SHRIMATI INDIRA GANDHI COLLEGE

(Nationally Accredited at 'A' Grade (3rd cycle) by NAAC)

Tiruchirappalli – 620 002.

COMPUTER NETWORK

DEPARTMENTS OF COMPUTER
SCIENCE, MCA
AND INFORMATION TECHNOLOGIES

Chapter 1
Introduction to computer networks

1.1 Introduction

- **Computer network** means an interconnected collection of autonomous computer. Two computers are said to be interconnected if they are able to exchange information. The connection need not be via a copper wire, laser, microwaves, and communication satellites can also be used.

Difference between Computer network and Distributed system:

Computer network:

- Large organizations having their offices spread over a records at the push of a button.

- The organizations computational needs are done by a large number of separate but interconnected computers. These systems are called Computer Networks.

- Two computers are said to be interconnected if they interchange information. The connection between the separate computers can be done via a copper wire, fiber optics, microwaves or communication satellite.

Distributed system:

- A system with one control unit and many slaves, or a large computer with remote printers and terminals is not called a **computer network, it is called a Distributed System.**

- In distributed systems the existence of multiple autonomous computers is not visible to the user. The user can type a command to run a program and it runs.

1.2 Goals and application of Network:

Goals:

- **Resource Sharing** is to make all programs and data available to any one on the network without regard to the physical location of the resource and user. In other words the mere fact that a user happens to be 1000 km away from his data should not prevent him from using the data as the were local. Load sharing is another aspect of resource sharing.

- **High Reliability** is to provide to having alternative source of supply. For example, all files could be replicated on two or three machines, so if one of them is unavailable (due to a hardware failure), other copies could be used. In addition, the presence of multiple CPUs means that if one goes down the other may be able to take over its work, although at reduce performance.

- **Saving Money** is small computer having a much better price/ performance ratio then large once. Mainframes are roughly a factor of ten faster then the fastest single chip microprocessor. But they cost a thousand times more. This goals leads to network with many computer located in the same building such a network is called **LAN (Local Area Network)** to contrast it with for flung **WAN (Wide Area Network)**, which is also called along haul network.

- **Communication medium:** yet another goal of setting up a computer network has little to do with technology. A computer can provide a powerful **communication medium** among widely-separated people. Using a network, it is easy for two or more people who live far apart to write a report together. In the long runs the use of networks to enhance human-to-human communication may prove more important then technical goals such as improve reliability.

Application of Networks:

- **Access to remote programs** a company that has produced a model simulating the world economy may allow its clients to log on over the network and run the program to see how various projected inflation rates, interest rates, and currency fluctuations might affect their businesses. This approach is often preferable to selling the program outright; especially if the model is constantly being adjusted or requires an extremely large mainframe computer to run.

- **Access to remote database** it may soon be easy for the average person sitting at home to make reservations for airplanes, trains, buses, boats, hotels, restaurants, theaters, and so on. Home banking and the automated newspaper also fall in this category.

All these applications use networking for economic reasons; calling up a distant computer via a network is cheaper then calling it directly. The lower rate is possible because a normal telephone call ties up an expense, dedicated circuit for the duration of the call, where as access via a network ties up long-distance lines only while data are actually being transmitted.

- **Value-added communication facilities** is potential widespread network use is as a communication medium. Computer scientists already take it for granted that they can send electronic mail from their terminal to their colleagues anywhere in the world. In the future, it will be possible for everyone, not just people in the computer business, to send and receive electronic mail. Furthermore, this mail will also be able to contain digitized voice, still picture and possibly even moving television and video image.

1.3 Network structure:

Network structure the medium through which a host computer transfers data to and from other computer is called the subnet.
In most wide area networks, the subnet consists of two distinct components:

- **Transmission lines** (also called circuits, channels, or trunks) move bits between machines.

- **Switching elements** are specialized computer used to connect two or more transmission lines.

There are two main types of communication subnets:

1. Broadcast networks:

- Broadcast networks have a single communication channel that is shard or used by all the machines on the network. Short messages called packets sent by any machine are received by all the others.
- Broadcast systems generally use a special code in the address field for addressing a packet to all the concerned computers. This mode of operation is called broadcasting.
- Some broadcast systems also support transmission to a subnet of the machines known as multicasting.
- Upon receiving a packet, a machine checks the address field. If the packet is addressed to it then the packet is processed, otherwise the packet is ignored.

2. Point-to-point networks:

Point to point networks consists of many connections between individual pairs of machines. To go from the source to destination a packet on this types of network may have to go through intermediate computers before they reach the desired computer.

- Often the packets have to follow multiple routes, of different lengths.
- Hence routing algorithms are very important in the point-to-point network.

1.4 Types of Network's:

Local Area Networks (LAN):

- The local area network (LAN) is a network which is designed to operate over a small physical area such as an office, factory or a group of buildings. LANs are very widely used in a variety of applications.
- The personal computers and workstations in the office are interconnected via LAN.
- The exchange of information and sharing of resources becomes easy because of LAN.
- In LAN all the machines are connected to a single cable. Different types of topologies such as Bus, Ring, Star, Tree etc. are used for LANs.
- LAN uses a layered architecture and they are capable of operating a hundreds of Mbits/sec.
- LANs are widely used to allow resources to be shared between personal computers or workstations. The resources to be shared can be hardware like a printer or software or data.

Metropolitan Area Network (MAN):

- A MAN is basically a bigger version of a LAN.
- It can be single network such as a cable TV network, or it be a means of connecting a number of LANs in to a larger network. So that resources can be shared LAN to LAN as well as device to device.

- A MAN is distinguished by the IEEE 802.6 standard or it is also known as Distributed Queue Dual Bus (DQDB).
- The DQDB consists of two unidirectional cables (buses) to which all the computers are connected.
- Each bus has a device which initiates the transmission activity called as the head-end.
- Traffic that is destined for a computer to the right of the sender uses the upper bus and to the left uses the lower bus.

Wide Area Network (WAN):

- When a network spans a large distance or when the computers to be connected to each other or at widely separated locations a local area network cannot be used.
- A wide area network (WAN) must be installed the communication between different users of “WAN” is established using leased telephone lines or satellite links and similar channels.
- It is cheaper and more efficient use the phone network for the links.
- Another example of WAN is an airline reservation system. Terminals are located all over the country which the reservation can be made.
- Because of the large distance involved in the wide area networks, the propagations delays and variable signal travel time are major problems.

Wireless Networks:

- The fastest growing segment of the computer industry is the mobile computers such as note book computers and personal digital assistant (PDAs).
- Wireless LAN is another example of wireless network. Direct digital cellular service CDPD (Cellular Digital Packet Data) is now becoming available.

Inter networks:

- Individual networks are joined in to inter networks by the used internetworking devices like bridges, routers and gateways.

Comparison of LAN and WAN:

S.No.	LAN	WAN
1	The LAN is owned by a person, college, factory etc. It is privately owned network.	WAN can be private or it can be public leased type network.
2	LAN is designed to operate over a small physical area such as office, factory or group of building.	WAN is used for the network that spans over a large distance such as system spanning states countries etc.
3	LAN are easy to design and easy to maintain.	WAN is not so easy to design and maintain.
4	The communication medium used for interconnection is a simple co-axial cable.	The communication medium used in WAN can be PSTN or satellite links due to longer distance involved.
5	Due to shorter distances, problems such as propagation delay do not exist. So LAN can be used for time critical applications.	Due to long distances involved, the problems such as propagation delay, variable signal travel time do exist. So WAN cannot be used for the time critical applications.
6	LAN can operate on very high data rates.	WAN operates on low data rates.
7	In a LAN each station can transmit and receive over the communication medium.	In WAN each station cannot transmit.
8	Local area network operates	WAN operates on the

	on the principle of broadcasting.	principle of switching.

1.5 Design Issues for the Layers:

Some of the key design issues that occur in computer net-workings are

1. Addressing
2. Direction of transmission
3. Error control
4. Avoid loss of sequencing
5. Ability of receiving long messages
6. To use multiplexing and de-multiplexing.

1. Addressing:

- For every layer, it is necessary to have a mechanism to identify senders and receivers.
- Since there are multiple possible destinations, some form of addressing is needed in order to specify a specific destination.

2. **Direction of Transmission:**
    - Another point in design issues is the direction of data transfer.
    - Based on whether the system communicates only in one direction or otherwise, the communication systems are classified as,

i. Simplex systems
ii. Half duplex systems
iii. Full duplex systems

I. Simple systems:

- In these systems the information is communicated in only one direction. For example the radio or TV broadcasting systems can only transmit. They cannot receive.
- In data communication system the simplex communication takes place.
- The communication from CPU to monitor or keyboard to CPU is unidirectional.
- Keyboard and traditional monitors are examples of simplex devices.

II. Half-duplex systems:

- These systems are bi-directional, i.e. they can transmit as well as receive but not simultaneously.
- At a time these systems can either transmit or receive, for example a transreceiver or walky-talky set.
- A data communication system working in the half-duplex mode.
- Each station can transmit and receive, but not at the same time. When one device is ending the other one is receiving and vice versa.

- In half duplex transmission, the entire capacity of the channel is taken over by the transmitting (sending).

III. Full duplex systems:

- These are truly bi-directional systems as they allow the communication to take place in both the directions simultaneously.
- These systems can transmit as well as receive simultaneously, for example the telephone systems.
- A full duplex data communication system each station can transmit and receive simultaneously.
- In full duplex mode, signals going in either direction share the full capacity of link.
- The link may contain two physically separate transmission paths one for sending and another for receiving.
- Otherwise the capacity of channel is divided between signals traveling in both directions.
- Many networks provide at least two logical channels per connection, one for the normal data and the other for the urgent data.

3. Error control:

- Another important issue is the error control because physical communication circuits are not perfect.
- Error detection and correction both are essential.
- Many error detecting and correcting codes are known out of which those agreed by sender and receiver should be used.
- The receiver should be able to tell the sender by some means, that it has received a correct message or a wrong message.

4. Avoid loss of sequencing:

- All the communication channels cannot preserve the order in which messages are sent on it.
- So there is a possibility of loss of sequencing.
- To avoid this, all the pieces should be numbered so that they can be put back together at the receiver in the appropriate sequence.

5. Ability of receiving long messages:

- At several levels, another problem should be solved, which is inability of all processes to accept arbitrarily long messages.
- So a mechanism needs to be developed to disassemble, transmit and then reassemble messages.

6. To use multiplexing and de-multiplexing:

- Multiplexing and de-multiplexing is to be used to share the same channel by many sources simultaneously.
- It can be used for any layer. Multiplexing is needed in the physical layer.

1.6 Connection Oriented and Connectionless Services:

Layers can offer two types of services to the layer above them

1. Connection oriented service
2. Connectionless service

1. Connection Oriented service:

- The connection oriented service is similar to the one provided in the telephone system.
- The service users of the connection oriented service undergo the following sequence of operation.

    1. Establish a connection.
    2. Use the connection.
    3. Release the connection.

- The connection acts like a tube. The sender pushes bits from one end of the tube and the receiver takes them out from the other end.
- The order is generally preserved. That means the order in which the bits are sent is same as the order in which they are received.
- Sometimes after establishing a connection, the sender and receiver can discuss and negotiate about

parameters to be used such as maximum message size, quality of service and some other issues.

2. Connectionless service:

- The connectionless service is similar to the postal service.
- Each message (analogous to a letter) carries the full address of the destination. Each message is routed independently from source to destination through the system.
- It is possible that the order in which the messages are sent and the order in which they are received may be different.

OSI reference model:

- The users of a computer network are locasted over a wide physical range i.e all over the world.
- These standards will fit in to frame work which has been developed by the international organization of standardization(ISO).

- This frame work is called as model for open system inter connection and it is normally referred to as OSI reference model

- The OSI model shown in fig1.7.1 does not contain the physical medium.
- This model is based on a proposal developed by the International Standards Organization (ISO).

- It is called as ISO-OSI (Open System Interconnection) reference model because it is designed to deal with open systems i.e. the systems which are open for communication with other systems.

Level	Name of the layer	Functions
1.	Physical layer	Make and break connections, define voltages and data rates, convert data bits into electrical signal. Decide whether transmission is simplex, half duplex or full duplex.
2.	Data link layer	Synchronization, error detection and correction. To assemble outgoing messages into frames.
3.	Network layer	Routing of the signals, divide the outgoing message into packets, to act as network controller for routing data.
4.	Transport layer	Decide whether transmission should be parallel or single path, multiplexing, splitting or segmenting the data, to break data into smaller units for efficient handling.
5.	Session layer	To manage and synchronize conversation between two systems. It controls logging on and off, user identification, billing and session

		management.
6.	Presentation layer	It works as a translating layer.
7.	Application layer	Retransferring files of information, LOGIN, password checking etc.

- The lower three layers are enough for the most of the applications. Each layer is built from electronic circuits and/or software and has a separate existence from the remaining layers.

- Each layer is supposed to handle message or data from the layers which are immediately above or below it.

- This is done by following the protocol rules. Thus each layer takes data from the adjacent layer, handles it according to these rules and then passes the processed data to the next layer on the other side.

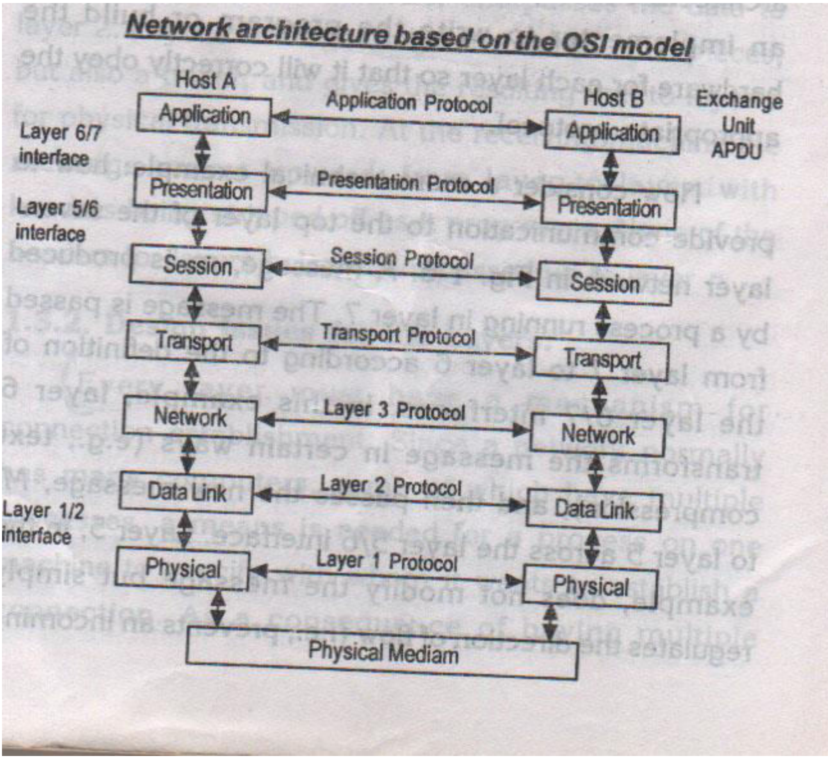


Fig1.7.1: The OSI reference model

Functions of different layers:

Layer1: The physical layer:

Functions of the physical layer are as follows:

- To activate, maintain and deactivate the physical connection.
- To define voltages and data rates needed for transmission.
- To convert the digital bits into electrical signal.
- To decide whether the transmission is simplex, half duplex or full duplex.

Layer2: Data link layer:

- Functions of the data link layer are synchronization and error control for the information which is to be transmitted over the physical link.
- To enable the error detection, it adds error detection bits to the data which is to be transmitted.
- The encoded data is then passed to the physical layer.
- These error detection bits are used by the data link on layer on the other side to detect and correct the errors.
- At this level the outgoing messages are assembled into frames, and the system waits for the acknowledgements to be received after every frame transmitted.

- Correct operation of data link layer ensures reliable transmission of each message. Examples of data layer protocols are HDLC, SDLC and X.25 protocols.

Layer3: The network layer:

The functions of network layer are as follows:

- To route the signals through various channels to the other end.
- To act as the network controller by deciding which route data should take.
- To divide the outgoing messages in to packets and to assemble incoming packets into messages for the higher levels.
- In short the network layers act as network controller for routing data.

Layer4: Transport layer:

As the name suggested this layer provides the transport services. The functions of the transport layers are as listed below:

- It decides if the data transmission should take place on parallel paths or single path.
- It does the functions such as multiplexing, splitting, or segmenting on the data.
- Transport layer guarantees transmission of data from one end to the other.

- It breaks the data groups in to smaller units so that they are handled more efficiently by the network layer.

Layer5: The session layer:

- This layer manages and synchronizes conversations between two different applications. This is the level at which the user will establish system to system connection.
- It controls logging on and off, user identification, billing and session management.
- In the transmission of data from one system to the other, at session layer streams of data are marked and resynchronized properly so that the ends of messages are not cut prematurely and data loss is avoided.

Layer6: The presentation layer:

- The presentation layer makes its sure that the information is delivered in such a form that the receiving system will understand and use it.
- The form and syntax (language) of the two communicating systems can be different. E.g. one system is using the ASCII code for file transfer and other one uses IBM’s EBCDIC.

