COMPUTER NETWORKS (23CY404)

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.

Computer network:

It is defined as the interconnected collection of autonomous computers.

Two computers are said to be interconnected if they are able to exchange information.

Uses of Computer networks:

1. Business applications
2. Home applications
3. Mobile users
4. Social issues.

1. Business applications:

- Advantages of business applications is resource sharing.
- Data available to anyone on the network without regard to the physical location of the source & the user.
- Ex: a group of office workers share a common printer.
- If a company's information system is consisting of one are more databases and some no of employees who need to access them remotely. In this case the data are stored on powerful computers called servers.
- All this data centrally housed and maintained by system administrator.
- The employer has simpler machines called clients.
- In client & server model, communication takes in the form of the request and reply.
- Here, the client process sending a message over the network to the server process.
- The client process then waits for a reply message.
- When the server process gets the request it performs the requested work or looks up the requested data and sends back a reply.

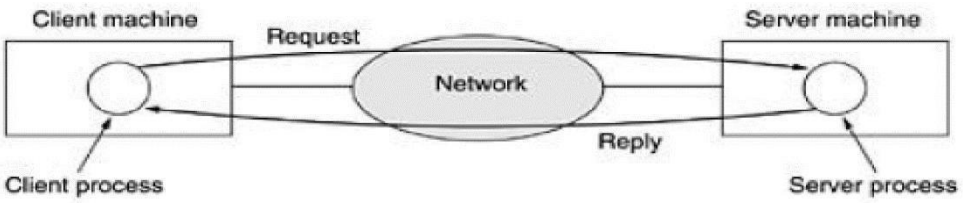


Fig:the client server model involves request – reply model.

- A computer network provide powerful communication medium. Ex: E-mail.
- Another form of computer assisted communication is video conferencing.
- Companies can do business electronically.
- Many companies provide catalogs of their goods & services online & take orders online. It is called e-commerce.
- Another goal is doing business with customers over the internet. Ex: airlines, bookstores…

2. Home applications:

1. Access to remote information.
2. Person-to-Person communication.
3. Interactive entertainment
4. Electronic commerce.

Access to remote information:

Ex: surfing the **World Wide Web** for information. Information available includes the arts, business, cooking, government, health, history, science, sports and many others.

Person-to-person communication:

Ex: **chat room** in which a group of people can type messages for all to see person-to-person communication is also called peer-to-peer communication.

Interactive entertainment:

Ex1: **video on demand:** it is possible to select any movie or television program ever made, in any country and have it displayed on your screen instantly.

Ex2: **Online gaming**

Electronic commerce:

Ex: **home shopping:** users can search the online catalogs of thousands of companies.

3. Mobile users:

Owners of notebook computers want to be connected to their home base even when away from home so, wireless networks became popular.

4. Social issues:

There are related with general applications like newspapers, channels etc. people can exchange messages with individuals.

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.

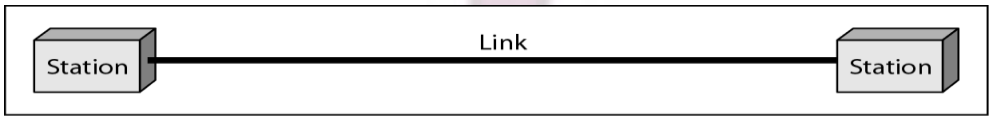
There are two possible types of connections: **point-to-point and multipoint.**

Point-to-Point

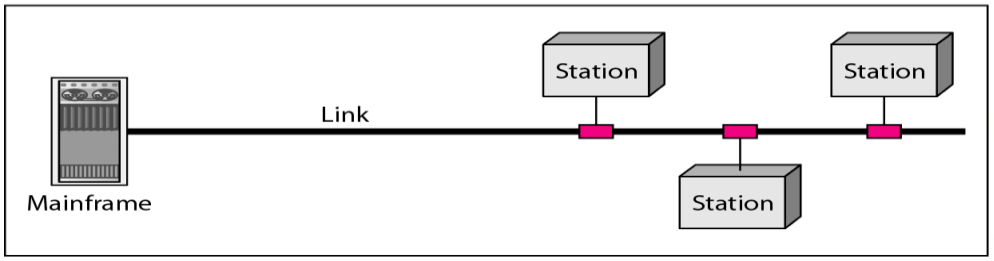
A point-to- point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite 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.



a. Point-to-point

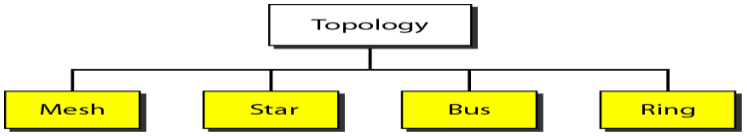


b. Multipoint

Physical Topology

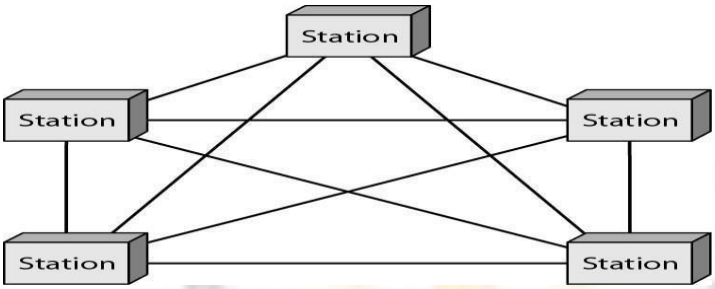
The term physical topology refers to the way in which a network is laid out physically.Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.

There are four basic topologies possible: mesh, star, bus, and ring



MESH:

A mesh topology is the one where every node is connected to every other node in the network.



A mesh topology can be a full mesh topology or a partially connected mesh topology.

In a full mesh topology, every computer in the network has a connection to each of the other computers in that network.

The number of connections in this network can be calculated using the following formula (n is the number of computers in the network): n(n-1)/2.

In a partially connected mesh topology, at least two of the computers in the network have connections to multiple other computers in the network.

It is an inexpensive way to implement redundancy in a network. In the event that one of the primary computers or connections in the network fails, the rest of the network continues to operate normally.

Advantages of a mesh topology

It can handle high amounts of traffic, because multiple devices can transmit data simultaneously.

A failure of one device does not cause a break in the network or transmission of data.

Adding additional devices does not disrupt data transmission between other devices.

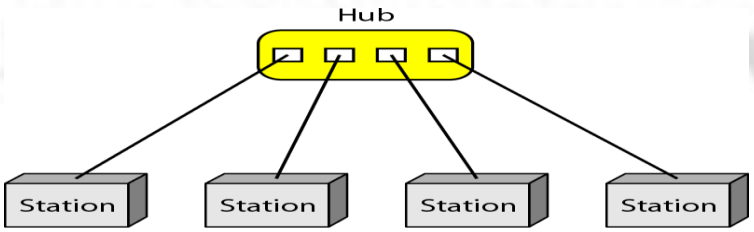
Disadvantages of a mesh topology

The cost to implement is higher than other network topologies, making it a less desirable option. Building and maintaining the topology is difficult and time consuming.

The chance of redundant connections is high, which adds to the high costs and potential for Reduced efficiency.

STAR:

A star topology is one of the most common network setups. In this configuration, every node connects to a central network device, like a hub, switch, or computer. The central network device acts as a server and the peripheral devices act as clients. Depending on the type of network card used in each computer of the star topology, a coaxial cable or a RJ-45network cable is used to connect computers together.



Advantages of star topology

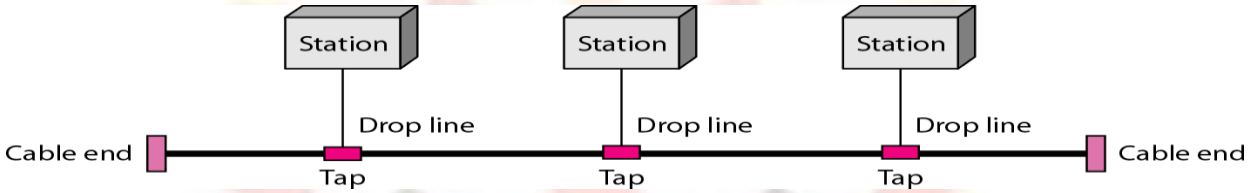
Centralized management of the network, through the use of the central computer, hub, or switch. Easy to add another computer to the network.
If one computer on the network fails, the rest of the network continues to function normally.
The star topology is used in local-area networks (LANs), High-speed LANs often use a star topology with a central hub.

Disadvantages of star topology

Can have a higher cost to implement, especially when using a switch or router as the central network device.
The central network device determines the performance and number of nodes the network can handle. If the central computer, hub, or switch fails, the entire network goes down and all computers are disconnected from the network

BUS:

In bus topology is a network setup in which each computer and network device are connected to a single cable or backbone.



Advantages of bus topology

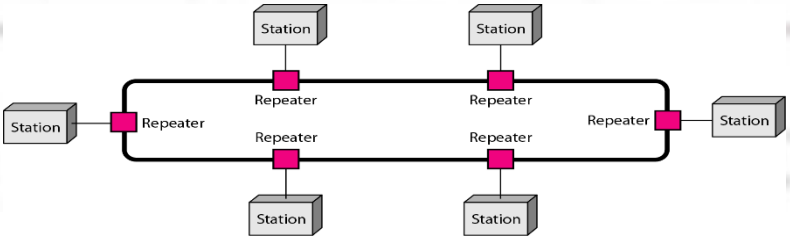
It works well when you have a small network.
It's the easiest network topology for connecting computers or peripherals in a linear fashion.
It requires less cable length than a star topology.

Disadvantages of bus topology

It can be difficult to identify the problems if the whole network goes down. It can be hard to troubleshoot individual device issues.
Bus topology is not great for large networks. Terminators are required for both ends of the main cable. Additional devices slow the network down.
If a main cable is damaged, the network fails or splits in to two.

RING

A ring topology is a network configuration in which device connections create a circular data path. In a ring network, packets of data travel from one device to the next until they reach their destination. Most ring topologies allow packets to travel only in one direction, called a unidirectional ring network. Others permit data to move in either direction, called bidirectional.



Advantages of ring topology

Ring topologies may be used in either local area networks (LANs) or wide area networks (WANs).
All data flows in one direction, reducing the chance of packet collisions.

