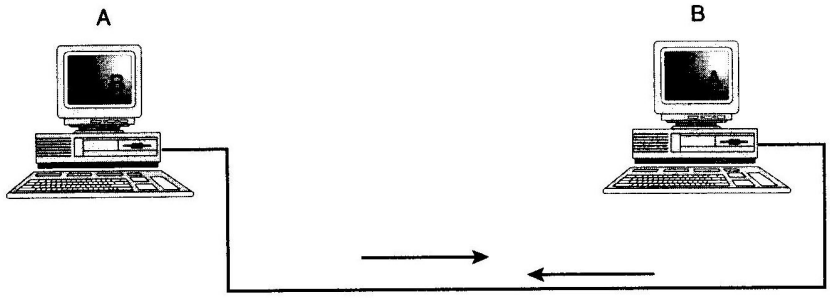
Introduction

Networking is the concept of sharing resources and services. A network of computers is a group of interconnected systems sharing resources and interacting using a shared communications link. A network, therefore, is a set of interconnected systems with something to share. The shared resource can be data, a printer, a fax modem, or a service such as a database or an email system. The individual systems must be connected through a pathway (called the transmission medium) that is used to transmit the resource or service between the computers. All systems on the pathway must follow a set of common communication rules for data to arrive at its intended destination and for the sending and receiving systems to understand each other. The rules governing computer communication are called protocols.

In summary, all networks must have the following:

1. A resource to share (resource)
2. A pathway to transfer data (transmission medium)
3. A set of rules governing how to communicate (protocols)



Figure(1) - Simplest form of a computer network

Having a transmission pathway does not always guarantee communication. When two entities communicate, they do not merely exchange information; rather, they must understand the information they receive from each other. The goal of computer networking, therefore, is not simply to exchange data but to understand and use data received from other entities on the network.

An analogy is people speaking, just because two people can speak, it does not mean they automatically can understand each other. These two people might speak different languages or interpret words differently. One person might use sign language, while the

other uses spoken language. As in human communication, even though you have two entities who "speak," there is no guarantee they will be able to understand each other. Just because two computers are sharing resources, it does not necessarily mean they can communicate.

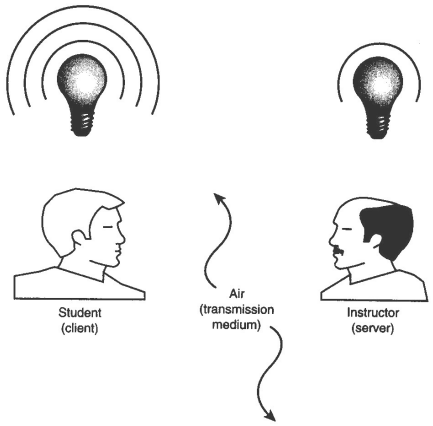


Figure (2) - An analogy of a computer network

Because computers can be used in different ways and can be located at different distances from each other, enabling computers to communicate often can be a daunting task that draws on a wide variety of technologies.

The two main reasons for using computer networking are to provide services and to reduce equipment costs. Networks enable computers to share their resources by offering services to other computers and users on a network. The following are specific reasons for networking PCs

1. Sharing files
2. Sharing printers and other devices
3. Enabling centralized administration and security of the resources within the system.
4. Supporting network applications such as electronic mail and database services
5. Limited resources
6. Desire to share the resources
7. Cost Reduction

Today, that's a limiting view, because the most important resource is information. Network lets us share information and Resource Sharing achieves the same.

Resource Sharing

The purpose of many computer networks is to permit a far-flung community of users to share computer resources. Many such users now have their own microcomputers, so the shared resources have to be interesting enough to warrant access via a network. The facilities accessible by networks are in fact becoming more interesting at a rapid rate.

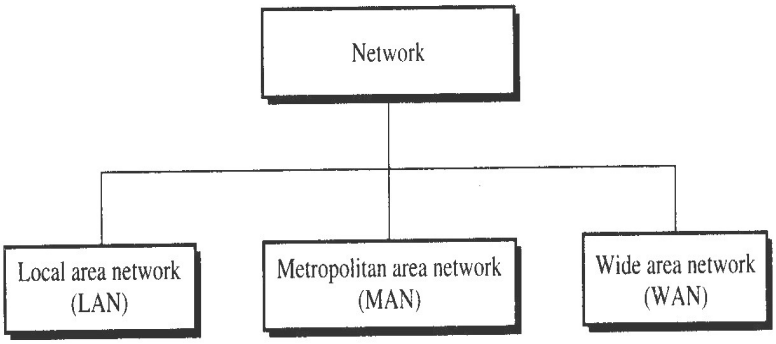
The remote computer may contain software that a user needs to employ. It may be proprietary software kept at one location. It may require a larger machine than any at the user's location. The distant computer may provide access to data that is stored and maintained at its location. Sometimes the remote machine controls a large or special printing facility. Sometimes the remote machine compiles programs that are used on smaller peripheral machines.

Cost Reduction

There are various aspects of technology that are likely to force the price of terminal usage drastically lower. This is important because almost all aspects of telecommunications are characterized by high price elasticity. In other words, when the price comes down, the usage goes up.

Types of Network- LAN, WAN and MAN

Today when we speak of networks, we are generally referring to three primary categories: local area networks, metropolitan area networks, and wide area networks. Into which category a network its size, its ownership, the distance it covers, and its physical architecture determine falls.



Figure(3) - Categories of networks

Local Area Network (LAN)

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office, or it can extend throughout a company and include voice, sound, and video peripherals. Currently, LAN size is limited to a few kilometers.

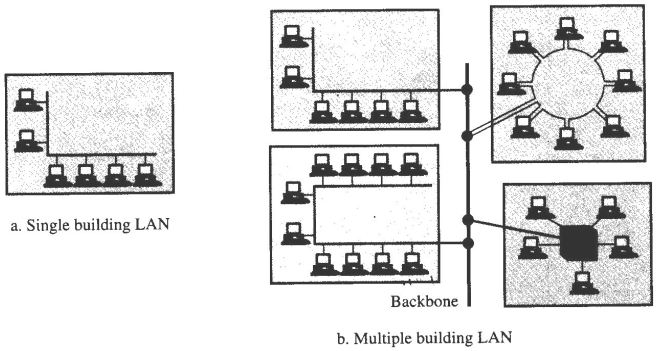


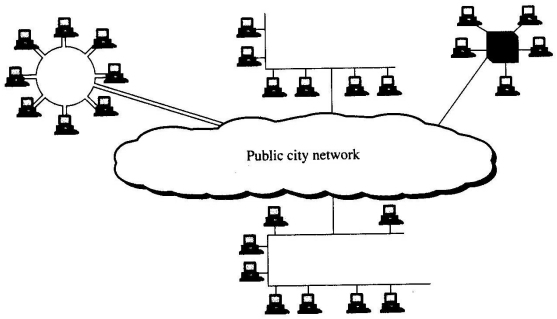
Figure (4) - LAN

LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware e.g., a printer, software e.g., an application program, or data. A common example of a LAN, found in many business environments, links a work group of task-related computers, for example, engineering workstations or accounting PCs. One of the computers may be given a large-capacity disk drive and become a server to the other clients. Software can be stored on this central server and used as needed by the whole group. In this example, the size of the LAN may be determined by licensing restrictions on the number of users per copy of software, or by restrictions on the number of users licensed to access the operating system.

In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star.
Traditionally, LANs have data rates in the 4 to 16 Mbps range. Today, however speeds are increasing and can reach 100 Mbps with gigabit systems in development.

Metropolitan Area Network (MAN)

A metropolitan area network (MAN) is designed to extend over an entire city. It may be a single network such as a cable television network, or it may be a means of connecting a number of LANs into a larger network so that resources may be shared LAN-to-LAN as well as device-to-device. For example, a company can use a MAN to connect the LANs in all of its offices throughout a city.