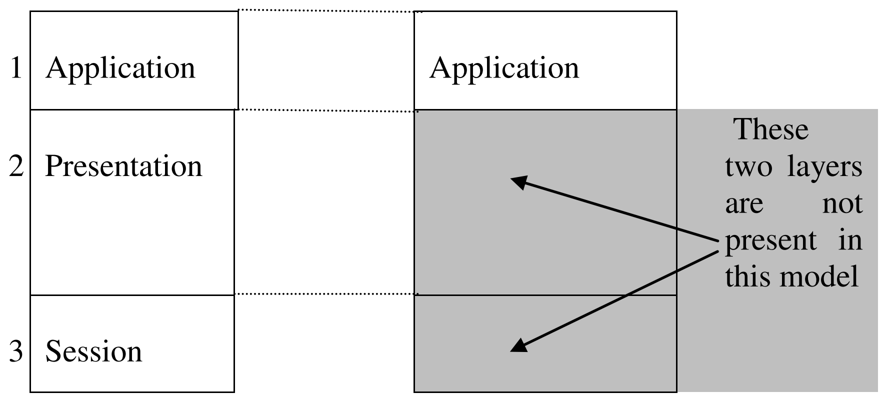
- Under such conditions the presentation layer provides the "translation" from ASCII to EBCDIC and vice versa.

Layer7: Application layer:

- It provides different services such as manipulation of information in various ways, retransferring the files of information, distributing the results etc. To the user who is sitting above this layer.
- The functions such as LOGIN or password checking are also performed by the application layer.

1.8 Description of TCP/IP model:

TCP/IP model has only 4 layers shown in the figure



4	Transport		Transport
5	Network		Internet
6	Data link		Host-to-network
7	Physical		

Fig1.8.1: TCP/IP model

Description of TCP/IP model

As shown in fig 1.8.1, the TCP/IP model has only four layers.

Internet layer:

- This layer is called as the internet layer and it holds the whole architecture together.
- The task of this layer is to allow the host to insert packets into any network and then make them travel independently to the destination.
- The order in which the packets are received can be different from the sequence in which they were sent.
- Then the higher layers are supposed to arrange them in the proper order.

- So routing of packets and congestion are important issues related to this layer.
- Hence TCP/IP internet layer is very similar to the network layer in OSI model.

Transport layer:

- The end to end protocols used here are TCP and UDP (User datagram protocol).
- TCP is a reliable connection oriented protocol. It allows a byte stream transmitted from one machine to be delivered to the other machine without introducing any errors.
- TCP also handles the flow control.
- UDP (user datagram protocol) is the second protocol used in the transport layer.
- It is an unreliable, connectionless protocol and used for the applications which do not want the TCP's sequencing or flow control.
- UDP is also preferred over TCP in those applications in which prompt delivery is more important than accurate delivery. It is used in transmitting speech or video.

Application layer:

- TCP/IP model does not have session or presentation layers, because they are of little importance in most applications.

- The layer on top of transport layer is called as application layer.

Host-to-network layer:

- This is the lowest layer in TCP/IP reference model.
- The host has to connect to the network using some protocol, so that it can send the IP packets over it.
- This protocol varies from host to host and network to network.

Chapter2

Physical layer

2.1 Introduction

The theoretical basic for data communication:

Information can be transmitted on wires by varying some physical property such a voltage or current. By representing the value of this voltage or current as a single valued function of time f(t) we can model the behavior of the single and analyze it mathematically. In early 19th century, the great French mathematician jean Fourier provides that any periodic function g(t) with a period T can be contrasted by summing an infinite number of sines and cosines called Fourier series. From the Fourier series the function can be reconstructed i.e., it the period T, is known and the amplitude is given the original function of time can be found from the sum of the series. A data signal that has a finite duration can handle by just imagining that it repeats the entire pattern over and over forever. Thus Fourier analysis from the theoretical basis for data communication.

2.2 Transmission Media

we can classify the transmission media as shown in fig2.2.1 into two categories.

Transmission Media:

Media are what the message is transmitted over. In other words a communication channel is also called as a medium.

Classification of Transmission Media

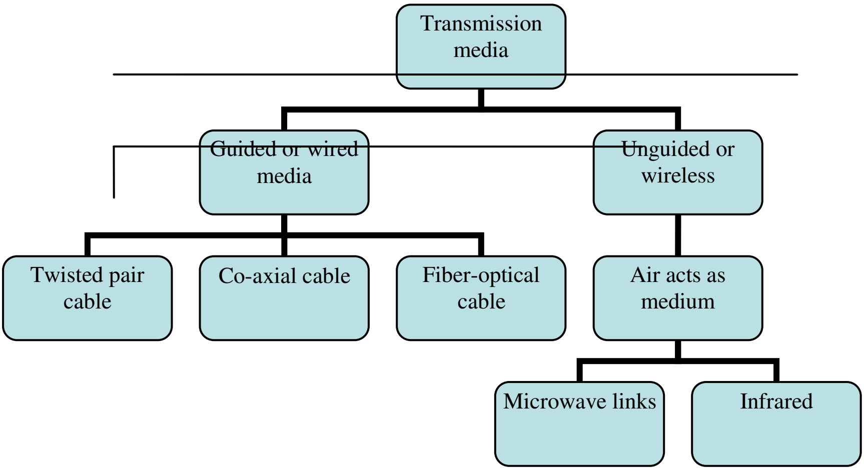


Fig 2.2.1 Classification of transmission media

Media are roughly grouped into two classes:

- Guided media
- Unguided media

I. Guided media: Guided media is a communication medium which allows the data to get guided along it. For this the media need to have a point to point physical connection.

II. Unguided media: The wireless media is also called as an unguided media.

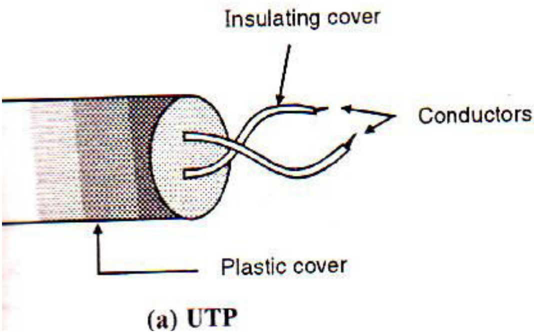
Types of Wired Media:

The most commonly used networking media are:

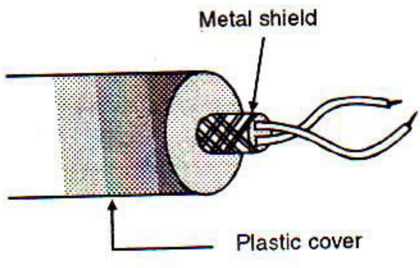
- ❖ Co-axial cable
- ❖ Twisted pair cable
- ❖ Optical fiber cable.

Twisted Pair Cables:

The construction of twisted pair cable is as shown in figure 2.1.2. This is also commonly used medium and it is cheaper than the co-axial cable.



(a) UTP



(b) STP

Fig2.1.2. Construction of twisted pair cables

Types of Twisted Pair cables:

- The two commonly used types of twisted pair cables are as follows
  - Unshielded twisted pair (UTP)
  - Shielded twisted pair (STP)

UTP:

- A twisted pair consists of two insulated conductor twisted together in the spiral form as shown in 2.1.2. It can be shielded or unshielded.
- The unshielded twisted pair cables are very cheap and easy to install. But they are badly affected by the noise interference.

STP:

- It reduces the interference of the noise but makes the cable bulky and expensive.
- So practically UTP is more used than STP. The STP was developed by IBM and is used primarily for the IBM only.
- Twisted pairs can be used for either analog or digital transmission. The bandwidth supported by the wire depends on the thickness of the wire and the distance travelled.
- Twisted pairs support several megabits/sec for a few kilometers and have less cost.

-

Applications of Twisted Pair Cables:

Some of the applications of twisted pair cables are as follows:

- In telephone lines to carry voice and data channels.
- In the local loop.
- Local area networks such as 10 Base-T and 100 Base-T. Use the twisted pair cables.
- In the ISDN (Integrated Services Digital Network).

Co-axial cables:

- The construction of co-axial cable is as shown in figure 2.1.3. It consists of two concentric conductors separated by a dielectric material.
- The external conductor is metallic braid and used for the purpose of shielding. The co-axial cable may contain one or more co-axial pairs.

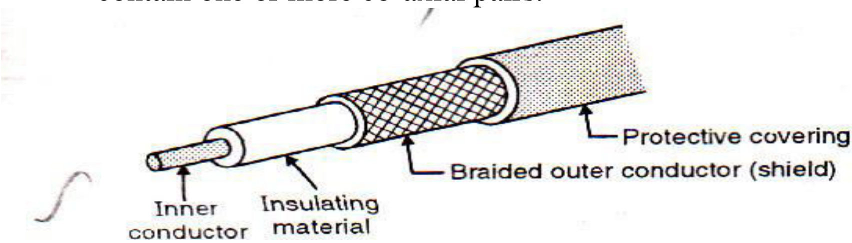


Fig 2.1.3 Construction of coaxial cable

- The co-axial cable was initially developed as the backbone of analog telephone networks where a single telephone cable would be used to carry more than 10,000 voice channels at a time.
- The co-axial cable is used for its large bandwidth and high noise immunity.

Characteristics of a Co-Axial cable:

The important characteristics of a co-axial cable are as follows:

- Two types of cable having 75ohms and 50ohms impedance are available.
- Due to the shield provided, this cable has excellent noise immunity.
- It has a large bandwidth and low losses.
- This cable is suitable for point to point or point to multipoint applications. In fact this is the most widely used medium for local area networks.
- These cables are costlier than twisted pair cables but they are cheaper than the optical fiber cables.
- It has a data rate of 10 Mbps which can be increased with the increase in diameter of the inner conductor.
- The specified maximum number of nodes on a thinnet segment is 30 nodes and on a thicknet it is 100 nodes.
- The attenuation is less as compared to the twisted pair cable.
- Co-axial cables are easy to install. They are often installed either in a device to device daisy chain (Ethernet0 or a star (ARC net).
- Co-axial cables are relatively inexpensive.
-

Applications of Co-axial Cables:

- Analog telephone networks
- Digital telephone network
- Cable TV
- Traditional Ethernet LANs

- Digital transmission
- Thick Ethernet

Optical Fiber Cables:

The construction of an optical fiber cable is shown in the figure

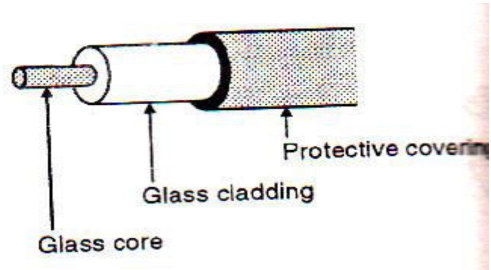


Fig 2.1.4 Construction of optical fiber cable

- It consists of an inner glass core surrounded by a glass cladding which has a lower refractive index.
- Digital signals are transmitted in the form of intensity-modulated light signal which is trapped in the glass core.
- Light is launched into the fiber using a light source such us a light emitting diode (LED) or laser.
- It is detected on the other side using a photo detector such as phototransistor.

- The optical fiber cables are costlier than the other two types but they have many advantages over the other two types.

Characteristics of Optical Fiber Cables:

- Higher bandwidth therefore can operate at higher data rates.
- Reduced losses as the signal attenuation is low.
- Distortion is reduced hence better quality is assured.
- They are immune to electromagnetic interferences.
- Small size and light weight.
- Used for point to point communication.

Applications:

- Optical fiber transmission systems are widely used in the back bone of networks. Current optical fiber systems provide transmission rates from 45 Mb/s to 9.6 Gb/s using the single wave length transmission.
- The installation cost of optical fibers is higher than that for the co-axial or twisted wire cables.
- Optical fibers are now used in the telephone systems.
- In the Local Area Networks (LANs).
- Optical fiber transmission systems are widely used in the back bone of networks. Current optical fiber systems provide transmission rates from 45 Mb/s to 9.6 Gb/s using the single wave length transmission.
- The installation cost of optical fibers is higher than that for the co-axial or twisted wire cables.
- Optical fibers are now used in the telephone systems.
- In the Local Area Networks (LANs).

Advantages of Optical Fibers:

Some of the advantages of fiber optic communication over the conventional means of communication are as follows

- **Small Size and Light Weight:**

The size (diameter) of the optical fiber is very small (it is comparable to the diameter of human hair). Therefore a large number of optical fibers can fit into a cable of small diameter.

- **Easy available and low cost:**

The material used for the manufacturing of optical fiber is "silica Glass". This material is easily available. So the optical fibers cost lower than the cable with metallic conductors.

- **No Electrical and Electromagnetic interference**:

Since the transmission takes place in the form of light rays the signal is not affected due to any electrical or electromagnetic interference.

- **Large Bandwidth:**

As the light rays have a very high frequency in the GHZ range, the bandwidth of the optical fiber is extremely large. This allows transmission of more number of channels. Therefore the information carrying capacity of an optical fiber is much higher than that of a co-axial cable.

- **Other Advantages:**

In addition to the advantages discussed earlier, the optical fiber communication has the following other advantages:

- No cross-talk inside the optical fiber cable.
- Signal can be sent up to 100 times faster.
- Intermediate amplifiers are not required as the transmission losses in the fiber are low.
- Group loops are absent.
- Installation is easy as the fiber optic cables are flexible.
- These cables are not affected by the drastic environmental conditions. Because of all these advantages the optical fiber cable is replacing the conventional metallic conductor cable rapidly in many areas.

Disadvantages of optical fiber:

Some of the disadvantages of optical communication system are:

1. Sophisticated plants are required for manufacturing optical fibers.
2. The initial cost incurred is high.
3. Joining the optical fibers is a difficult job.

Comparisons of wired Media:

S. No	Twisted Pair Cable	Co-axial cable	Optical fiber
1	Transmission of signals takes place in the	Transmission of signals takes place in the	Signal transmission takes place in

	electrical form over the metallic conducting wires.	electrical form over the inner conductor of the cable.	an optical form over a glass fiber.
2	Noise immunity is low. Therefore more distortion.	Higher noise immunity than the twisted pair cable.	Higher noise immunity as the light rays are unaffected by the electrical noise.
3	Affected due to external magnetic field.	Less affected due to external magnetic field	Not affected by the external magnetic field.
4	Short circuit between the two conductors is possible.	Short circuit between the two conductors is possible.	Short circuit is not possible.
5	Cheapest	Moderately expensive.	Expensive
6	Can support low data rates	Moderately high data rates.	Very high data rates.
7	Low bandwidth	Moderately high bandwidth.	Very high bandwidth.
8	Attenuation is very high.	Attenuation is low.	Attenuation is very low.
9	Installation is easy.	Installation is fairly easy.	Installation is difficult.
10	Electromagnetic interference (EMI) can take	EMI is reduced due to shielding.	EMI is not present.

	place.		

2.3 Network Topology:

What is a topology?

The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Physical topology should not be confused with logical topology which is method used to pass information between workstation.

Types of Topologies:

The following section discuss the physical topologies Used in networks and other related topics.

- Liner bus
- Star
- Star-wired Ring
- Tree
- Considerations when choosing a topology
- Summary chart.

<u>Linear Bus:</u>

- A linear bus topology consists of a main run of cable with a terminator at each end.

- All nodes (file server, workstations, and peripherals) are connected use a linear bus topology.

- Ethernet and local talk networks use a linear bus topology.

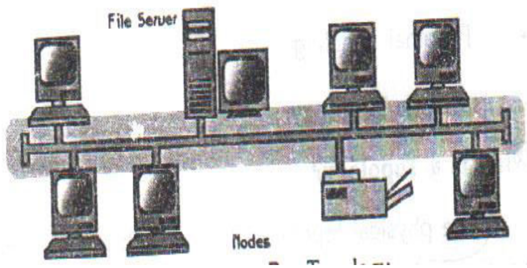


Fig 2.3.1. Linear Bus Topology

Advantage of linear bus topology:

- Easy to connect a computer or peripheral to a linear bus.

- Requires less cable length than a star topology.

Disadvantages of linear bus topology:

- Entire network shut down if there is a break in the main cable.

- Terminators are required at both ends of the backbone cable.

- Difficult to identify the problem if the entire network shuts down.

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

Star:

- A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub or concentrator.(see fig 2.3.2)
- Data on a star network passes through the hub or concentrator before continuing its destination.
- The hub or concentrator manages and controls all functions of the network.
- It also acts as a repeater for the data flow.
- This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.

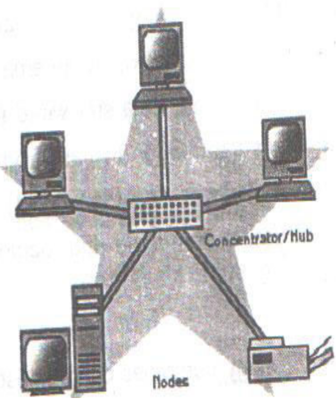


Fig 2.3.2 Linear bus topology

Advantage of star topology:

- Easy to install and wire.
- No disruptions to the network then connecting or removing devices.
- Easy to detect faults and to remove parts.

Disadvantage of star topology:

- Requires more cable length than a linear topology.
- If the hub or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the concentrators.
- Token ring uses a similar topology, called the star-wire ring.

Star-wired ring:

- 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 fig 2.3.3)

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

Tree:

- A tree topology characteristic of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable.

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

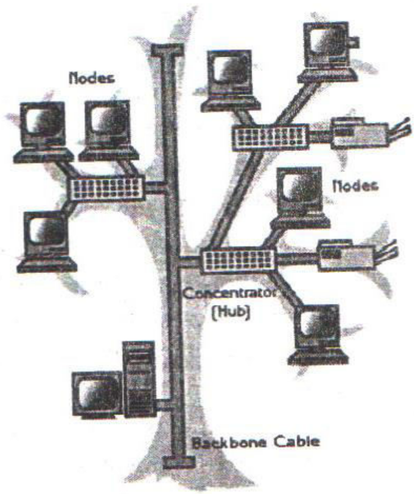


Fig 2.3.3 Tree topology

Advantage of Tree Topology:

- Point-to-point wiring for individual segments.

