COMPUTER NETWORKS (23CS502)

LECTURE NOTES

UNIT-I

Network hardware, Network software, OSI, TCP/IP Reference models, Example Networks: ARPANET, Internet.

Physical Layer: Guided Transmission media: twisted pairs, coaxial cable, fiber optics, Wireless transmission.

Network Hardware

Types of Connection: A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another.

There are two possible types of connections: **point-to-point and multipoint.**

Point-to-Point

A point-to- point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint

A multipoint (also called multi-drop) connection is one in which more than two specific devices share a single link In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

- **Netwroks based on scale:**

  The networks are classified based on their physical size. They are divided into

  LAN (local area network)

  MAN (metropolitan area network)

  WAN (wide area network).

Local area network:

- Lan's are privately owned networks with in a single buildings or campus of up to a few kilo meters in size.

- They are widely used to connect personal computers & workstations in company offices and factories to share resources (E.g.: printers) & exchange information.
- Lan's are distinguished from other kinds of network by three characters tics.

    1. Their size.
    2. Their transmission technology.
    3. Their topology.

- Lan's are restricted in size, which means that the worst-case transmission time is bounded and known in advance.
- It also simplifies network management.
- Lan's may use a transmission technology consisting of a cable to which all the machines are attached, like the telephone company party lines ones used in rural areas.

Broad cast networks can be further divided into static& dynamic.

- Static allocation would be to divide time into discrete intervals and use a round robin algorithm, allowing each machine to broad cast only .when its time slot comes up.
- In dynamic system attempts to allocate the channel on demand.

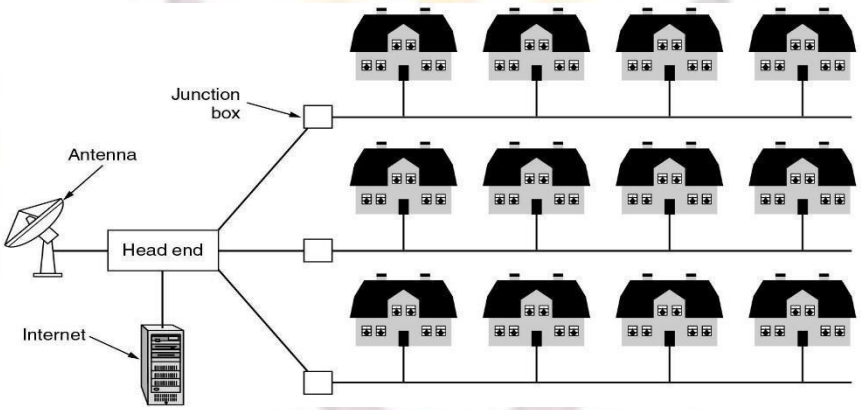
Dynamic allocation divided into 2 types

- Centralized.
- Decentralized.
- In centralized channel allocation method, there is a single entity, for example, a bus arbitration unit, which determines who goes next. It might do this by accepting requests and making a decision according to some internal algorithm.
- In decentralized channel allocation method, there is no central entity; each machine must decide for itself whether to transmit.

MAN(METROPOLITAN AREA NETWORK):

- It is basically bigger version of LAN and uses similar technology.
- It covers a city cable television network is the best example .

- Man is simplified network with no switching elements.
- Man has just one or two cables which is sent packets over one of several output lines.
- Best example for man is DQDB(distributed queue dual bus)
- DQDB consists of two unidirectional buses to which all computers are connected as shown in figure below.
- Each bus has head end, a device that initiates transmission activity.
- Traffic that is destined for a computer to the right of a center uses the upper bus; traffic to the left uses the lower bus.



WAN(WIDE AREA NETWORK):

- Wan s are spans a large geographical area, often a country or continent.
- It contains a collection of machines intended for running user programs, call this machine hosts.
- The hosts are connected by a communication subnet
- The job of the subnet is carry messages from host to host, like telephone system carries words from speakers to listener.
- The subnet consists of two distinct components: those are transmission lines and switching elements.
- Transmission lines, move bits between machines. They can be made of copper

wire, optical fiber, or even radio links.

- Switching elements are specialized computers that connect three or more transmission lines.
- When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them.
- These switching lines are also called routers.

- Here collection of routers & communication lines that move packets from the source host to destination host.
- When a packet is sent from one router to another via one or more intermediate routers, the packets is received at each intermediate router in it's entirely, stored their until the required output line is free, and then forward.
- A subnet is organized according to this principle is called a "store-and-forward" or "packet –switched" subnet.
- When packets are small &all the same size, they are often called cells.
- When a process on some host has a message to be sent to a process on some other host, the sending host first cuts the message into packets, each one bearing its number in the sequence.
- These packets are then injected into the network one at a time in a quick succession.
- The packets are transported individually over the network &deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process.

NETWORK SOFTWARE

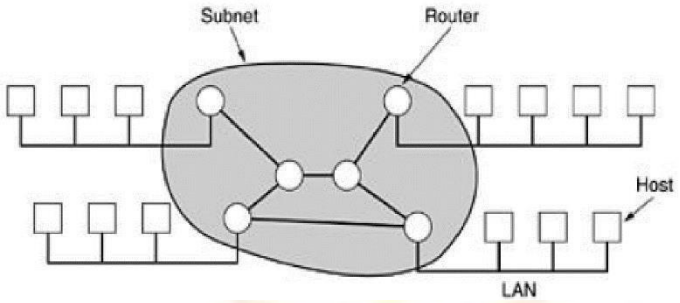
Network software is highly structured.

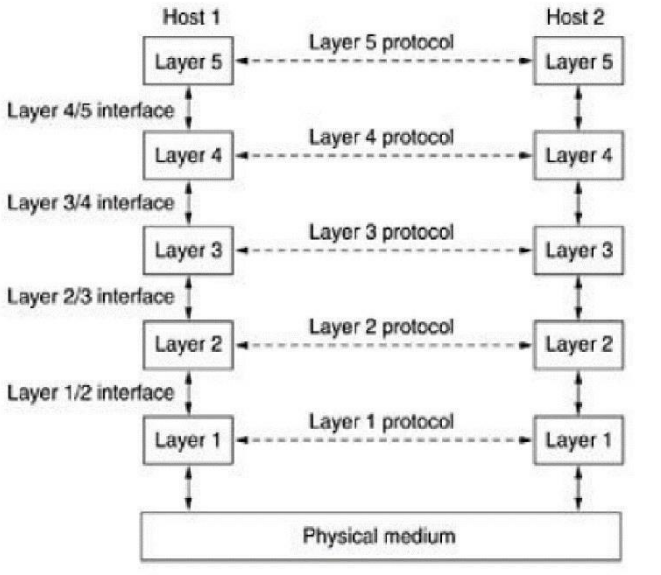
Protocol hierarchies:

- To reduce the design complexity, most networks are originated as a stack of layers or levels, each one built upon the one below it.
- The number of layers, the name of the each layer, the contents of each layer and the function of each layer differ from network to network.

- The purpose of each layer is to offer certain services to the higher layers.
- The fundamental ideas is that a particular piece of software or hard ware provides a service to its users but keeps the details of its internal state& algorithm hidden from them.
- A protocol is an agreement between the communicating parties on how communication is to proceed.
- The entities comprising the corresponding layers on different machines are called peers.
- The peer communicates by using protocol.
- In reality, no data are directly transferred from layer and on one machine to layer and on another machine.
- Instead, each layer passes data & control information to the layer immediately below it, until the lowest layer is reached.
- Below layer is the physical medium through which actual communication occurs.
- Between each pair of adjacent layers is an interface.
- The interface defines primitive operations & services .the lower layer makes available to the upper one.
- **A set of layers and protocols is called network architecture.**

- A list of protocols used by a certain system, one protocol per layer is called protocol stack.





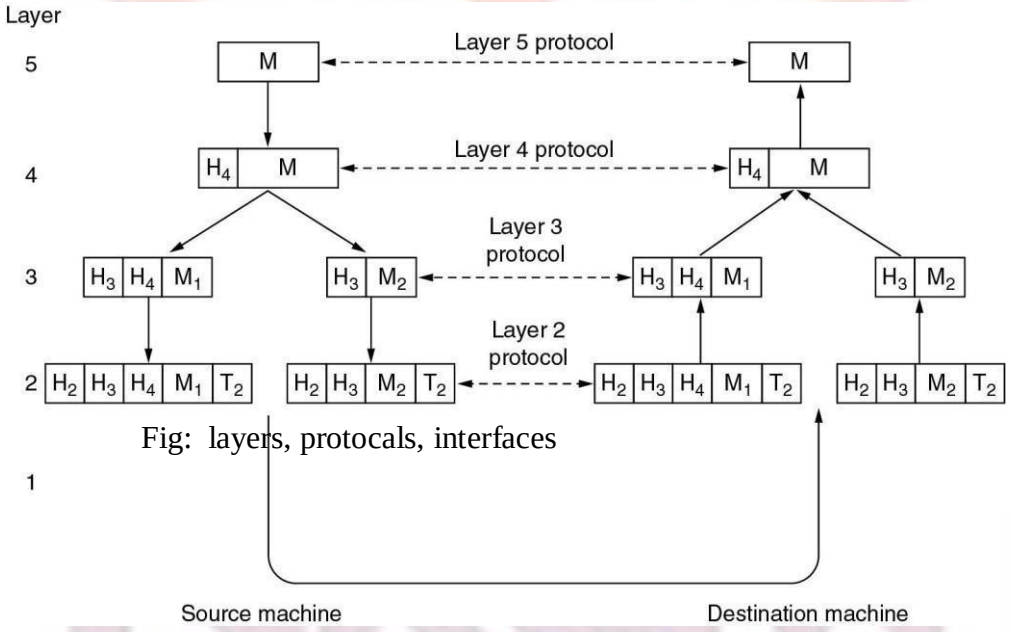


Fig: layers, protocals, interfaces

COMPUTER NETWORKS (23CS502)

DESIGN ISSUES FOR THE LAYERS:

- As a consequence of having multiple destinations, addressing is needed in order to specify a specific destination.
- Another set of design decision concerns the rules for data transfer.
- In some systems, data only travel in one direction, in other, data can go both ways.
- Many networks provide at least two logical channels per connection, one for normal data &one for urgent data.
- Error control is an important issue because physical communication circuits are not perfect. Many error –detecting &error –correcting codes are known, but both ends of the connection must agree on which one is being used.
- The receiver must have some way of telling the sender which messages have been correctly received & which has not.
- Flow control it occurs at every level how to keep a fast sender from swapping a slow receiver with data.
- Accepting long messages, this property lead to the mechanisms for disassembling, transmitting & then reassembling messages.

Connection –oriented & connectionless services:

- In connection oriented service, the service user first establishes a connection, uses the connection, and the releases the connection.
- The essential aspect of a connection is that it acts like a tube; the sender pushes objects (bits) in at one end, and receiver takes out at the other end.
- In most cases order is presented so that the bits arrive in order they were sent.
- Advantage is guarantee of data delivery.

  Ex: telephone system.
- In connection less service, no need of establishment the connection, uses the connection, the user just sends the data.

- Here no guarantee of data delivery.

  Ex: postal system.

- Services are reliable in the sense that they never lose data.

- A reliable service implemented by having the receiver acknowledges the receipt of each message so that sender is sure that it arrived.

- Reliable connection oriented service have two minor variations: message sequences & byte stream.

- Connection less service is also called datagram service.

- Connection oriented service is also called acknowledged datagram service.

  Ex: register post

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

SERVICE PRIMITIVES:

- A service is formally specified by a set of primitives (operations) available to a user process to access the service.

- The set of primitives available depends on the nature of the service being provided..

- As a minimal example of the service primitives that might provided to implement a reliable byte stream in a client-server environment is listed below.

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Fig: five service primitives for implementing a simple connection-oriented service.

The relationship of services to protocols:

- A service is a set of primitives (operations) that a layer provides to the layer above it.
- The service defines what operations the layer is prepared to perform on behalf of its users.
- A protocol is a set of rules used on how the communication should proceed.
- Lower layer is always a service provider.
- Upper layer is an always a service user.
- Protocol is used for implementation purpose.
- Service is not used for implementation purpose.

OSI REFERENCE MODEL

The OSI reference model:

The protocol associated with the OSI model are rarely used any more, the model itself is actually quit general and still valid.

- This model is developed by international standards organization.
- This model is also called ISOOSI model (open system interconnection).
- It deals with connecting open systems-that is, systems that are open for communication with other systems.
- The OSI model has several layers.

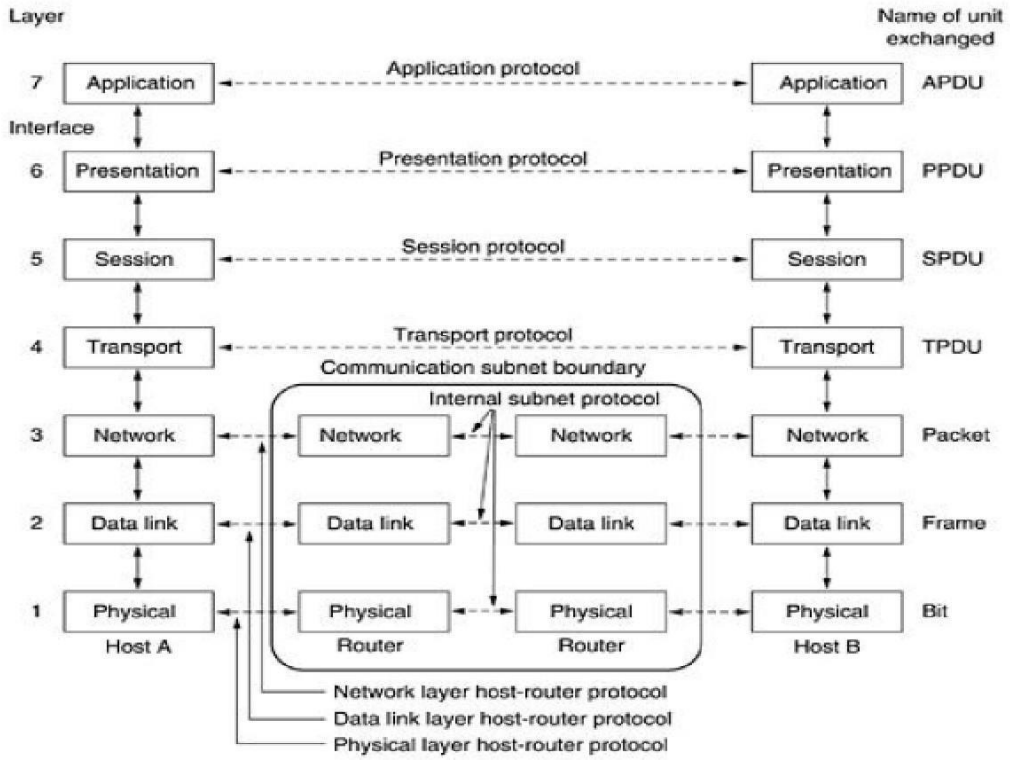
Principles:

1. Each layer should be created where a different level of abstraction is needed.
2. Each layer should perform well defined functions.
3. Each layer should define internationally standardized protocols.