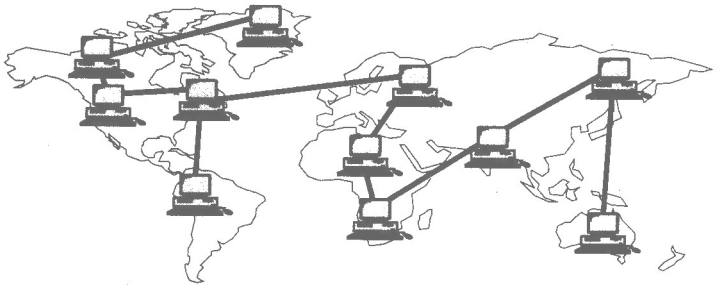
Figure(5) - MAN

A MAN may be wholly owned and operated by a private company, or it may be a service provided by a public company, such as a local telephone company. Many

telephone companies provide a popular MAN service called Switched Multi-megabit Data Services (SMDS).

Wide Area Network (WAN)

A wide area network (WAN) provides long-distance transmission of data, voice, image, and video information over large geographical areas that may comprise a country, a continent, or even the whole world.



Figure(6) - WAN

In contrast to LANs (which depend on their own hardware for transmission), WANs may utilize public, leased, or private communication devices, usually in combinations, and can therefore span an unlimited number of miles. A WAN that is wholly owned and used by a single company is often referred to as an enterprise network.

Criteria for Classification of Computer Network

The following are the characteristics used to classify different types of computer networks

Topology

Topology is nothing but the geometric management of positioning computer systems to involve them in the form of a network. For example, Star topology, Bus topology, etc.

Protocol

The protocols are nothing but the set of rules and signals that are used for communication in the network. For example, 'Ethernet' is one of the most popular protocols for LANs.

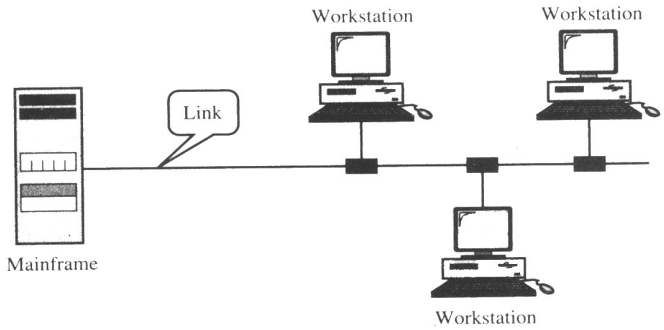
Architecture

Networks can usually be classified in the following two types -

1. Peer-to-peer architecture.
2. Client-Server architecture.

NETWORK TOPOLOGIES

The term topology refers to the way a network is laid out, either physically or logically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to each other. There are five basic topologies possible: mesh, star, tree, bus, and ring.



Figure(7) - Multipoint Line Configuration

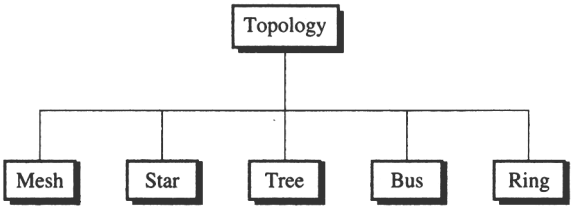


Figure (8) - Categories of Topologies

These five labels describe how the devices in a network are interconnected rather than their physical arrangement. For example, having a star topology does not mean that all of the computers in the network must be placed physically around a hub in a star shape. A consideration when choosing a topology is the relative status of the devices be linked. Two relationships are possible: peer-to-peer, where the devices share the link equally, and primary-secondary, where one device controls traffic and the others must

transmit through it. Ring and mesh topologies are more convenient for peer-to-peer transmission, while star and tree are more convenient for primary-secondary, bus topology is equally convenient for either.

Mesh

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. A fully connected mesh network therefore has n*(n - l)/2 physical channels to link n devices. To accommodate that many links, every device on the network must have 7 input/output (I/O) ports.

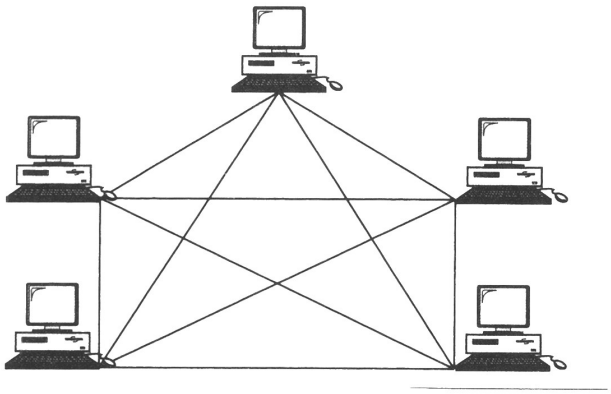


Figure (9) - Fully Connected Mesh Topology

A mesh offers several advantages over other network topologies. First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

Second, a mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

Another advantage is privacy or security. When every message sent travels along dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.

Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the

network manager to discover the precise location of the fault and aids in finding its cause and solution.

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required. First, because every device must be connected to ever other device, installation and reconfiguration are difficult. Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate. And, finally, the hardware required connecting each link (I/O ports and cable can be prohibitively expensive). For these reasons a mesh topology is usually implemented in a limited fashion—for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

Star

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to each other. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange. If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

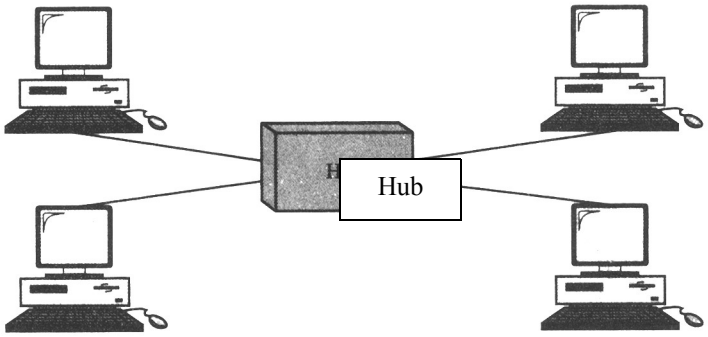


Figure (10) - Star topology

A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.

Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

However, although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason more cabling is required in a star than in some other topologies (such as tree, ring, or bus).

Tree

A tree topology is a variation of a star. As in a star, nodes in a tree are linked to a central hub that controls the traffic to the network. However, not every device plugs directly into the central hub. The majority of devices connect to a secondary hub that in turn is connected to the central hub.

The central hub in the tree is an active hub. An active hub contains a repeater, which is a hardware device that regenerates the received bit patterns before sending them out. Repeating strengthens trans- missions and increases the distance a signal can travel.

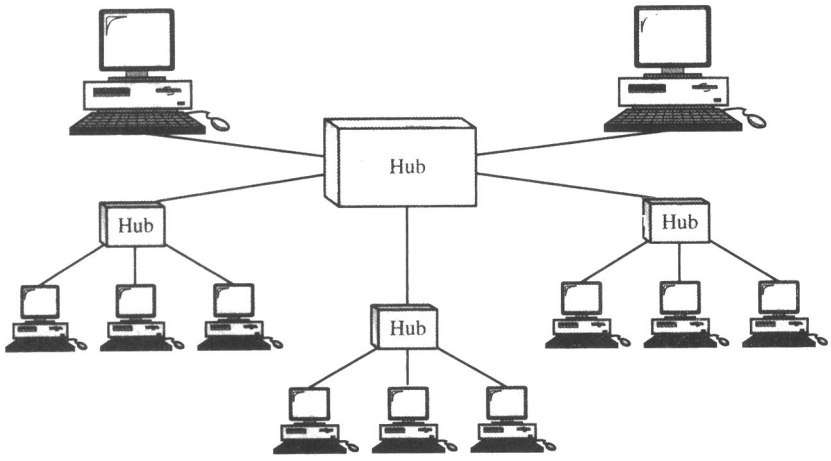


Figure (11) - Tree Topology

The secondary hubs may be active or passive hubs. A passive hub provides a simple physical connection between the attached devices.