- Supported by several hardware and software venders.

Disadvantage of a Tree Topology:

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

Considerations When Choosing a Topology:

- **Money.** A linear bus network may be the least expensive way to install a network; you do not have to purchase concentrators.
- **Length of cable needed.** The linear bus network uses shorter lengths of cable.
- **Future growth.** With a star topology, expanding a network is easily done by adding another concentrator.

- **Cable type.** The most common cable in schools is unshielded twisted pair, which is most often used with star topologies.

Summary Chart

Physical Topology	Common Cable	Common Protocol
Linear Bus	Twisted Pair, Coaxial, Fiber	Ethernet, Local Talk
Star	Twisted Pair , Fiber	Ethernet, Local Talk
Star-Wired Ring	Twisted Pair	Token Ring
Tree	Twisted Pair, Coaxial, Fiber	Ethernet

2.4 ISDN – INDEGRATED SERVICES DIGITAL NETWORK:

INTEGRATED SERCIVEC DIGITAL NETWORK, its primary goal the integration of voice and non-voice services. Since ISDN is basically a redesign of the telephone system, the international coordination is taking place within CCITT (Consultative Committee of International Telegraphic and Telephone) and its many study groups.

ISDN services:

ISDN data transmission services will allow users to connect their ISDN computer to any other one in the world in spite of incompatible national telephone systems. Closed user group, in which the members of the group can only call other members of the group, and no calls from outside the group can come in, is possible in data transmission. This feature makes if possible for a company to use the telephone system as a private network. A new communication services that is expected to become widespread with ISDN is videotext, which provides the following services.

- Interactive access to a remote database.
- Director assistance.
- Yellow pages (for advertisement).
- E- Commerce (Buy products or reserve a ticket in railways).
- E- Mail (send letters).

Another ISDN service is facsimile (fax), which is used to send charts, signatures, diagrams and blue prints. Video image transmission helps to prevent fraud in electronic fund transfer (EFT).

Chapter 3

THE DATA LINK LAYER

3.1 Data link layer design issues:

The data link layer has a number of specific functions to carry out. These functions include providing a well defined service interface to the network layer, determining how the bits of the physical layer are grouped into frames, dealing with transmission errors, regulating the flow of frames so that slow receivers are not swamped by fast senders, and general link management. In the following section we examine each of these issues in turn.

Services provided to the network layer:

The function of the data link layer is to provide services to the network layer. The principle service is transferring data from the network layer on the source machine to the network layer entity; call it a process, in the network layer that hands some bits to the data link layer for transmission to the destination. The job of the data link layer is to transmit the bits to the destination machine, so they can be handed over to the network layer there. The data link layer can be designed to offer various services. The actual services offered can vary from system to system. Three reasonable possibilities are:

Unacknowledged connectionless service:

No connection is established between the source and destination machine before or after the frame is sent and the destination machine sends no acknowledgement. If a frame is lost due to noise, no attempt is made to recover in the data link layer. Many LANs have unacknowledged connectionless service in the data link layer.

Acknowledged connectionless service:

When this service is offered, there are still no connections used, but each frame sent is individually acknowledged. In this way, the sender knows whether or not a frame has arrived safely. If it has not arrived within a specified time interval, it can be sent again.

Connection-oriented service:

With this service the source and destination machine establish a connection before any data are transferred. Each frame sent over the connection is numbered, and the data link layer guarantees that each frame sent is indeed received. In this service three phases:

Establishment,
Maintenance,
Termination of connection takes place.

Framing:

In order to provide service to the network layer, the data link layer must use the service provided to it by the physical layer. What the physical layer does is accept a raw bit stream and attempt to deliver it to the destination. This bit stream is not guaranteed to be error free. The data link layer to break the bit stream up into discrete frames and compute the destination, the checksum for each frame. When a frame arrives at the destination, the checksum is recomputed. If the newly computed checksum is different from the one contained in the frame, the data link layer knows that an error has occurred and takes steps to deal with it. The four commonly used methods for breaking the bit streams up into frames are:

Character count:

In this method a field is used as a header to specify the number of characters in the frame.

When the data link layer at the destination sees the character count, it knows how many characters follow, and hence where the end of the frame is.

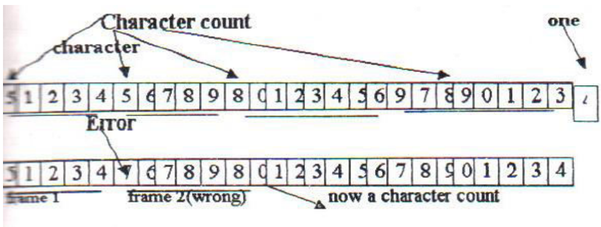
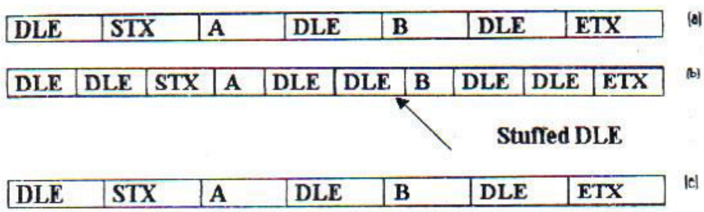


Fig 3.1.1Starting and ending characters, with character stuffing:

In this method each frame starts with the ASCII character sequence DLE STX and with the sequence

DLX ETX. (DLX is data link Escape, STX Start of Text, and ETX is End of Text)

In this way if the destination ever loses track of the frame boundaries, all it has to do is to look for DLE STX or DLE ETX characters to figure out where it is.

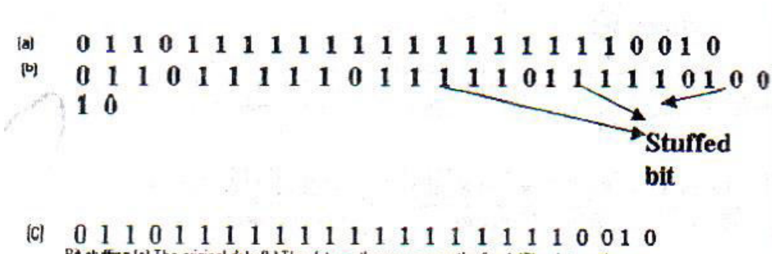


(a)data sent b the n/w layer (b) data after being char stuffed by the data link layer (c)data passed to the n/w layer on the received side

Fig 3.1.2 Starting and ending flags, with bit stuffing:

In this method each frame beings and ends with a special bit pattern, namely 01111110.

Whenever the sender's data link layer encounters five consecutive ones in the data, it automatically stuffs a 0 bit into the outgoing bit stream.



Bit stuffing (a) The original data (b) The data as they appear on the line (c)The data as they are stored in the receiver meomory after destuffing

Fig 3.1.3 Physical layer coding violations:

This method of framing is only applicable to networks in which the encoding on the physical medium contains some redundancy.

For example, Manchester encoding encodes each 1 bit as a high-low pair and each 0 bit as a low-high pair. The combinations high-high and low-low are not used for data.

3.2 ERROR DETECTION AND CORRECTION

Network designers have developed two basic strategies for dealing with errors. One way is to include enough redundant information along with each block of data sent to enable the receiver to reduce what the transmitted character must have been. This strategy uses error-correcting codes and the other way is only to include enough redundancy to allow the receiver to deduce that an error occurred but not which error, and have it request a transmission. This strategy is uses error detecting codes.

Error-correcting codes:

- A frame consists of m data bits and r redundant or check bits.
- Let the total length be n. an n-bit unit containing data and check bits is often referred to as codeword.
- The number of bit position in which two code words differ is called the Hamming distance.
- This distance is nothing but the number of 1's in EXCLUSIVE OR of the two codes. For example the hamming distance between 11001101 and 10000110 is4. Bit wise exclusive or gives the positions to be inverted as shown below.

```
11001101
     10000110
 ______________
     01001011
     ↑   ↑ ↑ ↑
```

- 1's are required to invert one code to get the other. Thus the distance between the codes is 4. The minimum distance between all possible pairs of code words given in a list is called the hamming distance of the complete code.

The error-correcting and error-detecting properties of a code depend on its hamming distance.

Theorem 1: If the hamming distance of a coding scheme is d+1 then at most d errors can be detected.

Theorem 2: If the hamming distance of a coding scheme is 2d+1 then at most d errors can be corrected.

Hence to detect a single bit error the minimum hamming distance must be 2 and to correct a single bit error the minimum hamming g distance must be 3.

Single bit error detection:

- This is achieved by appending a 0 or 1 at the end of BCD to make it even (or odd).
- After transmission the parity is checked. If there is disparity there is a single bit error.
- In general disparity indicates an odd number of errors (minimum 1) and parity indicates an odd even number of errors (minimum 0).

Burst Error Detection:

Suppose we want to transmit the BCD's of the sequence 8, 5, 6, 3, 6 i.e., 1000 0101 0110 0011 0110 arrange them in 5*5 matrix by adding the parity bit at each row so as to have even parity.

1	0	0	0	1
0	1	0	1	0
0	1	1	0	0
0	0	1	1	0
0	1	1	0	0

This matrix is transmitted column wise as

Transmitted: 10000|01101|00111|01010|10000
Suppose this is
Received as: 10000|01111|01011|01010|10000
There is burst error of length 5 as indicated. By arranging the received bits as 5*5 matrix and checking for parity of each row we can detect burst error of length <=5.

1	0	0	0	1	Even
0	1	1	1	0	Odd
0	1	0	0	0	Odd
0	1	1	1	0	Odd
0	1	1	0	0	Even

Burst error correction:

- In order to correct the burst errors instead of BCD codes the Humming codes are transmitted in the same way as done for detection.
- Since the Humming distance code has built in parity bits by considering the error codes of the received bits the exact location of the erroneous bits can be located.
- The corresponding Humming codes of BCD of the sequence 8, 5, , 3, 6 are (8)1001011, (5)0101101, (6)0110011, (3)0011110 (6)0110011. These are arranged as 5*5 matrix and this matrix is transmitted column wise.

1	0	0	1	0	1	1
0	1	0	1	1	0	1
0	1	1	0	0	1	1
0	0	1	1	1	1	0
0	1	1	0	0	1	1

Transmitted:
10000|01101|00111|11010|01010|10111|111
-1
Received as:
10000|01111|01011|11010|01010|10111|111
01

Burst error

There is a burst error of length 5 as indicated. By arranging the received bits as a 5*5 matrix and checking for parity of each row we can correct burst error of length<=5.

Received array							Error code			
1	0	0	1	0	1	1	4	2	1	
0	1	1	1	1	0	1	0	0	0	No error
0	1	0	0	0	1	1	1	0	1	Error in location 5
0	1	1	1	1	1	0	1	0	1	Error in location 5
0	1	1	0	0	1	1	1	1	0	Error in location 6

___	0	0	0	No error

3.3 Data Link Control and Protocol

Stop-and-wait protocol:

- This protocol is called one bit protocol because the maximum window size here i.e. n is equal to 1.
- It uses the stop-and-wait technique. The Sender sends one frame and Wait to get its acknowledgement.
- Only after receiving the acknowledgement, does it transmit the next frames.
- So one bit sliding window protocol is also called as **stop-and-wait protocol**.
- The sequence of events taking place when a frame is transmitted and received is as follows:
    1. The data link layer of the sending machine fetches the packet from its network layer.
    2. It builds the frame for it and sends it to receiver.
    3. The receiver data link layer checks the received frame for duplication.
    4. If ok, it passes the frame to its network layer.

The operation of protocol:

- The operation of this protocol is based on the ARQ(automatic repeat request) principle.
- In this method the transmitter transmits one frame of data and waits for an acknowledgement from the receiver.
- If it receives a positive acknowledgement (ACK) it transmits the next frame. If it receives a negative acknowledgement (NAK) it transmits the same frame.

Features added for retransmission:

For retransmission, four features are added to the basic flow control mechanism.

1) The transmitter stores the copy of last frames transmitted until it receives an acknowledgement for those frames.
2) For identification purpose both data and ACK frames are numbered alternately 0 and 1. A data 0 frame is acknowledged by an ACK 1 frame indicating that the receiver has received data 0 and is expecting the next data frame numbered 1.
3) If an error occurs while transmission, the receiver sends a NAK frame back to the transmitter for retransmission of the corrupted frame. NAK frame which are not numbered tell the transmitter to retransmit the last frame transmitted.
4) The transmitter has a timer to take care of the frame ACK which are lost. After a specified time if the transmitter does not receive a ACK or NAK frame it retransmits the last frame.

When is the retransmission necessary?

- The retransmission of frame is essential under the following events:
    1. If the received frame is damaged.
    2. If the transmitted frame is lost.
    3. If the acknowledgement from the receiver is lost.

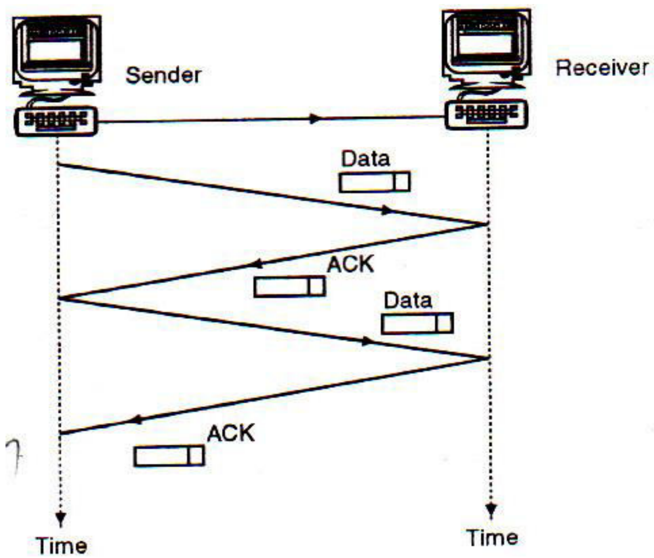


Fig 3.3.1 Stop-and-wait under normal condition

Disadvantage of stop-and-wait protocol:

1. Problem with Stop-and-Wait protocol is that it is very inefficient. At any one moment, only one frame is in transition.

2. The sender will have to wait at least one round trip time before sending next. The waiting can be long for a slow network such as satellite link.

Piggybacking:

- In all the practical situations, the transmission of data needs to be bi-directional. This is called as full-duplex transmission.
- One way of achieving full duplex transmission is to have two separate channels one for forward data transfer and the other for reverse transfer (for acknowledgement)
- But this will waste the bandwidth of the reverse channel almost entirely.
- A better solution would be to use each channel (forward and reverse) to transmit frames bothways, with both channels having the same capacity.
- Let A and B be the users. Then the data frames from A to B are intermixed with the acknowledgements from A to B.
- One more improvement can be made. When a data frame arrives, the receiver waits, does not send the control frame back immediately.
- The receiver waits until its network layer passes in the next data packet.

- The acknowledgement is then attached to this outgoing data frame.

- This technique in which the outgoing acknowledgement is delayed temporarily is called as piggybacking.

Advantage of piggybacking:

The major advantage of piggybacking is better use of available channel bandwidth.

Disadvantage:

1. The disadvantage of piggybacking is the additional complexity.
2. If the data link layer waits too long before transmitting acknowledgement, then the retransmission of frame would take place.

Sliding window Protocols:

Sequence number:

- One of the important features of all the sliding window protocol is that each outbound frame contains a sequence number, ranging from 0 to 2 power n-1.
- The value of n can be arbitrary.

Sliding window:

- Sliding window refers to imaginary boxes at the transmitter and receiver.
- This window holds the frames at either ends and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement.
- So in short we can say that, at any instant of time, the sender maintains a set of sequence numbers corresponding to the frames it is permitted to send.
- These frames which are being permitted to sent are said to be falling in the sending window.
- The receiver also maintains a receiver window. It corresponds to the set of frames it is permitted to accept.

A protocol using Go back-n

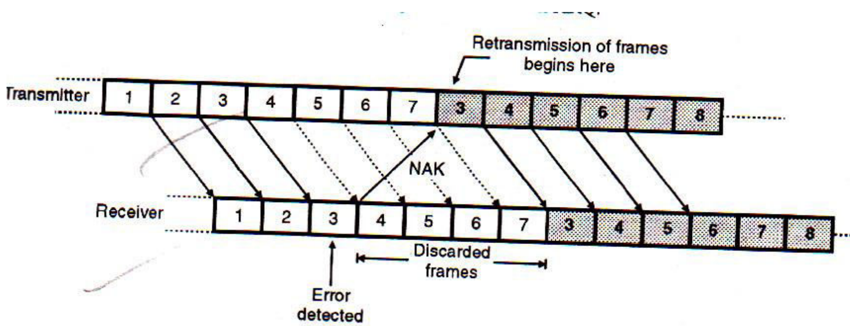


Fig 3.3.2Go back n ARQ system

- The major difference between this and the previous system is that the sender does not wait for ACK signal for the transmission of next frame.
- It transmits the frames continuously as long as it does not receive the "NAK" signal. NAK is the negative

acknowledgement signal sent by the receiver to the transmitter.

- When the receiver detects an error in the third frame as shown in the figure, the receiver sends a NAK signal back to sender.
- But this signal takes some time to reach the transmitter. By that time the transmitter has transmitted frames upto frame 7.
- On reception of the NAK signal, the transmitter will retransmit all the frames from three onwards. The receiver discards all the frames it has receive after three i.e. 3 to 7. It will then receive all the frames that are retransmitted by the transmitter.