4. Layer boundaries should be chosen to minimize the information flow across the interfaces.

5. The no .of layers should be appropriate for the requirements.

Fig: OSI reference model.



COMPUTER NETWORKS (23CS502)

Physical layer:

- It is concerned with transmitting raw bits over a communication channel.
- It is concerned with insuring that when one side sends a 1 bit, the otherside receives a 1 bit, not a '0' bit.
- Physical layer covers the interface between devices.
- It identifies the rules to pass bits from source to destination
- The design issues deal with mechanical, electrical, timing interfaces & the physical transmission medium.

Data link layer:

- The data link layer converts the raw transmission of bots into an error free data communication channel.
- It accomplishes this task by having the sender break up the input data into data frames & transmits the frames sequentially.
- If the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame.
- It handles loss, damage & duplicated frames. This process is called the error control.
- Handles slowing down a fast transmitter due to the slow receiver using the methods such as buffering. This process is called flow control.
- A sub layer of the data link layer called medium access control sub layer deals with the problems in broadcast network.

Network layer:

- The network layer controls the operation of the subnet.
- It routs packets from source to destination host.
- It controls the congestion, caused by hosts sending too many data packets into the network at a rate faster than the network can handle.
- Deals with addressing problem that arises when more than two dissimilar networks are

connected together.

- In a broadcast network the routing problem is simple, so the network layer is often thin or no existing.

Transport layer:

- The basic functions of the transport layer is to accept the data from above layer & split it up into smaller units, passes these to the network layer, and ensure that the pieces all arrive correctly at the other end.
- It provides some services to the session layer.
- The most popular type of service is an error free point-to-point channel that delivers messages or bytes in the order in which they were sent.
- Transport layer is a true end-to-end layer, all the from source to destination.
- A program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers & control messages.

The session layer:

- The session layers allow users on different machines to establish sessions between them.
- Sessions offer various services.
- Dialog control: keeping track of whose turn it is to transmit.
- Token management: preventing two parties from attempting the same critical operation at the same time.
- Synchronization: check pointing long transmissions to allow them to continue from where they were after a crash.

Presentation layer:

- The presentation layer deals with the syntax and semantics of the information transmitted.

- The presentation layer allows higher level data structure to be defined & exchanged.

Application layer:

- This layer contains protocols that are commonly needed by users.

- Widely used application protocol is HTTP (hyper text transfer protocol) which is basis for www.
- Other application protocols are used for file transfer, electronic mail & network news.

1.5.TCP/IP

The TCP/IP reference model:

This models it self is not of much use but the protocols are widely used.

TCP/IP transmission control protocol / internet protocol.

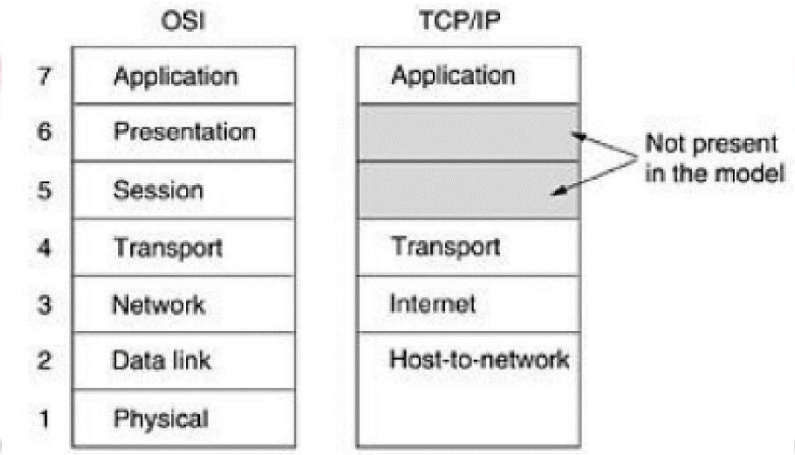
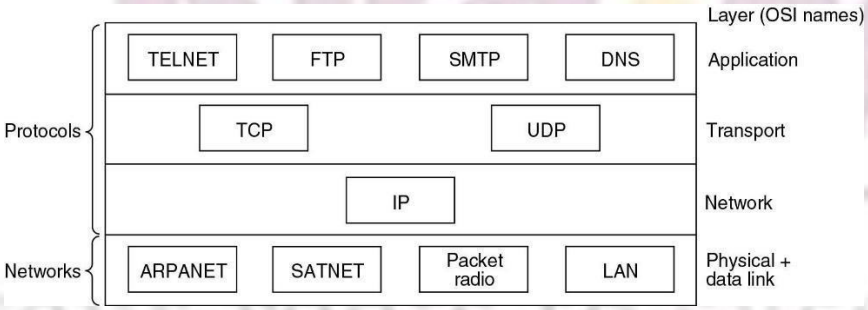


Fig:TCP/IP reference model.



Protocols and networks in the TCP/IP model

Host-to-network layer:

- It corresponds to physical & data link layer of OSI model.

- It does not say what happens here, except that host has to connect to the network using some protocol. So it can send IP packets to it.
- This protocol various from host to host and network to network.

Internet layer:

- It is similar to the network layer in the OSI reference model.
- The difference is it provides only connectionless service it is based on packet switching.
- The internet layer injects packets on the network and they travelled independently to destination.
- The internet layer defines an official packet format & protocol called IP.
- The job of the internet layer is to deliver IP packets to the destination and achieve congestion control.

Transport layer:

- It is equivalent to the transport layer in the OSI reference model except that it provides 2 types of services both connections oriented & connection less services.
- Connection oriented services is implemented by TCP.
- This allows a bytes stream originating on one machine to be delivered without error on any other machine in the internet.
- Connectionless service is implemented by UDP.
- It provides unreliable service & does not provide sequence & flow control.
- It is used in application such as client-server type reply quires & application in which prompt delivery is more important than accuracy.

Application layer:

- It contains all the higher level protocols dealing with applications such as file transferring, e-mails, telnet.
- The FTP provides where to move data efficiently from one machine to another.

- Other protocols SMTP, DNS, are also present in the application layer.

Difference between OSI and TCP/IP:

- Concepts of services, interfaces, protocols are not explained in TCP/IP.
- We can change the protocols easily in OSI than TCP/IP
- We can maintain sub layers in OSI & no need of maintaining sub layers in TCP/IP.
- In OSI reference network we are using both connection oriented and connection less services.
- In OSI transport layer we are using only connection oriented service.
- In TCP/IP network layer we are using only connection less service.
    - In TCP/IP transport layer we are using both connection less and connection orientedservices.

Criticism Of The TCP/IP Model And Its Protocols

The TCP/IP model and protocols have their problems too.

1. The model does not clearly distinguish the concepts of services, interfaces, and protocols.
2. TCP/IP model is not at all general and is poorly suited to describing any protocol stack other than TCP/IP.
3. **T**he link layer is not really a layer at all. The distinction between an interface and layer is crucial.

The TCP/IP model does not distinguish between the physical and data link layers. These are completely different. The physical layer has to do with the transmission characteristics of copper wire, fiber optics, and wireless communication. The data link layer's job is to delimit the start and end of frames and get them from one side to the other with the desired degree of reliability. A proper model should include both as separate layers. The TCP/IP model does not do this.

COMPUTER NETWORKS (23CS502)

ARPANET stands for **Advanced Research Projects Agency NET**. ARPANET was first network which consisted of distributed control. It was first to implement TCP/IP protocols. It was basically beginning of Internet with use of these technologies. It was designed with a basic idea in mind that was to communicate with scientific users among an institute or university.

EXAMPLE NETWORKS

History of ARPANET :

ARPANET was introduced in the year 1969 by Advanced Research Projects Agency (ARPA) of US Department of Defense. It was established using a bunch of PCs at various colleges and sharing of information and messages was done. It was for playing as long separation diversions and individuals were asked to share their perspectives. In the year 1980, ARPANET was handed over to different military network, Defense Data Network.

Characteristics of ARPANET :

1. It is basically a type of WAN.
2. It used concept of Packet Switching Network.
3. It used Interface Message Processors(IMPs) for sub-netting.
4. ARPANETs software was split into two parts- a host and a subnet.

Advantages of ARPANET :

- ARPANET was designed to service even in a Nuclear Attack.
- It was used for collaborations through E-mails.
- It created an advancement in transfer of important files and data of defense.

Limitations of ARPANET :

- Increased number of LAN connections resulted in difficulty handling.
- It was unable to cope-up with advancement in technology.

COMPUTER NETWORKS (23CS502)

INTERNET

Internet is a world-wide global system of interconnected computer networks. Internet uses the standard Internet Protocol (TCP/IP). Every computer in internet is identified by a unique IP address.

- Internet is a world-wide global system of interconnected computer networks.
- Internet uses the standard Internet Protocol (TCP/IP).
- Every computer in internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies acomputer location.
- A special computer DNS (Domain Name Server) is used to give name to the IP Addressso that user can locate a computer by a name.
- For example, a DNS server will resolve a name **http://www.google.com** to a particularIP address to uniquely identify the computer on which this website is hosted.
- Internet is accessible to every user all over the world.

The concept of Internet was originated in 1969 and has undergone several technological & Infrastructural changes as discussed below:

- The origin of Internet devised from the concept of **Advanced Research ProjectAgency Network (ARPANET).**
- **ARPANET** was developed by United States Department of Defense.
- Basic purpose of ARPANET was to provide communication among the various bodiesof government.
- Initially, there were only four nodes, formally called **Hosts.**
- In 1972, the **ARPANET** spread over the globe with 23 nodes located at different countries and thus became known as **Internet.**
- By the time, with invention of new technologies such as TCP/IP protocols, DNS, WWW, browsers, scripting languages etc.,Internet provided a medium to publish and access information over the web.

Advantages

Internet covers almost every aspect of life, one can think of. Here, we will discuss some of theadvantages of Internet:

- Internet allows us to communicate with the people sitting at remote locations. There arevarious apps available on the wed that uses Internet as a medium for communication. One can find various social networking sites such as:
    - Facebook

- Twitter
- Yahoo
- Google+
- Flickr
- Orkut

- One can surf for any kind of information over the internet. Information regarding various topics such as Technology, Health & Science, Social Studies, Geographical Information, Information Technology, Products etc can be surfed with help of a searchengine.
- Apart from communication and source of information, internet also serves a medium for entertainment. Following are the various modes for entertainment over internet.
    - Online Television
    - Online Games
    - Songs
    - Videos
    - Social Networking Apps
- Internet allows us to use many services like:
    - Internet Banking
    - Matrimonial Services
    - Online Shopping
    - Online Ticket Booking
    - Online Bill Payment
    - Data Sharing
    - E-mail
- Internet provides concept of **electronic commerce**, that allows the business deals to beconducted on electronic systems

Disadvantages

However, Internet has prooved to be a powerful source of information in almost every field, yet thereexists many disadvanatges discussed below:

- There are always chances to loose personal information such as name, address, credit card number. Therefore, one should be very careful while sharing such information. One should use credit cards only through authenticated sites.
- Another disadvantage is the **Spamming**.Spamming corresponds to the

unwanted e- mails in bulk. These e-mails serve no purpose and lead to obstruction of entire system.

- **Virus** can easily be spread to the computers connected to internet. Such virus attacks may cause your system to crash or your important data may get deleted.

- Also a biggest threat on internet is pornography. There are many pornographic sites that can be found, letting your children to use internet which indirectly affects the children healthy mental life.
- There are various websites that do not provide the authenticated information. This leadsto misconception among many people.

PHYSICAL LAYER

The purpose of the physical layer is to transport a raw bit stream form one machine to another fortransmission of data various physical media can be used.

- Media are roughly grouped into guided media and unguided media.

- In guided media the information is passed from source to destination using wires.

- In unguided media the information is passed from source to destination without using any wires.

GUIDED TRANSPORT MEDIA:

Guided media are of four types

1. Magnetic media
2. Twisted media
3. Coaxial media
4. Fiber optics.

Magnetic media:

- In this method the data is transmitted by writing them onto magnetic tape or removable mediaand transport the tape or disks physically to the destination machine.
- It is more cost effective for applications in which high bandwidth is the key factor.

- The delay characteristics are poor as the time measured in minutes or hours.
- The bandwidth characteristics of magnetic tape are excellent.

Twisted pair:

- Twisted pair consists of two insulated copper wires typically about 1mm thick.
- The two wires are twisted together because twisting two parallel line wires constitute a fineantenna.
- The main application is telephone system.
- For longer distances repeaters are needed.
- Can transmit either analog or digital signals.
- Bandwidth depends on the thickness of the wire and the distance traveled.
- These are widely used due to their adequate performance and low cost.
- Category 3 twisted pairs consist of two insulated wires gently twisted together.
- In a plastic sheath four such pairs are grouped to keep them together and to protect the wires.
- Category 5 twisted pairs are more advanced.

- These are similar to category 3 pairs but with more twists per centimeter.
- Over longer distances it provides better quality signal and suitable for high speed computer communication.

Fig: Category 3 Fig: Category 5

Coaxial cable:

- Coaxial cables can transmit data over longer distances at higher speeds. Two kinds of coaxial cable are used.
- 50-ohm cable is used for digital transmission.
- 75-onm cable is commonly used for analog transmissions and cable television.
- Coaxial cable consists of a shift copper wire as the surrounded by an insulating material.
- The insulator is encased by a cylindrical conductor, often as a closely woven braided mesh.
- The outer conductor is covered in a protective plastic sheath.
- Possibility of bandwidth depends on cable quality, length and data signal.
- Coaxial is still widely used for cable television and metropolitan area networks.

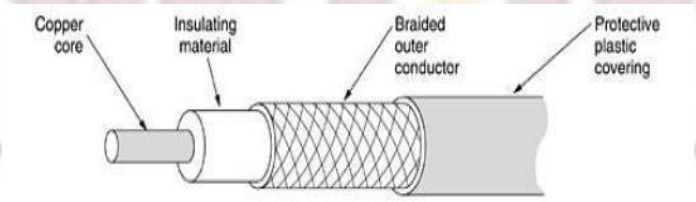


Fig: Coaxial Cable

Fiber optics:

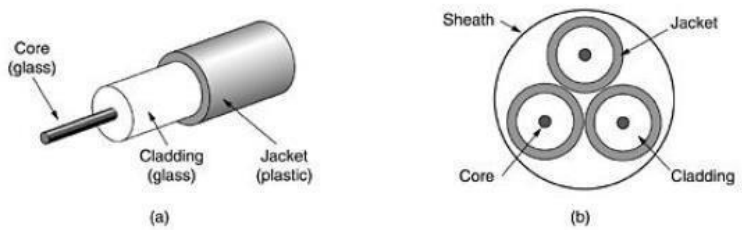


Fig: Side view of a single fiber **Fig: End view of sheath with 3 fibers**

- In this transmission medium we have three key components: light source, transmission medium and detector.
- Here pulse of light indicates a 1 bit and the absence of light indicates a 0 bit.
- Transmission medium is an ultra thin fiber of glass.
- Detector generates an electrical pulse when light falls on it.
- To an optical fiber one end is attached a light source and detector to the other end.
- Unidirectional data transmission we have it accepts an electrical signal converts & transmission by light pulses & then reconverts the o/p to an electrical signal at the receiving end.
- When a light ray passes from one medium to another the ray is refracted at the boundary
- Any light ray incident on the boundary above the critical angle will be reflected internally
- Many different rays will be bouncing around at different angles. Each ray is having a differentmode.
- It fibers diameter is reduced to a few wave lengths of light. The fiber acts like a wave guide &light travel in straight line.
- If light travel in it line in fiber is called " Single mode fiber"
- Single mode fibers are more expensive and are used for longer distances.