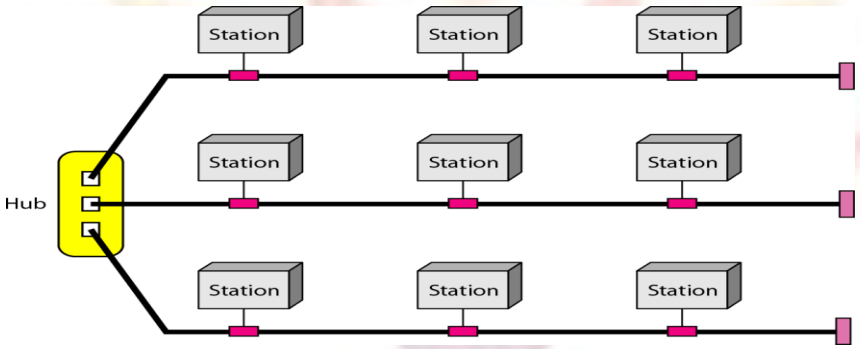
A network server is not needed to control network connectivity between each workstation. Data can transfer between workstations at high speeds.
Additional workstations can be added without impacting performance of the network.

Disadvantage of a ring topology

If any individual connection in the ring is broken, the entire network is affected.
All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.
The entire network will be impacted if one workstation shuts down.
The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches.

HYBRID

A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology.



Transmission technology

There are two types of transmission technologies are wide spread.

1. Broadcast links.
2. Point-to-point links.

Broadcast network:

- It contains a single communication channel that is shared by all the machines on the network.
- Short messages, called packets in certain contexts, sent by any machine are received by all the others
- An address fixed with in the packet specifies the intended recipient.
- Upon, receiving a packet, a machine cheeks the address field.
- If the packet is intended for the receiving machine, that machine processes the packet, it is just ignored.
- Broadcast systems generally also allow the possibility of addressing a packet to all destinations by using a special code in the address field.

- When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called "broadcasting".
- Some broadcasting systems also support transmission to a subset of the machines, something known as **multicasting.**
- Each machine can 'subscribe' to any or all of the groups.
- When a packet is sent to a certain group, it is delivered to all machines subscribing to that group.

Point-to point network:

- This network consists of many connections between individual pairs of machines.
- To go from the source to destination, a packet on this type of network may have to first visit one or more intermediate machines.
- Often multiple routes, of different lengths, are possible, so finding good ones is important in point-to-point networks.
- Routing algorithms are used for deciding best route in this network.
- Typically used for large network.
- Point-to-point transmission with one sender & one receiver is called **unicasting.**

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)

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

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.
- Lan's used various topologies like BUS, RING, STAR, MESH and HYBRID .

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.

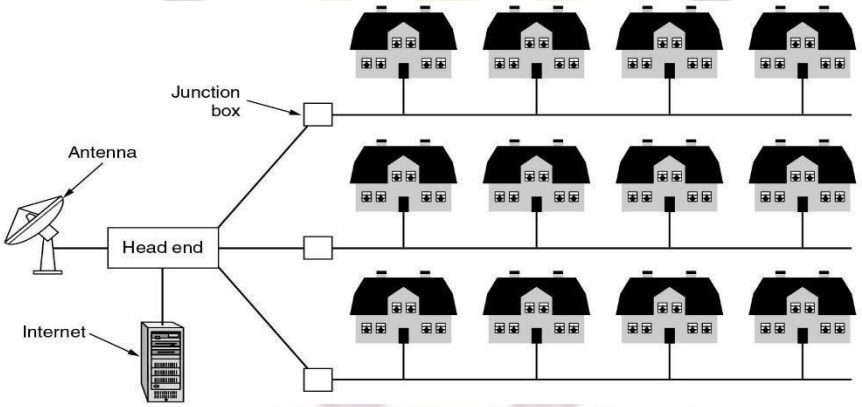
Dynamic allocation divided into 2 types

- 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.

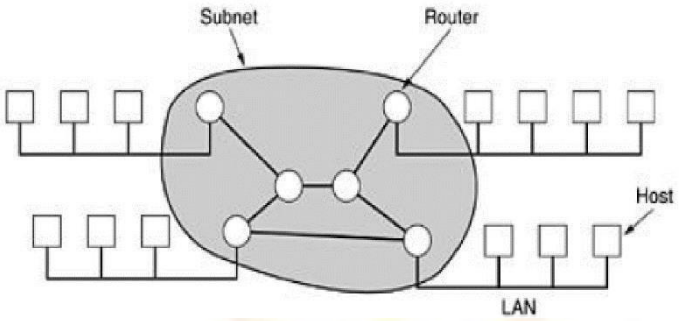


Fig: Relations between hosts and LANs and subnets.

- 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.
- A stream of packets resulting from initial message is illustrated in below figure:

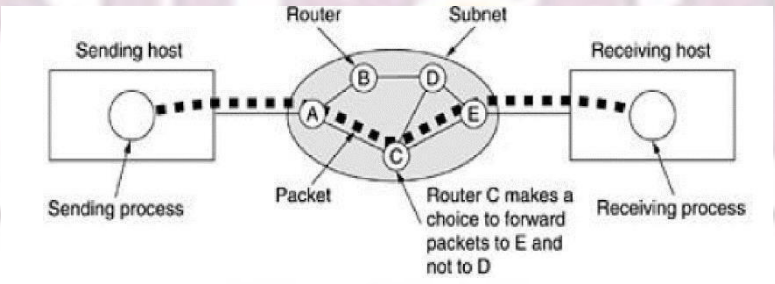


Fig:a stream of packets from sender to receiver.

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.

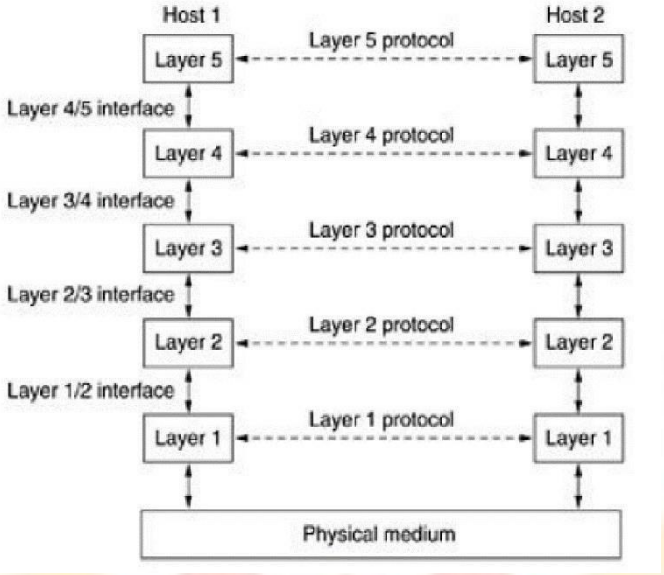
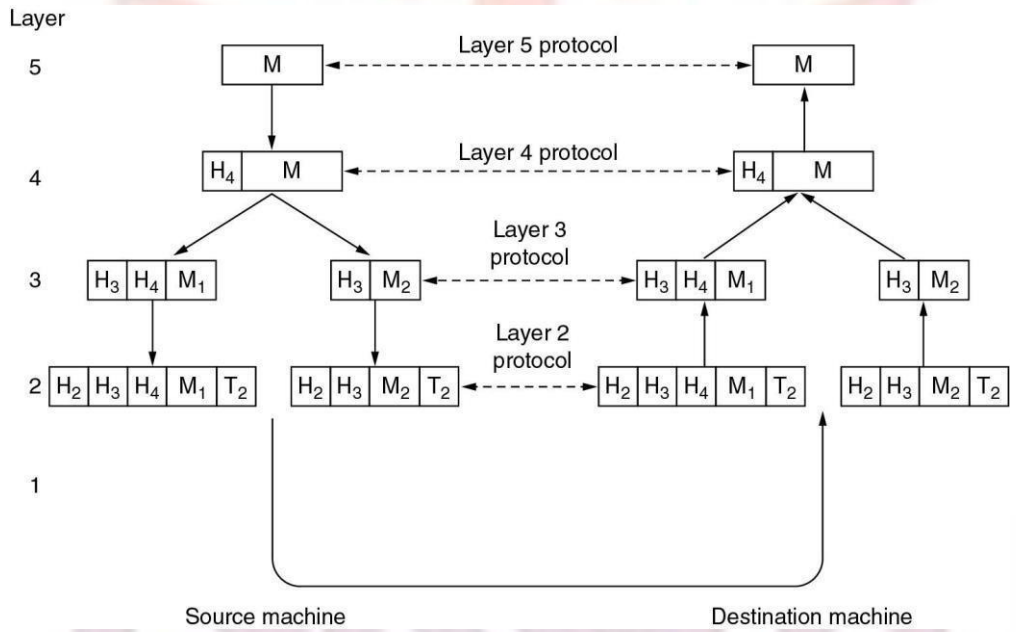


Fig: layers, protocals, interfaces



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.
- Each service can be characterized by quality of service.
- 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.
- The primitives for connection –oriented service are different from those of connectionless service.
- 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.

Listen: executed by server. It means server is ready to accept connection. It blocks the process of server until connection request comes.

Connect: executed by client to request the connection. It sends connection req. TPDU(transport protocol data unit) (packet) to server. If server is able to handle connection then it sends Connection accepted TPDU.

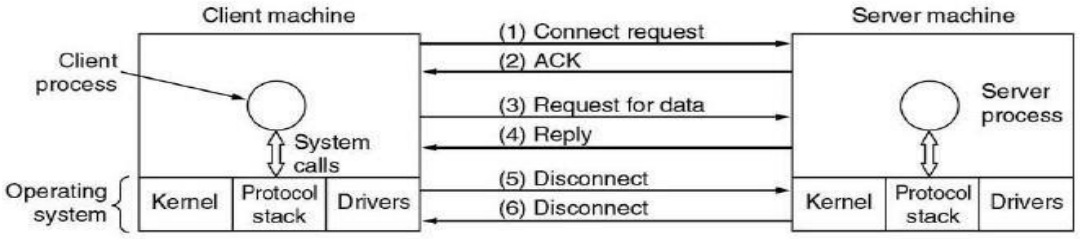
Send: executed to send data to other end.

Receive: when ever client or server is waiting for data, It executes Receive primitive. This is also blocking primitive.