The advantages and disadvantages of a tree topology are generally the same as those of a star. The addition of secondary hubs, however, brings two further advantages. First, it allows more devices to be attached to a single central hub and can therefore

increase the distance a signal can travel between devices. Second, it allows the network to isolate and prioritize communications from different computers. For example, the computers attached to one secondary hub can be given priority over computers attached to another secondary hub. In this way, the network designers and operator can guarantee that time-sensitive data will not have to wait for access to the network.

A good example of tree topology can be seen in cable TV technology where the main cable from the main office is divided into main branches and each branch is divided into smaller branches and so on. The hubs are used when a cable is divided.

Bus

The preceding examples all describe point-to-point configurations. A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in the network.

Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker the farther it has to travel. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh, star, or tree topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

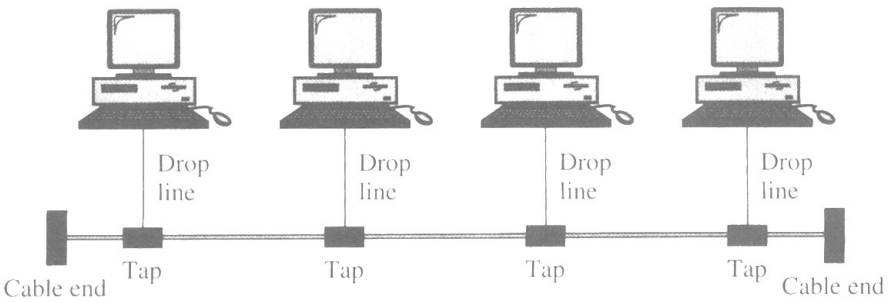


Figure (12) - Bus Topology

Disadvantages include difficult reconfiguration and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. As mentioned above, signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.

In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

Ring

In a ring topology, each device has a dedicated point-to-point line configuration only with the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

A ring is relatively easy to install and reconfigure. Each device is linked only to its immediate neighbors (either physically or logically). To add or delete a device requires moving only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not

receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

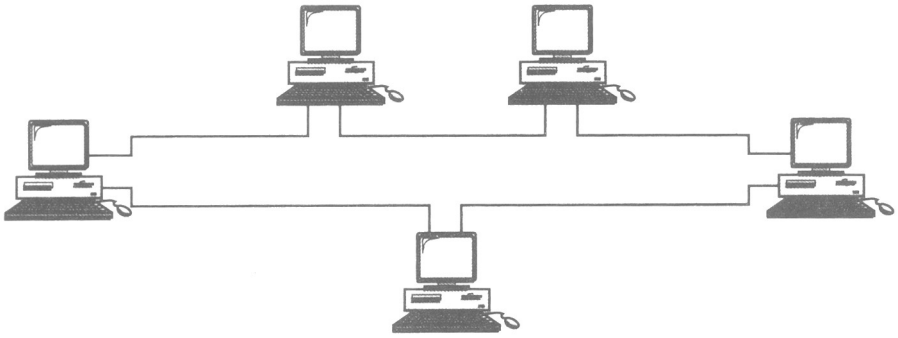


Figure (13) - Ring Topology

NETWORK PROTOCOLS

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. Examples include application programs, file transfer packages, browsers, database management systems, and electronic mail software. A system, is a physical object that contains one or more entities, Examples include computers and terminals. But two entities cannot just send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communication. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

Syntax

Syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first eight bits of data

to be the address of the sender, the second eight bits to be the address of the receiver, and the rest of the stream to be the message itself.

Semantics

Semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation. For example, does an address identify the route to be taken or the final destination of the message?

Timing

Timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and data will be largely lost.

In data communication, a protocol is a set of rules that govern all aspects of information communication.

Protocols Example

There are a many standard protocols to choose from, standard protocols have their own advantage and disadvantage i.e., some are simpler than the others, some are more reliable, and some are faster.

From a user's point of view, the only interesting aspect about protocols is that our computer or device must support the right ones if we want to communicate with other computers. The protocols can be implemented either in hardware or in software. Some of the popular protocols are:

1. TCP/IP
2. HTTP
3. FTP
4. SMTP

5. POP
6. Token-Ring
7. Ethernet
8. Xmodem
9. Kermit
10. MNP, etc.

CLIENT AND SERVERS

To use the services available on an Internet, application programs, running at two end computers and communicating with each other, are needed. In other words, in an Internet, the application programs are the entities that communicate with each other, not the computers or users.

The application programs using the Internet follow these client-server model strategies

1. An application program, called the client, running on the local machine, requests a service from another application program, called the server, running on the remote machine, Figure 2.12 illustrates this.

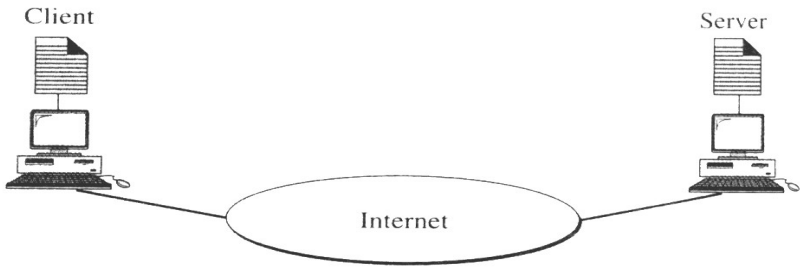


Figure (13) - Client-server Model

2. A server can provide a service for any client, not just a particular client. In other words, the client-server relationship is many-to-one. Many clients can use the services of one server.

3. Generally, a client program, which requests a service, should run only when it is needed. The server program, which provides a service, should run all of the time because it does not know when its service is needed.

4. Services needed frequently and by many users have specific client-server application programs. For example, we should have client-server application programs that allow users to access files, send e-mail, and so on. For services that are more customized, we should have one generic application program that allows users to access the services available on a remote computer.

Client

A client is a program running on the local machine requesting service from a server. A client program is finite, which means it is started by the user (or another application program) and terminates when the service is complete.

Server

A server is a program running on the remote machine providing service to the clients. When it starts, it opens the door for incoming requests from clients, but it never initiates a service until it is requested to do so.

A server program is an infinite program. When it starts, it runs infinitely unless a problem arises. It waits for incoming requests from clients. When a request arrives, it responds to the request.

LANs

A local area network (LAN) is two or more computers directly linked within a small well-defined area such as a room, building, or group of closely placed buildings. A LAN may be made up of only microcomputers or any combination of microcomputers and large systems.

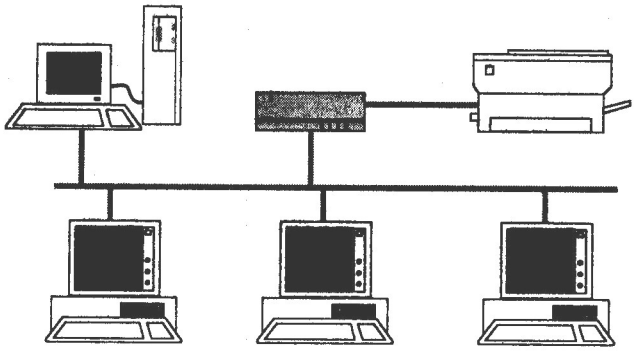


Figure (14) - Local Area Network

The computer network that connects the computers in the different parts of the same big city like metropolitan city may be referred to as Metropolitan Area Network (MAN).