Sources of error:

- The errors can get introduced, if the transmitted frames are damaged or lost or if the acknowledgement is lost.
- Let us consider the operation of this protocol under the conditions.

Operation when the frame is damaged:

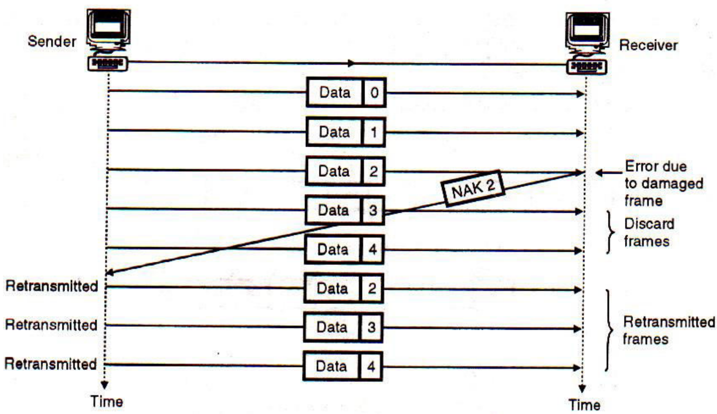


Fig 3.3.3. Go-back-n damaged data frame

- As seen in the figure 3.3.3 the transmitter transmits data frame numbered 0. The receiver returns 0. The receiver returns an ACK 1 indicating that data frame numbered 0 is received without any error.
- The process goes on this way, but if an error occurs the receiver sends a NAK requesting retransmission of the corrupted data frame.

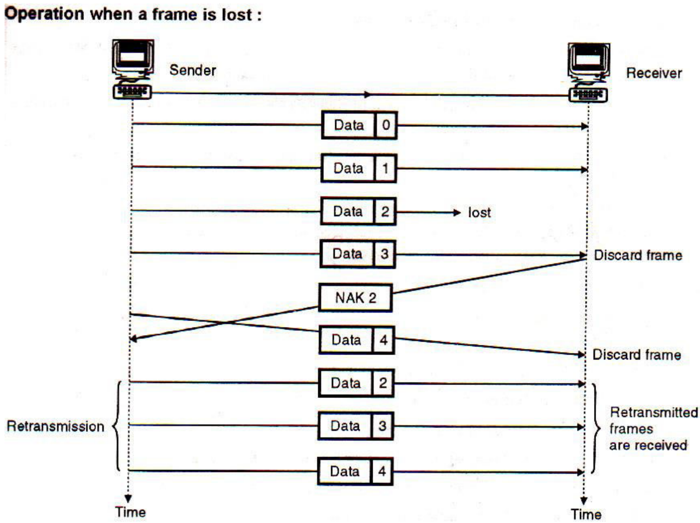


Fig 3.3.4. Go-back-n lost data frame

- The second data frame is damaged, so the error is detected and receiver sendNAK-2 signal back.
- On receiving this signal, the transmitter starts retransmission from frame 2.
- All the frames received after frame 2 are discarded by the receiver.
- The case of lost frame is also treated in the same manner as that of the damaged frame.
- The receiver, if it does not receive a particular data frame it sends a NAK to the transmitter and the transmitter retransmits all the frames sent since the last frame acknowledged.

Operation when the acknowledgement is lost:

- The fig3.3.5 shows the condition for lost acknowledgement. Incase of go-back –n method the transmitter dose not expects an acknowledgement after every data frame.
- It can’t use the absence of sequential ACK numbers identify lost ACK or NAK frames, instead it uses a timer.
- The transmitter can send as many frames as the window allows before waiting for an acknowledgment.
- Once the limit has been reached or the transmitter has no more frames to transmit it must wait till the timer goes off and transmit all the data frames again.
- The disadvantage of go –back-n ARQ protocol is that in noise channels it has poor efficiency because of the need to re transmit the frame in error and all the subsequent frames.

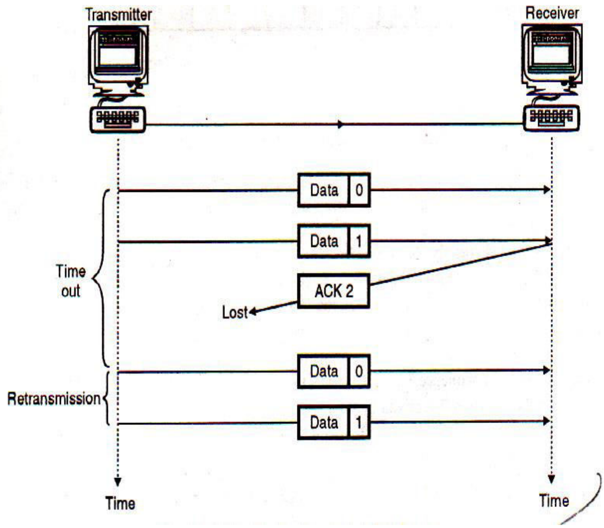


Fig 3.3.5 Go-back-n lost ACK frame

Pipelining:

- In networking a task is often begin before the previous task is complete. This is called Pipelining.
- There is no pipelining in stop-and-wait protocol but the concept of pipelining does apply to GO-Back-n protocol and the selective repeat protocol.
- Pipelining improves the efficiency of transmission

Selective Repeat Protocol:

1. In this method only the specified damaged or lost frame is retransmitted. A selective repeat systems differs from the go-back-n method in the following ways:
2. The receiver can do sorting of data frames and is also able to store frames received after a NAK has been sent until the damaged frame has been replaced.

3. The transmitter must contain a searching mechanism that allows it to find and select only the requested frame for retransmission.
4. The window size in this method is less than or equal to (n+1)/2, whereas in case of go-back-n it is n-1.
5. The principle of operation of this protocol is illustrated in figure 3.3.6

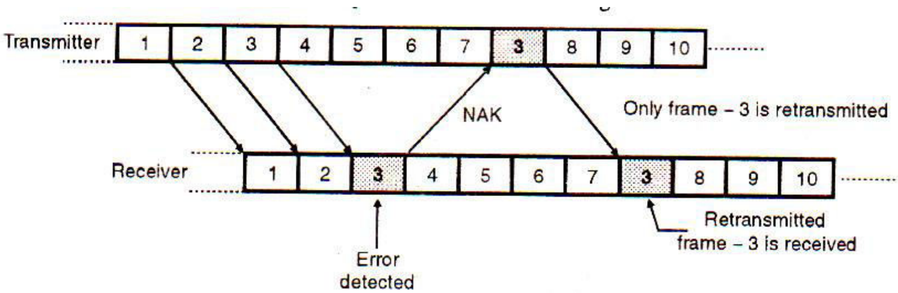


Fig 3.3.6 Selective repeat ARQ system

1. In this system as well, the transmitter does not wait for the ACK signal for the transmission of the next code word. It transmits the code words continuously till it receives the "NAK" signal from the receiver.

2. The receiver sends the "NAK" signal back to the transmitter as soon as it detects an error in the received frame. For example the receiver detects an error in the third frame.
3. By the time this "NAK" signal reaches the transmitter, it has transmitted the frames up to 7 as shown in figure

4. On reception of "NAK" signal, the transmitter will retransmit only the frame-3 and then continues with the sequence 8, 9… as shown in figure 3.3.6

5. The frames 4, 5, 6 and 7 received by the receiver are not discarded by the receiver. The receiver receives the retransmitted frames in between the regular frames. Therefore the receiver will have to maintain the frames sequentially.

6. Thus in selective repeat ARQ only the frame which is damaged or lost is retransmitted by the transmitter.

7. The lost ACK or NAK frames are treated in the same manner as the go-back-n method.

8. When the transmitter reaches either the capacity of its window [(n+1)/2] or the end of its transmission it sets the timer.

9.If no acknowledgement arrives in the time allotted, all the frames that remain unacknowledged are retransmitted.

- The disadvantage of this method is that because of the complexity of sorting and storage required by the receiver and the extra logic needed by the transmitter to select frames for retransmission, the system becomes more expensive.

- The advantage of this system is that it gives the best throughput efficiency. This is due to the use of pipelining selective repeat ARQ.

Protocol Performances:

- The throughput efficiency is the measure of the performance of an ARQ protocol. For any channel a certain bandwidth and bit error rate are specified.
- For such a channel there will be an optimum operating condition that will support for the maximum "Net Data Throughput" (NDT).
- NDT indicates the number of usable characters detected at the receiver. It indicates the number of correct bits detected in a specified period of time.
- This is done by distinguishing between the total number of bits received (including the parity bits) and the number of correct bits.
- Throughput efficiency is defined as

$$\eta = \frac{t_f}{t_f + t_p}$$

Where, t_f = transmission time required to transmit a frame

t_p = Propagation time required to reach destination for a transmitted bit

N=Frame size (bits)

R=Data rate

- Suppose A is a sender and B is a receiver. Then the assumptions are as follows

Assumption:

- Receiver sends an immediate acknowledgement on the reception of a data frame.
- Size of acknowledgement frame is very small.
- Flow is unidirectional.
- Sender receives the acknowledgement after $t_f + t_p + t_p$ time it can send data immediately after receiving acknowledgement.
- If tf and tp are constant, tp/tf is constant.

$$\text{Let } A = \frac{t_p}{t_f}$$

That is $\eta = 1/(1+2A)$

Prorogation time is equal to distance (d) of the link divided by velocity of propagation (v).

That is $t_p = d/v$

Transmission time is equal to the length of the frame (bits), divided by rate R.

That is $t_f = L/R$

$$\text{That is } a = \frac{(d/v)}{(L/R)}$$

$$= \frac{Rd}{Lv}$$

Functions of media access control sublayer:

- To perform the control of access to media
- It performs the unique addressing to stations directly connected to LAN
- Detection of errors.

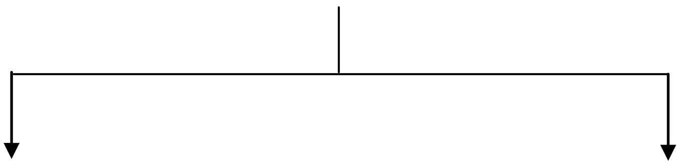
Function of Logical Link Control (LLC) sublayer:

- Error Recovery
- It performs the flow control operation
- User addressing.

The Channel Allocation Problem:

- In a broadcast network, the single broadcast channel is to be allocated to one transmitting user at a time.
- This is called channel allocation. There are two different schemes used for channel allocation as show in fig.

Channel allocation schemes



Static Channel allocation   Dynamic channel allocation

Static Channel Allocation in LANs and MANs:

- The traditional way of allocating a single channel, such as a telephone channel among many users is FDM.

- The Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM) are the examples of static channel allocation.
- In these methods either a fixed frequency or a fixed time slot is allotted to each user.
- The problem in these methods is that if all the N number of users are not using the channel the channel bandwidth is wasted and if there are more than N users who want to use the channel they cannot do so for the lack of bandwidth.
- To see the poor performance of Static Channel , let us consider an example for FDM system where the mean time delay (T) for a channel of capacity C bps, with an arrival rate of λ frames/sec.
- Each frame having a length drawn from an exponential probability density function with mean 1/μ bits/frame is given as,

$$T=1/\ \mu C-\ \lambda$$

- If the single channel is divided into N independent subchannels the above equation is modified as follows:

$$T_{FDM}=1/\mu(C/N)-(\ \lambda/N)\ =N/\mu C-\ \lambda$$

$$T_{FDM}=NT$$

- From the above equation, it is clear that the mean delay using FDM is worse. The static channel allocation has a poor performance with bursty traffic and hence generally dynamic channel allocation is used, for computer networks where the traffic is of bursty nature.

Dynamic Channel Allocation:

In this method no fixed frequency or fixed time slot is allotted to the user. The user can use the single channel as per his requirement. Following assumptions are made for the implementation of this method:

1. **Station model:** Consists of N independent stations each with a program or user that generates frames of transmission.
2. **Single channel:** A single channel is available for all communication.
3. **Collision:** If frames are transmitted at the same time by two or more stations, there is an overlap in time and the resulting single is garbled. This event is called as collision.
4. **Continuous or slotted time:** There is no master clock dividing time into discrete time intervals or time is divided into discrete intervals.
5. **Carrier or No carrier sense:** Stations sense the channel before transmission or they directly transmit without sensing the channel.

ALOHA System:

Systems in which multiple users share a common channel in a way that can lead to conflicts are widely known as Contention systems. The ALOHA system is a contention protocol which was developed at the University of Hawaii in the early 1970’s by Norman Abramson and his colleagues.

The ALOHA system has two versions:

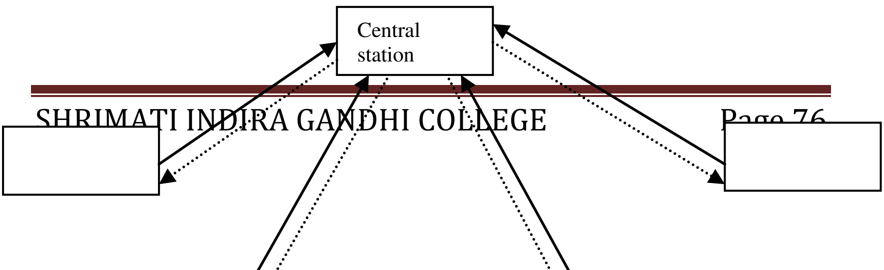
1. Pure ALOHA-does not require global time synchronisation.

2. Slotted ALOHA-requires time synchronisation.

Pure ALOHA:

Essentially it allows for any station the broadcast at any time. If two singles collide, each station simply waits a random time and try again.

When the central station receives a frame it sends an acknowledgement on a different frequency. If a user station receives an acknowledgement it assumes that the transmitted frame was successfully received and if it does get an acknowledgement if assumes that collision had occurred and is ready to retransmit.



F1 F1

F2 F1 F1 F2

Station Station

F2 F2

Station Station

F1=Broadcast

Frequency from the

Individual stations

F2=Broadcast frequency

From the central station

Fig 3.3.7 Pure ALOHA system

The advantage of pure ALOHA is its simplicity in implementation but it’s performance becomes worse as the data traffic on the channel increases.

Slotted ALOHA:

- To overcome the disadvantage of the pure ALOHA system Robert published a method for doubling the capacity of traffic on the channel.
- In this method time is divided up into discrete intervals, each interval corresponding to one frame.
- This method requires the users to agree on slot boundaries. In this method for synchronization one special station emits a pip at the start of each interval, like a clock.

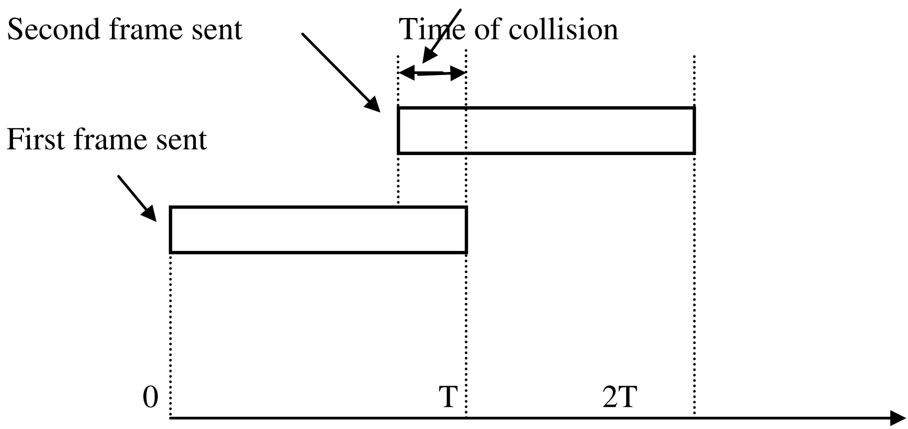


Fig3.3.8 Transmission using pure ALOHA

- Collisions occur if any part of two transmissions overlaps. Suppose that T is time required for one transmission and that two stations must transmit.

- The total time required for both stations to do so successfully is 2T as shown if fig.3.3.8 In case of pure ALOHA allowing a station to transmit at arbitrary times can waste time up to 2T.
- As an alternative, in the slotted ALOHA method the time is divided into intervals (slots) of T units each and require each station to begin each transmission at the beginning of a slot.
- In other words, even if station is ready to send in the middle of a slot, it must wait until the start of the next one as shown in fig.
- In this method a collision occurs when both stations become ready in the same slot.

Carrier Sense Multiple Access (CSMA):

The CSMA protocol operates on the principle of carrier sensing. In this protocol, a station listens to see the presence of transmission (carrier) on the cable and decides to act accordingly.

Non-Persistent CSMA: In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval if time. After this time, if again checks the status of the channel and if the channel is free it will transmit.

1-Persistent CSMA: In this scheme the station which wants to transmit, continuously monitors the channel unit it is idle and then transmits immediately. The disadvantage of this strategy, is that if two stations are waiting then they will transmit simultaneously and collision will take place. This will then require retransmission.

P-persistent CSMA: The possibility of such collisions and retransmissions is reduced in the p-persistent CSMA. In this scheme all the waiting stations are not allowed to transmit simultaneously as soon as the channel becomes idle. A station is assumed to be transmitting with a probability “P”. For example if P=1/6 and if 6 stations are waiting then on an average only one station will transmit and others will wait.