- The attenuation of light through glass depends on the wavelength of the light.
- Through fiber light pulses are sent they spread out in length as they propagate
- This spreading is called “chromatic dispersion” .

Fiber cables:

Fibers can be connected in three different ways

1. They can terminate in connectors and plugged into fiber sockets. Connections lose about 10 to 20 %of light.
2. They can be spliced mechanically mechanical splices lay the carefully cut ends next to each other ina special sleeve and clamp them in place
3. Two pieces of fiber can be fused to form a connection.

- LED’s (Light emitting Diodes) and semiconductor lasses are the two light sources used to dothe signaling.
- The receiving end of an optical fiber consists photodiode, which gives of an electrical pulsewhen struck by light.
- Fiber optics can be used for LANS.
- The problem is to realize that a ring network is just a collection of point-to-point links.
- The interface at each computer passes the light stream through the next link and allowcomputer to send and accept messages.
- Two types of interfaces are used
- A passive interface consists of taps fused on to the main fiber.
- One tap has an LED or laser diode at the end of it(for transmitting) and the other has a photodiode (for receiving)
- The tap is completely passive and reliable because a broken LED and photodiode does notbreak the ring. It just takes one computer offline.
- The other interface is active repeater. In this incoming light is converted into

electrical signal, if the signal is weak, it is regenerated to full strength, and retransmitted as light.

- If an active repeater fails, the ring is broken and network goes down.
- There is no limit on the total size of the ring as the signal is regenerated at each interface theindividual computer links can be kilometers long with no limit.
- The passive interface loses light at each junction the no of computers and ring lengths aregreatly restricted.
- We can build a LAN by using fiber optics other than ring topology.
- It is possible to have hardware broadcasting by using the passive star construction.
- Each interface has a fiber running from its transmitter to a silica cylinder, the incoming fiberare fused to one end of the cylinder.
- Fibers fused to other end of the cylinder are run to each of the receivers.
- In this broadcast is achieved, whenever an interface emits a light pulse. It is diffused insidethe passive star to illuminate all the receivers.

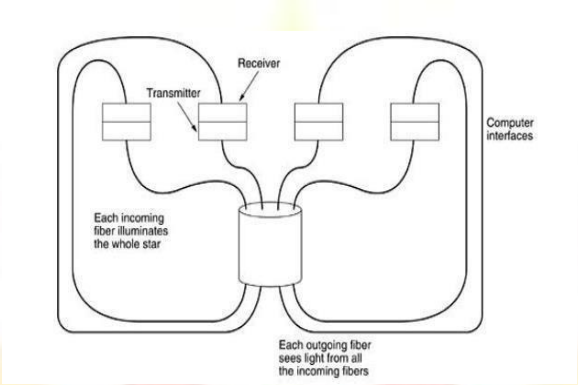


Fig: A Passive star connection with a fiber optics

COMPUTER NETWORKS (23CS502)

Unguided transmission media (or) wireless transmission:

Radio transmission:

These are widely used for communication because these waves are easy to generate, travel longdistances and penetrate buildings easily.

- Radio waves are Omni directional, means that the waves travel in all directions from thesource.
- No need to align the transmitter & receiver physically.
- Radio waves are frequency dependent.
- At low frequencies, radio waves pass through obstacles well, at high frequencies the wavestravel in straight lines and bounce off obstacles.

Microwave transmission:

- The waves travel in straight lines at above 100MHZ.
- The energy is concentrated into a small beam by means of a parabolic antenna.
- Here the transmitting and receiving antennas must be accurately aligned with each other.
- This allows multiple transmitters lined up in a row to communicate with multiple receivers ina row.
- At lower frequencies, microwaves do not pass through buildings.
- Even through the beam may be well focused at the transmitter there is some divergence inspace.
- Some waves may reflect and may take slightly longer to arrive than the direct waves.

- The delayed waves arrive out of phase with the direct waves and cancel the signal. This effectis called “multipath fading”.
- It is frequently and weather dependent.
- Microwave communication is widely used for long distance communication.
- It is also inexpensive.

Infrared and millimeter waves:

- In fared and millimeter waves are widely used for short range communication.
- These waves are directional, cheap and easy to build.
- These3 waves are used in remote controls used on television VCR’s and stereos.
- These infrared waves do not pass through solid objects.
- Infrared system in one room of a building will not interface with a similar system in adjacentrooms.

Light wave transmission:

- Main application is to connect the LAN’s in two buildings via lasers placed on their roof tops.
- Optical signaling using lasers is unidirectional.
- So each building needs its own laser & its own photo detector.
- This is of low cost and offers high band width and also easy to install.
- Disadvantage is that laser beams cannot penetrate rain or fog but normally work well on sunnydays.

COMPUTER NETWORKS (23CS502)

UNIT II

Data link layer: Design issues, framing, Error detection and correction.

Elementary data link protocols: simplex protocol, A simplex stop and wait protocol for an error-freechannel, A simplex stop and wait protocol for noisy channel.

Sliding Window protocols: A one-bit sliding window protocol, A protocol using Go-Back-N, Aprotocol using Selective Repeat, Example data link protocols.

Medium Access sub layer: The channel allocation problem, Multiple access protocols: ALOHA, Carrier sense multiple access protocols, collision free protocols. Wireless LANs, Data link layer switching.

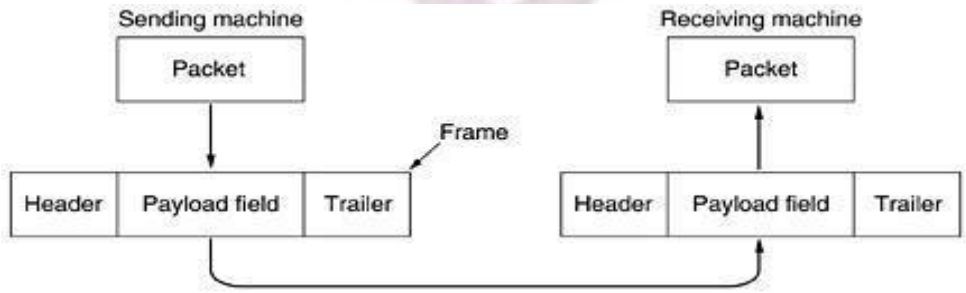
Data link layer: Design issues

Design issues for data link layer are

1. Providing well defined service interface to the network layer.
2. Dealing with transmission errors.
3. Regulating the flow of data.

To achieve these goals, the data link layer takes the packets it gets from the network layer and changeas them into frames for transmission.

Each frame contains a frame header, a payload field for holding the packet, and a frame trailer.



Services provided to the Network layer:

The principal service of data link layer is transferring data from the network layer on the sourcemachine to the network layer on the destination machine.

Three commonly provided services are:

1. Unacknowledged connection less service.
2. Acknowledged connection less service.

3. Acknowledged connection-oriented service.

1. Unacknowledged connection less service:

- The source m/c sends independent frames to the destination m/c.
- No logical connection is established between source & destination.
- If a frame is lost, no attempt is made to detect the loss of the frame.
- This service is appropriate when the error rate is low.
- In this the destination m/c does not send any acknowledgement back to the sender.
- It is useful when an error rate is very low.
- Most LAN's are used unacknowledged connectionless services.

2. Acknowledged connectionless service:

- No logical connection is established between source &destination machine.
- But the receiver sends an acknowledgement back to the sender.
- By receiving the acknowledgement the sender knows that the frame has arrived correctly.
- If the acknowledgement is not received with in a specified time interval, it can be sent again.
- The network layer can always send a packet and wait for it to be acknowledged.
- If the acknowledgement is not forthcoming before the timer expires, thesender can just send the entire message again.
- The trouble of this strategy is that frames usually have a strict maximum length imposed by thehardware and network layer packets do.

3. Acknowledgement connection –oriented service:

- Before any data is transferred a connection is established between source & destinationmachines.
- It guarantees that each frame is received exactly once and that all frames are received in theright order.
- In this service the data transfer goes through three distinct phases.
- In the first phase, the connection is established variables are initiated & counters keep track ofwhich frames have been arrived &which once have not.

- In the second phase, one or more frames are actually transmitted.
- In the third phase, the connection is released freeing up the variables, buffer &other resources.
- Ex: In a WAN subnet consisting of routers connected by point-to-point leased telephone lines.
- When a frame arrives at a router, the hardware checks it for errors then passes the frame to thedata link layer software.
- The data link layer software checks to see if this is the frame expected, and if so, gives thepacket contained in the payload field to the routing software.
- The routing software then chooses the appropriate outgoing line and passes the packet backdown to the data link layer software.

FRAMING:

- In order to provide services to the network layer, the data link layer must use the services fromthe physical layer.
- The physical layer sends the bit stream to the data link layer.
- The no. of bits received may be different from the no. of bits transmitted.
- The data link layer convert the bit stream into data frames and compute the checksum for eachframe.
- At the destination, the check sum is recomputed.
- If the recomputed check sum is different from the one contained in the frame.
- An error has occurred and the data link layer deals with the errors.
- To mark the start and end of each frame, we use *four methods*. They are

1. Character count.
2. Flag bytes with byte stuffing.
3. Starting and ending flags with bit stuffing.
4. Physical layer coding violations.

1. Character count:

This method uses a field in the header to specify the number of characters in the frame.

- At the destination the data link layer sees the character count, it knows how many characters followand where the end of the frame is

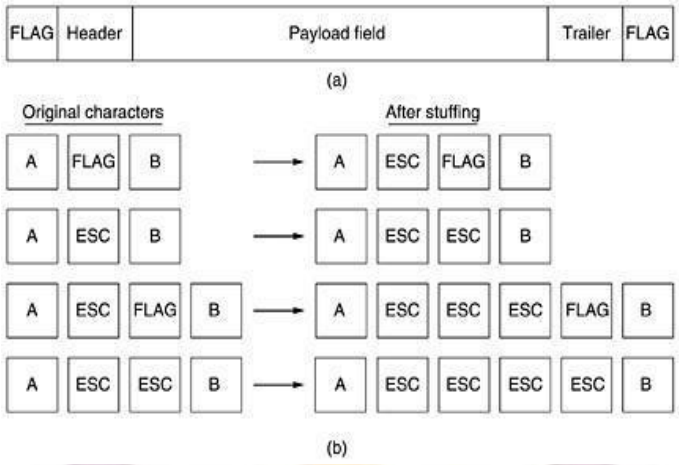
For example, if the characters count of 5 in the second frame becomes a 7.

- The destination will go out of synchronize and will be unable to locate the start of the next frame.

- The destination does not know how many characters to skip over to get to the start of the retransmission. For this reason, the character count is rarely used.

2. Flag bytes with byte stuffing:

- In this method, each frame start and end with special bytes.
- Most protocols have used the same byte called a flag byte as FLAG at both starting &ending ofthe frame.
- Even if the receiver ever loses synchronization, it can just search for the flag byte to find the endof the current frame.
- Two consecutive flag byte indicates the end of one frame and start of the next one.
- **Fig . (a) A frame delimited by flag bytes. (b) Four examples ofbyte sequences before and after byte stuffing**



- The sender's data link layer inserts a special escape byte "ESC"just before each flag byte the data.
- At the receiving end, the data link layer removes the escape byte before the data are given tothe network layer.
- This technique is called" byte stuffing" or "character stuffing".
- A framing flag byte can be identified by the absence or presence of an escape byte in the data.
- If an escape byte occurs in the middle of data that, too, is stuffed with an escape byte.
- Any single escape byte is part of an escape sequence, where as a doubled one indicates that asingle escape occurred naturally in the data.
- Examples of the byte sequences before &after byte stuffing.
- A major disadvantage of this framing method is it is used for 8-bit character only.
- Not all character codes use 8-bit characters, some use 16-bit characters, so a new technique hadto developed to allow sized characters.

3. Starting and ending flags, with bit stuffing:

- In this method, each frame begins and ends with a special bit pattern, 01111110 a flag byte.
- When the sender's data link layer encounters five consecutive 1's in the data, it automaticallystuffs a 0 bit into outgoing bit stream.
- This bit stuffing is similar to byte stuffing.
- When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automaticallydeletes the 0 bit.
- The boundary between two frames can be recognized by the flag pattern.
- If the receiver losses its track the receives has to scan the input for flag sequences.
- The flag sequences occur only at frame boundaries and never with in the data.

4. Physical layer coding violations:

This framing method is used in the networks in which physical medium contains someredundancy.

A 1 bit is a high –low pair & a 0 bit is a low-high pair. It means that every data bit has a transmissionin the middle. It makes easy for the receiver to locate the bit boundaries.

Error control:

- To make sure that all frames are eventually delivered to the network layer at the destination &in the proper order.
- The protocol calls for the receiver to send back special control frames bearing positive ornegative acknowledgements about the incoming frames.
- If a +ve acknowledgement is received the frame has arrived safely.
- If a – ve acknowledgement is received the frame has gone wrong & the frame must betransmitted again.
- If a frame is lost due to hardware failure the receiver will not react & does not send anyacknowledgement.
- Timers are introduced into the data link layer.
- When a frame is exacted the timer also starts, the frame will be correctly received & theacknowledgement will get back before the timer runs out.
- If the frame or acknowledgement is lost the timer will go off, here the frame is transmittedagain.
- If a frame is transmitted multiple times the receiver may accept the same and pass it to thenetwork layer more than once.
- To prevent this, sequence numbers are assigned to outgoing frames, so that the receiver candistinguish retransmission from originals.

Flow control:

- Flow control occurs when the sender wants to transmit frames faster than the receiver can acceptthem.
- Even if the transmission is error free, the receiver will simply be unable to handle the frames asthey arrive & will start to lose them.
- Feed back based flow control & rate based flow control are the two approaches that are commonlyused.

- In feedback –based flow control, the receiver sends back information to the sender giving itpermission to send more data.

- In rate based flow control, the protocol has a built – in –mechanism that limits the rate at whichsenders may transmit data, with out using feedback from the receiver.

Error detection and correction:

Data can be corrupted during transmission .for reliable communication; error must be detected&corrected.

Error correction: error correction can be done in two ways. When an error is discovered, the receivercan ask the sender to re –transmit the entire data unit.