Interest in local area networks is constantly growing due to following two developments

1. Developments in communication technology
2. The difference between a LAN and Development of powerful and user-friendly micro-computers

   A multi-user system is that a LAN is made up of stand-alone computers whereas a multi-user system typically has one computer that is shared among two or more terminals.

   A LAN usually consists of the following-

1. Two or more computers
2. Peripheral devices such as printers and hard-disk drives
3. Software to control the operation of the computers or other devices connected to the LAN
4. Special cables, usually coaxial or fiber optic, to connect the computers and other devices
5. A plug-in board to handle the data transmissions.
6. A benefit of a LAN is the reduction of hardware costs because several computers and users can share peripheral devices such as laser printers, hard-disk drives, color plotters, and modems. Another advantage is the users can share data.

Ensuring the security and privacy of data are two concerns of LAN users. The LAN must get the data to its destination, transmit the data correctly, and prevent unauthorized users from gaining access to that data. These tasks are accomplished through both the hardware and LAN software.

They vary in the type and number of computers that can be connected, the speed at which data can be transferred, and the type of the software used to control the network. Some LANs require that all the computers be of a certain brand, while others allow a variety of brands to be connected. The number of computers in a LAN varies widely from smaller LANs that typically connect 2 to 25 computers, to large LANs that can connect as many as 10,000 computers.

The length of the cable connecting a computer to a LAN also varies depending on the LAN. Most LANs allow cables of about 1000 feet, but some allow cables of several miles to be used. The data transfer speeds range from several thousand bits per second to around 10 million bits per second. The programs that control the LANs also vary in the features they offer. Some programs allow the use of more than one operating system; others allow only one. On some LANs, file access is limited to one user at a time; on others, more than one user can access a file simultaneously.

Hardware Requirements For LAN

The following are major hardware components/devices required for establishing LAN

1. Transmission Channel
2. Network Interface Unit (NIU)
3. Servers
4. Workstations

5. Transmission Channel For LAN
6. Generally four types of channels are used for data transmission in a LAN. These are-

i. Twisted Pair Cable
ii. Coaxial Cable
iii. Fiber-Optic Cables
iv. Radio Waves

Network Interface Unit

Network interface units connect each device in the LAN network to shared transmission device. It contains the rules or logic to access the LAN. NIU is also used to implement LAN protocols and for device attachments. Its function depends on the type of topology used in LAN.

Servers & Workstations

One of the major benefits of implementation of LAN is sharing expensive resources such as storage devices, printers etc. This is achieved through providing servers on the LAN. It is dedicated computer that controls one or more resources. This contains both hardware and software interface for LAN. Three major categories of services used in LANs are

1. File Server
2. Printer Server
3. Modem Server

In networking, file server is used to share storage space for files. Besides providing storage space for files in a LAN environment, it is used for taking periodical backup, and also to provide gateway to other servers within and between LANs.

Similarly printer server is used to handle printing works of all workstation connected in the network.

In LAN environment also modem is required to get connected to other network or simply to use a telephone. A modem server is used to share this expensive resource by all connected workstations in a network ring.

LAN Software

LAN operating system is required to operate on the LAN system. It has basically two aspects

1. Server Software
2. Workstation Software

LAN operating system facilitates

i. Sharing of expensive resources e.g. printer, storage space etc.
ii. Security for data

iii. Connection to other network.

There are various types of LAN operating system. Some popular LAN operating system are-

i. Novel Netware
ii. Ethernet
iii. Curves
iv. ArcNet
v. LAN Server
vi. Omni Net
vii. PC Net
viii. IBM PC LAN
ix. Etherlik Plus, etc.

INTRODUCTION TO ETHERNET

History of the Ethernet

Ethernet is a well-known and widely used network technology that employs bus topology. Ethernet was invented at Xerox Corporation's Palo Alto Research Center in the early 1970s. Digital Equipment Corporation, Intel Corporation, and Xerox later cooperated to devise a production standard, which is informally called DIX Ethernet for the initials of the three companies. IEEE now controls Ethernet standards. In its original version, an Ethernet LAN consisted of a single coaxial cable, called the ether, to that multiple computers connect. Engineers use the term segment to refer to the Ethernet coaxial cable. A given Ethernet segment is limited to 500 meters in length, and the standard requires a minimum separation of 3 meters between each pair of connections.

The original Ethernet hardware operated al a bandwidth of 10 Megabits per second (Mbps); a later version known as Fast Ethernet operates at IUU Mbps. and the most recent version, which is known as Gigabit Ethernet operates at 1000 Mbps or 1 Gigabit per second (Gbps).

Sharing on an Ethernet

The Ethernet standard specifies all details, including the format of frames that computers send across the ether, the voltage to be used, and the method used to modulate a signal.

Because it uses a bus topology, Ethernet requires multiple computers to share access to a single medium. A sender transmits a signal, which propagates from the sender toward both ends of the cable. Figure 1.8 illustrates how data flows across an Ethernet.

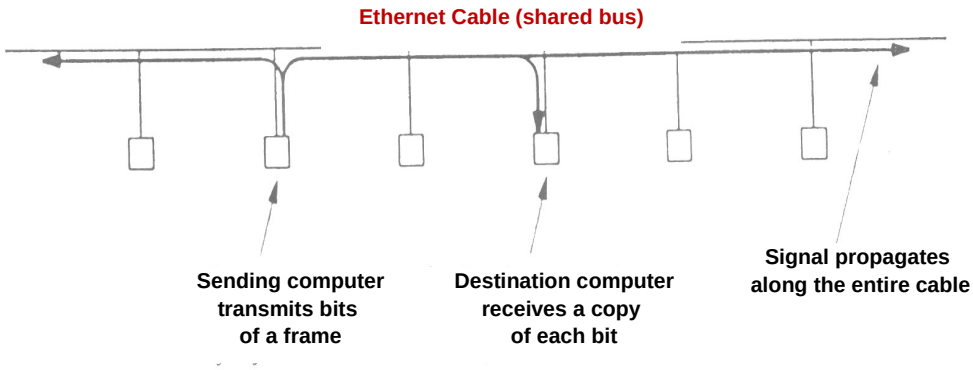


Figure (15) - Conceptual flow of bits across an Ethernet

A signal propagates from the sending computer to both end of the shared cable. It is important to understand that sharing in local area network technologies does not mean that multiple frames are being sent at the same time. In stead, the sending computer has exclusive use of the entire cable during the transmission of a given frame- other computers must wait. After one-computer finishers transmitting one frame, the shared cable becomes available for another computer to use.

Ethernet is a bus, network in which multiple computers share a single transmits a frame to another, and all other computers must wait.

Carrier Sense on Multi-Access Networks (CSMA)

The most interesting aspect of Ethernet is the mechanism used to coordinate transmission. An Ethernet network does not have a centralized controller that tells each computer how to take turns using the shard cable. Instead, all computers attached to an Ethernet participate in a distributed coordination scheme called Carrier Sense Multiple Access (CSMA). The scheme uses electrical activity on the cable to determine status.

When no computer is sending a frame, the ether does not contain electrical signals. During frame transmission, however, a sender transmits electrical signals used to encode bits. Although the signals differ slightly from the carrier waves, they are informally called a carrier. Thus, to determine whether the cable is currently being used, a computer can check for a carrier. If no carrier is present, the computer can transmit a frame. If a carrier is present, the computer must wait for the sender to finish before proceeding. Technically, checking for a carrier wave is called carrier sense, and the idea of using the presence of a signal to determine when to transmit is called Carrier Sense Multiple Access (CSMA).

Collision Detection and Back off with CSMA/CD

Because CSMA allows each computer to determine whether a shared cable is already in use by another computer, it prevents a computer from interrupting an ongoing transmission. However, CSMA cannot prevent all possible conflicts. To understand why, imagine what happens if two computers at opposite ends of an idle cable both have a frame ready to send at the same time. When they check for a carrier, both stations. Find the cable idle, and both start lo send frames simultaneously. The signals travel at approximately 70% of the speed of light, and when the signals transmitted by two computers reach the same point on the cable, they interfere with each other.