Bit-map Protocol:

- Bit-map protocol is collision-free protocol. In bit-map method, each contention period consists of exactly N slots. If any station has to send frame, then it transmits a 1 bit in the respective slot.
- For example, if station 2 has a frame to send, it transmits a 1 bit during the second slot. In general, station 1 may announce the fact that it has a frame to send by inserting a 1 bit into slot i.
- In this way each station has complete knowledge of which stations wish to transmit. Since everyone agrees on who goes next, there will never be any collisions.
- Protocols like this in which the desire to transmit is broadcast before the actual transmission are called reservation protocols.

8 contention slots Frame

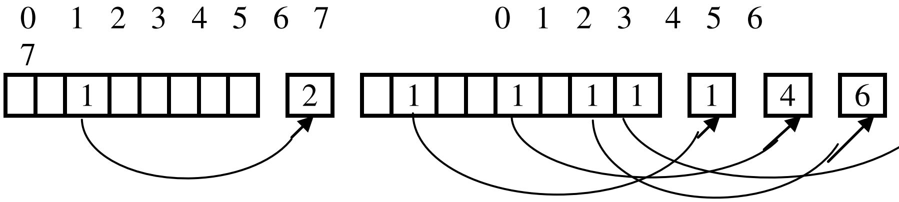


Fig3.3.9 A bit-map protocol

- For analyzing the performance of this protocol, we will measure time in units of the contention bit slot, with data frame consisting of d time units.
- Under low load conditions, the bit map will simply be repeated over and over, for lack of data frames.
- At high-load, when all the stations have something to send all the time, the N bit contention period is prorated over N frames, yielding an overhead of only 1 bit per frame.
- Generally high numbered stations have to wait half a scan (N/2 bit slots) before starting to transmit, low-numbered stations have to wait on an average 1.5 N slots.

Binary Countdown:

- Binary Countdown protocol is used to overcome the overhead 1 bit per station. In binary countdown binary station addresses are used.
- A station wanting to use the channel broadcasts its address as a binary bit string, starting with the high-order bit. All address are assumed to be of same length.

- Here we will see the example to illustrate the working of binary countdown. In this method different station address are ORed together to decide the priority of transmitting.

- If these stations 0001, 1001, 1100, 1011, all are trying to seize the channel for transmission. All the stations at first will broadcast its most significant address bit i.e. 0,1,1,1 respectively.

- The most significant bits are ORed together. Station 0001 see the 1 MSB in other station addresses and knows that a higher numbered station is competing for the channel, so it gives up for the current round.

- Other three stations 1001, 1100, 1011 will continue. The next is 1 at stations 1100, so station 1011 and 1001 give up. Then station 1100 starts transmitting a frame, after which another bidding cycle starts.

Bit time ↓	0 0 0 1	1 0 0 1	1 1 0 0	1 0 1 1	Result of oring
→	0	1	1	1	

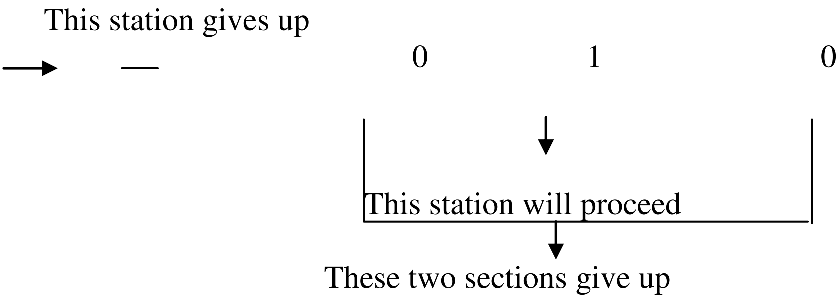


Fig3.3.10Binary countdown

The Adaptive Tree Walk Protocol:

- The assignment of stations to the slots can be done with the help of a simple algorithm called adaptive tree walk protocol.
- It is imagined that the stations are leaves of a binary tree as shown in fig3.3.11
- The tree for eight stations is shown fig3.3.11. as shown in fig 3.3.11 in the first contention slot which is slot 0 if a successful frame transmission occurs all stations are allowed to compete for the channel.
- If there is a collision then during slot 1 only those stations falling under node 2 in the tree may compete. If one of the station acquires the channel, the slot following the frame is reserved for stations falling under node3.
- If on the other hand of there is a collision under node 2 during slot 1 then during slot 2 it is the turn of stations falling under node 4 to compete for the channel.

- If a collision occurs during slot 0, the entire tree is searched, depth first to locate all ready stations. Each bit is associated with some particular node in the tree.
- If a collision occurs, the search continues recursively with the nodes left and right children. If a bit slot is idle or if there is only one station that transmits in it, the

searching of its node can stop, because all ready stations have been located.

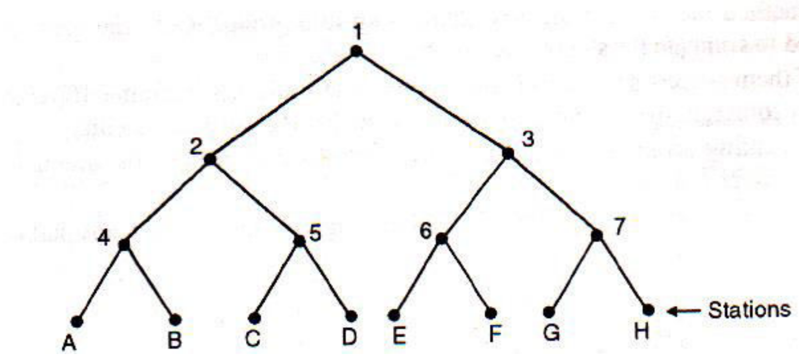


Fig3.3.11 Adaptive tree walk protocol

Chapter 4

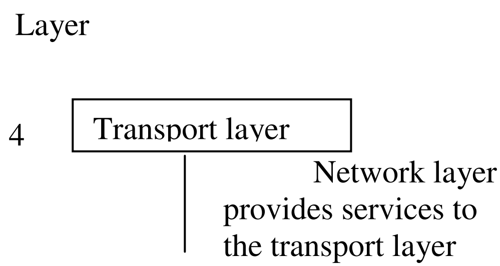
Network Layer

4.1 Introduction

- The network layer is responsible for carrying the packet from the source all the way to destination. In short it is responsible for host-to-host delivery.
- The network layer has a higher responsibility than the data link layer, because the data link layer is only supposed to move the frames from one end of the wire to the other end.
- Thus network layer is the lowest layer that deals with the end to end transmission.

Position of Network Layer:

Fig 4.1.1 shows the position of network layer in the 5 layer internet model. It is the third layer.



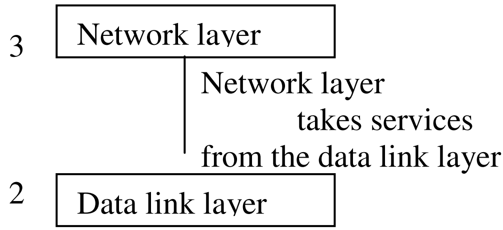


Fig4.1.1. Position of network layer

- It receives services from the data link layer and provides services to the transport layer.

4.1.2Network Layer Functions:

Functions of the network layer

Internet Addressing Routing Packetizing
Fragmenting
working

1. **Internetworking:**

It provides the logical connection between different types of networks

2. **Addressing:**

- Addressing is necessary to identify each device on the internet uniquely. This is similar to a telephone system.
- The addresses used in the network layer should uniquely and universally define the connection of a computer.

3**. Routing:**

In a network, there are multiple roots available from a source to a destination and one of them is to be chosen. .The network layer decides the root to be taken.

4. **Packetizing:**

- The network layer encapsulated the packets received from upper layer protocol and makes new packets.

- This is called as Packetizing.

5. **Fragmenting:**

The datagram can travel through different networks. Each router decapsulates the IP datagram from the received frame. Then the datagram is processed and encapsulated in another frame.

3.3 Network Layer Design Issues:

- The important network layer design issues include the service provided to the transport layer and the internal design of subnet.

Services Provided to the Transport Layer:

- The network layer services are designed to achieve the following goals:

1. The services should be independent of the subnet technology.
2. Transport layer should be shielded from the number, type and topology of the subnet.
3. The network address which is made available to the transport layer must use a uniform numbering plan.

- The network service can be connectionless or connection oriented.
- The internet has a connectionless network layer whereas the ATM networks have a connection oriented network layer.

- The connection oriented and connectionless services both have their own sets of advantages and disadvantages.
- Finally we can say that the network layer should provide a raw means to send packets from a to b and that is all.

Internal Organization of the Network Layer:

- Basically there are two philosophies for organizing the subnet.

1. To use connection oriented service
2. To use connectionless service.

- In the connection oriented service, a connection is called as **Virtual circuit.** It is similar to a physical connection.
- In the connectionless organization, the independent packets are called as **datagrams,** in analogy with telegrams.

Virtual Circuits:

- The principle behind the virtual circuits is to choose only one route from source to destination.
- When a connection is established, it is used for all the traffic flowing over the connection.
- When the connection is released, the virtual circuit is terminated.

Datagram:

- With a datagram, the routes from source to destination are not worked out in advance.
- Each packet sent is routed independently. Successive packets can follow different routes.
- The datagram subnets have to do more work but they are more robust and deal with failures and congestion more easily as compared to virtual circuit subnets.

Features of Virtual Circuits:

- In virtual circuits every router has to maintain a table.
- Each packet must have a virtual circuit number field in its header in addition to sequence number checksum etc.
- Circuit ser up required in virtual circuits. The virtual circuit can be initiated from either end. But problem can arise if call set ups are propagating in both directions simultaneously.
- The users are charged for connect time as well as for data transported.

Features of a datagram:

- The routers do not have to maintain any tables.
- Each datagram must contain full destination address. These address can be very long.
- When a packet comes in, the router finds an available outgoing line and sends the packet out on that line.

3.4 Routing Algorithms:

- One of the important functions of the network layer is to route the packets from the source machine to the destination machine.
- The major area of network layer design includes the algorithms which choose the routes and the data structures which are used.

Desired Properties of a Routing Algorithm:

- There are certain properties of a routing algorithm as follows:

1. Correctness
2. Robustness
3. Stability
4. Fairness and
5. Optimality

Types of Routing Algorithm:

Routing algorithms can be divided into two groups.

1. Nonadaptive algorithms.   2. Adaptive algorithms.

1. **Nonadaptive algorithms:**

- In this algorithm, the routing decision is not based on the measurement or estimation of current traffic and topology.
- However the choice of the route is done in advance, off line and it is downloaded to the routers.
- This is called as static routing.

2. **Adaptive algorithms:**

- In this the routing decision can be changed if there are any changes in topology or traffic tec.
- This is called as dynamic routing.

Shortest Path Routing:

- This algorithm is based on the simplest and most widely used principle. Here a graph of subnet is built in which each node representing the router and each are representing a link or a communication line.
- So as to choose a path between a pair of router, this algorithm simply finds the shortest path between them.

How to decide the shortest path?

- one way of measuring the path length is the number of hops. Another way (metric) is the geographical distance in kilometers.
- Some other metrics are also possible. For example we can label each arc (link) with the mean queueing and transmission delay and obtain the shortest path as the fastest path.

Labels on the arc:

- The labels on the arcs can be computed as a function of distance bandwidth, average traffic, mean queue length, cost of communication, measured delay etc.
- The algorithm weighs various parameters and computes the shortest path, based on any one or combination of criterions stated above.

Flooding:

- This is another static algorithm.
- In this algorithm every incoming packet is sent out an every outgoing line except the line on which it has arrived.
- One disadvantage of flooding is that it generate a large number of duplicate packets. In fact it produces infinite numbers of duplicate packets unless we somehow damp the process.
- There are various damping techniques such as,

1. Using a hop counter.
2. To keep a track of which packets have been flooded.
3. Selective flooding.

- To prevent endless copies of packets circulating indefinitely through the network a hop count may be used to suppress onwards transmission of packets after a number of hops exceeding the network "diameter".
- The destination must be prepared to receive multiple copies of an incoming packet.
- Flooding has two interesting characteristics that arise from the fact that all possible routes are tried:

1. As long as there is a route from source to destination the delivery of the packet is guaranteed.
2. One copy if the packet will arrive by the quickest possible route.

Selective flooding:

- This is slightly more practical variation of flooding.
- In this algorithm every incoming packet is not sent out on every output line.

- Instead packet is sent only on those lines which are approximately going in the right direction.

Application of flooding:

- Flooding does have much practical applications.
- But it is useful in military applications where a large number of routers are blown into pieces at any instant.
- In such applications robustness of flooding is very much desirable.
- Second application is in the distributed database applications.
- Flooding always choose the shortest path so it produces the shortest possible delay.

Flow Based Routing;

- This is static algorithm which uses topology and load condition (traffic) for deciding a route.
- For example in fig.4.3.1, there is always a huge traffic from A to B. Then the traffic from A to C should not be routed through B.
- Instead route it through AGEFC even though it is a longer path than ABC. This is called as a **Flow based routing**.

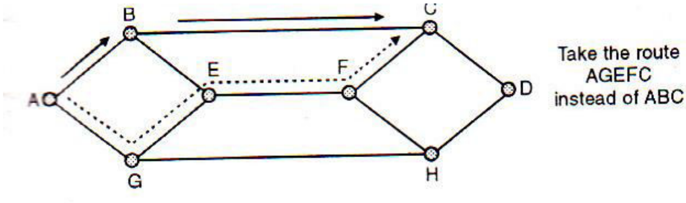


Fig4.3.1. Flow based routing

- It is possible to optimize the routing by analyzing the data flow mathematically. This is possible if the average traffic from one node to the other is known in advance and it is constant in time.
- The mathematical analysis is based on idea that for a given line if the capacity and average data flow are know, then it is possible to calculate the mean packet delay using the Queuing theory.
- From the mean delays on all the lines it is possible to calculate the mean packet delay for the whole subnet.
- To use the technique flow based routing. The following information should be known in advance.

1. Subnet topology
2. Traffic matrix
3. Line capacity matrix which specifies capacity of each line.

Dynamic Routing Algorithms:

- Two dynamic routing algorithms namely distance vector routing and link state routing are popular.

Distance Vector Routing Algorithm:

- In this algorithm, each router maintains a table called vector, such a table gives the best known distance to each destination and information about which line to be used to reach there.
- This algorithm is sometimes called by other name such as,

1. Distributed Bellman-Ford routing algorithm.
2. Ford-Fulkerson algorithm

- In distance vector routing, each router maintains a routing table. It contains one entry for each router in the subnet.
- This entry has two parts:

1. The first part shows the preferred outgoing line to be used to reach the destination and
2. Second part gives an estimate of the time or distance to the destination.

- The metric used can be one of the following:

1. Number of hops
2. Time delay
3. Number of packets in a queue etc.

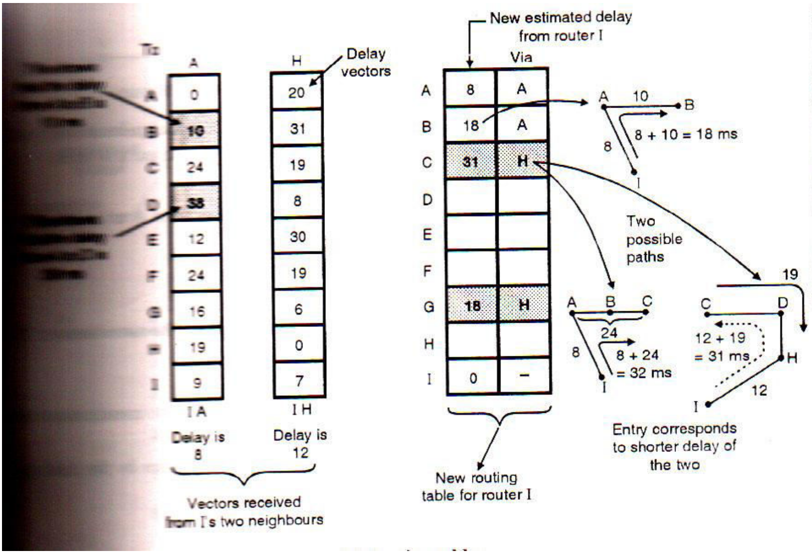


Fig 4.3.2 Routing tables

- The example of a subnet is shown in fig4.3.2. and the routing tables are shown in fig4.3.2,
- The entries in router table fig4.3.2, are the delay vectors. For example consider the shaded boxes of fig.4.3.2
- The entry in the first shaded box shows that the delay from A to B is 10 msec, whereas the entry in the other shaded box indicates that the delay from A to D is 38 msec.
- Consider how router I computes its new route G.Fig 4.3.3. shows the two possible routes between I and G.

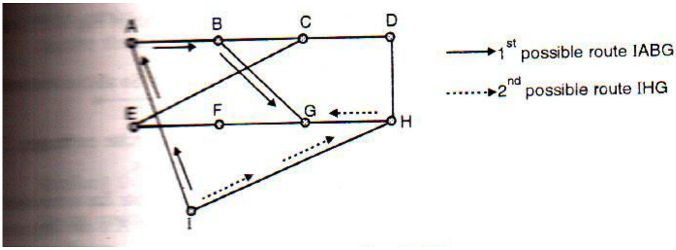


Fig 4.3.3

- I knows that the reach G via A, the delay required is:

I to A Delay=8 ms
A to G Delay =16 ms   I to G Delay=8+16=24 msec

- whereas the delay between I and G via H (route IHG) is:

I to H Delay = 12 ms
H to G Delay = 6 ms   I to G Delay = 12+6 = 18 msec

- The best of these values is 18 msec corresponding to the path IHG. Hence it makes an entry in its routing table (I's table) that the delay to G is 18 msec and that the route to use it is via H.
- The new routing table for router I is shown in fig 4.3.2

- Similarly we can calculate the delays, from I to different destinations from A to I and enter the minimum possible delay into the I's router table.

