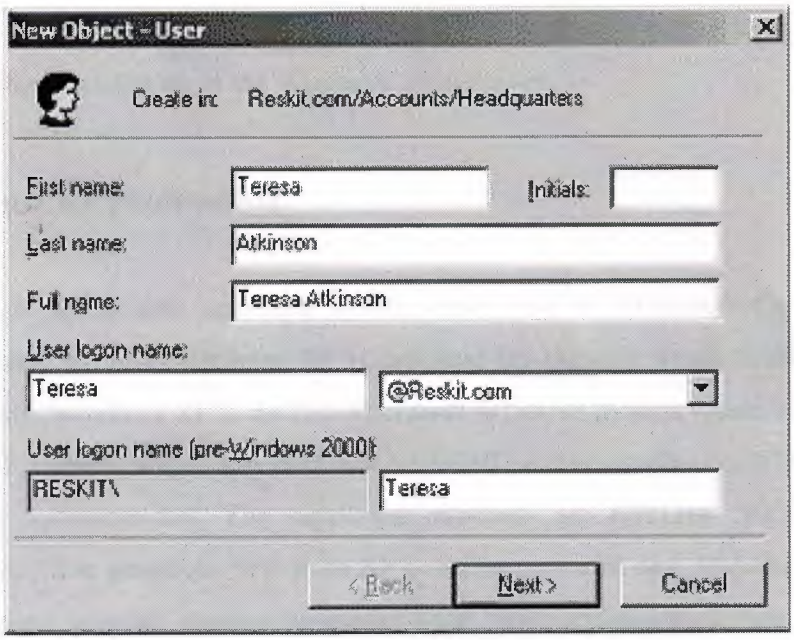
6. Click Accounts in the left pane. Its contents now display in the right pane (it is empty to start).
7. Right-click Accounts, point to New, and click Organizational Unit.
8. Type Headquarters, and click OK.

Repeat steps 6 and 7 to create the Production and Marketing OUs under Accounts.

9. In the same way, create Desktops, Laptops, and Servers under the Resources OU.
10. 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 we need the following steps:

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 4.7.



First name: Teresa
Initials:
Last name: Atkinson
Full name: Teresa Atkinson
User logon name:
Teresa
@Reskit.com
User logon name (pre-Windows 2000):
RESKIT\
Teresa

Figure 4.7 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 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. Repeat steps 2 through 4 to add members to the Non-management group.

5. 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.
- 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 4.8 shows the LAN connection

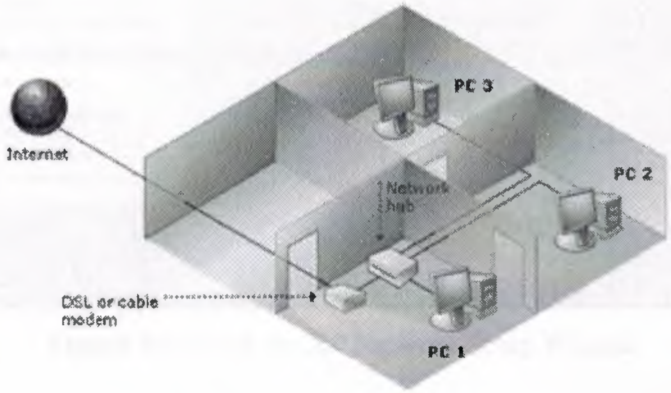


Figure 4.8 LAN Connection

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 4.9 shows the network set up wizard.