Disconnect: to disconnect connection. Two variants of disconnect.

1. Asymmetric: either side issues disconnect, connection will be released.

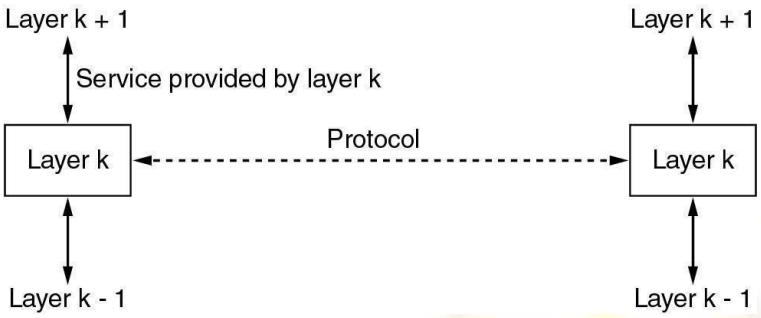
2. Symmetric: both the side need to separately execute disconnect.



Packets sent in a simple client-server interaction on a connection-oriented network.

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.

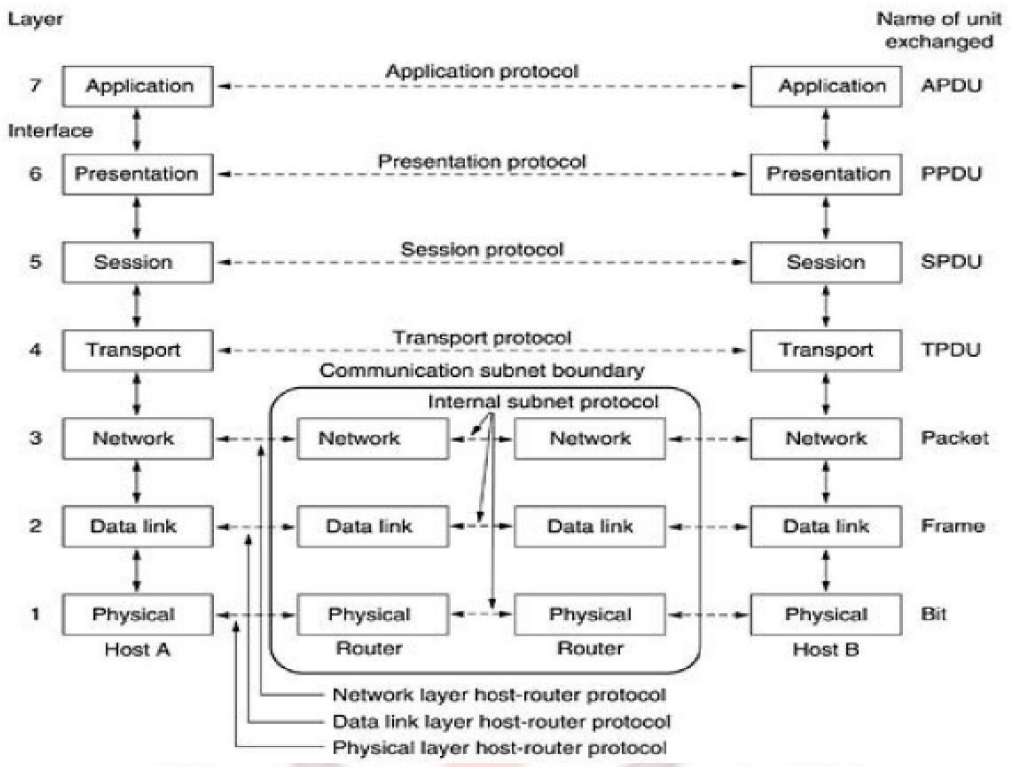


Fig: OSI reference model.

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.

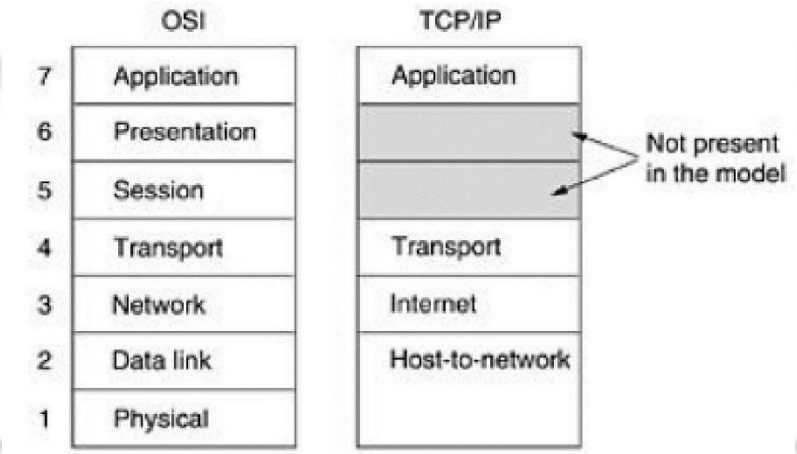
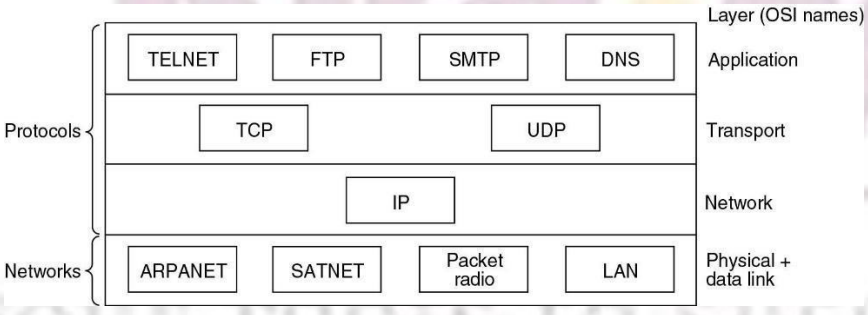


Fig:TCP/IP reference model.



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 oriented services.

Criticism Of The OSI Model And Its Protocols

Neither the OSI model and its protocols nor the TCP/IP model and its protocols are perfect. The criticism of the OSI model and its protocols can be summarized as:

1. Bad timing.
2. Bad technology.
3. Bad implementations.
4. Bad politics.

Bad timing

- essential that standards are written in between trough
  - written too early
    - subject is poorly understood
  - written too late
    - they are ignored by companies who have committed billions of dollars
- OSI protocol became crushed
- TCP/IP already in use by research universities by time ISO OSI appeared
  - vendors were offering TCP/IP products (cautiously)
- no company wanted to be first offering ISO OSI
  - it never happened

Bad technology

- model and protocol flawed
  - session layer little used
  - presentation layer tiny in most applications
- modelled after IBM SNA (Systems Network Architecture)
- bulky solution which was difficult to understand
  - from the initial printed standards

Bad implementations

- initial implementations were *slow*
  - ISO OSI-7 layer model was associated with *bad quality*
- TCP/IP available within Berkeley UNIX
  - was free and reasonably good

Bad politics

- TCP/IP & UNIX was much loved in academia
- ISO OSI-7 layer model throught to be a creature of:
  - European telecommincation
  - European community
  - and govenment of USA
  - also thought to be technically inferior to TCP/IP
- people on the ground reacted badly to this and supported TCP/IP

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.

EXAMPLE NETWORKS

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.

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.

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.

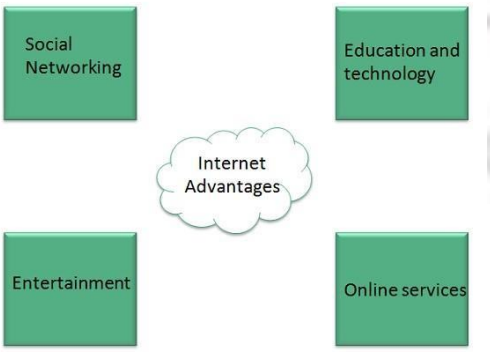
- Internet is a world-wide global system of interconnected computer networks.
- Internet uses the standard Internet Protocol (TCP/IP).
- Every computer in internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.
- A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.
- For example, a DNS server will resolve a name **http://www.google.com** to a particular IP 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 Project Agency Network (ARPANET).**
- **ARPANET** was developed by United States Department of Defense.
- Basic purpose of ARPANET was to provide communication among the various bodies of 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

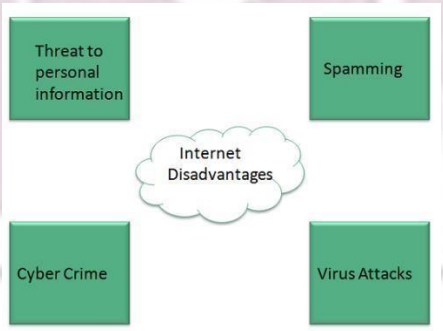
Internet covers almost every aspect of life, one can think of. Here, we will discuss some of the advantages of Internet:



- Internet allows us to communicate with the people sitting at remote locations. There are various 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 search engine.
- 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 be conducted on electronic systems

Disadvantages

However, Internet has prooved to be a powerful source of information in almost every field, yet there exists 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 leads to misconception among many people.

PHYSICAL LAYER

The purpose of the physical layer is to transport a raw bit stream form one machine to another for transmission 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 media and 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 fine antenna.
- 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.

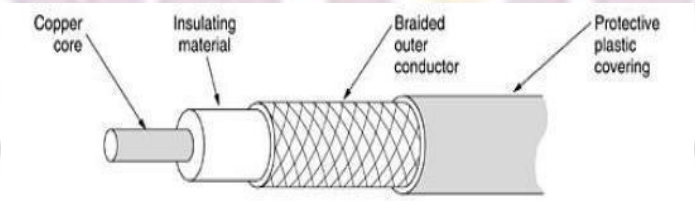


Fig: Coaxial Cable

Fiber optics:

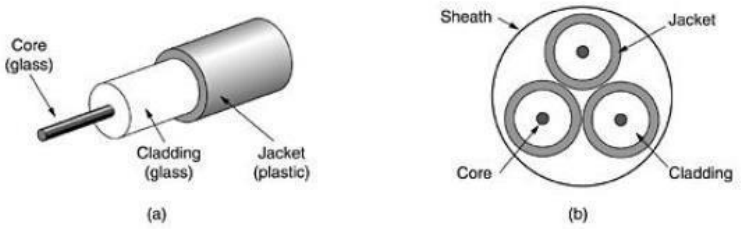


Fig: Side view of a single fiber Fig: End view of sheath with 3 fibers

- 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 different mode.
- 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 in a special sleeve and clamp them in place
3. Two pieces of fiber can be fused to form a connection.