The interference between two signals is called a collision. Although a collision does not harm the hardware, it produces a garbled transmission that prevents either of the two frames from being received correctly. To ensure that no other computer transmits simultaneously, the Ethernet standard requires a sending station to monitor signals on the cable. If the signal on the cable differs from the signal that the station is sending, it means that a collision has occurred. Whenever a collision is detected, a sending station immediately stops transmitting. Technically, monitoring a cable during transmission is known as Collision Detect {CD), and the Ethernet mechanism is known as Carrier Sense Multiple Access with Collision Detect (CSMA/CD).

CSMA/CD does more than merely detect collisions - it also recovers from them. After a collision occurs, a computer must wail for the cable to become idle again before transmitting a frame. However, if the computers begin to transmit as soon as the ether becomes idle another collision will occur. To avoid multiple collisions, Ethernet requires

each computer to delay after a collision before attempting to retransmit. The standard specifies a maximum delay, d, and forces each computer to choose a random delay less than d. In most cases, when a computer chooses a delay at random, it will select a value that differs from any of the values chosen by the other computers – the computer that chooses the smallest delay will proceed to send a frame and the network will return to normal operation.

If two or more computers happen to choose nearly the same amount of delay after a collision, they will both begin to transmit at nearly the same time, producing a second collision. To avoid a sequence of collisions, Ethernet requires each computer to double the range from which a delay is chosen after each collision. Thus, a computer chooses a random delay from 0 to d after one collision, a random delay between 0 and 2d after a second collision, between 0 and 4d after a third, and soon after a few collisions, the range from which a random value is chosen becomes large, and the probability is high that some computer will choose a short delay and transmit without a collision.

Technically, doubling the range of the random delay after each collision is known as binary exponential back off. In essence, exponential back off means that an Ethernet can recover quickly after a collision because each computer agrees to wait longer times between attempts when the cable becomes busy. In the unlikely event that two or more computers choose delays that are approximately equal, exponential back off guarantees that contention for the cable will be reduced after a few collisions.

Computers attached to an Ethernet use CSMA/CD in which a computer waits for the ether lo be idle before transmitting a frame. If two computers transmit simultaneously, a collision occurs: the computers use exponential back off to choose which computer will proceed. Each computer' delays a random time before trying to transmit again, and then doubles the delay for each successive collision.

Basis and Working

Ethernet is a very popular local area network architecture based on the CSMA/CD access method. The original Ethernet specification was the basis for the IEEE 802.3 specifications. In present usage, the term "Ethernet" refers to original Ethernet (or Ethernet II, the latest version) as well as the IEEE 802.3 standards. The different varieties of Ethernet networks are commonly referred to as Ethernet topologies. Typically,

Ethernet networks can use a bus physical topology, although, as mentioned earlier, many varieties of Ethernet such as 10BASE-T use a star physical topology and a bus logical topology. (Microsoft uses the term "star bus topology" to describe 10BASE-T.)

Ethernet networks, depending on the specification, operate at 10 or 100Mbps using base band transmission. Each IEEE 802.3 specification prescribes its own cable types.

OSI Model

This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers. The model is called the ISO-OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems. We will usually just call it the OSI model for short.

The OSI model has seven layers. The principles that were applied to arrive at the seven layers are as 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 should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy.

Below we will discuss each layer of the model in turn, starting at the bottom layer. Note that the OSI model itself is not network architecture because it does not specify the exact services and protocols to be used in each layer. It just tells what each layer should do. However, ISO has also produced standards for all the layers, although these are not part of the reference model itself. Each one has been published as a separate international standard.

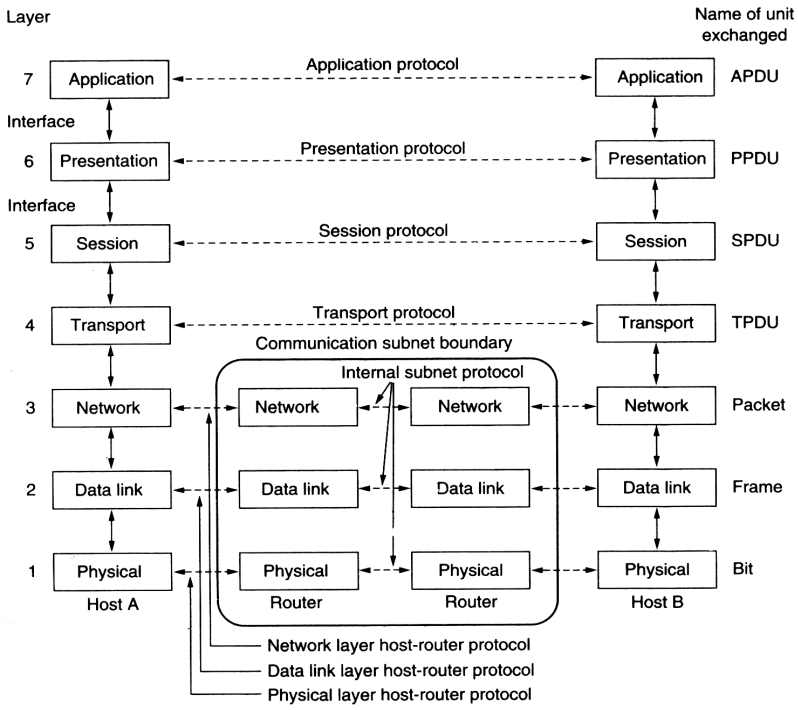


Figure (16) - The OSI Reference Model

The Physical Layer

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit. Typical questions here are how many volts should be used to represent a 1 and how many for a 0, how many microseconds a bit lasts, whether transmission may proceed simultaneously in both directions, how the initial connection is established and how it is torn down when both sides are finished, and how many pins the network connector has and what each pin is used for. The design issues here largely deal with mechanical, electrical, and procedural interfaces, and the physical transmission medium, which lies below the physical layer.

The Data Link Layer

The main task of the data link layer is to take a raw transmission facility and transform it into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break the input data up into data

frames (typically a few hundred or a few thousand bytes), transmit the frames sequentially, and process the acknowledgement frames sent back by the receiver. Since the physical layer merely accepts and transmits a stream of bits without any regard to meaning or structure, it is up to the data link layer to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. If these bit patterns can accidentally occur in the data, special care must be taken to make sure these patterns are not incorrectly interpreted as frame delimiters.

A noise burst on the line can destroy a frame completely. In this case, the data link layer software on the source machine can retransmit the frame. However, multiple transmissions of the same frame introduce the possibility of duplicate frames. A duplicate frame could be sent if the acknowledgement frame from the receiver back to the sender were lost. It is up to this layer to solve the problems caused by damaged, lost, and duplicate frames. The data link layer may offer several different service classes to the network layer, each of a different quality and with a different price.

Another issue that arises in the data link layer (and most of the higher layers is well) is how to keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanism must be employed to let the transmitter know how much buffer space the receiver has at the moment. Frequently, this flow regulation and the error handling are integrated.

If the line can be used to transmit data in both directions, this introduces a new complication that the data link layer software must deal with. The problem is that the acknowledgement frames for A to B traffic compete for the use of the line with data frames for the B to A traffic.

Broadcast networks have an additional issue in the data link layer to control access to the shared channel. A special, sub layer of the data link layer, the medium access sub layer, deals with this problem.

The Network Layer

The network layer is concerned with controlling the operation of the subnet. A key design issue is determining how packets are routed from source to destination.

Routes can be based on static tables that are "wired into" the network and rarely changed. They can also be determined at the start of each conversation, for example a terminal session. Finally, they can be highly dynamic, being determined anew for each packet, to reflect the current network load.