Disadvantages:

1. The problem with distance vector routing is its slowness in converging to the correct answer. This is due to a problem called count-to-infinity problem
2. This problem can be solved by using the split horizon algorithm.
3. Another problem is that this algorithm does not take the line bandwidth into consideration when choosing root.
4. This is a serious problem which led to the replacement of this algorithm by the link state Routing algorithm.

Link State Routing:

- Distance vector routing was used in ARP ANET upto 1979. After that it was replaced by the link stat routing.
- Variants of this algorithm are now widely used
- The link state routing is simple and each router has to perform the following five operations

Router operation:

1. Each router should discover its neighbours and obtain their network, addresses.

2. Then it should measure the delay or cost to each of these neighbours.
3. It should construct a packet containing the network address and the delays of all the neighbours.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

- The complete topology and all the delays are experimentally measured and this information is conveyed to each and every router.
- Then a shortest path algorithm such as Dijktra's algorithm can be used to find the shortest path to every other router.

Protocols:

- Link state routing is popularly used in practice.
- The OSPF protocol which is used in the Internet uses the link state algorithm.
- IS-IS i.e. Intermediate system – Intermediate system is the other protocol which uses the link state algorithm.
- IS-IS is used in Internet backbones and in some digital cellular systems such as CDPD.

Limitations of link state routing;

1. It is necessary to measure all the delays experimentally which is practically difficult.
2. Shortest path needs to be calculated every time.

Hierarchical Routing:

- As the size of the network increase, the size of the routing tables of the routers also increases.
- As a result of large routing tables, a large router memory is consumed, more CPU time is needed to scan the tables and more bandwidth is required to send status report about the tables.
- Sometimes the network becomes so large that the size of the router table becomes excessively large and practically it becomes impossible for every other router.
- Then the hierarchical routing such as the one used in telephone networks should be adopted.
- In this type of routing the total number of routers are divided into different **regions.**
- A router will know everything about the other routers in its own region only. It does not know anything about the internal structure of other regions. This reduces the size of the router table.
- When various networks are connected together, each network is treated as a separate region.
- For very large networks the hierarchy is prepared as follows:

  Level 1: Regions
  Level 2: Clusters: it is a group of regions
  Level 3: Zones: Zone is a group of clusters.
  Level 4: Groups: group contains may zones.

Two level hierarchical routing:

- For networks of smaller size, a two level hierarchical routing is sufficient.
- Fig 4.3.4 (a), shows network containing 3 regions fig, shows the full routing table of router 1A which has 9 entries.
- Now with two levels hierarchical routing. The routing table of the same router reduces to a much smaller size shown in fig 4.3.4 (c). This table has only 5 entries.

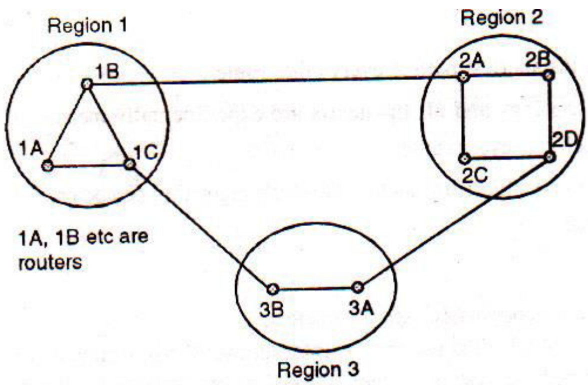


Fig 4.3.4 (a) A network

Full routing table for 1A

Destination	Line	Hops
1 A	-	-
1 B	1 B	1
1 C	1 C	1

2 A	1 B	2
2 B	1 B	3
2 C	1 B	3
2 D	1 B	4
3 A	1 C	3
3 B	1 C	2

Fig 4.3.4(b) Full routing table for router 1A

Hierarchical routing table

For 1 A

	Destination	Line	Hops
Region 1	1 A	-	-
	1 B	1 B	1
	1 C	1 C	1
Region2 →	2	1 B	2
Region3 →	3	1 C	2

Fig 4.3.4(c)Hierarchical routing table for router 1A

- In the hierarchical table of fig4.3.4 (c), there are entries for all local routers (1A, 1B and 1C) as before. But there are no detailed entries for the other regions.
- Instead all other regions have been condensed into a single router per region. For example traffic from 1A to any router in region-2 is via 1B-2A line as shown by the shaded entry in fig 4.3.4(c), similarly all the traffic from 1A to region 3 is routed through the line 1C-3B.

- Comparison of fig 4.3.4(b), and 4.3.4 (c) shows hierarchical routing reduces the size of routing tables.

Disadvantage:

The reduced table size has a price tag attached to it. It comes at the expense of increased path length. But it is practically acceptable.

Broadcast Routing:

- Sending a packet to all destinations simultaneously is called as **broadcasting.**
- Various methods of broadcasting are
  1. Simple broadcasting
  2. Flooding
  3. Multidestination routing.

Broadcasting

SimpleBroadcasting **Flooding** **Multidestination routing**

1. Simple broadcasting:

- In this method the source will simply send a distinct packet to each destination.
- This method has two drawbacks.

1. It wastes the bandwidth

2. The source has to have a complete list of all destinations.

2. **Flooding:**

- Flooding is another method used for broadcasting. The problem with flooding is that it has a point to point routing algorithm.
- So it consumes a lot of bandwidth and generates too many packets.

3. Multidestination routing:

- This is the third algorithm used for broadcasting.
- In this algorithm each packet will contain a list of destination or a bit map which indicates the desired destination.
- When such a packet arrives at a router, the router first checks all the destinations. Then it decides the set of output lines that will be required.
- The router then generates a new copy of the received packet for each output line to be used. It includes a list of only those destinations that are to use the line in each packet going out on that line.

Multicast Routing:

- For certain applications, widely separated processes need to work together in groups.

- A Process has to send a message to all other processes in the group. For a small group it is possible to send a point-to-point message.
- But this is expensive if the group is large, so we have to send messages to a well defined groups which are small compared to the network size.
- Sending message to such a group is called **multicasting** and the routing algorithm used for multicasting is **multicast routing.**
- To carry out multicast routing group management is required.
- Multicasting provides some ways to create and destroy group and also for a process to join and leave groups. How is it done depends on the type of routing algorithm used.
- When a process joins a group, it informs this to its host. The routers must know which of their hosts belong to which groups.
- This information is then given to the neighbouring routers. So that the information is propagated through the subnet
- Each router computes a spanning tree which covers all other routers in the subnet.
- When a process sends a multicast packet to a group the first router examines its spanning tree and prunes it to removes all the lines which do not hosts that are members of groups.
- The pruning of the spanning tree can be performed using various ways. One of the ways can be to use the link state routing.

- Another way of pruning is by using the distance vector routing. This method will prune the spanning tree in a recursive manner.

4.5 Internetworking:

- An internet is a general term for connection of different types of networks together
- When we have different networks we have to deal with different protocols. Each machine will not use same protocol in each layer.
- A variety of protocols such as TCP/IP, SNA, DEC, NCP/IPX and specialized protocols used for satellites and cellular networks are around.
- All the networks being connected to each connected to each other may not use the same technology. The technology used for ATM and wireless networks is entirely different so the protocols for such networks can be completely different.
-

Types of Networks:

The types of networks that are interconnected are LANs, MANs, different types of WANs etc.

Connection between two networks:

- The black boxes used for connecting two networks to each other depend on the layer that does the work.
- Table shows the layer, corresponding name of the connector and its function

Layer Number	Connector	Function

Layer 1	Repeater	Copy individual bits between cable segments.
Layer 2	Bridges	Store and forward data link frames.
Layer 3	Routers	Multiprotocol routers forward packets between dissimilar networks
Layer 4	Transport gateways	They connect byte streams in the transport layer
Layer 5 and above	Application gateways	Allow internetworking above layer 4.

- We have already discussed **repeaters** and **bridges** **multi-protocols routers** are conceptually similar to bridges but they are network layer devices.
- **Transport gateways** are used for making a connection between two networks at the transport layer.
- **Application gateways** are used to connect two parts of an application in the application layer.
- Practically an application gateway is ripped into two parts. Each one is called a **half gateway** and the two half gateways are connected by a wire.

Differing Factors in Various Networks:

- Networks can differ from each other in many different ways. Following are some of the differences in the network layer.

1. **Service offered:** It can be connection oriented or connectionless service.
2. **Protocols used:** Some of the possible protocols are IP, CLNP, and DEC net etc.
3. **Addressing:** It can be flat or hierarchical.
4. **Multicasting**: Can be present or absent.
5. **Packet size:** It depends on the network.
6. **Error handling:** We can get sliding window, rate control etc.
7. **Flow control:** We can get sliding window, rate control etc.
8. **Congestion Control:** Different algorithms such as leaky bucket, choke packets are available.
9. In addition to this the networks differ in terms of security, parameters, accounting and quality of service.

While carrying out internetworking, one has to take into account all these differing factors

Style of Internetworking:

The two commonly used models of internetworking are show in fig. below

Internetworking

Connectionoriented virtual circuit model

Datagram Model

Concatenated Virtual Circuits:

A concatenated virtual circuit model is shown in the fig 4.5.1

Process of Virtual circuit establishment:

- The subnet shows that the type of destination is remote destination and builds a virtual circuit to the route nearest the destination network.
- Next it constructs a virtual circuit from that router to an external gateway (multiprotocol router)

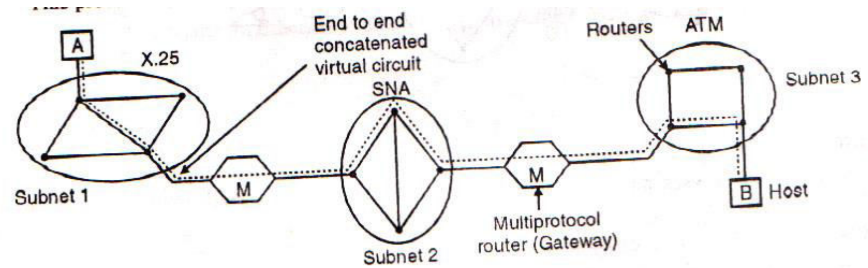


Fig4.5.1. Concatenated virtual circuit

- After building the virtual circuit, the data packets will begin to flow along the path, via various gateways.

Connectionless Internetworking:

- The networking which uses the Datagram model
- This is connectionless internetworking.
- The network layer injects the datagrams into the subnet. This is the only service offered by the network layer to the transport layer.
- All the packets may or may not traverse the same sequence of gateways.
- The datagram for host A to host B, showing different paths taken by the datagram packets.
- The packets travel individually and the routing decision is made separately for each packet.

Comparison of two models of networking:

Advantage and disadvantages of concatenated virtual circuit model:

- The advantage of concatenated virtual circuit model are as follows;

1. Buffers can be reserved in advance.
2. Sequencing can be guaranteed.
3. Short headers can be used.
4. The problems caused by delayed duplicate packets can be avoided.

- The disadvantages of concatenated virtual circuit model are as follows:

1. Space for each open connection has to be kept in the router tables.
2. There is no alternate route available to avoid the congestion areas.
3. This scheme is vulnerable to router failure along a path.

Advantages and disadvantages of datagram model:

Advantages of datagram model are:

1. It is possible to adapt to the congestion problem in a better way.
2. It is more robust in the event of router failure.
3. Various adaptive routing algorithms are possible to be used.
4. It can be used over the subnets which do not use the virtual circuit inside.

Disadvantages of the datagram model are as follows:

1. There is more potential for congestion 2. Longer header are needed.

4.5 Congestion control algorithms

There are different ways to control congestion. Some of these are explained here:

- Pre-allocation of buffers
- Packet Discarding
- Choke packets

Pre-allocation of Buffers

- In a situation where virtual circuits are being used within the subnet, it is possible to get rid of the problem of congestion.
- In the virtual circuit setup, table entries are made in the Imps that the call request packets (This is a packet which is sent of in advance of the data packets from source to destination. It tells the destination IMP that a communication is required). Pass through on their way to their destination.
- If the call-request packet is made to reserve buffers for the ensuring data packets, then the problem of congestion can be eliminated altogether.
- If an insufficient number of buffers are available, then the call-request packet will be re-routed or returned with a busy signal. Once a path from source to destination has been charted and reserved, the data packets can be sent.

Advantages

- Substantial resources are permanently allocated to specific connections, whether or not there is any traffic.

- Congestion is impossible because all the resources needed to process have already been reserved.

Disadvantages

- There is a potentially inefficient use of the resources because resources not being used by the connection to which they are allocated are nevertheless unavailable to anyone else.

Packet Discarding

- Packet discarding operates at the other end of the scale to reallocation of buffers. If a packet arrives at one of the intermediate Imps and there are no free buffers, then the packet will just be thrown away.
- One buffer on each line can be permanently reserved to accept any incoming packet and look at its contents to see if it would be useful. Its contents can then be utilized or the packet discarded. Either a new buffer will become the 'customs' buffer or the old one will be cleared ready for the next packet to arrive and be checked. In this way, packets are not thrown away to the detriment of the network.

Advantages

- Having seven packets queued instead of four will not pump the bits out any faster, but it will allow traffic for the other lines to forwarded immediately, possibly doubling or tripling the output rare of the IMP.

Disadvantages

- Extra bandwidth is needed for the duplicates.

- Solution to the above is to systematically discard packets that have not traveled far and hence do not represent a large investment in resources.

Choke Packet

- This model of controlling congestion is advancement on that proposed by flow control. If there is no congestion, then flow control only serves to limit the potential of the subnet between any two uncontested points.
- A better method is to have each IMP monitor the level of traffic on its output lines.
- If this is below a certain level then everything is fine, but if the traffic goes above this level then the IMP in question generates a choke packet containing the destination address of the offending packets.
- The source then retransmits that packet with a flag set so that no more choke packets will be generated because of it.
- It then slows down the rate at which it is currently sending. Any packets already on the move will be allowed to continue.
- If the congestion clears, then the source can move back up to its normal speed.

A. Weighted Fair Queuing

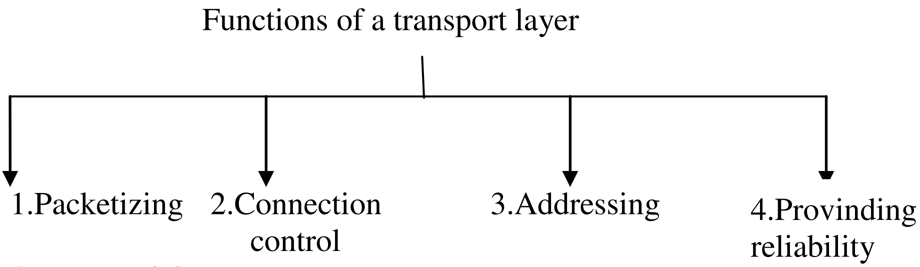
A problem with using choke packets is that the action to be taken by the source host is voluntary. Suppose that a router is being swamped by packets from four sources, and it sends choke packets to all of them. One of them cuts back, as it is supposed to, but the other three just keep blasting away. To get around this problem, and thus make compliance more attractive the fair queuing algorithm was proposed. The essence of the algorithm is that routers have multiple queues for each output line, one for each source.

B. Hop-by-Hop Choke Packets - at high speeds and over long distances, sending a choke packet to the source host does not work well because the reaction is so slow. An alternative approach is to have the choke packet take effect at every hop it.

Chapter 5

Transport Layer

5.1 Introduction



1. Packetizing:

- The transport layer creates packets out of messages received from the application layer. Packetizing is a process of dividing a long message into smaller ones.
- These packets are then encapsulated into the data field of the transport layer packet and headers are added.
- The length of the message which is to be divided can vary from several lines to several pages.
- But the size of the message can become a problem. The message size can be larger than the maximum size that can be handled by the lower layer protocols.

- Hence the message must be divides into smaller sections. Each small section is then encapsulated into a separate packet.
- Then a header is added to each packet to allow the transport layer to perform its other functions.

2. Connection control:

Transport layer protocols are divides into two categories:

1. <u>Connection oriented delivery:</u>

- A connection oriented transport layer protocol establishes a connection i.e. virtual path between sender and receiver.
- This is a virtual connection. The packet may travel out of order. The packets are numbered consecutively and communication is bi directional.

2. <u>Connectionless delivery:</u>

A connectionless transport protocol will treat each packet independently. There is no connection between them. Each packet can take its own different route.

3. Addressing:

The client needs the address of the remote computer it wants to communicate with. Such remote computers have a unique address so that it can be distinguished from all the other computers.

4.**Providing reliability:**

- For high reliability the flow control and error control should be incorporated.
- **Flow control:** we know that data link layer can provide the flow control. Similarly transport layer also can provide flow control. But this flow control is performed end to end rather than across a single link.
- **Error control:** The transport layer can provide error control as well. But error control at transport layer is performed end to end rather than across a single link. Error correction is generally achieved through retransmission.

Congestion control and Quality of Service:

The transport layers enhance the Quality of Service provided by the network layer.

- The typical QoS parameters for transport layer are:
  - ➢ Connection establishment delay.
  - ➢ Connection establishment failure probability.
  - ➢ Throughput.
  - ➢ Transit delay.
  - ➢ Protection.
  - ➢ Residual error ratio.

- Priority.
- Resilience.

The transport layer services:

- The task of transport layer is to provide reliable, cost effective transport of data from source machine to destination machine.
- To achieve this goal the transport layer makes use of the services provided by the network layer.