- Or the receiver can be use an error- correcting code, which automatically corrects errors.

Error detecting codes:

For error detecting we use polynomial code also known as CRC is used. Polynomial codes are based upon treating bit strings as representations of polynomials with coefficients of 0 and 1 only.CRC cyclic redundancy check

1. Let us consider a data unit of 'm' bits.
2. A string of (n-1) 0's is append to the data unit where 'n' is number of bits of the divisor. 3.The new data unit with m+ (n-1) bits is divided by divisor using modulo -2 division method.

The resulting remainder is having (n-1) bits .this remainder is called CRC remainder.

4. The CRC remainder of (n-1) bits obtained from step 3 replaces the already append 0's in step2.
5. The data unit followed by CRC reaches the receiver.
6. The receiver divides the CRC appended data unit using the same divisor by the module -2division method.

If the data unit, received by the receiver is without any error then the remainder obtained from step6 will be zero.

Other wise the remainder will be non zero.

Ex: using error detecting code find the transmitted frame for a given frame of 1101011011 using thegenerator.

Frame : 1 1 0 1 0 1 1 0 1 1
Generator: 1 0 0 1 1
Message after 4 zero bits are appended: 1 1 0 1 0 1 1 0 1 1 0 0 0 0

Frame: 1101011011

Generator it becomes 10011

In the given generator the highest power is 4, so we have to add 4 zero's to the fram

Now, the transmitted frame is:

11010110111110

The frame is transmitted to the destination.

At the destination it again performs the same operation.

If the remainder is 0 the data is without errors & is accepted. Otherwise, the data is discarded.

Elementary data link protocols

Elementary data links protocols are 3 types:

1. An unrestricted simplex protocol.
2. A simplex stop-and – wait protocol.
3. A simplex protocol for a noisy channel.

1. An unrestricted simplex protocol:

- Data is transmitted in one direction only.
- transmitting and receiving network layers are always ready.
- processing time can be ignored.
- Infinite buffer space is available.
- Communication channel between the data link layers never damages ar loses frames.
- Here in this protocal, no sequence numbers as acknowledgements are used.

2) A Simple stop-and-wait Protocol:

- The communication channel is error free.
- Mai problem is how to prevent the sender from flooding the receiver with data faster than it is ableto process it.
- To prevent sender from sending more frames than the receiver can accept.

- After a packet is passed to the network layer, the receiver sends a little dummy frame back to thesender, so it gets permission to transmit the next frame.
- Sender sends one frame and then waits for an acknowledgement before proceeding is called "Stop-and-wait".
- This protocol has strict alternation of flow first the sender sends a frame, the receiver sends anacknowledgement, then only the sender sends another frame, then the receiver sends &soon.

3) A Simplex protocol for a Noisy channel:

- The communication channel makes errors. Frames may be damaged or lost completely.
- If a frame is damaged the receiver hardware will detect the error when it computes the checksum.
- If a damaged frame arrived at the receiver, it would be discarded.
- The sender sends the frame again after the time out.
- The receiver must be able to distinguish a frame from retransmission.
- To achieve this sender put a sequence number in the header of each frame it sends.
- The receiver checks the sequence number of each arriving frame to see if it is a new frame.
- If it is duplicate frame, it is discarded
- Protocols I which the sender waits for a positive acknowledgement before advancing to the next data is called (Positive Acknowledgement with Retransmission) PAR or (Automatic Repeat request) ARQ.

Sliding Window Protocol

In the previous protocols, data frames are transmitted in one direction only. There is need fortransmitting data in both directions.

- We have two separate physical circuits, each with a "forward" channel for transmitting data anda "reverse" channel for transmitting acknowledgements.
- The bandwidth of the reverse channel is entirely wasted as it sends only acknowledgements.
- To effectively use the bandwidth of the reverse channel. The receiver may wait for sometimefor the next data packet and with data pocket it sends the acknowledgement.

- The acknowledgement is attached to the outgoing data frame.
- The technique of temporarily delaying outgoing acknowledgements so that they can be attachedto the next outgoing data frame is known as "***Piggy Backing".***
- The advantage of using piggy backing is better use of the available channel bandwidth.
- All sliding window protocols maintains" sending window" and "receiving window"
- The sender maintain a set of sequence numbers corresponding to frames it is permitted to send
- These frames are in "sending windows"
- The receiver maintains a set of frames it is permitted to accept. These frames are in "receivingwindows"
- The three sliding windows protocols differ in terms of efficiency complexity and bufferrequirements.
- The three sliding windows protocol are
    1) A one bit sliding window protocol
    2) A Protocol using go back n
    3) A protocol using selective repeat

1) A one bit sliding window protocol

- Maximum windows size is one, search protocol uses stop- and –wait, here the sender transmitsa frame and wait form it's acknowledgement before sending the next one
- The starting machine fetcher the first packet from its network layer builds a frame from it andsender it.
- When the frame arrives the receiving data link layer checks to see if it is a duplicate.
- If it is the expected frame, it is passed to the network layer and the receiver's window is slidup.

- The acknowledgement field contains the number of the last frame received with out error.
- If it agrees with the sequence number of the frame it fetches the next packet from n/w layer.
- If the sequence number disagrees, it must continue trying to send the same frame.

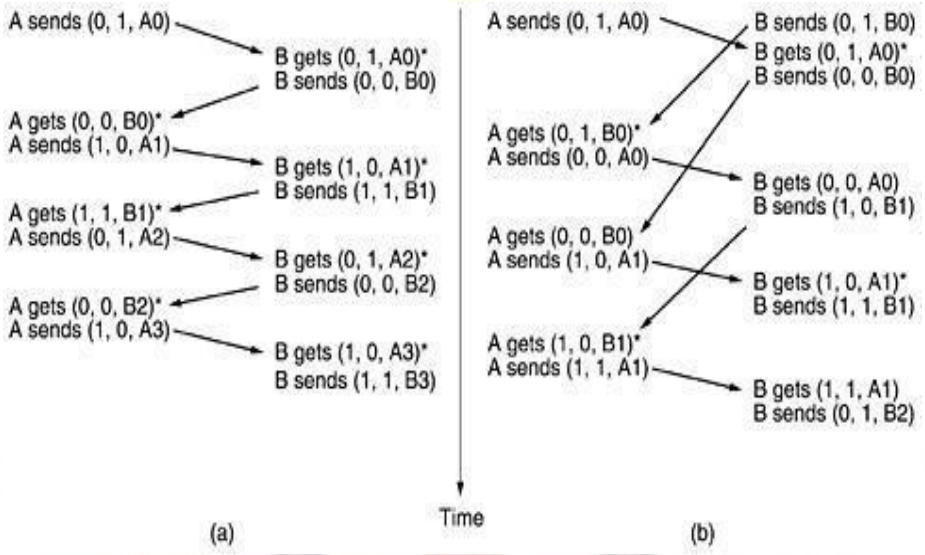


Fig. Two scenarios for protocol 4. (a) Normal case. (b)Abnormal case. The notation is (seq, ack, packet number). An asteriskindicates where a network layer accepts a packet.

2) A protocol using go back n

- To achieve better efficiency the solution is to allow the sender to transmit up to w frames beforeblocking instead of 1.
- If we take 'w' as 26, the sender begins sending frames 0 at t=520 it has finished sending 26frames, the acknowledgement for frame 0 will have just arrived.
- Acknowledgements will arrive after every 20 m sec sender always get's permission tocontinues when it's it
- This technique is known as "pipelining"

- Pipelining frames over a communication channel has same problems. If a damaged framesoccurs in the middle of a long steam frame.
- Go-back-n and selective repeat are the two ways to deal with errors in pipelining
- In Go-back-n the receiver simple discards all subsequent frames, sender no acknowledgementsfor the discarded frames.
- After the senders time out it retransmit all unacknowledged frames in order, starting withmanaged or lost one.
- It wastes a lost of band width, if error rate is high.

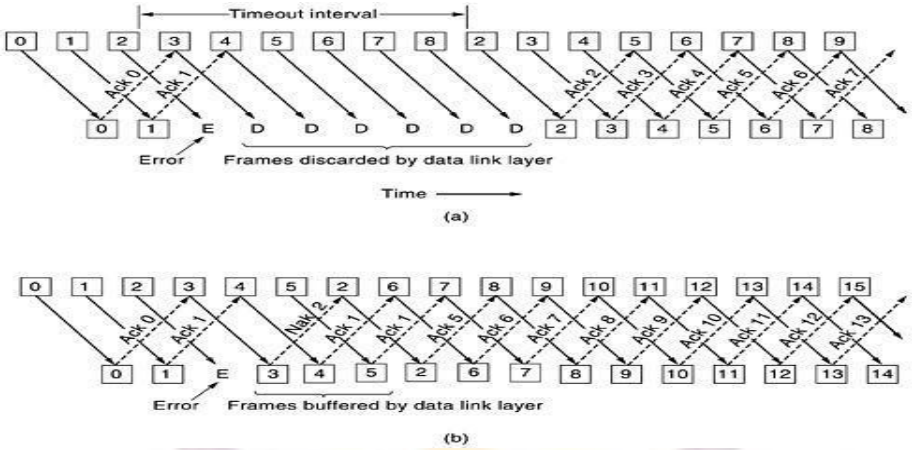
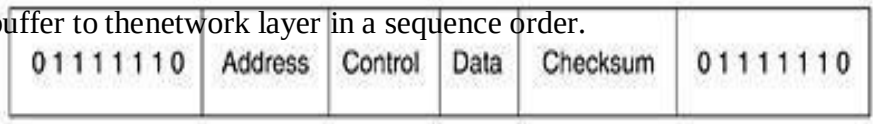


Fig. Pipelining and error recovery. Effect of an error when (a)receiver's window size is 1 and (b) receiver's window size is large.

A protocol using selective repeat:

- The receiver is allowed to accept and buffer the frames fallowing a damaged or lost frame.
- When a receiver suspects than an error has occurred, it sends a negative acknowledgment frameback to the sender.
- It is a request for retransmission of the frame in the NAK specified.
- After the time out the senders transmit the lost frame.
- After lost frame send to the network layer it transmit the other frames stored in the buffer to thenetwork layer in a sequence order.



Multiple access protocol:

A new and elegant method to solve the channel allocation problem is called the ALOHA system, used ground-based radio broadcasting, the basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared channel.

ALOHA 2 types PURE aloha & slotted aloha

PURE ALOHA: not divided according to time intervals do not require global time synchronization.***SLOTTED ALOHA***: divided according to time intervals. Slotted ALOHA need global time synchronization.

PURE ALOHA:

- When data is ready in it, it sends it directly.
- We do not know whether the channel is empty or not then the frames undergo collisions.
- All the frame lengths should be equal, then we get high throughput.
- Checksum recognizes if there is collision or not. It detects the collisions.
- If there is collision will wait for some random time & transmit the next frame. This is knownas retransmission.

Contention system: having single communication channel, where multiple users are competing for thatchannel then those systems are contention systems.

- Work load increasing.
- If N>1 , then we are unable to handle problems.

0<N<1, at least handle and transmit the frames. N-represents data frames which are to be sent. G-represents retransmit.
S-represents the total probability.

- When less no of data frames, then G=S (low loads) when load is over & over(high loads) G>S
- At low loads pure aloha is working well.
- Probability is given by S=GP0 (pure aloha)

P0-the frame which is transmitted without undergoing a collision.Pure aloha, S=Ge

Vulnerable period: the last bits of one frame is collided with the starting bits of another frame

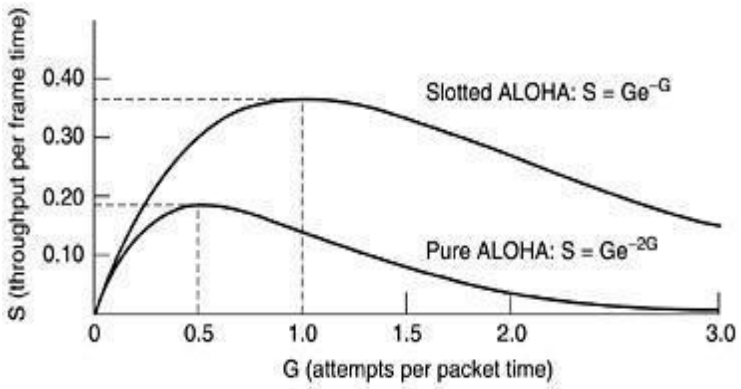
is calledvulnerable period.

- Here we have more collisions in aloha in this period.
- If we have 'K' frames which are to be sent then, position distribution equation

SLOTTED ALOHA:

- It need global time synchronization
- Slotted aloha is better than pure aloha in channel utilization.
- Probability of slotted aloha, S=
- If retransmission G increases, collision also increases if G decreases, graph falls down.
- Slotted aloha is not sensing the channel before transmit ion
- The total channel efficiency for pure aloha is S=1/2e.
- the total channel efficiency for slotted aloha is S=1/e.

Fig. Throughput versus offered traffic for ALOHA systems.



carrier sense multiple access protocols:

protocols in which stations listen for a carrier and act accordingly are called carrier senseprotocols.

1- persistent CSMA(carrier sense multiple access):

- when a station has data to send, it first listen to the channel to see if anyone else is transmittingat that moment.
- If the channel is busy, the station waits until it becomes idle.
- When the station detects an idle channel, it transmits the frame.
- This protocol is called 1-persistent because the station transmits with a probability of 1 whenits finds the channel idle

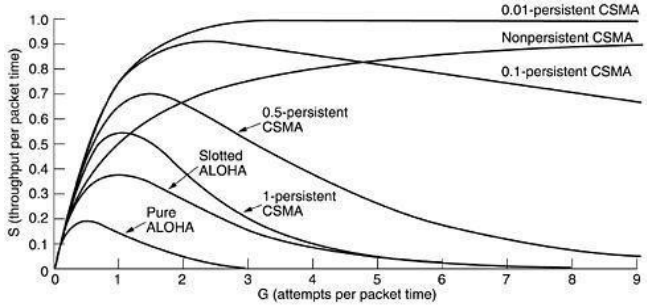
Non persistent CSMA:

- Before sending the data , a station sends the channel.
- If no one else is sending, the station begins sending frames.
- If the channel is already in use, the station does not continuously sense it.
- It waits a random of time & then repeats the algorithm.
- This algorithm leads to better channel utilization than 1-persistant CSMA.

p-persistent CSMA:

- It applies to slotted channels
- When a station ready to sends it senses the channel.
- If it is idle, it transmits with a probability P.
- With a probability Q=1-p it differs until the next slot.
- This process repeat until either the frame has been transmitted.
- If the station initially senses the channel busy, it waits until the next slot& applies the algorithm.

Fig. Comparison of the channel utilization versus load for various random access protocols.



CSMA/CD: (CSMA with collision detection.)