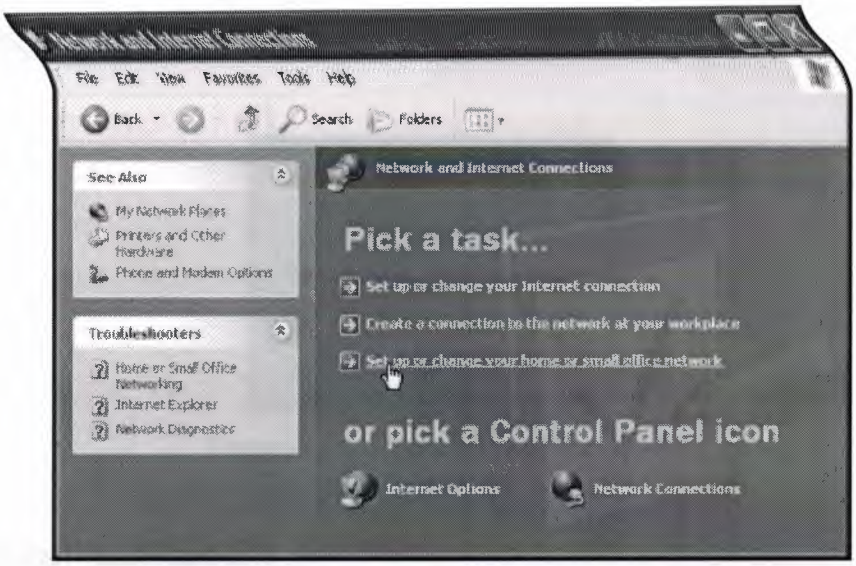

Network and Internet Connections
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
See Also
My Network Places
Printers and Other Hardware
Phone and Modem Options
Troubleshooters
Home or Small Office Networking
Internet Explorer
Network Diagnostics
Network and Internet Connections
Pick a task...
Set up or change your Internet connection
Create a connection to the network at your workplace
Set up or change your home or small office network
or pick a Control Panel icon
Internet Options
Network Connections

Figure 4.9 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

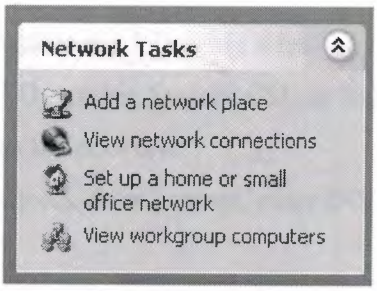
To do so:

- 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.

11. 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 4.10



Network Tasks

Add a network place

View network connections

Set up a home or small office network

View workgroup computers

Figure 4.10 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.

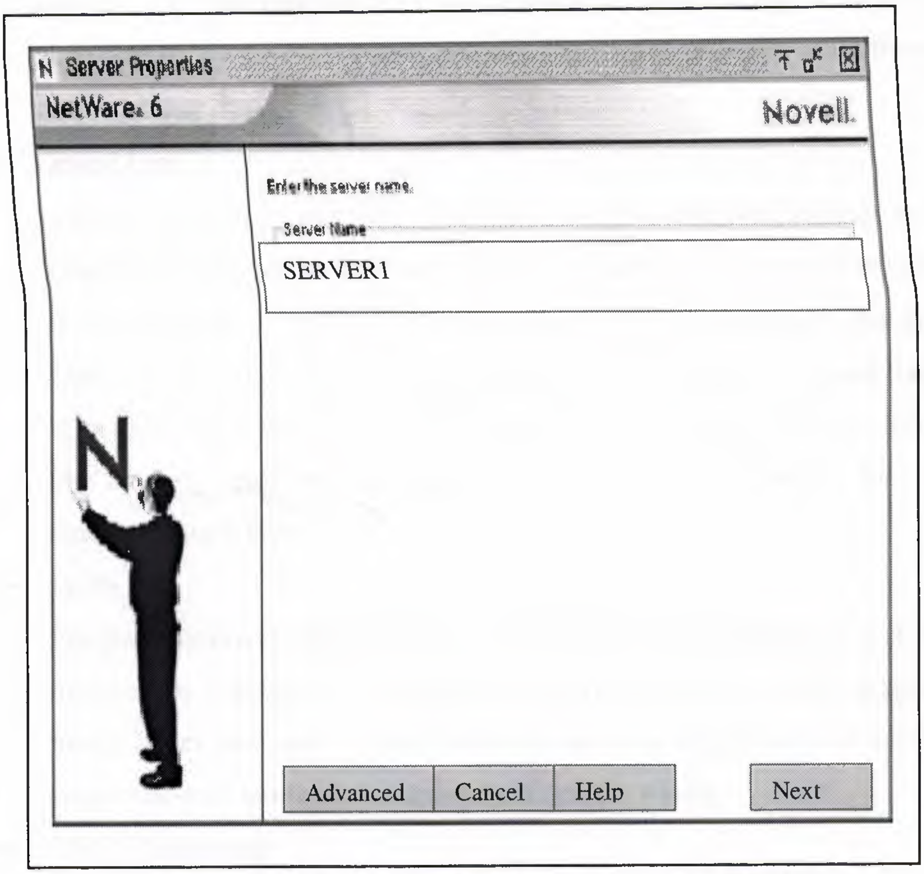
1. Insert the NetWare 6 Operating System CD, or log in to the network to access the installation files on the network.
2. At the CD drive or network drive prompt, enter INSTALL.

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 4.11 shows the NetWare server properties window.



Enter the server name.

Server Name

SERVER1

Figure 4.11 Novell NetWare Server Properties Window

For 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.

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] 'Thomas Robert M., *Introduction to Local Area Networks*, Sybex Computer Books Inc. U.S.A, 1996

[4] Microsoft, *Networking Essentials*, Microsoft Corporation, Washington, 1996