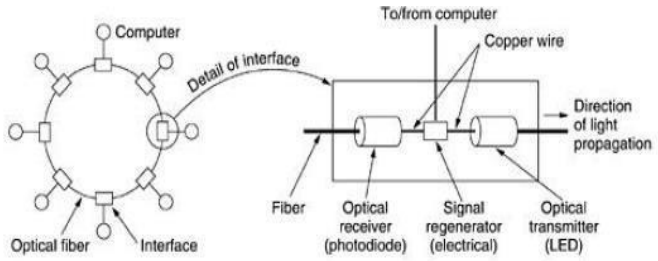


Fig: A Fiber Optic Ring with Active Repeaters

- LED's (Light emitting Diodes) and semiconductor lasses are the two light sources used to do the signaling.
- The receiving end of an optical fiber consists photodiode, which gives of an electrical pulse when 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 allow computer 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 photo diode (for receiving)
- The tap is completely passive and reliable because a broken LED and photodiode does not break 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 the individual computer links can be kilometers long with no limit.
- The passive interface loses light at each junction the no of computers and ring lengths are greatly 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 fiber are 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 inside the passive star to illuminate all the receivers.

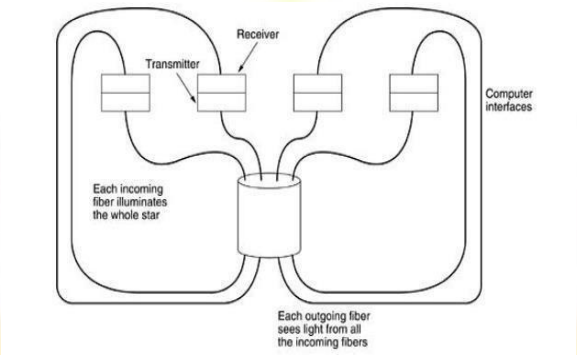


Fig: A Passive star connection with a fiber optics

Unguided transmission media (or) wireless transmission:

Radio transmission:

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

- Radio waves are Omni directional, means that the waves travel in all directions from the source.
- 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 waves travel 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 in a 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 in space.
- 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 effect is 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 adjacent rooms.

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 sunny days.

Switching:

It is a technique used to route the data from source to destination in the physical layer.

Circuit switching:

- When a telephone call is made the switching equipment with in the telephone system seeks out a physical path from sender's telephone to receiver's telephone.
- In circuit switching diagram the six rectangles represent a carrier switching office.
- Each office has three incoming lines and three outgoing lines.
- A physical path is established when a call passes it is shown by the dotted lines.
- Once a call has been set up, a dedicated path between both ends exists and will continue to exist until the call is finished.
- No congestion occurs as the path is established before the data transmission.
- Circuit switching reserves the required bandwidth in advance.

- in circuit switching the packets are delivered in order to the destination.
- The sender and receiver can use any bit rate, format, or framing method they want.

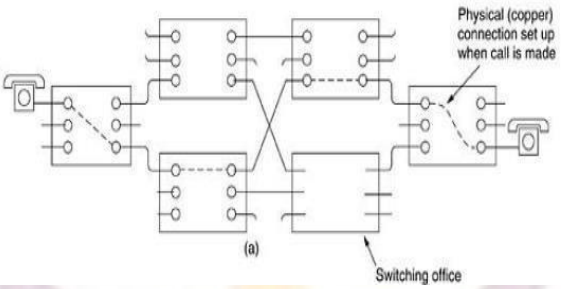


Fig: Circuit Switching

Message Switching:

- ✓ No physical path is established in advance between sender and receiver.
- ✓ Here, when the sender has a block of data to be sent, it is stored in the first switching office and then forwarded later, one block at a time.
- ✓ When each block is received, it is inspected for errors and then retransmitted.
- ✓ This technique is called a "Store-and-forward" network.
- ✓ Message switching is used in telegrams.
- ✓ In this switching, there is no limit on block size.

Packet switching:

- ✓ It is well suited for handling interactive traffic because no user can control any Xian line very long.
- ✓ The advantage of packet switching over message switching is in a multipacket message first packet can be forwarded before the second one has fully arrived.
- ✓ It reduces delay and improves through put.
- ✓ Because of this computer networks are usually packet switched.
- ✓ In packet switching the first packet can send as soon as it is available, it does not require any advance connection set up.
- ✓ The packets may arrive out of order because different packets follow different paths.
- ✓ No bandwidth is reserved in advance.

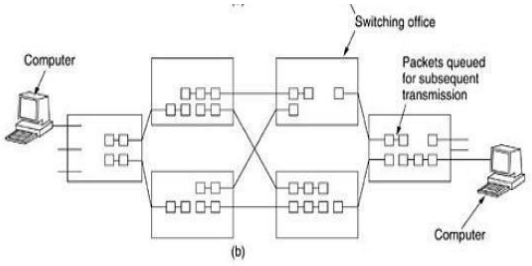
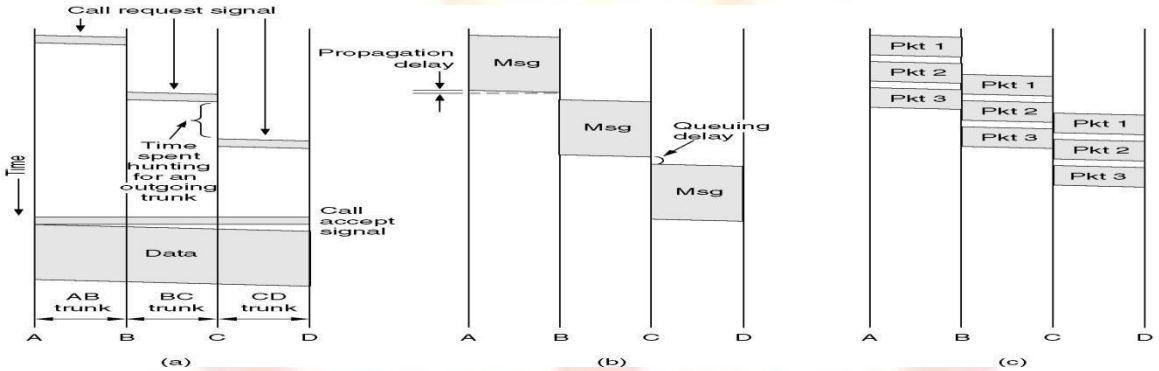


Fig: Packet Switching



(a) Circuit switching **(b) Message switching** **(c) Packet switching**

Crossbar switches:

- ✓ Crossbar switches is called as the cross point switch the crossbar switch has n*n intersections called cross points.
- ✓ Input and output line may be connected by semiconductor switch.
- ✓ for example line 0 is connected to line 4, line 1 is connected to line 7, line 2 is connected to line 6.line 3 and line 5 are not connected.
- ✓ All the bits that arrive at the switch from line 4 are immediately sent out of the switch on line 0.
- ✓ It implements circuit switching by making a direct electrical connection.

Space Division switches:

- ✓ Space divisions switches are built by splitting the cross are switch into small & interconnecting them with fewer cross points.
- ✓ We consider a three stage switches for example
- ✓ In the first stage, each crossbar has n inputs so we need N/n to handle all N incoming lines.
- ✓ Second stage has K crossbars, each with N/n inputs &N/n outputs.
- ✓ Third stage is a repeat of the first stage, but reversed left to right.
- ✓ Intermediate crossbar is connected to each input crossbar and each output crossbar.
- ✓ Using either first or second intermediate crossbar we can connect every input to every output.

Time Division Switches:

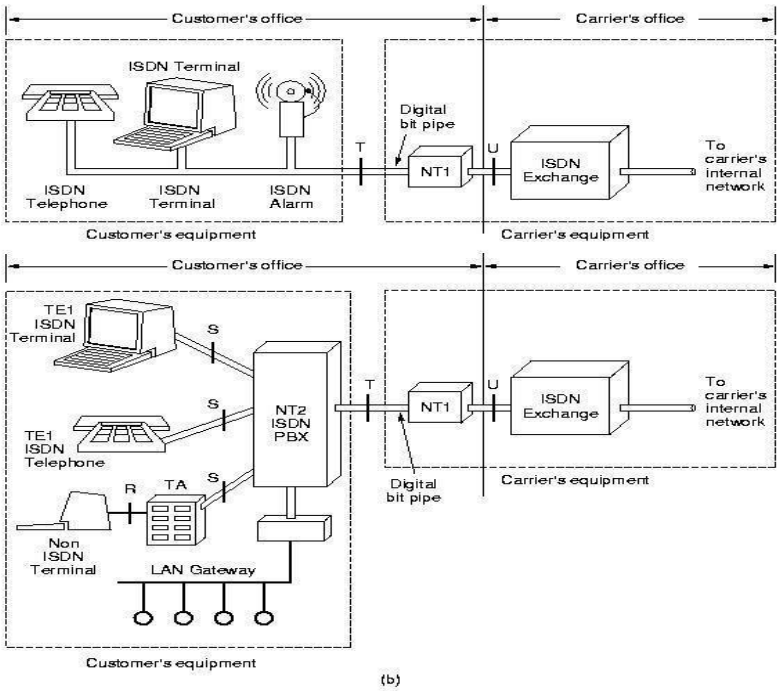
- ✓ In this n input lines are scanned in sequence to build an input frame with n slots. Each slot has k bits.
- ✓ Time slot interchanges accepts the input frames and produces output frames in which time slots have been reordered.
- ✓ In given figure input slot 4 is output first, then slot 7 & so on.
- ✓ The output frame is de multiplexed, with output slot 0 (input slot 4) going to line 0 & so on.
- ✓ There are no physical connections in this but it represents a circuit switch.

Working of Time Slot Interchange:

- ✓ When an input frame is ready to processed, each byte in the input frame is written into RAM buffer inside the interchanger.
- ✓ All the slots of the input frame have been stored in the buffer.
- ✓ In a different order, the output frame is constructed by reading out the words again.
- ✓ Mapping table is read out and used to address the RAM table.
- ✓ If word 0 of mapping table contains a 4, word 4 of the RAM buffer will be read out first.
- ✓ Word 4 of the input frame placed as the first word or slot of the output frame.
- ✓ The contents of the mapping table determine which input frame will be generated as the output frame.
- ✓ It also determines which input line is connected to which output line.