- Terminating damaged frames quickly saves time and bandwidth.
- At to, a station has finished transmitting its frame.
- Any other station having a frame to send may attempt now.
- If two or more stations decide to transmit simultaneously, there will be a collision.
- After a station detects a collision, it aborts its transmission waits a random time & then triesagain, assuming that no other station has X'ted in the meantime.
- Therefore, CSMA/CD consisting of alternating contension and transmission periods, with idleperiods occurring when all stations are quiet.
- Systems in which multiple users share a common channel in a way that can lead to conflicts areknown as contention systems.
- It works well on low loads.

Collision free protocol

collisions do not occur with CSMA/CD. But it can occur during the contention period. These collisions affect the system performance, especially when the cable is long (i.e., large t) and the frames are short. some protocols that resolve the contention for the channel without any collisions at all, not even during the contention period. Most of these are not currently used in major systems, but in a rapidly.

Collision free protocols are:

1. **Bit map protocol.**
2. **Binary count down protocol.**

BIT MAP protocol:

- Each contention period consists of exactly N slots.
- If station 0 has a frame to send, it transmits a 1 bit during the 0^{th} slot.
- No other station is allowed to transmit during this slot.
- In general, station J may announce that it has a frame to send by inserting a 1 bit into slot J.
- After all N slots have passed by each station has complete knowledge of which station andwish to transmit.
- At that point, they begin transmitting numerical order.
- Since every one agrees on who goes next, there will never be any collision.
- The protocols desire to transmit is broadcast before the actual transmission are calledreservation protocols.
- At low loads average waiting time 1.5N slots.
- At high loads average waiting time 0.5N slots.
- Efficiency at low loads = d/(N+d).
- Efficiency at high loads = d/(d+1).

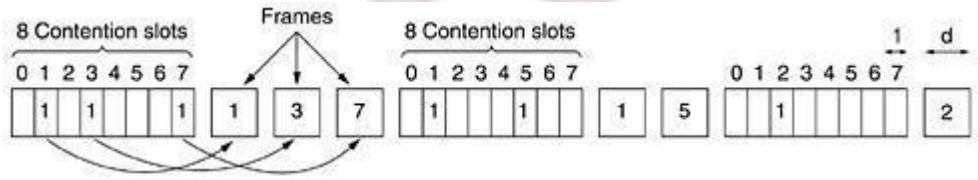


Fig: The basic bit-map protocol.

Binary cut down protocols:

- The station wants to use the channel now broadcasts its address as a binary bit string, startingwith the high order bit.
- All addresses are assumed to be the same length.this protocol is called binary cut down.
- To avoid conflicts, based on choice rule must be applied.
- As a station sees a high order bit position that is 0 in its address has ben overwritten with a 1.

- For example: if stations 0010, 0100, 1001 & 1010 are all trying to get the channel.
- In the first bit time the stations X'mit 0,0,1 & 1 respectively.
- Stations, 0010 & 1010 continue.
- The next bit is 0 & both stations continue.
- The next bit is 1 so station 1001 gives up.
- The winner is station 1010 because it has the highest address.
- It now transmits the frame.
- Channel efficiency=d/d+log.

Wireless LAN protocol

A system of portable computers that communicate by radio can be regarded as a wireless LAN.

- Wireless LAN are based on radio signals for transmission.
- The competitor who wants to access the channel is too far from the station so the problem iscalled hidden station problem.
- If two stations are out of the range the stations get bad reception the problem is called exposedstation problem.
- To overcome the problems we use MACA & MACAW protocols.

MACA-multiple access with collision avoidance

MACAW-MACA improve its performance & renamed their new protocol MACAW.If A sends message RTS to B, if RTS is reached B it sends message CTS to A. RTS□request to send.
CTS□ clear to send.

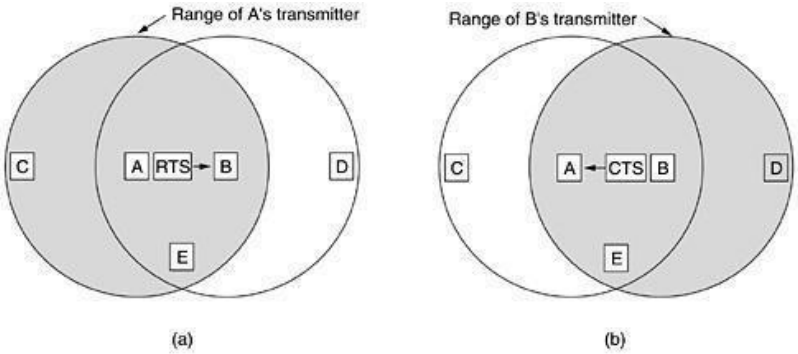


Fig: The MACA protocol. (a) *A* sending an RTS to *B*. (b) *B* responding with a CTS to *A*.

IEEE standards for LAN:

IEEE proposed some channel allocation protocols for LANs and MANs.

– logical link control protocol.

– Ethernet.

– token bus

– token ring

– distributed queue dual bus.

Ethernet:

Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

- Ethernet refers to the cable.
- Four types of cabling are commonly used

Fig: The most common kinds of Ethernet cabling.

- 10 base 5 called as thick Ethernet.

- Connections are made using vampire taps.
- 10 base 5 means it operates at 10 mbps.uses baseband signaling & support segments of up to500 meters.
- 10Base5, a **transceiver** is clamped securely around the cable its tap makes contact with theinner core.
- The transceiver contains the electronics that handle carrier detection and collision detection.
- When a collision is detected, the transceiver also puts a special invalid signal on the cable toensure that all othertransceivers also realize that a collision has occurred.
- With 10Base5, a **transceiver cable** or **drop cable** connects the transceiver to an interface boardin the computer.
- The transceiver cable may be up to 50 meters long and contains five
- individually shielded twisted pairs.
- Two of the pairs are for data in and data out, respectively.
- Two more are for control signals in and out. The fifth pair, which is not always used, allowsthe computer to power the transceiver electronics
- The transceiver cable terminates on an interface board inside the computer. The interface boardcontains a controller chip that transmits frames to, and receives frames from, the transceiver.
- The controller is responsible for assembling the data into the proper frame format, as well as computing checksums on outgoing frames and verifying them on incoming frames.
- 10 base 2 also called as thin Ethernet.
- Connections are made using industry standards BNC connectors to form T junctions, ratherthan using vampire taps.
- With 10 base2, the connection to the cable is just a passive BNC t-junction connector. BNCconnectors are easier to use and more reliable.
- Thin Ethernet is much cheaper and easier to install, but it can run for only 185 meters persegment, each of which can handle only 30 machines.
- Detecting cable breaks, excessive length, bad taps, or loose connectors can be a major problemwith both media.
- For this reason, techniques have been developed to track them down.
- A pulse of known shape is injected into the cable. If the pulse hits an obstacle or the

end of thecable, an echo will be generated and sent back.

- By carefully timing the interval between sending the pulse and receiving the echo, it is possible to localize the origin of the echo. This technique is called **time domain reflectometry**.
- 10 base T uses twisted pair cable.
- In 10 base T all stations have a cable running to a central hub.
- With 10 base T, there is no cable at all just hub.
- Adding or removing a station is simpler in this configuration, & cable breaks can be detectedeasily.
- The advantage is the maximum cable run from the hub is only 100 meters.
- base F uses fiber optics.

- This is expensive due to the cost of the connectors and terminators.
- We use for different topologies they are linear, spine , tree, & segmented.
- To allow larger networks, multiple cable can be connected by repeaters.
- A repeater is a physical layer device it receives, amplifiers & retransmits signals in both directions.

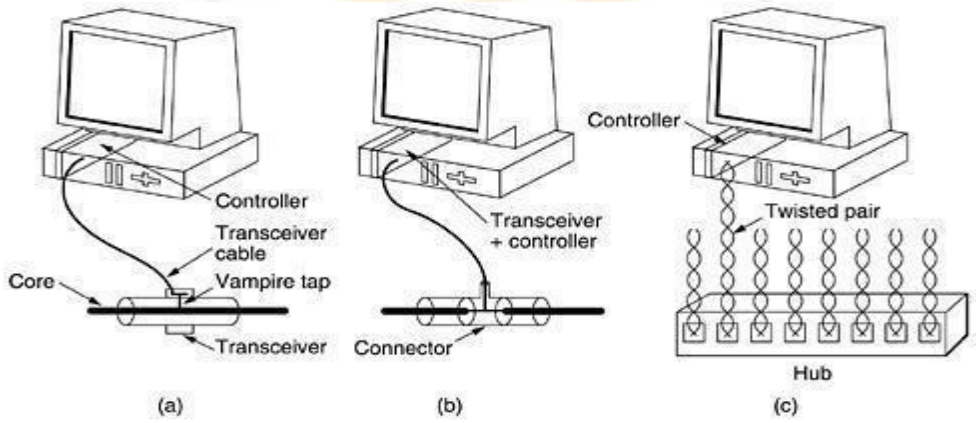


Fig: Three kinds of Ethernet cabling. (a) 10Base5. (b) 10Base2.(c) 10Base-T.

Manchester Encoding:

- To determine the start, end, or middle of each bit without reference to an external clock. Two such approaches are called Manchester encoding & differential Manchester encoding.
- With Manchester encoding, each bit period is devided into two equal intervals.
- A binary 1 bit is sent by having first high & then low.
- A binary is 0 is just reverse first low & then high.
- Every bit period has a transition in the middle, making it easy for the receave to synchronize with the sender.
- The disadvantages is it requires twice as much bandwidth as straight binary encoding.
- Differential Manchester encoding is a variation of basic Manchester encoding.
- A 1 bit is indicated by the absence of a transition at the start of the interval.
- A 0 bit is indicated by the presence of a transition at the start of the interval.

- In both cases, the transition in the middle.

- The high signal is + 0.85 volts & the low signal is _ 0.85 volts.

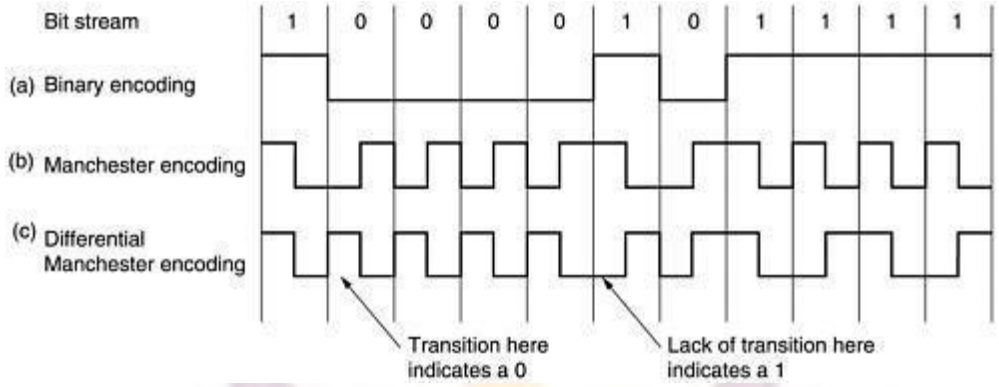


Fig: (a) Binary encoding. (b) Manchester encoding. (c)Differential Manchester encoding.

- Ethernet does not use differential Manchester encoding.
- All Ethernets use Manchester encoding.

MAC sublayer protocol:

- Each frame starts with a preamble of 7 bytes, each containing the bit pattern 10101010.
- Start of frame byte containing 10101011 to denote the start of the frame itself.
- The frame contains 2 addresses, one for the destination & and one for the source.
- It allows 2-byte & 6-byte addresses.
- The length field, tells how many bytes are present in the data field, from a min of 0 to a maxof 1500 bytes.
- The valid frames must be at least 64 bytes long, from destination address to checksum.
- If the data portion of a frame is less than 46 bytes, the pad field is used to fill out the frameto the minimum size.
- Frames with fewer bytes are padded out to 64 bytes.
- Checksum is used for error detection.

Binary exponential back of algorithem:

- This algorithm was chosen to dynamically adapt to the number of stations trying to send.
- After a collision, each station waits either 0 or 1 slot times before trying again.
- In general, after i collision, a random number between 0 and 2i-1 is chosen, & that noof slots is skipped.
- If the randomization interval for all collisions was 1023, the chance of two stationscolliding for a second time would be negligible.
- By having the randomization interval grow exponentially as more & more consecutivecollision occur.
- The algorithm ensures a low delay when only a few stations collide but also ensures thatthe collision is resolved in a reasonable interval when many stations colloid.
- All that needed is reserve the first contention slot fallowing successful X'ion for thedestination station.

COMPUTER NETWORKS (23CS502)

UNIT –III

NETWORK LAYER

Network Layer: Design issues, Routing algorithms: shortest path routing, Flooding, Hierarchical routing, Broadcast, Multicast, distance vector routing, Congestion Control Algorithms, Quality of Service, Internet working, The Network layer in the internet.

Network Layer:

- The network layer is concerned with getting packets from the source all the way to thedestination.
- The network layer must know about the topology of the communication subnet in the set of allrouters, and choose appropriate paths through it.
- Network layer is the lowest layer that deals with end-to –end transmission.

Design Issues

The design issues include the service provided to the transport layer & the internal design ofthe subnet.

Services provided to the transport layer:

- The network layer provides services to the transport layer at the network layer / transportlayer interface.
- The network layer services have been designed with following goals:

1. The services should be independent of the router technology.
2. The transport layer should be shielded from the number, type, and topology of the routers present.
3. The network address made available to the transport layer should use a uniform numberingplan, even across LAN'S & mans.

IMPLEMENATION OF CONNECTIONLESS SERVICE:

- If CL service is offered, packets are injected into the subnet individually & routedindependently of each other.
- No advance setup is needed.
- Packets are called datagram's &the subnet is called a datagram subnet.
- Process p1 has a long message for p2. It sends the message to the transport layer withinstructions to deliver it to process p2 on host H2.
- The message is four times longer than the maximum packet size, so the network layer hasto break it into router A using some point – to – point protocol.
- Every router has a table telling it where to send packets for each possible destination.
- Each table entry is a pair of destination & the outgoing line to use for that destination.
- 'A' has only two outgoing lines to B & C- so every incoming packet must be sent to one ofthese routers , even if the ultimate destination is some other router.
- As they arrived at A, packets 1,2, &3 were stored each was forwarded to C. packet 1 wasthen forwarded to E& then to F.
- When the packet reaches F, it was encapsulated in a data link layer frame & sent to H2 overthe LAN.
- Packets 2 and 3 follow the same route.
- For some reason , A decided to send packet H via a different route than that of the firstthree.
- It learned of a traffic jam somewhere along the ACE path & updated its routing table.
- The algorithm that manages the tables & makes the routing decisions is called the "routingalgorithm".