Quality of Service

The Quality of Service (QoS) parameters are as follows:

1. **Connection establishment delay:**
   - The time difference between the instant at which a transport connection is requested and the instant at which it is confirmed is called as **connection establishment delay.**
   - The shorter the delay the better the service.
2. **Connection establishment failure probability:**
   - It is the probability that connection is not established even after the maximum connection establishment delay.
   - This can be due to network congestion, lack of table space or some other problems.
3. **Throughput:**
   - It measures the number of bytes of user data transferred per second, measured over some time interval.
   - It is measured separately for each direction.

4. **Transit delay:**
    - It is the time between a message being sent by the transport user on the source machine and its being received by the transport user on the destination machine.
5. **Residual error ratio:**
    - It measures the number of lost or garbled messages as a fraction of the total messages sent.
    - Ideally the value of this ratio should be zero and practically it should be as small as possible.
6. **Protection:**

This parameter provides a way to protect the transmitted data from being read or modified by some unauthorized parties.

7. **Priority:**
    - This parameter provides a way for the user to show that some of its connections are more important (have higher priority) than the other ones.
    - This is important while handling the congestions. Because the higher priority connections should get service before the low priority connections.
8. **Resilience:**

Due to internal problem or congestion the transport layer spontaneously terminates a connection. The resilience parameter gives the probability of such a termination.

Transport Service Primitives:

- The transport service primitives allow the transport user such as application programs to access the transport service.
- Each transport service has its own access primitives.
- The transport service is similar to network service but there are some important differences. The main difference is that the connection-oriented transport service reliable.
- The second difference between the network service and transport service is whom the services are transport service for. The transport primitives are seen many programs and programmers. Hence the transport service is convenient and easy to use.

Primitives for a simple transport service

Sr. no	**Primitive**	**TPDU sent**	**Meaning**
1.	LISTEN	None	Block until some process tries to connect
2.	CONNECT	Connection request	Actively attempt to establish a connection.

s	SEND	Data	Send data.
4.	RECEIVE	None	Block until data TPDU arrives.
5.	DISCONNECT	Disconnection request	Release the connection.

Elements of Transport Protocols:

- In odder to implement the transport layer service to the transport entities, we have to use **transport protocol**.
- The transport protocol have to deal with the following tasks
  - Error control
  - Sequencing and
  - Flow control
- Following are some of the important elements of transport protocols.
  1. Addressing
  2. Establishing a connection
  3. Releasing a connection
  4. Flow control and buffering
  5. Multiplexing
  6. Crash recovery

Addressing in Transport Layer:

- At the data link layer we need a MAC address, at the network layer we need an IP address to choose on host among millions. A datagram in the network layer needs a destination IP address for delivery and source IP address for the destination's reply.
- At the transport layer a transport layer address called a port number is required to choose among multiple processes running on the destination host.
- The destination port number is required for delivery and the source **port number** is needed for the reply.
- In the Internet model, the port numbers are 16 bit integers between 0 and 65,535.
- The client program defines itself with a port number but this port number can not be chosen randomly.
- The internet uses universal port numbers for servers and these numbers are called as **well known port numbers.**
- Every client process knows the well known port numbers of the corresponding server process.
- For example, a Day time client process can use an ephemeral (temporary) port number 43000 for number 15.

What is Difference between IP Addresses and Port Numbers?

- The IP addresses and port numbers play different roles in selecting the final destination of data.

- The destination IP address defines the host among the millions of hosts in the world.
- After a particular host is selected, the port number defines one of the processes on this selected host.

Connection-oriented Service:

In a connection oriented service, a connection is established between source and destination. Then the data is transferred and at the end the connection is released.

Connection Establishment:

Refer fig 5.3.1to understand the host connection establishment.

- Following steps are involved in establishing a connection.
    1. Host A sends a connection request packet to host B. this includes the initialization information about traffic from A to B.
    2. Host B sends the packet of acknowledgement to confirm that it has received the request from A.
    3. Host B sends a connection request to A along with the initialization information about traffic from B to A.

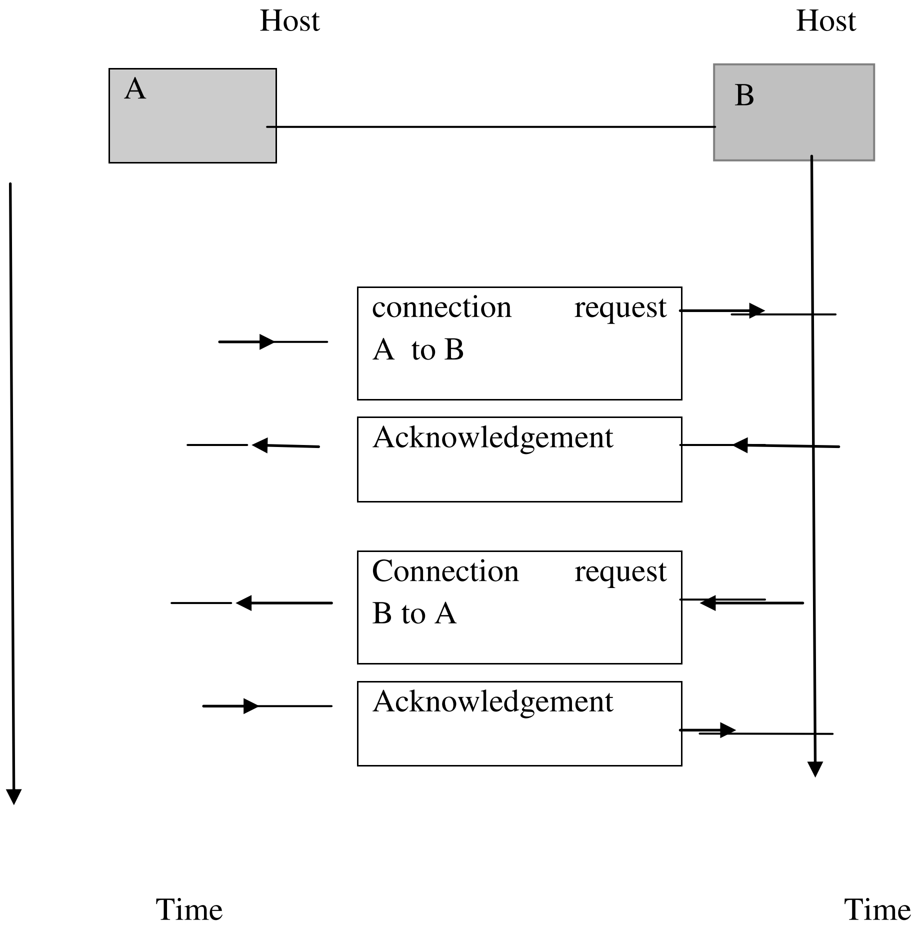


Fig5.3.1: Establishing a connection

4. Host A sends a packet of acknowledgement to confirm the request of B.

- It is possible to merge the steps 2 and 3.

- Note that each connection request must have a sequence number which is helpful in recovering from the loss or duplication of the packets.
- For the same reason, each acknowledgement also should have an acknowledgement number.
- The first sequence number in each direction should be random for each connection established. This is to ensure that a sender can not create more than one connection which starts with the same sequence number This is to recognize the duplication of packets.
- Since a sequence number is required for each connection, the receiver has to keep the history of sequence number for a special time.

Three way handshake technique:

- The delayed duplicate packet problem can be solved by using a technique called three way handshake.
- The principal of three way handshake is shown in fig.5.3.2

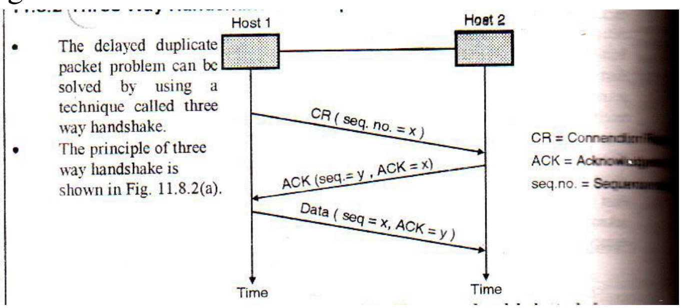


Fig 5.3.2Three way handshake technique

Normal operation:

1. Host 1 chooses a sequence number x and sends a connection request (CR) TPDU containing to host 2.
2. Host 2 replies with a connection accepted TPDU to acknowledge x and announce its own sequence number y.
3. Host 1 acknowledges host 2 and send the first data TPDU.

Operation in the abnormal circumstances:

- Now let us how the three way handshake works in presence of delayed duplicate control TPDUs.
- Refer fig 5.3.3. The first TPDU is a delayed duplicate CONNECTION REQUEST from an old connection. Accept TPDU.
- Host 2 receives this TPDU and sends host 1, a connection accepted TPDU.
- But host 1 is not trying to establish any connection so it sends a REJECT along with ACK=y.
- So host 2 realizes that it was fooled by a delayed duplicate and abandons the connection.

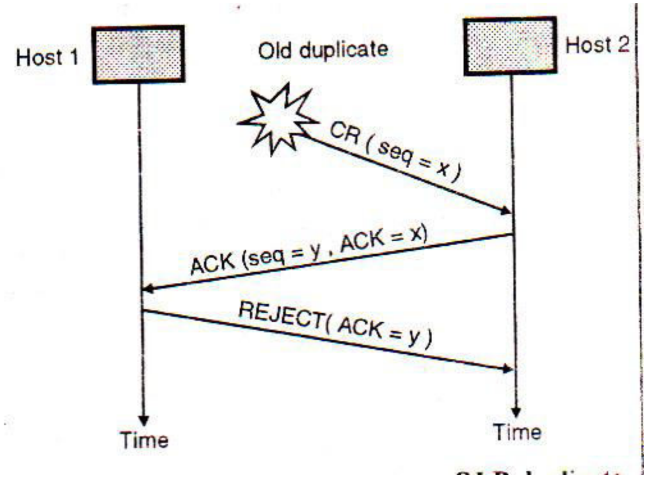


Fig5.3.3. Response to an OLD duplicate

Duplicate CR and duplicate ACK:

- This is another abnormal situation. Refer fig.5.3.4, to understand this situation.
- This is the worst case in which delayed duplicates of connection request (CR) and acknowledgement (ACK) are floating around in the subnet.
- Host 2 gets a CR and it replies to it by sending ACK. Note that host 2 has proposed a connection with a sequence number y.
- When the second delayed TPDU (duplicate) arrives at host 2 it understands that z has been acknowledged and not y. So it understands that this too is an OLD duplicate.

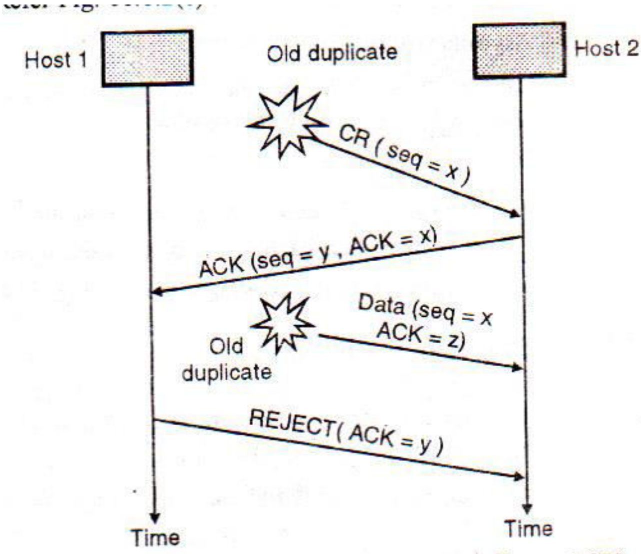


Fig 5.3.4. Duplicate CR and duplicate ACK

Connection Release:

- Any one of the two parties involved in data exchange can close the connection.
- But the problem is that, when connection is terminated from one end, the other party can continue to send data in the other direction.
- Hence, to ensure a proper connection release one has to follow the steps given below.

Procedure to release a connection:

Refer fig5.3.5., to understand this procedure.

- Host 1 sends a connection release request to host 2.

- Host 2 sends an acknowledgement to confirm the request of host 1.
- After this the connection is closed in one direction but host 2 can continue to send data to host 1.
- When host 2 finishes sending his data, it sends a connection release request to host 1.
- Host 1 acknowledges (confirms) the request made by host 2 and the connection is released from both ends.

- Releasing a connection is easier than established it. There are two styles of releasing a connection.

1. Asymmetric release:

In asymmetric release, when one party hangs up the connection is broken. It is an abrupt release and may result in loss of data.

2. Symmetric release:

- Symmetric release treats the connection as two separate unidirectional connections and requires each one to be released separately.

- Symmetric release is as shown in fig.5.3.5, and does not involve any loss of data.

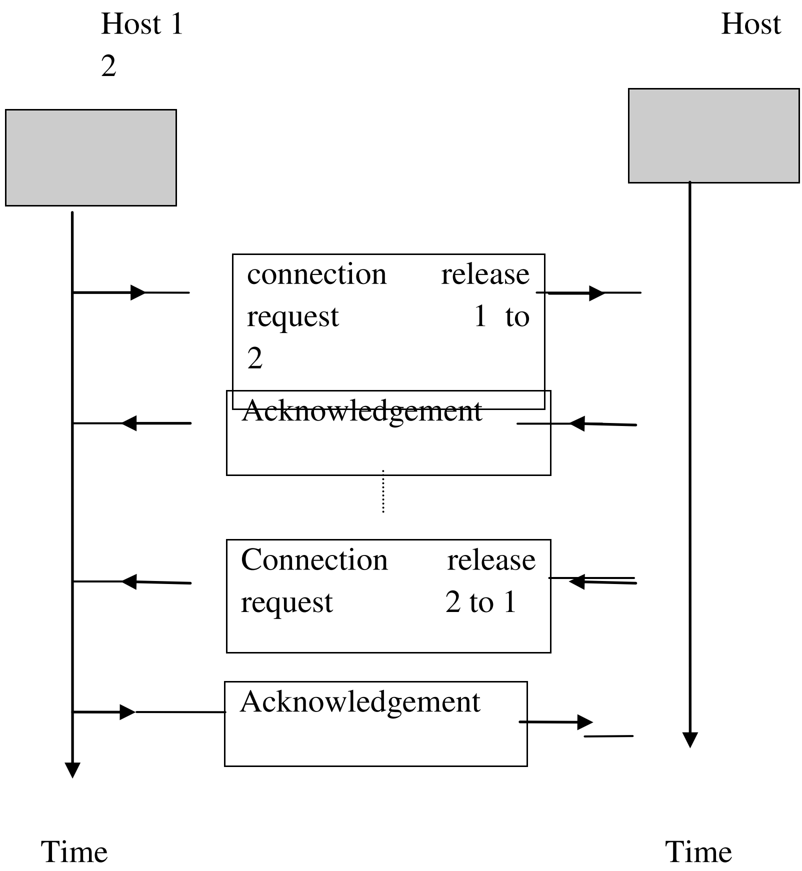


Fig5.3.5 Connection release

5.3.4 Multiplexing:

- At the sending end, there are several processes that want to send packets. But there is only one transport layer protocol (UDP or TCP).
- This is a many-to-one relationship and hence requires multiplexing.
- The protocol accepts messages from different processes. These messages are separated from each other by their port numbers.

- Then the transport layer adds header and passes the packet to the network layer as shown in fig.5.3.6,

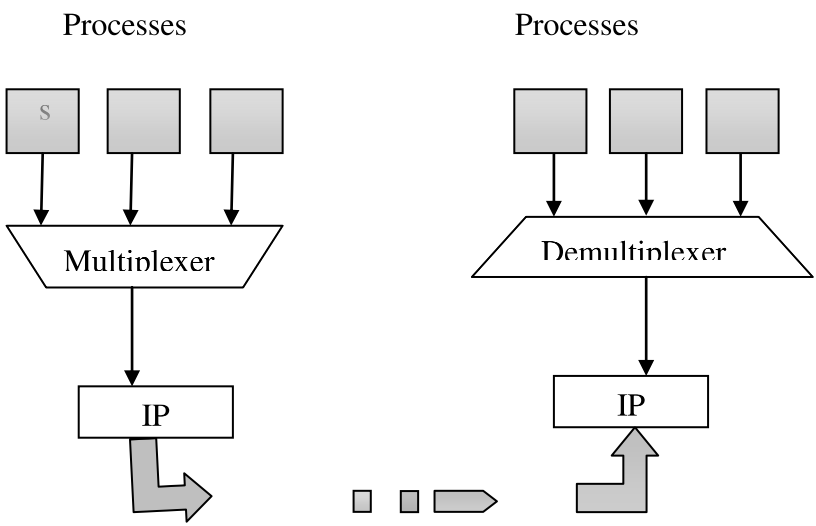


Fig5.3.6 Multiplexing and demultiplexing

De multiplexing:

- At the receiving end, the relationship is one as to many. So we need a de multiplexer.
- First the transport layer receives data grams from the network layer.
- The transport layer then checks for errors and drops the header to obtain the messages and delivers them to appropriate process based on the port number.

Crash Recovery:

- The host and routers are subject to crashes, and the recovery from such crashes is essential. Such crashes will result in loss of data packets.
- If the transport entity is completely inside the hosts then the recovery from the network and router crashes is simple. This is as explained below.
- In case of a router crash, the two transport entities must exchange information after the crash to determine which TPDUs were received and which were not. The crash can be recovered by retransmitted the lost ones.
- If the network layer provides connection oriented service, then the loss of a virtual circuit (crash) can be handled by establishing a new virtual circuit.
- Then the remote transport entity can be asked about which TPDUs it has received and which TPDUs are lost. Those lost can be retransmitted over the newly established virtual circuit.
- It is very difficult to recover from the host crash.
- Suppose that the sender is sending a long file to the receiver using a simple stop-and-wait protocol. Part way through the transmission the receiver crashes.
- When the receiver comes back up, it might send a broadcast TPDU to all other hosts, requesting the other hosts to inform it of the status of all open connections before the crash.