Narrowband ISON:

- ✓ ISON – Integrated Services Digital Network
- ✓ This system was designed for both voice and non voice services.
- ✓ Voice is the key ISON service with many added features.
- ✓ One feature is telephones that displays the callers telephone number, name and address on display while ringing.



(b)

ISDN System Architecture:

- ✓ The key idea of ISDN is digital bit pipe.
- ✓ Through this pipe bits flow between the customer and the carrier.
- ✓ Bits can flow through the pipe in both directions.
- ✓ For digital bit pipe, exact format of bit stream and its multiplexing must carefully defined.
- ✓ Bit pipe with low bandwidth used for home
- ✓ Bit pipe with high bandwidth used for business that supports multiple channels that are identical to home use channel.
- ✓ Business may have multiple bit pipes if they need additional capacity.
- ✓ For home or small business a carrier places a network terminating device, NT1, on the customer's premises & connects it to the ISDN exchange in the carrier's office using twisted pair.
- ✓ NT1 box has a connector on it, a passive bus cable can be inserted into it.
- ✓ For large businesses, more telephone conversations go on simultaneously than the bus can handle.
- ✓ We have a device NT2 called a PBX (Private Branch Exchange) connected to NT1 which provides real interface for telephones, terminals & other equipment.
- ✓ In between the various devices we have R, S, T and U reference points.
- ✓ The 'U' reference point is the connection between the ISDN exchange in the carrier's office and NT1.

- ✓ The 'T' reference point is what the connector on NT1 provides to the customer.
- ✓ The 'S' reference point is the interface between the ISDN PBX and the ISDN terminals.
- ✓ The 'R' reference point is the connection between the terminal adapter and non-ISDN terminals.
- ✓ ISDN is focused on 64 kbps channels; we refer it as N-ISDN Narrow band ISDN.

Broadband ISDN and ATM:

- ✓ Broadband ISDN is a digital virtual circuit for moving fixed size packets i.e.; cells from source to destination at 155 mbps.
- ✓ Bandwidth increases over narrow band ISDN by a factor of 2500.
- ✓ Broadband ISDN is based on ATM technology it is a packet switching technology.
- ✓ Narrowband ISDN is circuit switching technology.
- ✓ Broadband ISDN cannot be sent over existing twisted pair wiring for any distance. It must be put in either category 5 twisted pair or fiber.

Transmission in ATM Networks:

- ✓ ATM stands for Asynchronous Transfer Mode.
- ✓ Cells arrive randomly from different sources.
- ✓ It does not standardize the format for transmitting cells.
- ✓ The transmission medium for ATM is fiber optics. Fiber sense can be many kilometers.
- ✓ Each link goes between a computer and an ATM switch or between two ATM switches. All ATM links are point-point.
- ✓ The ATM physical medium Dependent sub layer is concerned with getting the bits on and off the wire.
- ✓ Transmission convergence sub layer provide uniform interface to the ATM layer in both directions.
- ✓ Out band, ATM layer provides a sequence of cells and the PMD sub layer encodes them as necessary &pushes them as a bit stream.
- ✓ In band, PMD sub layer takes the incoming bits from the network and delivers a bit stream to the TC sub layer.
- ✓ TC sub layer tell where one cell ends and the next one begins.

ATM Switches:

- ✓ ATM cell switch contains same number of input lines and output lines, as these lines are bidirectional.

- ✓ ATM switches are synchronous; one cell is taken from each i/p line, passed into the internal switching fabric and transmitted on the appropriate output line.
- ✓ Any cell fully arrived is eligible for switching during the cycle.
- ✓ Until the next cycle the cell not fully arrived has to wait.
- ✓ Switch all the cells with as loss rate should be as small as possible.
- ✓ The cells must arrive in same order with no exceptions. Output port the problem occurs.
- ✓ Holding one cell to progress of other cell is called head of line blocking.
- ✓ In input queue a cell has to keep until signal comes back.
- ✓ The switch requires extra logic, reverse signaling path and more delay.
- ✓ In output queuing it does not exhibit head of line blocking.
- ✓ If two cells want to go to same output line, both are passed through the switch.
- ✓ One of them is placed on the output line & the other cell is queued on the output line.
- ✓ Output queuing is more efficient than input queuing.

Architecture of ATM:

- ✓ In ATM information is passed in the form of cells. Cells are fixed size packets.
- ✓ Each cell is of 53 bytes in which 5 bytes header and 48 bytes user data.
- ✓ The ATM architecture is 3D which is different from OSI & TCP/IP.

Physical Medium Dependent (PMD) sub layer.
Transmission Convergence (TC) sub layer.AAL - ATM Adoption Layer
Convergence (CS) sub layer
Segmentation & Reassembly (SAR)

PMD fns: bit timing &voltages &other functionalities called physical n/w access.

- ✓ TC : acts like simple interference between physical & ATM layer.
- ✓ Function: Convert bit to cell stream.
- ✓ ATM function: Cell transport, addressing & congestion control.
- ✓ AAL function: Segmentation & reassembly.
- ✓ CS – Interface between AAL & upper layers.
- ✓ User Plane : Deals with problems of error &flow ctel.
- ✓ Ctel Plane : Used for connection management.

- ✓ Layer management used for further resource management.
- ✓ Plane management used for interlayer coordination.

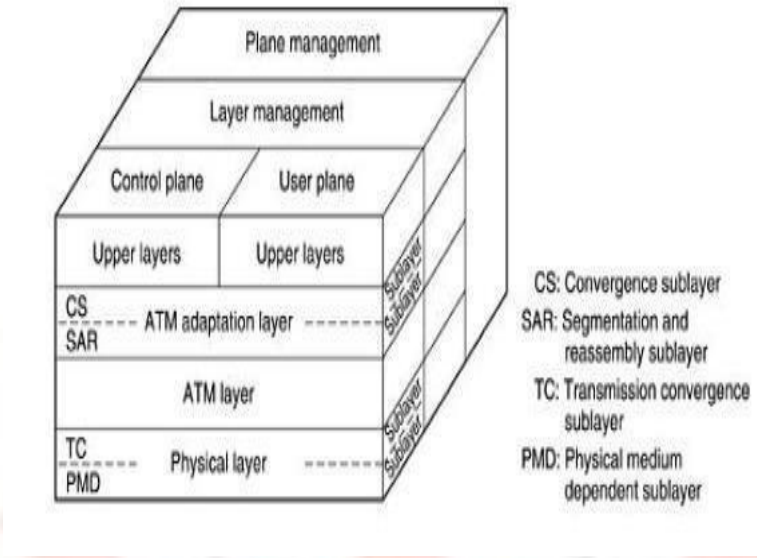


Fig: ATM Architecture

COMPUTER NETWORKS (23CY404)

UNIT II

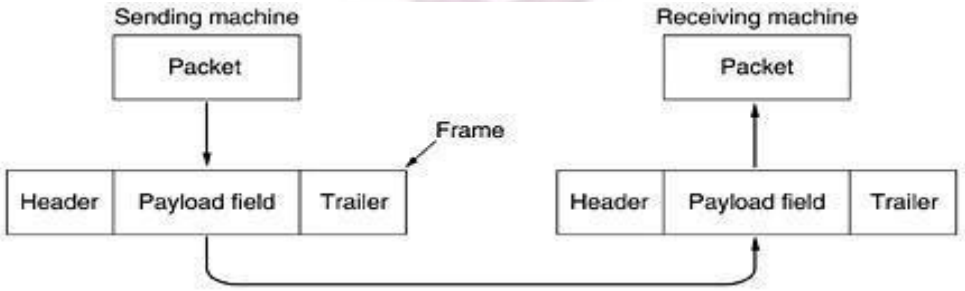
Data link layer: Design issues, framing, Error detection and correction.
Elementary data link protocols: simplex protocol, A simplex stop and wait protocol for an error-free channel, A simplex stop and wait protocol for noisy channel.
Sliding Window protocols: A one-bit sliding window protocol, A protocol using Go-Back-N, A protocol 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 change as 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 source machine 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, the sender can just send the entire message again.
- The trouble of this strategy is that frames usually have a strict maximum length imposed by the hardware and network layer packets do.

3. Acknowledgement connection –oriented service:

- Before any data is transferred a connection is established between source & destination machines.
- It guarantees that each frame is received exactly once and that all frames are received in the right 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 of which 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 the data link layer software.
- The data link layer software checks to see if this is the frame expected, and if so, gives the packet contained in the payload field to the routing software.
- The routing software then chooses the appropriate outgoing line and passes the packet back down to the data link layer software.

FRAMING:

- In order to provide services to the network layer, the data link layer must use the services from the 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 each frame.
- At the destination, the check sum is recomputed.
- If the recomputed check sum is different from the one contained in the frame.

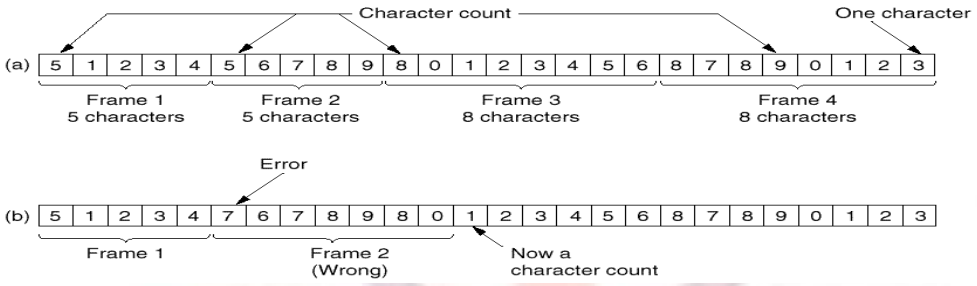
- An error has occurred and the data link layer deals with the errors.
- To mark the start and end of each frame, we use *four methods*. They are

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 follow and where the end of the frame is



(a) With out error (b) with error

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 re transmission. 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 of the frame.
- Even if the receiver ever loses synchronization, it can just search for the flag byte to find the end of the current frame.
- Two consecutive flag byte indicates the end of one frame and start of the next one.