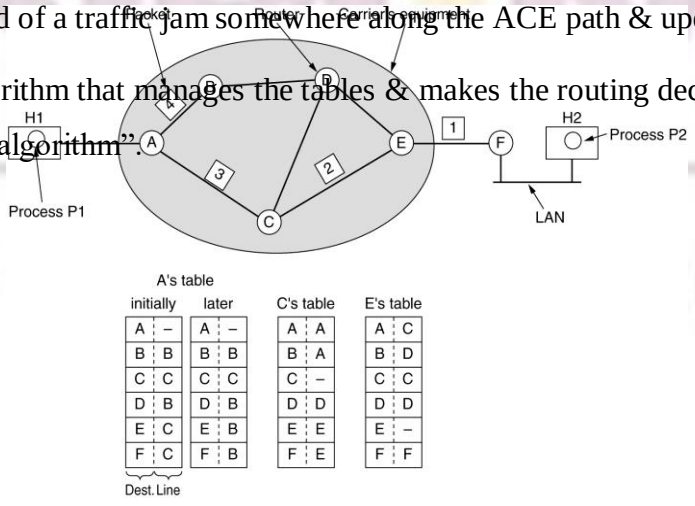


Fig: Routing within a diagram subnet

IMPLEMENTATION OF CONNECTION –ORIENTED SERVICE:

If connection oriented service is used a path from the source route to the destinationrouter must be established before any data packets can be sent.

- This connection is called a virtual circuit(VC) and the subnet is called a virtual circuit subnet.
- The idea of virtual circuits is to avoid having to choose a new route for every packet sent.
- When a connection is established, a route from the source machine to the destination machineis chosen as part of the connection setup & stored in tables inside the routers.
- That route is used for all traffic flowing over the connection.
- When the connection is released , the virtual circuit is also terminated.
- With connection- oriented service, each packet carries an identifier telling which virtual circuitit belongs to.
- Host H1 has established connection 1 with host H2.
- A's table says if a packet bearing connection identifier 1 comes in from H1, it is to be sent torouter C & given connection identifier 1.
- If H3 also wants to establish a connection to H2.
- It chooses connection identifier 1 & tells the subnet to establish the virtual circuit.
- 'A' can easily identified the connection 1 packets from H1 & connection 1 packets from H3,'c' cannot do this.
- 'A' assigns a different connection identifier to the outgoing traffic for the second connection.
- To avoid the conflicts routers replace connection identifier in out going packets.

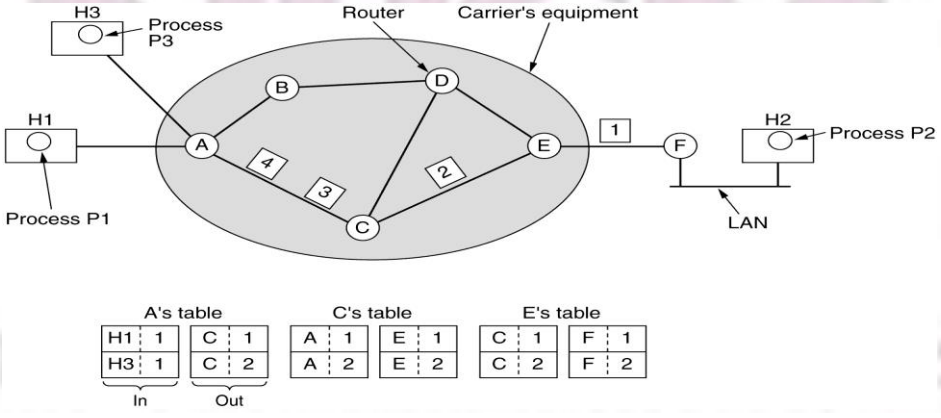


Fig: Routing within a virtual-circuit

subnetComparison of virtual –circuit &

datagram subnets:

Issue	Datagram subnet	Virtual circuit subnet
Circuit steup	Not needed	Required
Addressing	Each packet contains the full source & destination address	Each packet contains a short VC number.
State information	Routers do not hold state information about connections	Each VC requires router tablespace per connection
Routing	Each packet is routed independently	Route chosen when VC is setup ;all packets follow it.
Effect of router failures	None,except for packets lostduring the crash	All VC's that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources canbe allocated in advance for each VC.

Routing Algorithms

- The main function of the network layer is routing packets from the source machine to the destination machine.
- The routing algorithm is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.
- If bnet uses datagram's internally, this decision must be made a new for every arrivingdata packet since the best route may have changed since last time.

the su

- If the subnet uses virtual circuits internally, routing decisions are made only when a new virtual circuit is being set up.
- Routing algorithms can be grouped into two major classes:

  1. non adaptive 2. adaptive.

- Nonadaptive algorithms do not base their routing decisions on measurements or estimates ofthe current traffic and topology. This procedure is sometimes called static routing.
- Adaptive algorithms, in contrast, change their routing decisions to reflect changes in the topology, and usually the traffic as well. This procedure is sometimes called Dynamic routing.
- Static algorithms are shortest path routing algorithm
- Flooding algorithm
- Dynamic algorithms are distance vector routing algorithm.

OPTIMALITY PRINCIPLE:

- Optimality principle state that no loops should be present in transferring the information.
- The set of optimal routes from all sources to a given destination form a tree rooted at thedestination. Such a tree is called a **sink tree.**

SHORTEST PATH ROUTING ALGORITHM:

In this routing algorithm we need to choose shortest path from source to destination.

- To choose a route between a given pair of routers, the algorithm just finds the shortest pathbetween them.
- One-way of measuring path length is the number of hops.
- Another metric is the geographic distance in kilometers.
- Several algorithms for computing the shortest path between two nodes are known.
- Each node is labeled with its distance from the source node along the best known path.
- Initially no paths are known, so all nodes are labeled with infinity.
- As the algorithm proceeds and paths are found, the labels may change, reflecting betterpaths.
- A label may be either temporary or permanent.
- When it is discovered that a label represents the shortest possible path from the source tothat node, it is made permanent & never changes thereafter.

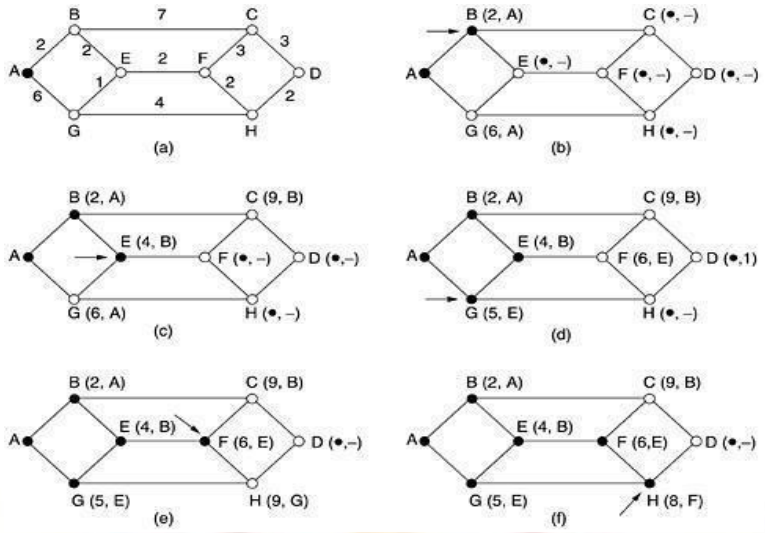


Fig. The first five steps used in computing the shortest path from *A* to *D*. The arrows indicate the working node.

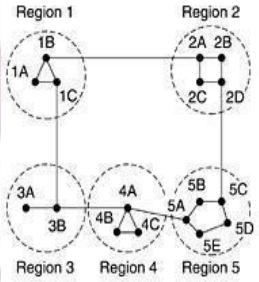
FLOODING:

- Flooding is another static algorithm.
- In flooding, every incoming packet is sent out on every outgoing line except the one itachieved on.
- Flooding generates vast number of duplicate packets, an infinite number we need to takemeasures to damp the process.
- One such measure is to have a hop counter contained in the header of each packet, whichis decremented at each hop, with the packet being discarded when the counter reaches zero.
- The hop counter should be initialized to the length of the path from source to destination.
- To avoid duplicates, the source router put a sequence number in each packet it receivesfrom its hosts.
- Each router needs a list per source router telling which sequence numbers originating atthat source have already been seen.
- If an incoming packet is on the list, it is not flooded.
- Each list should be maintained a counter, k, and mean that all sequence numbers through khave been seen.

- When a packet comes in. it is easy to check if the packet is a duplicate; if so, it is discarded.
- A variation of flooding is selective flooding.
- In selective flooding algorithm the routers do not send every incoming packet out on everyline.
- Only on those lines that are going approximately in the right direction.
- Flooding can be useful in distributed database applications to update all the databasesconcurrently.

HIERARCHICAL ROUTING:

- As networks grow in size, the router routing tables grow proportionally.
- It takes more CPU time is needed to scan them and more bandwidth is needed to send statusreports about them.
- When hierarchal routing is used the routers are divided into regions.
- Each router know the details about how to route packets to destinations with in its own region.
- Knowing nothing about the internal structure of the regions.
- When different networks are interconnected , we can assume the network as a separate region in order to free the routers in one network from having to know the topological structure of theother ones.
- Above fig. is an example of routing in a two level hierarchy with five regions.
- The full routing table for router 1A has 17 entries.
- When routing is done hierarchically , there are entries for all the local routers as before, but allother regions have been condensed into a single router, so all traffic for region 2 goes via the 1B-2A line.
- But, the rest of the remote traffic goes via the 1C-3B line.
- Hierarchical routing has reduced the table from 17 to 7 entries.
- The savings in the table space increase & there is problem of increased path length.
- Example is the best route from 1A to 5C is via region 2.
- But with hierarchical routing all traffic to region 5 goes via region 3, because that is better formost destinations in region 5.



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Fig. Hierarchical routing

Broadcast Routing:

- Sending a packet to all destinations simultaneously is called broadcasting.
- Various methods are used for broad casting.
- One broadcasting method is the source simply sends a distinct packet to each destination.
- In this bandwidth is wasted & the source has to maintain the list of all destinations.
- The second broadcasting method is flooding. Flooding is useful as a broadcasting methodif none of the above methods described below are applicable.
- The problem with flooding is it generates too many packets and consumes too muchbandwidth.
- A third algorithm is multi destination routing. In this method, each packet contains a list ofall destinations.
- When a packet arrives at a router, the router checks all the destinations to determine the setof output lines that will be needed.
- A fourth broadcast algorithm use the sink tree for the router initiating the broadcast or anyother spanning tree.
- A spanning tree is a subset of the subset of the subnet that includes all the routers but contains no loops.
- If each router knows which of its lines belong to the spanning tree , except the line it arrivedon, it copy an incoming broadcast packet onto all the spanning tree lines.
- It makes use of bandwidth, generating the minimum number of packets necessary to do thejob.
- Last broadcast algorithm is to approximate the behavior of the previous one, even when therouters do not know anything at all about spanning trees.
- When a broadcast packet arrives at a router, the router checks if it is on the line that isnormally used for sending packets to the source of the broadcast.
- If so, the broadcast packet itself followed the best route from the router & is therefore thefirst copy to arrive at the router.
- The router forwards copies of it onto all lines except the one it arrived on.
- If the broadcast packet arrive on a line other than the preferred one for reaching the source, the packet is discarded as a duplicate. The algorithm called ***reverse path forwarding***.

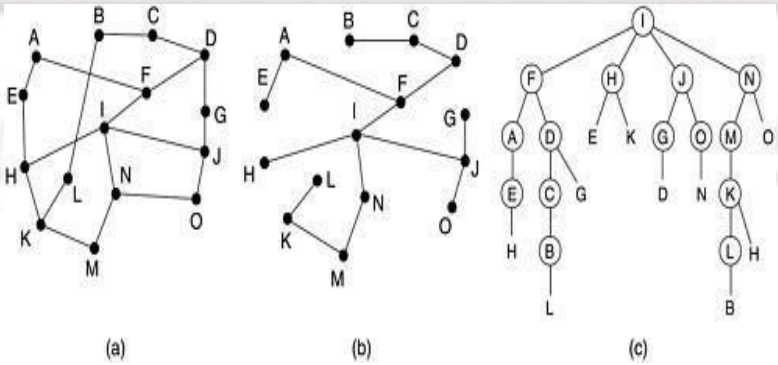


Fig. Reverse path forwarding. (a) A subnet. (b) A sink tree.
(c)The tree built by reverse path forwarding.

Multicast Routing:

- Some applications need processes work together in groups, a group of processesimplementing a distributed database system.
- It is frequently necessary for one process to send a message to all other members of thegroup.
- Sending a message to such a group is called multicasting. The routing algorithm is called multicast routing.
- To do multicasting, group management is required.
- When a process joins a group, its informs its host.
- The routers must know which of their hosts belong to which groups.
- Hosts must inform their routers about changes in group membership, or routers must querytheir hosts periodically.
- In multicast routing, each router computes a spanning tree covering all other routers in thesubnet.
- Some routers are attached to hosts that belong to one or both of these groups.
- The spanning tree for the leftmost router is as shown below.
- The process sends a multicast packet to a group.
- The first router examines its spanning tree & prunes it, removing all the lines that do

not leadto hosts that are members of the group.

- Multicast packets are forwarded only along the appropriate spanning tree.
- Multicast tree for group 1 is shown below:
- Multicast packets are forwarded only along the appropriate tree.
- Pruning the spanning tree is possible by using link state routing & distance vector routing.
- If link state routing is used , the spanning tree can be pruned by starting at the end of each path& working toward the root , removing all routers that do not belong to the group.
- If distance vector routing is used, whenever a router with no hosts interested in a particular group, the other routers receives a multicast message for that group, it responds with a PRUNEmessage, telling the sender not to send it any more multicasts for that group.
- The disadvantage of that algorithm is not used for large networks.

DISTANCE VECTOR ROUTING:

- Distance vector routing algorithm is the dynamic algorithm.
- Distance vector routing algorithm is also called as bellman- ford (or) ford-Fulkerson algorithm.
- Distance vector routing algorithm operate by having each router maintain a table giving thebest known distance to each destination & which line use to get there.
- The tables are updated by exchanging information with the neighbors'.
- Each router maintains a routing table, containing one entry for each router in the subnet.
- Entry contains two parts: the outgoing line to use for that destination& an estimate of the timeor distance to that destination.
- Router knows the delay to each of its neighbor.
- Once every T msec each router sends to each neighbor a list of its estimated delays to eachdestination. It also receives the similar list from each neighbor.
- If a table has come in from neighbor X. X is estimate how long it takes to get to route I isindicated as xi.
- If the delay to router x is M msec, if can reach the router I via x in Xi+M msec.
- For each neighbor by performing this calculation a router can find out which estimate seems the best & use that estimate & the corresponding line in its new routing table.