If too many packets are present in the subnet at the same time, they will get in each other's way, forming bottlenecks. The control of such congestion also belongs to the network layer.

Since the operators of the subnet may well expect remuneration for their efforts, there is often some accounting function built into the network layer. At the very least, the software must count how many packets or each customer sends characters or bits, to produce billing information. When a packet crosses a national border, with different rates on each side, the accounting can become complicated.

When a packet has to travel from one network to another to get to its destination, many problems can arise. The addressing used by the second network may be different from the first one. The second one may not accept the packet at all because it is too large. The protocols may differ, and so on. It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.

In broadcast networks, the routing problem is simple, so the network layer is often thin or even nonexistent.

The Transport Layer

The basic function of the transport layer is to accept data from the session layer, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. Furthermore, all this must be done efficiently, and in a way that isolates the upper layers from the inevitable changes in the hardware technology.

Under normal conditions, the transport layer creates a distinct network connection for each transport connection required by the session layer. If the transport connection requires a high throughput, however, the transport layer might create multiple network connections, dividing the data among the network connections to improve throughput. On the other hand, if creating or maintaining a network connection is expensive, the transport

layer might multiplex several transport connections onto the same network connection to reduce the cost. In all cases, the transport layer is required to make the multiplexing transparent to the session layer.

The transport layer also determines what type of service to provide the session layer, and ultimately, the users of the network. The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were sent. However, other possible kinds of transport service are transport of isolated messages with no guarantee about the order of delivery, and broadcasting of messages to multiple destinations. The type of service is determined when the connection is established.

The transport layer is a true end-to-end layer, from source to destination, in other words, a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages. In the lower layers, the protocols are between each machine and its immediate neighbors, and not by the ultimate source and destination machines, which may be separated by many routers. There is a difference between layers 1 through 3, which are chained, and layers 4 through 7, which are end-to-end. Many hosts are multi-programmed, which implies that multiple connections will be entering and leaving each host. Their needs to be some way to tell which message belong to which connection. The transport header is one place this information can be put.

In addition to multiplexing several message streams onto one channel, the transport layer must take care of establishing and deleting connections across the network. This requires some kind of naming mechanism, so that a process on one machine has a way of describing with whom it wishes to converse. There must also be a mechanism to regulate the flow of information, so that a fast host cannot overrun a slow one. Such a mechanism is called flow control and plays a key role in the transport layer (also in other layers). Flow control between hosts is distinct from flow control between routers, although we will later see that similar principles apply to both.

The Session Layer

The session layer allows users on different machines to establish sessions between them. A session allows ordinary data transport, as does the transport layer, but it also provides enhanced services useful in some applications. A session might be used to allow a user to log into a remote timesharing system or to transfer a file between two machines.

One of the services of the session layer is to manage dialogue control. Sessions can allow traffic to go in both directions at the same time, or in only one direction at a time. If traffic can only go one way at a time (analogous to a single railroad track), the session layer can help keep track of whose turn it is.

A related session service is token management. For some protocols, it is essential that both sides do not attempt the same operation at the same time. To manage these activities, the session layer provides tokens that can be exchanged. Only the side holding the token may perform the critical operation.

Another session service is synchronization. Consider the problems that might occur when trying to do a 2-hour file transfer between two machines with a 1-hour mean time between crashes. After each transfer was aborted, the whole transfer would have to start over again and would probably fail again the next time as well. To eliminate this problem, the session layer provides a way to insert checkpoints into the data stream, so that after a crash, only the data transferred after the last checkpoint have to be repeated.

The Presentation Layer

The presentation layer performs certain functions that are requested sufficiently often to warrant finding a general solution for them, rather than letting each user solve the problems. In particular, unlike all the lower layers, which are just interested in moving bits reliably from here to there, the presentation layer is concerned with the syntax and semantics of the information transmitted.

A typical example of a presentation service is encoding data in a standard agreed upon way. Most user programs do not exchange random binary bit strings. They exchange things such as people's names, dates, amounts of money, and invoices. These items are represented as character strings, integers, floating-point numbers, and data structures composed of several simpler items. Different computers have different codes

for representing character strings, integers, and so on. In order to make it possible for computers with different representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire." The presentation layer manages these abstract data structures and converts from the representation used inside the computer to the network standard representation and back.

The Application Layer

The application layer contains a variety of protocols that are commonly needed. For example, there are hundreds of incompatible terminal types in the world. Consider, the plight of a full screen editor that is supposed to work over a network with many different terminal types, each with different screen layouts, escape sequences for inserting and deleting text, involving the cursor, etc.

One way to solve this problem is to define an abstract network virtual terminal that editors and other programs can be written to deal with. To handle each terminal type, a piece of software must be written to map the functions of the network virtual terminal onto the real terminal. For example, when the editor moves the virtual terminal's cursor to the upper left-hand corner of the screen, this software must issue the proper command sequence to the real terminal to get its cursor there too. All the virtual terminal software is in the application layer.

Another application layer function is file transfer. Different file systems have different file naming conventions, different ways of representing text lines, and so on. Transferring a file between two different systems requires handling these and other incompatibilities. This work, too, belongs to the application layer, as do electronic mail, remote job entry, directory lookup, and various other general purpose and special-purpose facilities.

TCP/IP Model

Let us now turn from the OSI reference model to the reference model used in the grandparent of all computer networks, the ARPANET, and its successor, the worldwide Internet. Although we will give a brief history of the ARPANET later, it is useful to mention a few key aspects of it now. The ARPANET was a research network sponsored

by the DOD (U.S Department of Defense). It eventually connected hundreds of universities and government installations using leased telephone lines. When satellite and radio networks were added later, the existing protocols had trouble interworking 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 later became known as the TCP/IP Reference Model, after its two primary protocols.

Given the DOD's worry that some of its precious hosts, routers, and internet work gateways might get blown to pieces at a moment's notice, another major goal was that the network be able to survive loss of subnet hardware, with existing conversations not being broken off. In other words, DOD wanted connections to remain intact as long as the source and destination machines were functioning, even if some of the machines or transmission lines in between were suddenly put out of operation. Furthermore, a flexible architecture was needed, since applications with divergent requirements were envisioned, ranging from transferring files to real-time speech transmission.

The Internet Layer

All these requirements led to the choice of a packet-switching network based on a connectionless Internet work layer. This layer, called the Internet layer, is the linchpin that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network). They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired. Note that "internet" is used here in a generic sense, even though this layer is present in the Internet.

The analogy here is with the mail system. A person can drop a sequence of international letters into a mailbox in one country, and with a little luck, most of them will be delivered to the correct address in the destination country. Probably the letters will travel through one or more international mail gateways along the way, but this is transparent to the users. Furthermore, that each country has its own stamps, preferred envelope sizes, and delivery rules is hidden from the users. The Internet layer defines an

official packet format and protocol called IP (Internet Protocol). 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 the TCP/IP Internet layer is very similar in functionality to the OSI network layer. Figure 2.15 shows this correspondence.