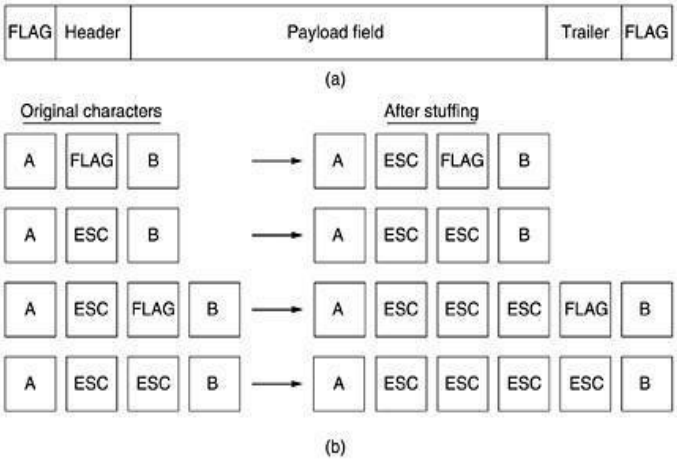


Fig . (a) A frame delimited by flag bytes. (b) Four examples ofbyte sequences before and after byte stuffing.

- 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 to the 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 a single 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 had to 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 automatically stuffs 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 automatically deletes 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.

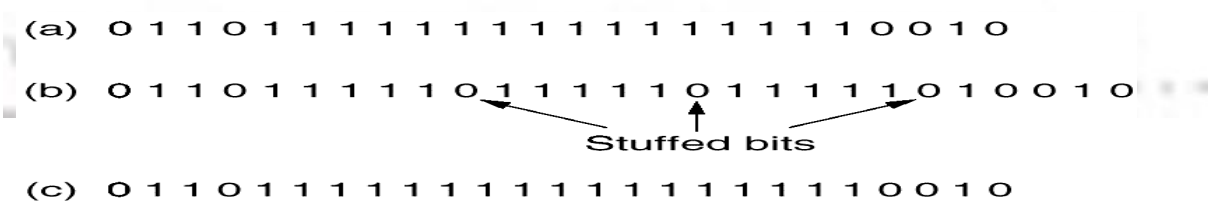


Fig. 3-5. Bit stuffing. (a) The original data. (b) The data as they appear on the line. (c) The data as they are stored in the receiver's memory after destuffing.

4. Physical layer coding violations:

This framing method is used in the networks in which physical medium contains some redundancy.
A 1 bit is a high –low pair & a 0 bit is a low-high pair. It means that every data bit has a transmission in 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 or negative 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 be transmitted again.
- If a frame is lost due to hardware failure the receiver will not react & does not send any acknowledgement.
- Timers are introduced into the data link layer.
- When a frame is exacted the timer also starts, the frame will be correctly received & the acknowledgement will get back before the timer runs out.
- If the frame or acknowledgement is lost the timer will go off, here the frame is transmitted again.
- If a frame is transmitted multiple times the receiver may accept the same and pass it to the network layer more than once.
- To prevent this, sequence numbers are assigned to outgoing frames, so that the receiver can distinguish retransmission from originals.

Flow control:

- Flow control occurs when the sender wants to transmit frames faster than the receiver can accept them.
- Even if the transmission is error free, the receiver will simply be unable to handle the frames as they arrive & will start to lose them.
- Feed back based flow control & rate based flow control are the two approaches that are commonly used.
- In feedback –based flow control, the receiver sends back information to the sender giving it permission to send more data.
- In rate based flow control, the protocol has a built – in –mechanism that limits the rate at which senders 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 receiver can ask the sender to re –transmit the entire data unit.

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

- Single bit error occurs when the receiver reads a 1 bit as a 0 or a 0 bit as a 1.to correct the error, the receiver simply reverse the value of the altered bit.

Hamming code:

hamming code can be applied to data units of any length & uses the relationship between data & redundancy bits or check bits.

Here, m is the no. of redundancy bits & r is the no. of redundancy bits added to the bits.

Consider, m=7 &r=4

Here redundancy bits are occupy the positions

Each redundancy bit is the parity bit which depends on the combination of data bits at different positions.

Redundancy bit	the bit positions from which the bit value are task for calculating the redundancy by value .
1	1,3,5,7,9,11
2	2,3,6,7,10,11
4	4,5,6,7
8	8, 9, 10, 11

Calculating the redundant bit values.

In the calculation of redundancy bits, even parity is considered in the total number of 1's is even.

Redundancy bit	Positions used for redundancy Bit calculation	Bit values in the positions mentioned in column 2	Bit required for creating even parity(redundancy bit values)
R1	1,3,5,7,9,11	Nill,1,0,1,0,1	1
R2	2,3,6,7,10,11	Nil,1,1,1,0,1	0
R4	4,5,6,7	Nil,0,1,1	0
R8	8,9,10,11	Nil,0,0,1	1

After adding the redundancy bits in the proper positions along with the data unit we will be getting hamming code.

The hamming code is 10011100101

This code will be transmitted.

Error detecting codes:

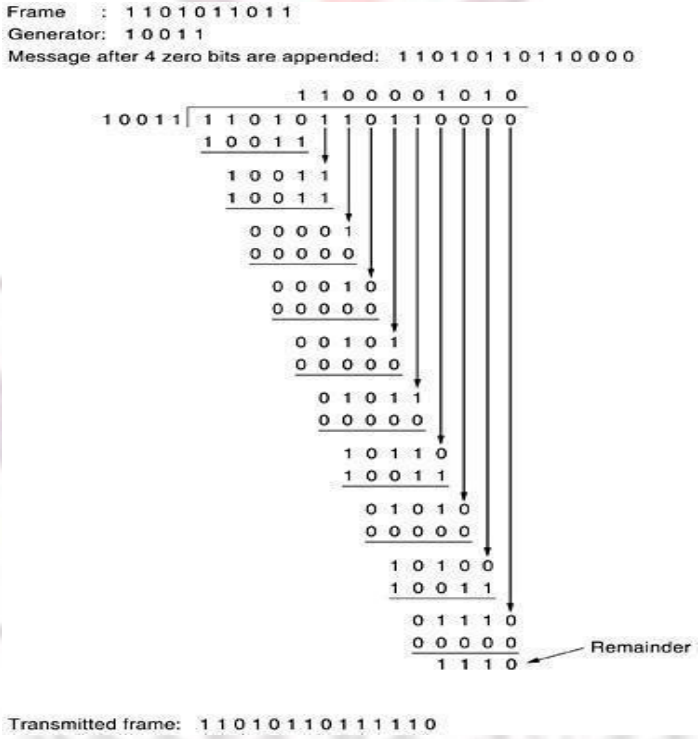
For error detecting we use polynomial code also known as CRC is used. Polynomial codes are

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 step 2.
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 -2 division method.

If the data unit, received by the receiver is without any error then the remainder obtained from step 6 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 the generator.

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 frame.



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 able to 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 the sender, 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 an acknowledgement, 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 for transmitting data in both directions.

- We have two separate physical circuits, each with a "forward" channel for transmitting data and a "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 sometime for 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 attached to 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 "receiving windows"
- The three sliding windows protocols differ in terms of efficiency complexity and buffer requirements.
- 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 transmits a 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 and sender 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 slid up.

- 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.

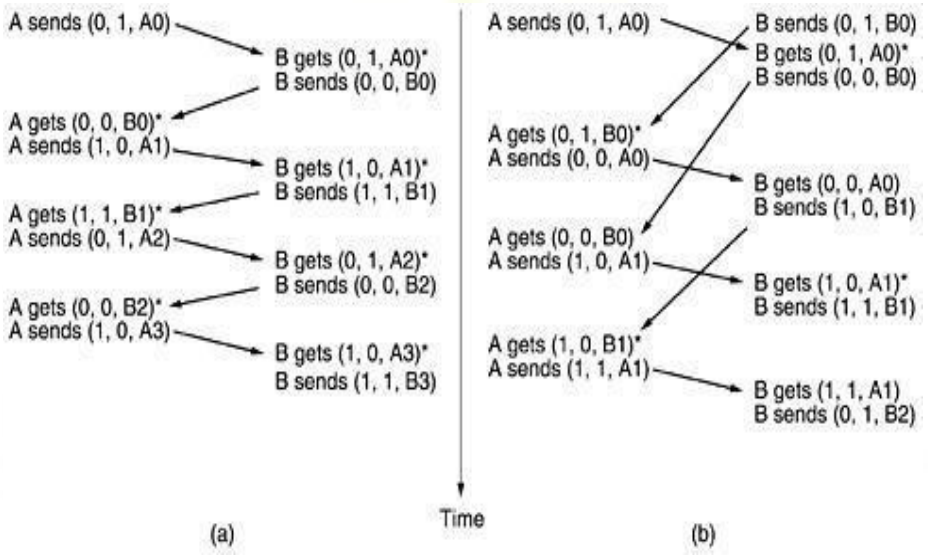


Fig. Two scenarios for protocol 4. (a) Normal case. (b)Abnormal case. The notation is (seq, ack, packet number). An asteriskindicates where a network layer accepts a packet.

2) A protocol using go back n

- To achieve better efficiency the solution is to allow the sender to transmit up to w frames before blocking instead of 1.
- If we take 'w' as 26, the sender begins sending frames 0 at t=520 it has finished sending 26 frames, the acknowledgement for frame 0 will have just arrived.
- Acknowledgements will arrive after every 20 m sec sender always get's permission to continues when it's it
- This technique is known as "pipelining"
- Pipelining frames over a communication channel has same problems. If a damaged frames occurs 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 acknowledgements for the discarded frames.
- After the senders time out it retransmit all unacknowledged frames in order, starting with managed or lost one.
- It wastes a lost of band width, if error rate is high.