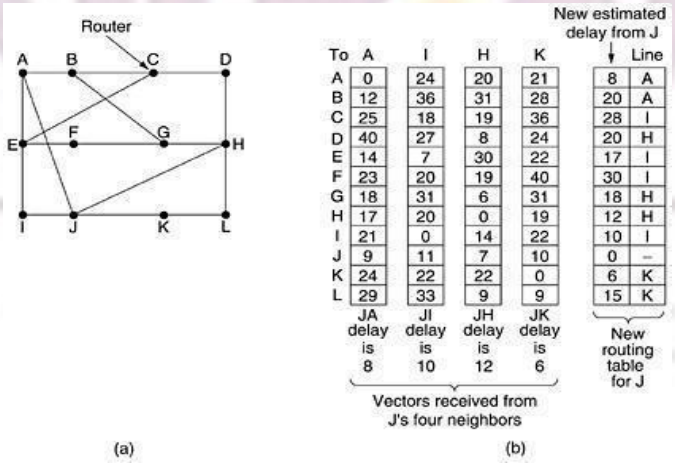


Fig: (a) A subnet. (b) Input from *A*, *I*, *H*, *K*, and the new routing table for *J*.

- The delay vectors received from the neighbors of router j.
- In the example, A has delay of 12 msec to B, 25 msec to C, 40 msec to D etc.
- J has measured its delay to its neighbors' A,I,H, &K as 8,9,10,12 & 6 msecrespectively.
- Now J computes its new route to router G.
- A can get to G in 18 msec,J can get to A in 8 msec.
- J knows it can count on a delay of 26 msec to G.
- Similarly, it computes the delay to G via I,H,& K as 41,18,&37 msec respectively.
- The best of these values is 18 msec so it makes an entry in its routing table that the delay to Gis 18 msec. & that the route to use is via H.

Congestion control algorithms

- When too many packets are present in the subnet, performance degrades. This situation is calledcongestion.
- Congestion ctrl occurs if move no .of packets are transmitted with in the maximum range ofcarrying capacity.
- Congestion problem occurs when

1. The processor is slow.

2. If more input lines & only one output line.
3. Bandwidth of lines may be less than what we required.

- The difference between congestion ctrl & flow control is.
- Congestion ctrl make sure the subnet is able to carry the offered traffic.

- If involves the behavior of all the hosts, all the routers, the store- and –forwarding processingwith in the routers & all other factors that relate to the carrying capacity of the subnet.
- Flow control relates to the point –to – point traffic between a given sender & a given receiver.
- It make sure that a fast sender cannot continually transmit data faster than the receiver canabsorb it.
- Flow control involves some direct feedback from the receiver to the sender.

General principles of congestion control:

- General principles are divided into open loop and closed loop.
- Open loop: no modifications are allowed in the execution while the information is goingon. Open loop is provided by good design.

- Closed loop or feedback loop: this approach has 3 packets.

1. We have to monitor the system when & where congestion occurs.
2. We have to inform to source which can take action regarding the congestion.
3. We have to adjust the total system operation to correct the problem.

Congestion prevention policies:

- Congestion control in open loop systems.
- These systems minimize congestion in the first place.
- We see different policies that can affect congestion at data link , network & transport layer.

At the data link layer:

1. Retransmission policy.
2. Out of order caching policy.
3. Acknowledge meant policy.

4. Flow control policy.

At the network layer:

1. Compare virtual circuit & datagram inside the subnet.
2. Packet queuing &service policy.
3. Packet discards policy.
4. Routing algorithm.
5. Packet lifetime management.

At the transport layer:

1. Retransmission policy.
2. Out of order caching policy.
3. Acknowledgement policy.
4. Flow control policy.
5. Time out determination.

Traffic shaping:

- Regulating the average rate of data transmission is called traffic shaping.
- Traffic shaping reduces congestion.
- Monitoring a traffic flow is called traffic policy.
- Algorithms of traffic shaping are
    1. The leaky bucket algorithm.
    2. The token bucket algorithm.

The leaky bucket algorithm:

- The rate at which water enters the bucket, the outflow is at a constant rate, r, when there is anywater in the bucket and zero when the bucket is empty.
- Also, once the bucket is full, any additional water entering it spills over the sides and is lost
- It is a single server queuing system with constant service time.
- Each host is connected to the network by an interface containing a leaky bucket is a finiteinternal queue.
- If a packet arrives at a queue when it is full, the packet is discarded.
- The host is allowed to put one packet per clock tick onto the network.
- This mechanism turns an uneven flow of packets from the user processes inside the

host intoan even flow of packets onto the network.

- It greatly reduces the chances of congestion.
- When packets are all the same size. e.g.: ATM cells this algorithm can be used as described.
- When variable sized packets are used, it allows a fixed number of bytes per tick, rather just onepacket.
- If the byte count is too low, the next packet must wait until the next tick.

Token bucket algorithm:

In this algorithm, the leaky bucket holds tokens, generated by a clock at the rate of one token everydelta Tsec.

- For a packet to be transmitted, it must capture and destroy one token.
- We have a bucket holding three tokens, with five packets waiting to be transmitted
- Three of the five packets have passed, but the other two are waiting for two more tokens to begenerated.
- Token bucket algorithm provides a different kind of traffic shaping than the leaky bucketalgorithm.
- The difference between two algorithms is token bucket algorithm throws away tokens when thebucket fills up but never discards packets.
- The leaky bucket algorithm discards packets when the bucket fills up.
- In token bucket algorithm a packet can only be transmitted if enough tokens are available.
- The implementation of token bucket algorithm is just a variable that count tokens.
- The counter is incremented by one every delta T and decremented by one whenever a packet issent.
- When the counter hits zero, no packets may be sent.

- One way to get smoother traffic is to put a leaky bucket after the token bucket.
- The network has to simulate the algorithm &make sure that no more packets or bytes are being sent than are permitted.

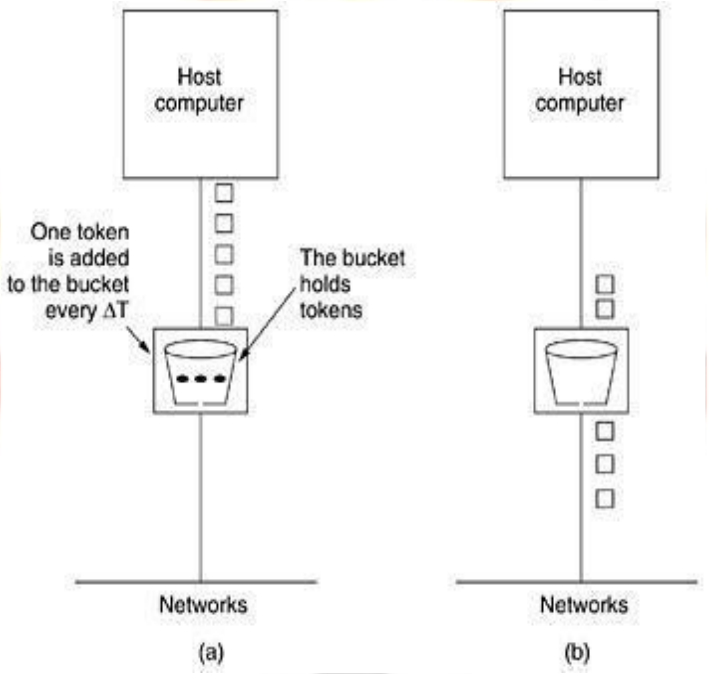


Fig: The token bucket algorithm. (a) Before. (b) After.

Congestion control in virtual circuit subnets:

- We ctrl congestion in virtual circuits dynamically.
- 'Admission control' is widely used to keep congestion that has already started from getting worse.
- Congestion ctrl in virtual circuit comes under closed loop.
- Once Congestion has been signaled, no more virtual circuits are set up until the problem has solved.
- With this, the setup to new transport layer connection fails.
- An alternative approach is to allow new virtual circuits but carefully route all new virtual circuits around problem areas.
- Another approach is to make an agreement between the host & subnet when a virtual circuit isset up.
- This agreement specifies the volume & shape of the traffic, quality of service required, & otherparameters.

- In this way, congestion is unlikely to occur on the new virtual circuits because all the necessaryresources and guaranteed to be available.

Congestion control in datagram subnets:

- Each router can easily monitor the utilization of its output lines & other resources.
- Each newly-arriving packed is checked to see if its output line is in warning state.
- If it is, in warning state an action can be taken in several alternatives.

Warning bits:

- As the route was in the warning state, it continued to set the acknowledgements with it set.
- The source monitored the fraction of acknowledgements with the bit set & adjusted itstransmission rate accordingly.
- As the warning bits continued to flow in, the source continued to decrease its transmission rate.

Choke packets:

- The router sends a choke packet back to the source host.
- When the source host gets the choke packet, it is required to reduce the traffic sent to thespecified destination by x percent.
- Other packets aimed at the same destination generate more choke packets. The host shouldignore choke packets referring to that destination for a fixed time interval.
- After the time period expired, if one choke packet arrives, the line is still congested, so the hostreduces the flow & begins ignoring choke packets again.
- If no choke packets arrive during the time period , the host may increase the flow again

Hot-by-hop chokes packets:

- Sending a choke packet to the source hosts over long distances does not work well as thereaction is so slow.
- An approach is to have the choke packet take effect at every hop it passes through.
- The effect of this hop-by-hop scheme is to provide quick relief at point of congestion.

Load shedding:

- With this we can completely eliminate the congestion.
- Load shedding gives priority to all the packets which we are transmitting
- In this we can eliminate some messages at the sender.

Jitter control:

- If we are sending audio or video at constant rate in quality should be high.

- The variations in packet arrival time are called jitter.
- When a packet arrives at a router, the router checks to see how much the packet is behind orahead of its schedule.
- The packets that are ahead of schedule get slowed down & packets that are behind scheduleget speeded up.

Congestion control for multicasting:

- In multicasting we need to send messages to a group. There are multiple senders and multiplereceivers.
- We use protocol called RSVP (Resource Reservation Protocol).
    - Rsvp: Resource Reservation Protocol
- This protocol is used for making the reservations other protocols are used for sending the data.
- Rsvp allows multiple senders to transmit to multiple groups of receivers.
    - Note: refer text book for diagram
- Hosts 1&2are multicast senders, hosts 3, 4 &5are multicast receivers.
- To eliminate congestion, any of the receivers in a group can send a reservation message up thetree to the sender.
- At each step, the router notes the reservation and reserves the necessary bandwidth
- If insufficient band with is available it reports back failure.
- Host 3 has requested a channel a host 1
- Once it has been established packets can flow 1 to 3 with out congestion.
- If host 3 next reserves a channel to the other sender host to a second path is reserved
- When making a reservation, a reserve can specify one or more sources that it wants to receivefrom.
- The routers use this information to optimize band width planning.

COMPUTER NETWORKS (23CS502)

Internet working

- Different networks are connected together to form an internet.
- The purpose of inter connecting all these networks is to allow users on one network to communicate with users on other network & also sending packets from one network to other network.

Networks can differ in many ways: the networks differ based on the following

Item	Some Possibilities
Service offered	Connection oriented versus connectionless
Protocols	IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.
Addressing	Flat (802) versus hierarchical (IP)
Multicasting	Present or absent (also broadcasting)
Packet size	Every network has its own maximum
Quality of service	Present or absent; many different kinds
Error handling	Reliable, ordered, and unordered delivery
Flow control	Sliding window, rate control, other, or none
Congestion control	Leaky bucket, token bucket, RED, choke packets, etc.
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, by packet, by byte, or not at all

Networks can be interconnected by different devices.

- In the physical layer, networks can be connected by repeats or hubs.
- In the data link layer, networks can be connected by bridges and switches.
- In the network layer, routers are used to connect two networks.

  A router that can handle multiple protocols is called a multiprotocol router. in the transport layer, to interface between two transports connections we use transport gateways.

  In the application layer, networks can be connected by application gateways. In the application layer, networks can be connected by application gateways.
- Application gateways translate message semantics.
- Internetworking is possible in 2 ways:
- Connection oriented concatenation of virtual – circuit subnets.
- Connection less internetworking.

Concatenated virtual circuit:

- In this circuits a connection to a host in a distant network is set up in a way the connectionsare normally established.
- The subnet builds a virtual circuit to the router nearest the destination network as thedestination is remote.
- It constructs virtual circuits from that router to an external gateway. (Multiprotocol Router)
- The gateway records the existence of the virtual circuits in its tables.
- It builds other virtual circuits to a router in the next subnet.
- This process continues until the destination host has been reached.
- Data packets begin flowing along the path.
- All data packets must traverse the same sequence of gateways.
- Packets in a flow are never reordered by the network.

- In this approach a sequence of virtual circuits is set up from the source through one or moregateways to the destination.
- This works better when all the networks have the same properties.

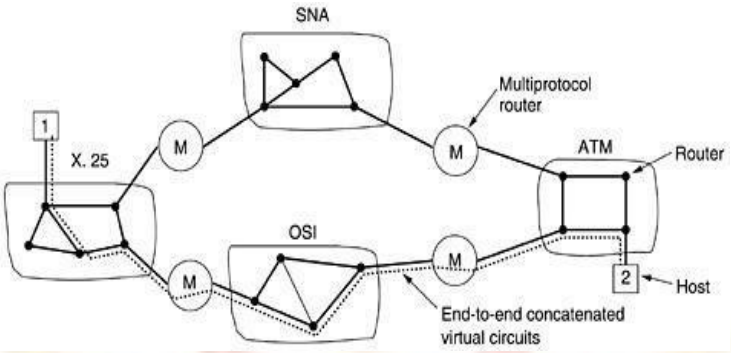


Fig: Internetworking using concatenated virtual circuits.

Connectionless internetworking:

- This model does not require all packets belonging to one connection to traverse the same sequence of gateways.
- From host-1 to host -2 datagram's take different routers through the internetwork.
- Routing decision made separately for each packet, depending on the traffic at the moment the packet is sent.
- There is no guarantee that the packet arrive at the destination in order, assuming that they arrive at all.
- If each network has it s own network layer protocol, it is not possible for a packet from one network to transit another one.
- Multiprotocol routers translate from one format to another if the formats are with same information fields.

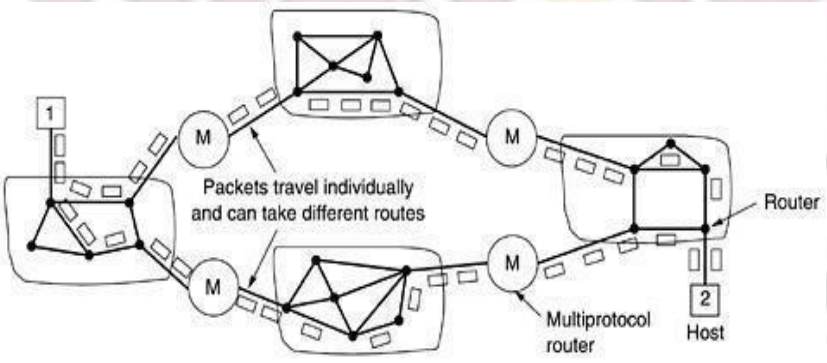


Fig: A connectionless internet.

- We can design a universal internet packet & have all routers recognize it.
- IP packet is designed to be carried through many networks.