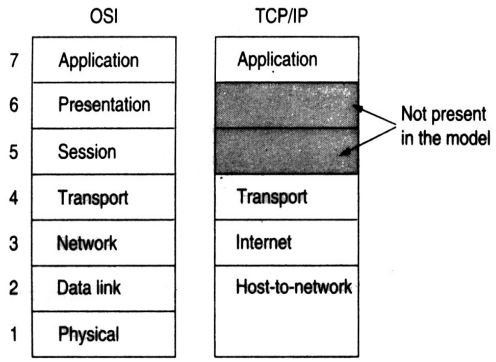


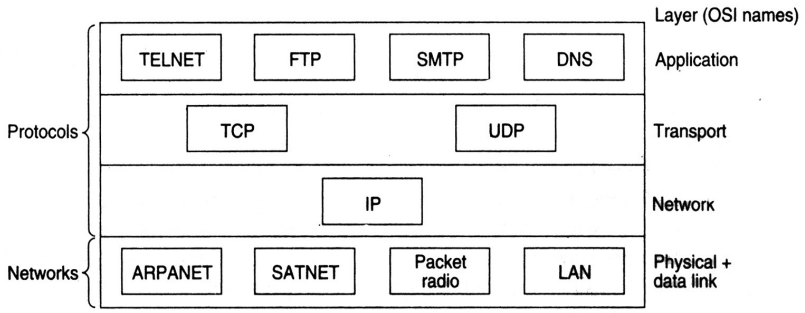
Figure (17) - The TCP/IP Reference Model

The Transport Layer

The layer above the Internet layer in the TCP/IP model is now usually called 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. Two end-to-end protocols have been defined here. The first one, TCP (Transmission Control Protocol) is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the Internet. It fragments the incoming byte stream into discrete messages and passes each one onto the Internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

The second protocol in this layer, UDP (User Data gram Protocol), is an 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 for one-shot, client-

server type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. The relation of IP, TCP, and UDP . Since the model was developed, IP has been implemented on many other networks.



Figure(18) - Protocols and Networks in the TCP/IP Model Initially

The Application Layer

The TCP/IP model does not have session or presentation layers. No need for them was 'perceived, so they were not included. Experience with the OSI model has proven this view correct: they are of little use to most applications.

On top of the transport layer is the application layer. It contains all the Higher Level Protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP). The virtual terminal protocol allows a user on one machine to log into a distant machine and work there. The file transfer protocol provides a way to move data efficiently from one machine to another. Electronic mail was originally just a kind of file transfer, but later a specialized protocol was developed for it. Many other proto- cols have been added to these over the years, such as the Domain Name Service (DNS) for mapping host names onto their network addresses, NNTP, the protocol used for moving news articles around, and HTTP, the protocol used for fetching pages on the World Wide, and many others.

The Host-to-Network Layer

Below the Internet layer is a great void. The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets over it. This protocol is not

defined and varies from host to host and network to network. Books and papers about the TCP/IP model rarely discuss it.

Ethernet Cabling

The types of Ethernet cables available are

1. Straight-through cable
2. Crossover cable
3. Rolled cable

Straight-through cable

Four wires are used in straight-through cable to connect Ethernet devices. It is relatively simple to create this type. Only pins1, 2, 3 and 6 are used. Just connect 1 to1, 2 to 2, 3 to 3 and 6 to 6 and you will be up and networking in no time while practically we connect all 4 pairs straighten of CAT-5. However, this would be an Ethernet only cable and would not work with Voice, Token Ring, ISDN, etc. This type of cable is used to connect

1. Host to switch or hub
2. Router to switch or hub

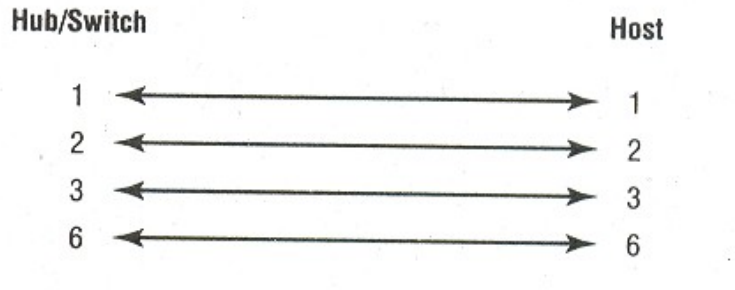


Figure (19) - Straight-through cable

Crossover Cable

Four wires are used in straight-through cable to connect Ethernet devices. Only four pins are used in this type of cabling. In crossover cable we connect 1 to3 and 2 to 6 on each side of cable. This type of cable is used to connect

1. Switch to switch
2. Hub to hub
3. Host to host
4. Hub to switch
5. Router direct to host

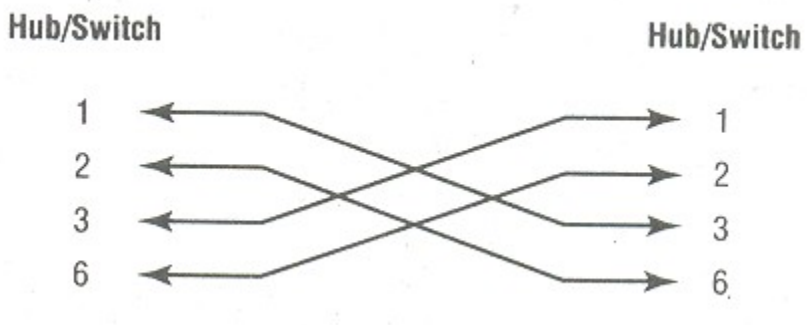


Figure (20) - Cross over cable

Rolled Cable

Although rolled cable is not used to connect any Ethernet connections together, you can use a rolled Ethernet cable to connect a host to a router console serial communication (com) port. If you have a Cisco router of switch, you would use this cable to connect your PC running Hyper Terminal to the Cisco hardware. Eight wires are used in this cable to connect serial devices, although not all eight are used to send information, just as in Ethernet networking

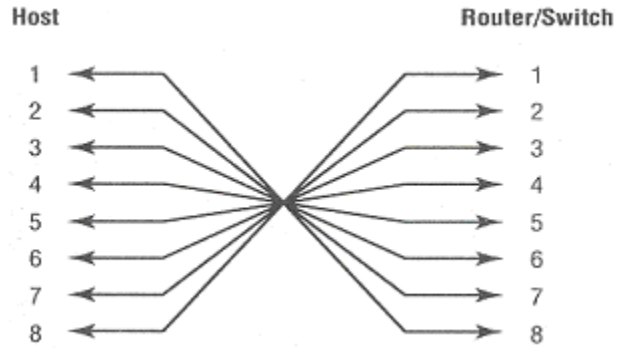


Figure (21) - Rolled cable

Ethernet Addressing

MEDIA ACCESS CONTROL ADDRESS

Ethernet addressing uses Media Access Control (MAC) Address burned into each and every Ethernet Network Interface Card (NIC). The MAC or hardware address, is a 48-bit (6-byte) address written in a hexadecimal format.

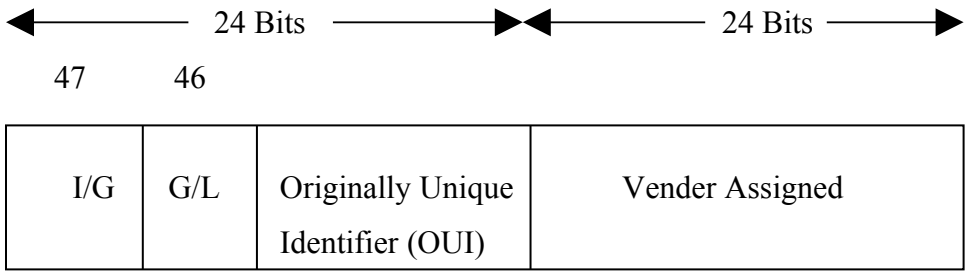


Figure (22) – Ethernet addressing using MAC addresses

The organizationally unique identifier (OUI) is assigned by the IEEE to an organization. It's composed of 24 bits, or 3 bytes. The organization, in turn, assigns a globally administered address (24 bits, or 3 bytes) that is unique (supposedly, again-no guarantees) to each and every adapter they manufacture. The high-order bit is the individual/Group (I/G) bit. When it has a value of 0, we can assume that the address is MAC address of a device and May well appear in the source portion of the MAC header. When it is a 1, we can assume that the address represents either a broadcast or multicast address in Ethernet, or a broadcast .The next bit is the G/L bit (also known as U/L, where U means universal). When set to 0,this bit represents a globally administered address (as by IEEE). When the bit is 1, it represents a locally governed and administered address (as in DECnet). The low-order 24 bits of an Ethernet address represent a locally administered or manufacturer-assigned code. This portion commonly starts with 24 0s for the first card made and continues in order until there are 24 1s for the last card made. You will find that many manufacturers use these same six hex digits as the last six characters of their serial number on the same card.