- The sender can be in one of two states: one TPDU outstanding, or no TPDUs outstanding, what happens if the sender retransmits?
- Think about the situation when the receiver first sends an ACK and then performs the write (to the output stream), but crash occurs in the middle (lost TPDU).
- How about reversing the order of sending ACK and performing the write? It does not help (duplicated TPDU). No matter how the sender and receiver are programmed, there are always situations where the protocol fails to recover properly.

5.5 User Datagram Protocol:

Source port	Destination port
Length	UDP checksum
DATA	

Fig 5.5.1 User Datagram Protocol

Source port:

Source Port is an optional field, when meaningful, it indicates the port of the sending process, and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.

Destination port:

Destination Port has a meaning within the context of a particular Internet destination address.

Length:

This is the size in bytes of the UDP packet, including the header and data. The minimum length is 8 bytes, the length of the header alone.

UDP Checksum:

This is used to verify the integrity of the UDP header. The checksum is performed on a "pseudo header" consisting of information obtained from the IP header (source and destination address) as well as the UDP header.

5.6 Transmission Control Protocol (TCP):

- The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model.
- Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.
- TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork.
- TCP offers efficient floe control, which means that, when sending acknowledgement back to the source, the receiving TCP process indicates the highest

sequence number that it can receive source, the receiving TCP process indicates the highest sequence number that it can receive without overflowing its internal buffers.

- Full-duplex operation means that processes can both send and receive at the same time.

The TCP Protocol:

Every byte on a TCP connection has its own 32-bit sequence number. These numbers are used for both acknowledgement and for window mechanism.

Segments:

The sending and receiving TCP entities exchange data in the form of segments. A segment consists of a fixed 20 byte header (plus and optional part) followed by zero or more data bytes.

Segment size:

The segment size is decided by the TCP software. Two limits restrict the segment size as flows:

1. Each segment including the TCP header must fit in the 65535 byte IP payload.
2. Each segment must fit in the MTU (Maximum Transfer Unit). Each network has a maximum transfer unit. Practically an MTU which is a few thousand bytes defines the upper limit on the segment size.

Fragmentation:

- If a segment is too large, then it should be broken into small segments using fragmentation by a router.

- Each new segment gets a new IP header. So the fragmentation by router will increase the overhead.

Timer:

- The basic protocol used by TCP entities is the sliding window protocol. A sender starts a timer as soon as a sender transmits a segment.
- When the segment is received by the destination, it sends back acknowledgement along with data if any. The acknowledgement number is equal to the next sequence number it expects to receive.
- If the timer at the sender goes out before the acknowledgement reaches back, it will **retransmit** that segment again.

The TCP Segment Header:

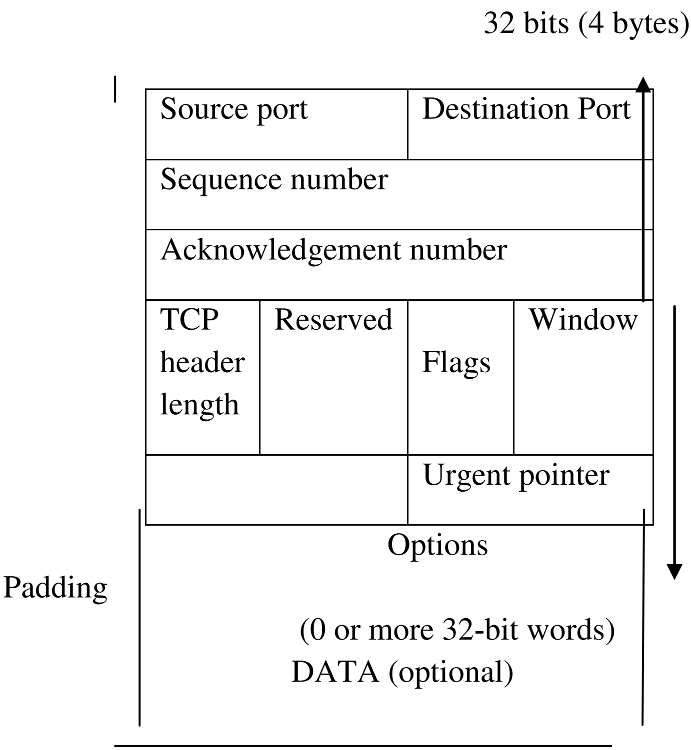


Fig5.5.2: TCP header format

- Fig.5.5.2, shows the layout of a TCP segment. Every segment begins with a 20 byte fixed format header.
- The fixed header may be followed by option.

- After the option, if any, up to 65535- 20- 20 = 65495 data bytes may follow. Notes that the first 20 bytes correspond to the IP header and the next 20 correspond to the TCP header.
- The TCP segments without data are used for sending the acknowledgement and control messages.

Source port:

- A 16- bit number identifying the application the TCP segment originated from within the sending host.
- The port numbers are divided into three ranges, well-known ports (0 through 1023), registered ports (1s024 through 49151) and private ports(49152 through 65535). Port assignments are used by TCP as an interface to the application layer.

Destination port:

A 16- bit number identifying the application the TCP segment is destined for on a receiving host. Destination ports use the same port number assignments as those set aside for source ports.

Sequence Number:

A 32-bit number identifying the current position of the first byte in the segment within the entire byte stream for the TCP connection. After reaching 2^{32}-1, this number will wrap around to 0.

Acknowledgement Number:

A 32-bit number identifying the next data the sender expects from the receiver. Therefore, the number will be one greater than the most recently received data byte. This field is only used when the ACK control bit is turned on.

Header Length or Offset:

- A 4-bit field that specifies the total TCP header length in 32-bit words (or in multiples of 4 bytes if you prefer).
- Without options, a TCP header is always 20 bytes in length. The largest a TCP header may be is 60 bytes. This field is required because the size of the options field(s) cannot be determined in advance.
- Note that this field is called "data offset" in the official TCP standard, but header length is more commonly used.

Reserved:

A 6-bit field currently unused and reserved for future use.

Control Bits or Flags:

1. **Urgent Pointer (URG):** If this bit field is set, the receiving TCP should interpret the urgent pointer field.
2. **Acknowledgement (ACK):** If this bit field is set, the acknowledgement field described earlier is valid.
3. **Push Function (PSH):** If this bit field is set, the receiver should deliver this segment to the receiving application as soon as possible. An example of its use may be to send a Control-BREAK request to an application, which can jump ahead of queued data.
4. **Reset the Connection (RST):** If this bit is present, it signals the receiver that the sender is aborting the

connection and all queued data and allocated buffers for the connection can be freely relinquished.

5. **Synchronize (SYN):** When present, this bit field signifies that sender is attempting to “synchronize” sequence numbers. This bit is used during the initial stages of connection establishment between a sender and receiver.
6. **No More Data from Sender (FIN):** If set, this bit field tells the receiver that the sender has reached the end of its byte stream for the current TCP connection.

Window:

- A 16-bit integer used by TCP for flow control in the form of the transmission window size. This number tells the sender how much data the receiver is willing to accept.
- The maximum value for this field would limit the window size to 65,535 bytes; however a “window scale” option can be used to make use of even larger windows.

Checksum:

- A TCP sender computes a value based on the contents of the TCP header and data fields.
- This 16-bit value will be compared with the value the receiver generates using the same computation. If the values match, the receiver can be very confident that the segment arrived intact.

Urgent pointer:

- In certain circumstances, it may be necessary for a TCP sender to notify the receiver of urgent data that should be processed by the receiving application as soon as possible.
- This 16-bit field tells the receiver when the last byte of urgent data in the segment ends.

Options:

- In order to provide additional functionality, several optional parameters may be used between a TCP sender and receiver.
- Depending on the option(s) used, the length of this field will vary in size, but it cannot be larger than 40 bytes due to the size of the header length field (4 bits).
- The most common option is the maximum segment size (MSS) option. A TCP receiver tells the TCP sender the maximum segment size it is willing to accept through the use of this option. Other options are often used for various flow control and congestion control techniques.

Padding:

Because option may vary in size, it may be necessary to “pad” the TCP header with zeros so that the segment ends on a 32-bit word boundary as defined by the standard.

Data:

Although not used in some circumstance (e.g. acknowledgement segments with no data in the reverse direction), this variable length field carries the application data from TCP sender to receiver. This field coupled with the TCP header fields constitutes a TCP segment.

5.7 Application Layer

Introduction:

- The application layer is the topmost (fifth layer) of the Internet model.
- The application layer allows people to use the internet.
- The layers below the application layer provide reliable transport but they do not do any real work for the users.
- The application layer receives services from the transport layer.

5.8 Domain Name System (DNS):

Addressing:

- For communication to take place successfully the sender and receiver both should have addresses and they should be known to each other.
- The addressing in application program is different from that in the other layers. Each program will have its own address format. It is important to note that there is an alias name for the address of remote host. The application program uses an alias name instead of an IP address.
- This type of address is varying convenient for the human beings to remember and use. But it is not suitable for the IP protocol.

- So the alias address has to be mapped to the IP address. For this an application program needs service of another entity.
- This entity is an application program called DNS is not used directly by the user. It is used by another application programs for carrying out the mapping.

How does DNS work?

- To map a name onto an IP address, an application program calls a library procedure called the **resolver**. The name is passed on to the resolver as a parameter.
- The resolver sends a UDP packet to a local DNS server which looks up the name and returns the corresponding IP address to the resolver.
- The resolver then sends this address of the caller. Then the program can establish a TCP connection with the destination or sends in the UDP packets.

The DNS Name Space:

- Conceptually the Internet has been divided into hundreds of top level domains. Each domain covers many hosts.
- Each domain is divided into several subdomains and they are further partitioned and so on.
- These domains can be represented by a tree as shown fig.5.8.1

- The top level domains are of two types namely generic and countries.

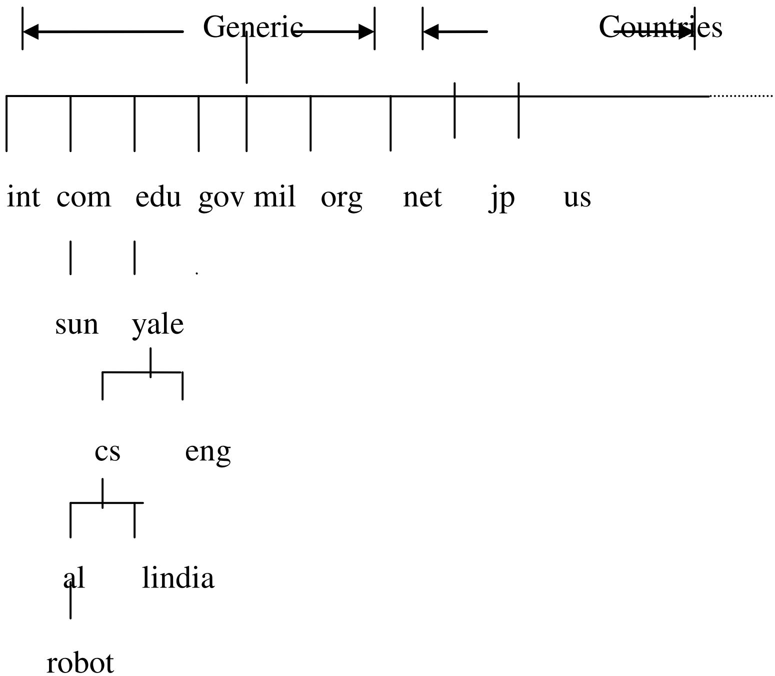


Fig5.8.1. A portion of Internet domain name space

Generic domains:

- The generic domains are com (commercial), edu (educational institutions), gov (government), int (some international organizations), mil (military), net (network providers) and org (nonprofit organizations).
- The country domains include one entry for every country.
- Each domain is named by following an upward path. The components are separated by dots. For example **eng.sun.com.** This is called hierarchical naming.
- Another example of hierarchical naming is shown in fig.5.8.2 The upward followed path has been shown by an arrow.

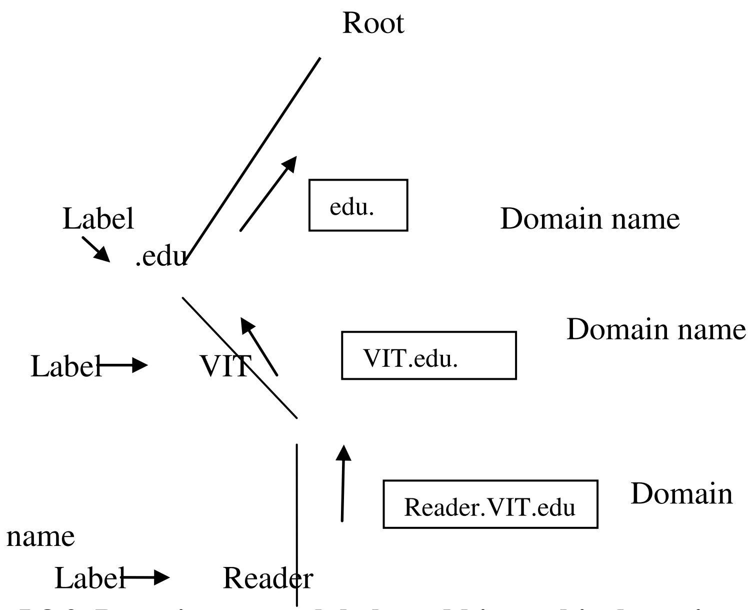


Fig5.8.2. Domain names, labels and hierarchical naming

Electronic Mail:

- One of the most popular network services is electronic mail (e-mail).
- Simple Mail Transfer Protocol (SMTP) is the standard mechanism for electronic mail in the internet.

E-mail Architecture and Services:

An e-mail system consists of two subsystems

1. **User agents:** They allow the people to read and send e-mail.
2. **Message transfer agents:** They move the messages from the source to the destination.

Basic functions:

E-mail systems support five basic systems which are as follows:

1. Composition
2. Transfer
3. Reporting
4. Displaying and
5. Disposition

1. **Composition:**

The process of creating messages and to answer them is known as composition. The system can also provide assistance with addressing and a number of header fields attached to each message.

2. **Transfer:**
    - It is the process of moving message from the sender to the recipient.
    - This includes establishment of a connection from sender to the recipient.
    - This includes establishment of a connection from sender to destination or some intermediate machine, outputting the message, and releasing the connection.

3. **Reporting:**
   This is telling the sender about whether the message was delivered or rejected or lost.
4. **Displaying:**
   It is the process of displaying the incoming messages. For this purpose simple conversions and formatting are required to be done.
5. **Disposition:**
    - This is concerned with what the recipient does with the message after receiving it.
    - Some of the possibilities are as follows:
        1. Throw after reading
        2. Throw before reading
        3. Save messages
        4. Forward messages
        5. Process messages in some other way.

Advanced features of E-mail systems:

Some of the advanced features included in addition to the basic functions are as follows:

1. Forwarding an e-mail to a person away from his computer.
2. Creating and destroying mailboxes to store incoming e-mail.
3. Inspecting contents of mailbox insert and delete messages from the mailboxes.
4. Sending a message to a large group of people using the idea of mail list.
5. To provide registered e-mail.
6. Automatic notification of undelivered e-mails.
7. Carbon copies.
8. High priority e-mail.
9. Secret (encrypted e-mail).
10. Alternative recipient.

5.10 File Transfer Protocol (FTP):

- FTP is a standard mechanism provided by the Internet for copying a file from one host to the other.
- Some of the problems in transferring files from one system to the other as follows:
    1. Two systems may use different file name conventions.
    2. Two systems may represent text and data in different types.
    3. The directory structures of the systems may be different.

- FTP provides a simple solution to all these problems.
- The basic model of FTP is shown in fig.,
- FTP establishes two connections between the client and server. Once is for data transfer and the other is for the control information.
- The fact that FTP separates control and data makes it vary efficient.
- The control connection uses simple rules of communication. Only one line of command or a line of response is transferred at a time.
- But the data connection uses more complex rules due to the variety of data types being transferred.
- FTP uses port 21 for the control connection and port 20 for the data connection.
- As shown in fig.5.10.1 the client has three components namely:
    1. User interface
    2. Control process and
    3. Data transfer process.

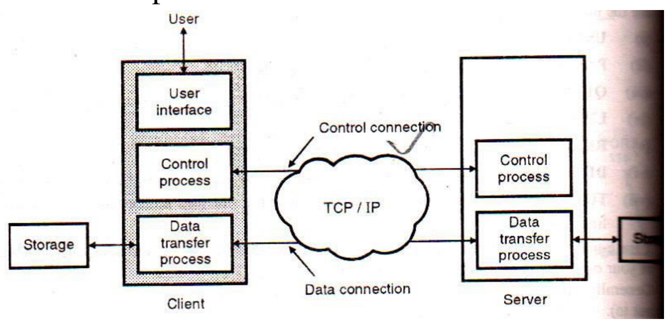


Fig5.10.1. Basic model of FTP

- The server has two components: the control process and data transfer process.
- The control connection is made between the control processes while data connection is made between the data transfer processes.
- The control connection is maintained during the entire interactive FTP session. The data connection is first opened, file is transferred and data connection is closed. This is done for transferring each file.