INTERNETWORK ROUTING:

- Consider an example in which the internetwork of five networks are connected by 6 routes
- Make a graph in that every route can directly access to every other router connected to anynetwork to which it is connected.
- In the above example B can directly access A and C via network 2 and also D via network 3
- A two level routing algorithm is used
- With in each network an interior gate way protocol is used
- Between in the network an exterior gate way protocol is used
- Each network in an inter network is independent of all the others

Fragmentation:

- Problem occurs when a large packets wants to travel through a N/W whose maximum packetssizes is too small
- The solution to this problem is to allow gate ways to break up packets in to fragments
- Which fragment is send as separate internet packets
- For recombining the fragments back in to the original packet we use two approaches
- *Transparent fragmentation*
- *Non Transparent fragmentation*
- In Transparent fragmentation we reassemble the fragment at each gate way until the designationis reached
- In Non Transparent fragmentation we reassemble the fragments only at the digestion

- an IP datagram consists off a header part and a test part
- the header has 20 bits fixed part and variable length optional part

- Version fields are which version of the protocol the datagram belongs.
- IHL field tell how long the header is in 32-bit words
- Type of service specifies what kind of service we are applying.
- Total length indicates both header and data.
- Maximum length 65,535 bytes.
- Identification field identifies the new fragment arrived.
- All the fragments of a datagram's contains the same identification value.
- DF stands for don't fragment.
- If the DF bit is set, data is not fragmented it is send as a single datagram.
- MF stands for more fragments.
- It is used to know when all fragments of a datagram have arrived.
- Fragment offset determine s where the fragment belongs in the current datagram.
- All the fragments except last are in a datagram must be a multiple of 8bytes.
- There is a maximum of 8192 fragments per datagram.
- Time to live field used to specify the packet life time.
- Protocol field tells which transport process to give it to. TCP&UDP some others are used.
- Head checksum field verifies the header only.
- The source address and destination address indicates the network number and host number.
- Option field is variable length .if uses the options that are defined.

IP ADDRESS:

- On the Internet every host & router has an IP address.
- IP address consists of network number and host number.
- Network numbers are managed by a nonprofit corporation called *ICANN (Internet Corporationfor Assigned Names and Numbers)* to avoid conflicts.
- No two machines on the Internet have the same IP address.
- If host belongs 2 networks, host contains 2 IP addresses.
- IP addresses are 32 bits long & are used in the source Address & Destination Address fields of IP packets.
- IP packet does not actually refer to a host, it refers only network interface.
- IP addresses are in dotted decimal notation.
- IP address is of 32 bits & representation is ().().().()
- IP address are of five different classes based on host range address.
- Least IP address is 0.0.0.0
- Highest IP address is 255.255.255.255

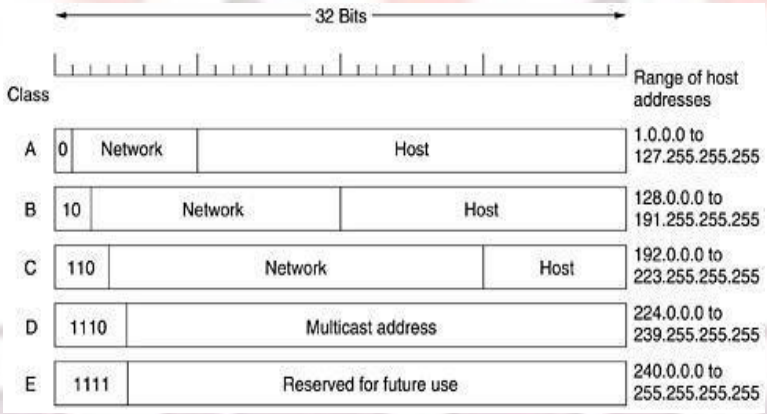


Fig: IP address formats.

- The value 0 means this network or this host current network.
- The value 1 used to indicate all hosts on the indicated network.

COMPUTER NETWORKS (23CS502)

UNIT-IV

Transport Layer: Transport Services, Elements of Transport protocols, Connection management, TCP and UDP protocols.

Transport Services

The services provided by the transport layer are similar to those of the data link layer. The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks. The data link layer controls the physical layer while the transport layer controls all the lower layers.

- End-to-end delivery
- Addressing
- Reliable delivery
- Flow control
- Multiplexing

End-to-end delivery:

The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-enddelivery of an entire message from a source to the destination.

Reliable delivery:

The transport layer provides reliability services by retransmitting the lost and damaged packets.

The reliable delivery has four aspects:

- Error control
- Sequence control
- Loss control
- Duplication control

Error Control

- The primary role of reliability is **Error Control**. In reality, no transmission will be 100 percent error-free delivery. Therefore, transport layer protocols are designed to provide error-free transmission.

- The data link layer also provides the error handling mechanism, but it ensures only node-to- node error-free delivery. However, node-to-node reliability does not ensure the end-to-end reliability.
- The data link layer checks for the error between each network. If an error is introduced inside one of the routers, then this error will not be caught by the data link layer. It only detects those errors that have been introduced between the beginning and end of the link. Therefore, the transport layer performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.

Sequence Control

- The second aspect of the reliability is sequence control which is implemented at the transport layer.
- On the sending end, the transport layer is responsible for ensuring that the packets received from the upper layers can be used by the lower layers. On the receiving end, it ensures that the various segments of a transmission can be correctly reassembled.

Loss Control

Loss Control is a third aspect of reliability. The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receivers transport layer to identify the missing segment.

Duplication Control

Duplication Control is the fourth aspect of reliability. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers are used to identify the lost packets; similarly, it allows the receiver to identify and discard duplicate segments.

Flow Control

Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.

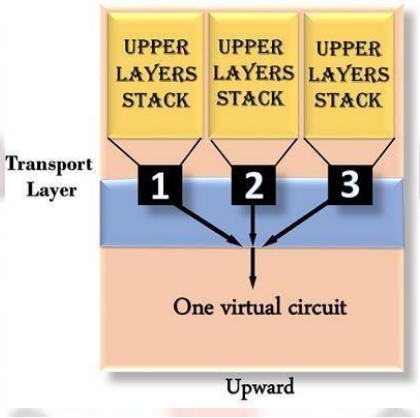
Multiplexing

The transport layer uses the multiplexing to improve transmission efficiency.

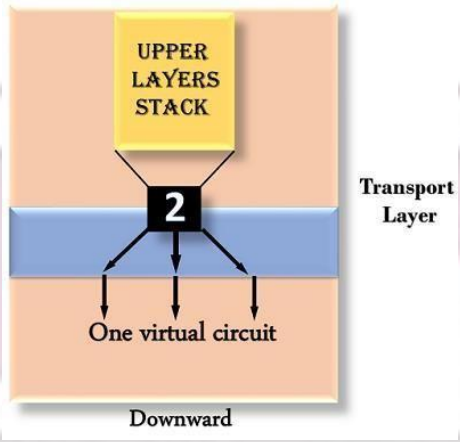
Multiplexing can occur in two ways:

- **Upward multiplexing:** Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.

- through upward multiplexing.



- **Downward multiplexing:** Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used

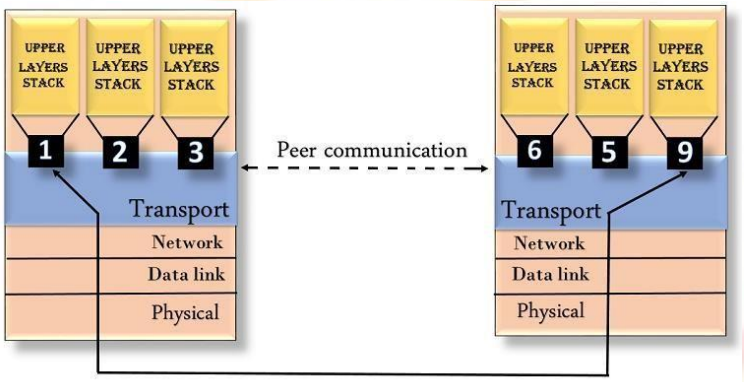


Addressing

- According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be

transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.

- The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.
- The transport layer protocols need to know which upper-layer protocols are communicating.



The connection is established in TCP using the three-way handshake to create a connection. One side, say the server, passively stays for an incoming link by implementing the LISTEN and ACCEPT primitives, either determining a particular other side or nobody in particular.

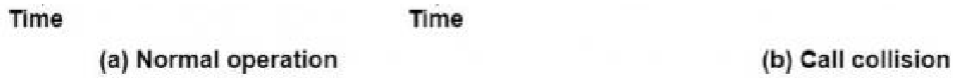
Connection Management

The other side performs a connect primitive specifying the IP port to which it wants to join.

The maximum TCP segment size available, other options are optionally like some private data (example password).

The CONNECT primitive transmits a TCP segment with the SYN bit on and the ACK bit off and waits for a response.

The sequence of TCP segments sent in the typical case, as shown in the figure below −



TCP Connection Management

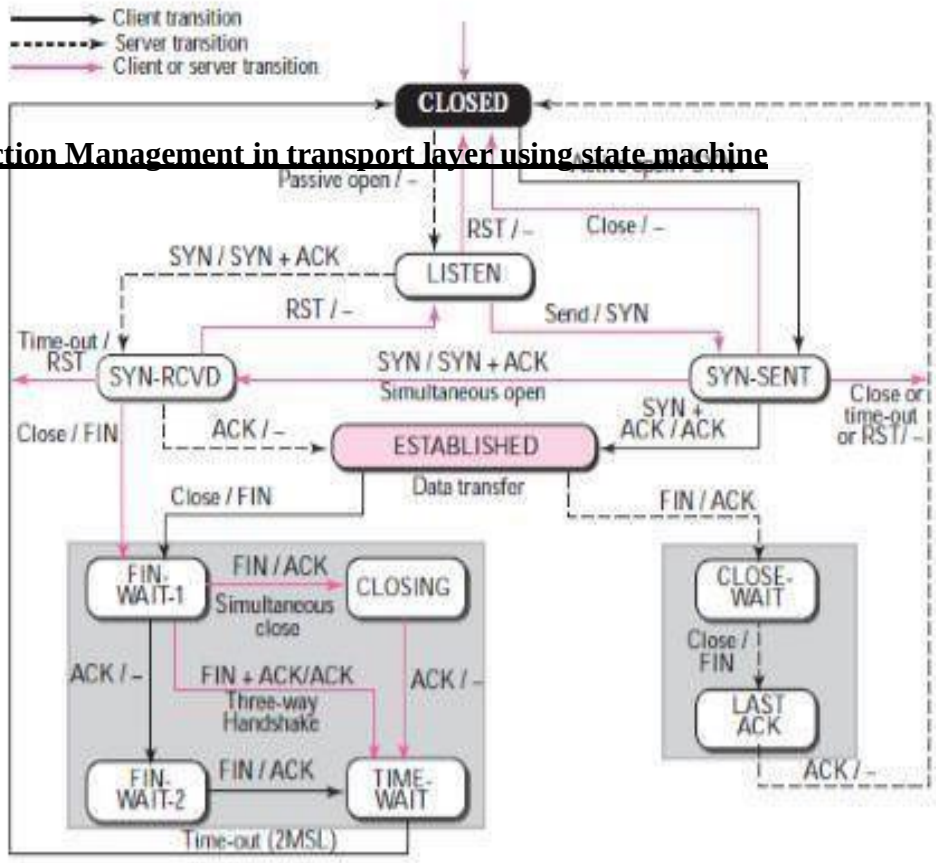
When the segment sent by Host-1 reaches the destination, i.e., host -2, the receiving server checks to see if there is a process that has done a LISTEN on the port given in the destination port field. If not, it sends a response with the RST bit on to refuse the connection. Otherwise, it governs the TCP segment to the listing process, which can accept or decline (for example, if it does not look similar to the client) the connection.

TCP Connection Termination

TCP (Transmission Control Protocol) is a transmission protocol that ensures data transmission in an ordered and secure manner. It sends and receives the data packets in the same order. TCP is a **four-layer** protocol compared to OSI (Open System Interconnection Model), which is a **seven-layer** transmission process. It is recommended to transmit data from high-level protocols due to its integrity and security between the server and client.

TCP needs a 4-way handshake for its termination. To establish a connection, TCP needs a 3-way handshake

Connection Management in transport layer using state machine



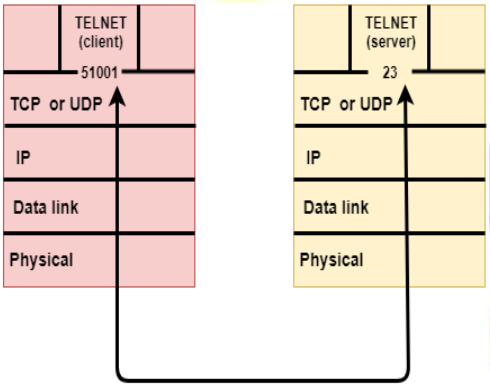
The client application opens a connection to the server by sending a TCP segment which only the header is present (no data). This header contains a flag SYN stands for "Synchronize" and the TCP port number the server (application). The client is in SYN_SENT state (SYN sent).

The server (application) is listening (listen) and on receipt of the SYN from the client, it changes of state and responds with a SYN and ACK flag. The server is then able SYN_RCVD (SYN received).

The client receives the server's TCP segment with SYN ACK indicators and move in status ESTABLISHED. He also sent a response ACK to the server that also passes in status ESTABLISHED.

This exchange in three phases (three-way handshake) complete the establishment of the TCP connection can now be used to exchange data between the client and server.

- An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.Each port is defined by a positive integer address, and it is of 16 bits.

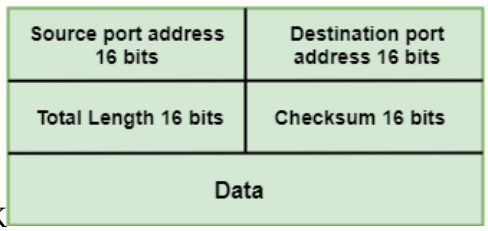


UDP

- UDP stands for **User Datagram Protocol**.
- UDP is a simple protocol and it provides nonsequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.
- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

User Datagram Format

The user datagram has a 16-byte header which is shown below:



633.7K 7eginners

- **Source port address:** It defines the address of the application process that has delivered amessage. The source port address is of 16 bits address.
- **Destination port address:** It defines the address of the application process that will receive themessage. The destination port address is of a 16-bit address.
- **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.
- **Checksum:** The checksum is a 16-bit field which is used in error detection.
- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

Disadvantages of UDP protocol

TCP

- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

Features Of TCP protocol

- **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
- **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval,

  The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.

- **Flow Control:** When receiving TCP sends an acknowledgement back to the sender
- indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any

  problem. This mechanism is also referred to as a window mechanism.

Multiplexing: Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.

- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bitsequence number field represents the position of the data in an original data stream.
- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data fromother communicating devices. If ACK field is set to 1, then it specifies the sequence number.

COMPUTER NETWORKS(CS3103PC)

Differences b/w TCP & UDP

Basis for Comparison	TCP	UDP
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Orientedprotocol	It is a Connectionless protocol
Speed	Slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement	It waits for	It neither takes the acknowledgement, nor it retransmits the damaged frame.