IP ADDRESSING

An IP address is a numeric identifier assigned to each machine on an IP network. It designates the specific location of a device on the network.

An IP address is a software address, not a hardware address- the latter is hard-coded on a Network Interface Card (NIC) and used for finding hosts on a local network. IP addressing was designed to allow a host on one network to communicate with a host on a different network, regardless of the type of LANs the hosts are participating in.

There are two IP addressing schemes:

1. Hierarchical IP addressing
2. Private IP Addressing

Hierarchical IP addressing

An IP address consists of 32 bits of information. These bits are divided into four sections, referred to as octets or bytes, each containing 1 byte (8 bits). You can depict an IP address using one of three methods:

1. Dotted-decimal, as in 172.16.30.56
2. Binary, as in 10101100.00010000.00011110.00111000
3. Hexadecimal, as in AC.10.1E.38

All these examples represent same IP address. The 32-bit IP address is a structured or hierarchical address, as opposed to a flat or nonhierarchical address. Although either type of addressing scheme could have been used, hierarchical addressing was chosen for a good reason. The advantage of this scheme is that it can handle a large number of addresses, namely 4.3 billion. The disadvantage of the flat addressing scheme, and the reason it's not used for IP addressing, relates to routing. If every address were unique, all routers on the Internet would need to store the address of each and every machine on the Internet. This would make efficient routing impossible, even if only a fraction of the possible addresses were used.

The solution to this problem is to use a two or three-level, hierarchical addressing scheme that is structured by network and host, or network, subnet, and host.

This two- or three-level scheme is comparable to a telephone number. The first section, the area code, designates a very large area. The second section, the prefix, narrows the scope to a local calling area. The final segment, the customer number, zooms in on the specific connection. IP address uses the same type of layered structure. Rather than all 32 bits being treated as a unique identifier, as in flat addressing, a part of the address is designated as the network address, and the other part is designated as either the subnet and host or just the node address.

NETWORK ADDRESSING

The network address (which can also be called the network number) uniquely identifies each network. Every machine on the same network shares that network address as part of its IP address. In the IP address 172.16.30.56, for example, 172.16 is the network address.

The nodes address is assigned to, and uniquely identifies, each machine on a network. This part of the address must be unique because it identifies a particular machine-an individual as opposed to a network, which is a group. This number can also be referred to as a host address. In the sample IP address 172.16.30.56 is the node address.

The designers of the Internet decided to create classes of networks based on network size. For the small number of networks possessing a very large number of nodes, they created the rank *Class 'A' network.* At the other extreme is the *Class 'C' network*, which is reserved for the numerous networks with a small, is predictably called the *Class 'B' network.*

Subdividing an IP address into a network and node address is determined by the class designation of one's network

	8 Bits	8 Bits	8 Bits	8 Bits
Class 'A' :	Network	Host	Host	Host

	8 Bits	8 Bits	8 Bits	8 Bits
Class 'B' :	Network	Network	Host	Host

	8 Bits	8 Bits	8 Bits	8 Bits
Class ‘C’ :	Network	Network	Network	Host

Class ‘D’ : Multicast

Class ‘E’ : Research

Figure (23) - Summary of the three classes of Networks

To ensure efficient routing, Internet designers defined a mandate for the leading-bits section of the address for each different network class. For example, since a router knows that a Class ‘A’ network address always starts with a 0, the router might be able to speed a packet on its way after reading only the first bit of its address. This is where the address schemes define the difference between a Class ‘A’, a Class ‘B’, and a Class ‘C’ address. In the next section, I will discuss the differences between these three classes, followed by a discussion of the Class ‘D’ and Class ‘E’ address.

Network Address Range - Class ‘A’

The designers of the IP address scheme said that the first bit of the first byte in a Class ‘A’ network address must always be off, or 0. This means a Class ‘A’ address must be between 0 and 127. So a Class ‘A’ network is defined in the first octet between 0 and 127, and it can’t be less or more.

Network Address Range - Class ‘B’

In a Class ‘B’ network, the RFCs state that the first bit of the first byte must always be turned on, but the second bit must always be turned off. If you turn the other 6 bits all off and then all on, you will find the range for a Class ‘B’ network, thus a Class ‘B’ network is defined when the first byte is configured from 128 to191.

Network Address range - Class 'C'

The first three bytes of a Class 'C' network address are dedicated to the network portion of the address, with only one measly byte remaining for the node address. Thus a class 'C' network is defined when first byte is configured from192 to 223.

Private IP Addresses

These addresses can be used on a private network, but they are not routable through the Internet. This is designed for the purpose of creating a measure of well-needed security, but it also conveniently saves valuable IP address space.

If every host on every network had to have real routable IP address, we would have run out of IP address to hand out years ago. But by using private IP address, ISPs, corporation, and home users only need a relatively tiny group of bona fide IP addresses to connect their networks to the Internet. This is economical because they can use private IP addresses on their inside networks and get along just fine.

To accomplish this task, the ISP and the corporation-the end user, no matter who they are-need to use something called a Network Address Translation (NAT), which basically takes a private and converts it for use on the Internet. Many people can use the same real IP address to transmit out onto the Internet.

APPLICATIONS

There is a long list of application areas, which can be benefited by establishing Computer Networks. Few of the potential applications of Computer Networks are:

1. Information retrieval systems which search for books, technical reports, papers and articles on particular topics
2. News access machines, which can search past news, stories or abstracts with given search criteria.
3. Airline reservation, hotel booking, railway-reservation, car-rental, etc.

4. A writer's aid: a dictionary, thesaurus, phrase generator, indexed dictionary of quotations, and encyclopedia.
5. Stock market information systems which allow searches for stocks that meet certain criteria, performance comparisons, moving averages, and various forecasting techniques.
6. Electronic Financial Transactions (EFT) between banks and via cheque clearing house.
7. Games of the type that grow or change with various enthusiasts adding to the complexity or diversity.
8. Electronic Mail Messages Systems (EMMS).
9. Corporate information systems such as marketing information system, customer information system, product information system, personnel information system, etc.
10. Corporate systems of different systems such as Order-Entry System, Centralized Purchasing, Distributed Inventory Control, etc.
11. On-line systems for Investment Advice and Management, Tax Minimization, etc.
12. Resources of interest to a home user.
13. Sports results.
14. Theatre, movies, and community events information.
15. Shopping information, prices, and advertisements.
16. Restaurants; good food guide.
17. Household magazine, recipes, book reviews, film reviews.
18. Holidays, hotels, travel booking.
19. Radio and TV programmes.
20. Medical assistance service.
21. Insurance information.
22. Computer Assisted Instruction (CAI).
23. School homework, quizzes, tests.
24. Message sending service.
25. Directories.

26. Consumer reports.
27. Employment directories and Job opportunities.
28. Tax information and Tax assistance.
29. Journey planning assistance viz. Train, bus, plane etc.
30. Catalogue of Open University and Virtual University courses.

CONCLUSION

After completion of this practical training I conclude that training in the Engineering is an essential task for each and every student and it must be taken seriously. The practical training is a chance to the trainee to gain the practical knowledge in the field and to work in the scheduled environment. Apart from these things it improves the managing qualities, which are essential for an engineer.

It is very fruitful experience for me to overcome my weaknesses and how to face and solve the difficulties arises in the field.

REFERENCES

1) Computer Networks By Andrew S. Tanenbaum.
2) Computer Networks By William Stalling.
3) Wireless Communication & Networking By William Stalling.
4) CCNA Study Guide By BPB Publications.