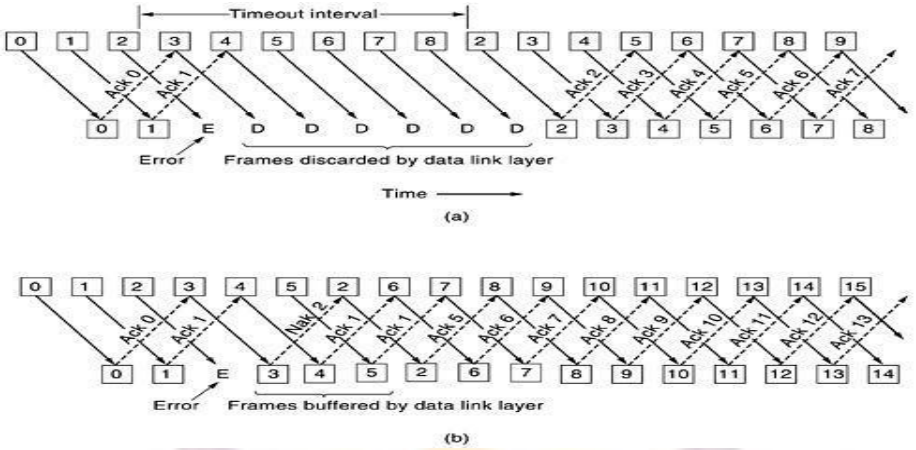


Fig. Pipelining and error recovery. Effect of an error when (a)receiver's window size is 1 and (b) receiver's window size is large.

A protocol using selective repeat:

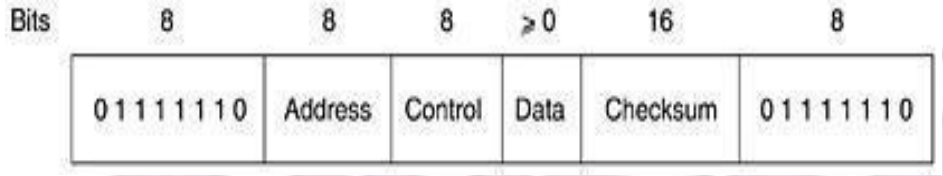
- The receiver is allowed to accept and buffer the frames fallowing a damaged or lost frame.
- When a receiver suspects than an error has occurred, it sends a negative acknowledgment frame back to the sender.
- It is a request for retransmission of the frame in the NAK specified.
- After the time out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

DATA link protocols

HDLC:

All the data link protocols are bit oriented, and use bit stuffing for data transparency.

The frame format is



- When multiple terminals are connected address field is used to identify one of the terminal.
- Control field is used for sequence numbers, acknowledgments and for other purposes.
- The data field may contain arbitrary long information. The efficiency of checksum falls with increasing frame length.
- The check sum field is used to detect the last flag bytes.
- The frame is identified if it starts & ends with a flag sequence 01111110.
- The minimum frame contains three fields & total 32 bits excluding flags on either end.
- We have three kinds of frames:
  - Information frame
  - Supervisory frame
  - UN numbered frame
- The control field for these frames are

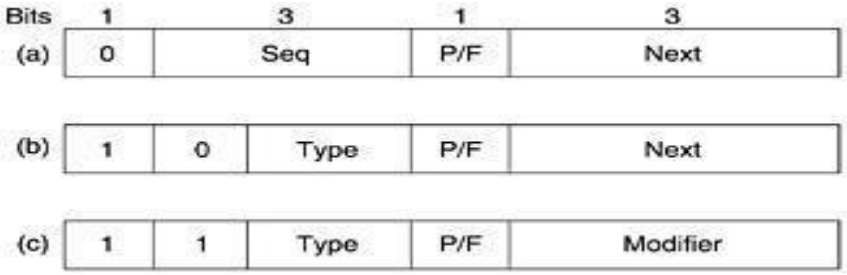


Fig. Control field of (a) an information frame, (b) a supervisory frame, (c) an unnumbered frame.

Information frame:

- The sequence field is the frame sequence number.
- Next field is the piggybacked acknowledgment
- The p/f bits stands for poll/final. When P is used the computer invites terminals to send data.
- All the frames sent by the terminal, the p/f bit set to p.
- The final one is set to f.
- The bit has some minor use in connection with the UN numbered frame.

Supervisory frame:

- Supervisory frames are distinguished by the type field.
- Type 0 is called RECEIVE READY used to indicate the next frame expected.
- Type 1 called REJECT used to indicate that a transmission error has been detected.
- Type 2 called RECEIVE NOT READY is used to indicate to send signal certain temporary problems with the receiver, such as storage of buffers when the condition has been repaired the receiver sends a RECEIVE READY, REJECT or certain ctrl frames.
- Type 3 called SELECTIVE REJECT it is used for retransmission of only the frame specified.

Unnumbered frame:

- UN numbered frame is used for control purpose & also used to carry the data when unreliable connectionless service is called.
- Control frames may be lost or damaged, just like data frames, so the control frames must be acknowledged.
- A special control frame called UA (unnumbered acknowledgement) is provided for this purpose.

Data link layer in the internet:

Two protocols are widely used in the internet. SLIP & PPP

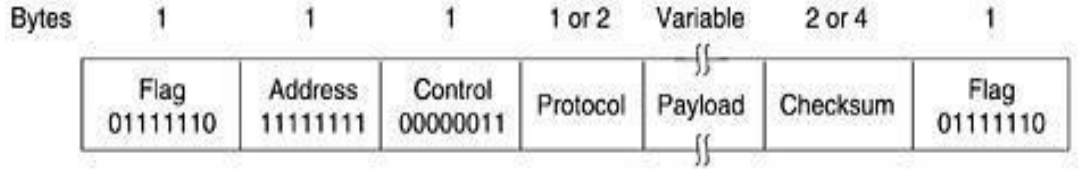
SLIP: (Serial Line IP)

- The work station sends IP packets with a special flag byte at the end for framing.
- SLIP attaches a flag byte to both the front & back of each IP packet sent.
- SLIP has some problems.
- 1.it does not support error detection & correction
  2. SLIP supports only IP
  3. Each side must know the others IP address in advance.
  4. It does not provide any form of authentication.
  5. SLIP is not an approved internet standards.
- PPP solved all these problems and become an official internet standard.

PPP: ***(Point- to -point protocol)***

- PPP is an official internet standard.
- PPP handles error detection, supports multiple protocols, allows IP addresses, permits authentication
- PPP provides framing method that describes the end of one frame & the start of the next one frame format also handles error detection.
- Link protocol for bringing lines up, testing them & bringing them down again when they are no longer needed.
- Network control protocol method chooser to have a different NCP for each network layer supported.

PPP frame format:



- All PPP frames begin with the std HDLC flag byte 01111110.
- Address field indicate that all stations accept the frame. It always sets to binary value 111111111.
- Control field indicates an unnumbered frame. Its default value is 00000011.
- Protocol field indicates the type of packet in payload field.
- Protocol starting with 0 bit is network layer.
- Protocol starting with 1 are other protocols
- Payload field is variable length, if the length is not defined using LCP, a default length of 1500 bytes is used.
- Checksum field is used for error detection.
- The simplified phase diagram shows the phases that a line goes through when it is brought up, used & taken down again.

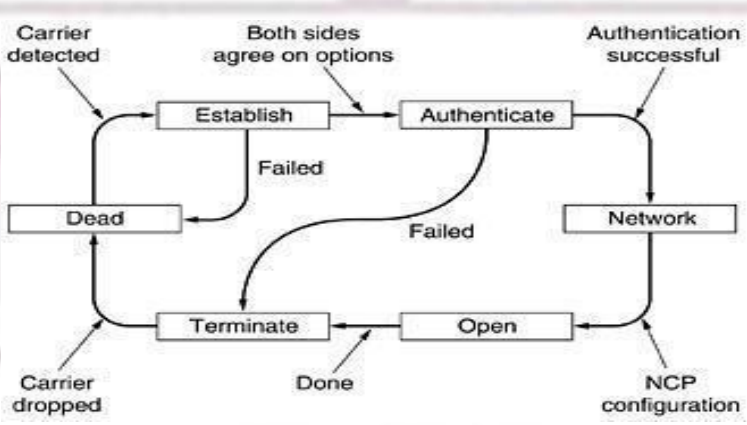


Fig. A simplified phase diagram for bringing a line up and down.

- The protocol starts with the line in the *DEAD* state, which means that no physical layer carrier is present and no physical layer connection exists.
- After physical connection is established, the line moves to *ESTABLISH*.
- At that point LCP option negotiation begins, which, if successful, leads to *AUTHENTICATE*.
- Now the two parties can check on each other's identities if desired.
- When the *NETWORK* phase is entered, the appropriate NCP protocol is invoked to configure the network layer.

- If the configuration is successful, *OPEN* is reached and data transport can take place.
- When data transport is finished, the line moves into the *TERMINATE* phase, and from there, back to *DEAD* when the carrier is dropped.

Data link layer in ATM:

Cell transmission:

Each cell contains a 5 byte header in which 4 bytes of virtual circuit & control information and 1 byte checksum.

- 8-bit checksum field is called the HEC header error control.
- HEC corrects all single bit errors & detects many multi bit error.
- If HEC has been inserted into cell header, the cell is ready for transmission.
- Transmission media are two types.
- **Asynchronous medium:**
- Cell can be sent whenever it is ready to go no timing restrictions.
- **Synchronous medium:**
- Cell must be transmitted according to predefined timing pattern.
- If no data cell is available the TC sub layer invents idle cells.
- Non data cell is the OAM (operation and maintenance)
- OAM cells are used for exchanging to control & information necessary for system running.
- OAM contains first 3 bytes of header to all 0's which is not allowed for data cells.4 byte describes the nature of OAM cell.

Cell reception:

- On output the job of the TC sub layer is to take a sequence of cells add a HEC to each one convert the result to bit stream, match the bit stream to the speed of the physical transmission medium by inserting AOM cells.
- On i/p it takes an incoming bit stream locate the cell boundaries, verifies the headers, process the OAM cells and passes the data cells to the ATM layer.
- Flag bytes are present to mark the start and end of the cell.
- Here , the hardest part is locating the cell boundaries in the incoming bit stream.
- A cell is just a sequence of 53x8=424 bits.
- Here 2 methods are used to identify the cell boundaries;
- In *first method* TC sublayer maintains a 40-bit shift register, with bits entering on the left and exiting on the right.
- The TC sublayer then inspects the 40 bits to see if it is potentially a valid cell header.
- If it is, the rightmost 8 bits will be valid HEC .
- Otherwise , the bits in the buffer are shifted right one bit, and a new input bit is inserted at the left end.
- This process is repeated until a valid HEC is located.
- The trouble with this process is HEC is only 8 bit wide.
- Another way of identifying the cell boundaries is the ***finite state machine*** .
- Three states are used: HUNT, PRESYNCH, SYNCH.
- In the HUNT state the TC sub layer is shifting bits into the shift registers one at a time looking for a valid HEC.
- As soon as one if found, the finite state machine switches to PRESYNCH state, meaning that it has tentatively located a cell boundary.
- It now shifts in the next 424 bits without examining them.
- If the cell boundary was correct, the shift register should now contain another valid cell header, so it once again runs the HEC algorithm.
- If the HEC is incorrect, the TC goes back to the HUNT state and continues to search bit-by-bit for a header whose HEC is correct.
- If the second HEC is also correct, TC shifts in another 424 bits and tries again.
- In PRESYNCHSTATE it checks cell-by-cell.

- It is synchronized and moves into the SYNCH state to start normal operation.
- If it is not synchronized , it returns to HUNT state.

Medium Access Sub Layer

MAC (medium access control) sub layer deals with broadcast network and their protocols.

- In broadcast network the key issue is how to determine to use the channel when there is competition for it.
- Broadcast channels are also called multi access or Random access channels. Eg: conference call
- The protocols used to determine who goes next on a multi-access channel belong to a sub layer of the data link layer called MAC.
- How to allocate a single broadcast channel among computing users is called channel allocation problem.
- Channel allocation problems are two types

  1.static channel allocation
  2.dynamic channel allocation

1. static channel allocation:

- Allocating a static channel among multiple users is by using frequency division multiplexing(FDM)
- If there are 'n' users the bandwidth is divided into n equal sized portions each user assigned one portion.
- When there is small and fixed no of users FDM is simple & efficient.
- If there are n regions fewer than n users are currently interested in communicating a large piece of information will be wasted.
- If more than 'n' users want to communicate some of them will be denied permission for lack of bandwidth.
- One of the users is not using the portion no one else is allowed to use it.
- Most of the channels will be idle most of the time.
- Static FDM use poor performance.
  - T=1/uc where T-meantime delay
    - C-channel capacity bits/ sec
    - -arrival rate of frames / sec
  - /u-mean bits/ frame.
- Single channel is divided into 'n' independent sub channels with capacity c=c/n bits/sec.(symbols)

2. Dynamic channel allocation:

Channel allocation problem assumptions : there are 5 key assumption.

1. Station model: the model consists of 'n' stations each with a one program or user that generates frames for transmission.

- once a frame has been generated the station is blocked & does nothing until the frame has been successfully transmitted.

- Stations are independent.

2. Single channel assumption:

A single channel is available for all types of communication.

3. Collision assumption:

If two frames are transmitted simultaneously they overlap in time called collision.all stations can detect collisions.

4. Continuous time:

Frame transmission can begin at any time. There is no master clock dividing the time into discrete intervals
Slotted times: time is divided into discrete intervals.

- Frame transmission always begin at the start of a slot.

5. carrier sence:

- Stations can tell if the channel is in use before trying to use it.

- If the channel is sensed as busy no station will attempted to use it until it goes idle.

No carrier sence: stations cannot sence the channel before trying to use it.

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 known as retransmission.

Contention system: having single communication channel, where multiple users are competing for that channel 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 called vulnerable 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.

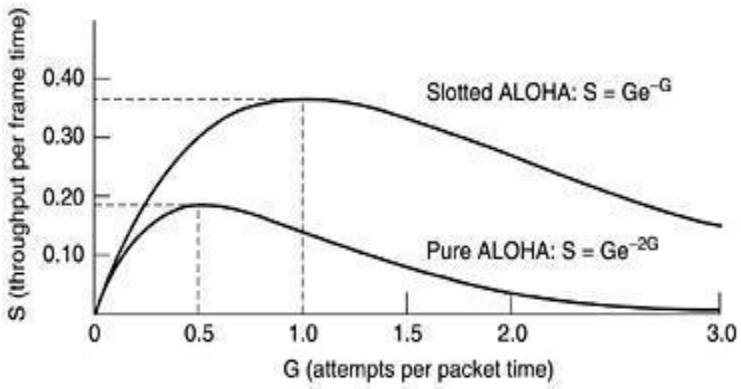


Fig. Throughput versus offered traffic for ALOHA systems.

carrier sense multiple access protocols:

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

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 transmitting at 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 when its 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.

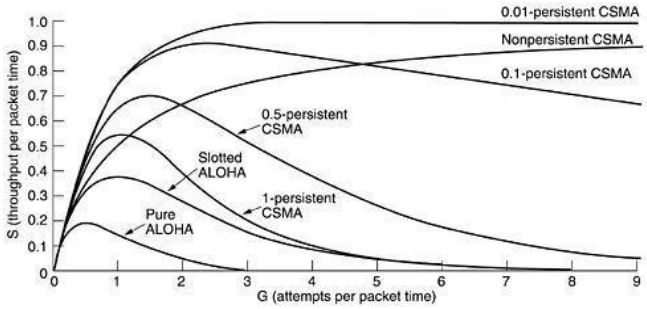


Fig. Comparison of the channel utilization versus load for various random access protocols.

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 tries again, assuming that no other station has X'ted in the meantime.
- Therefore, CSMA/CD consisting of alternating contension and transmission periods, with idle periods occurring when all stations are quiet.
- Systems in which multiple users share a common channel in a way that can lead to conflicts are known as contention systems.
- It works well on low loads.

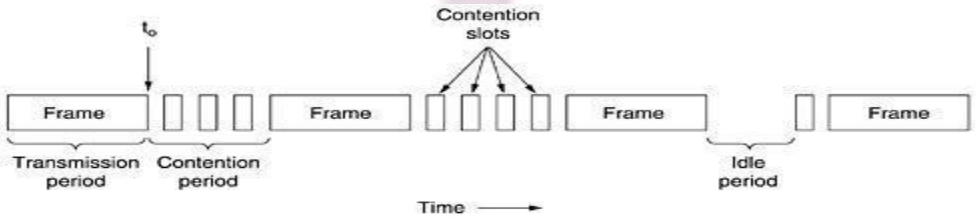


Fig: CSMA/CD can be in one of three states: contention, transmission, or idle

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 and wish 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 called reservation 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).

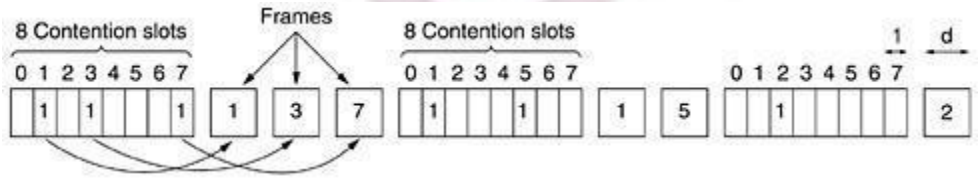


Fig: The basic bit-map protocol.

Binary cut down protocols:

- The station wants to use the channel now broadcasts its address as a binary bit string, starting with 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.

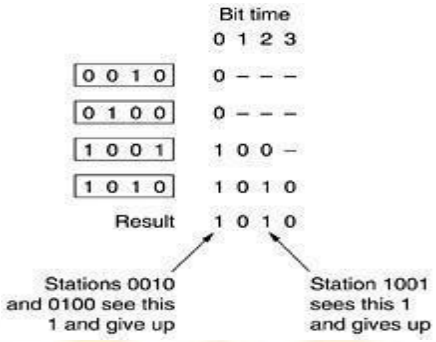


Fig: The binary countdown protocol. A dash indicates silence.

Limit contention protocols:

- Here we mix the properties.
- CSMA/CD working better at low loads & collision free protocol working better at high loads.
- The total information is divided into groups.
- Only members of group 0 are permitted to complete for slot 0.
- If one of them succeeds, it acquires the channel& transmits its frame.
- If there is a collision, the members of group 1 contend for slot 1.
- If more & more stations are assigned to the same slot, the probability of collision grows.
- At low loads, we need to use more members for stations.
- At high loads, we need to use less members for station.
- As frames increases, collisions increases & probability decreases.

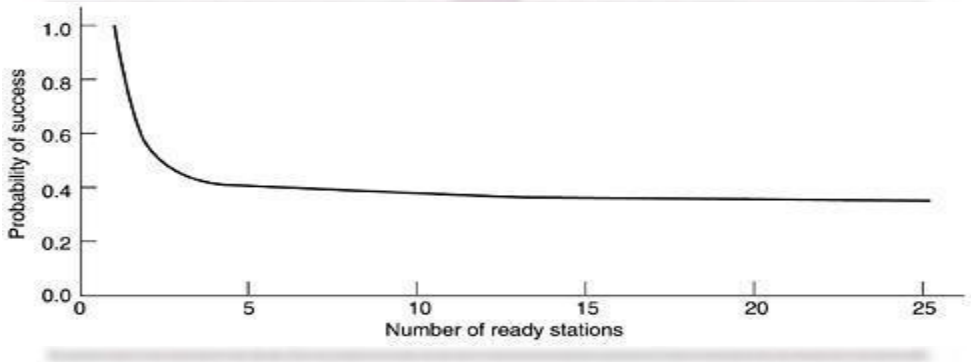


Fig: Acquisition probability for a symmetric contention channel.

Adaptive tree walk protocol:

- Total information is divided into levels in binary tree approach. We should always adopt the left side path.
- In the first contention slot fallowing a successful frame transmission, slot 0 all stations are permitted to acquire the channel.

- If there is a collision, during slot 1 only those stations falling under node 2 in th tree may complete.
- If one of them acquires the channel, the slot fallowing the frame is reserved for those stations under node 3.

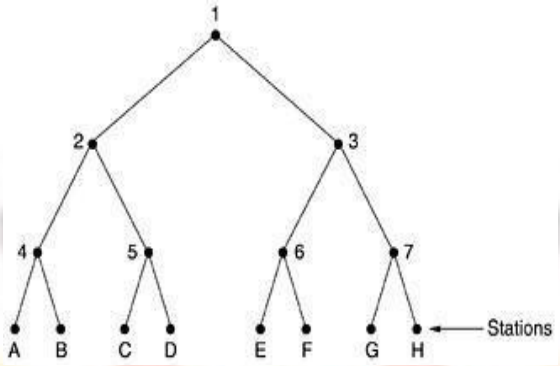


Fig: The tree for eight stations

- If a collisions occurs during slot 0, the entire tree is searched, depth first, to locate all ready stations.

WDMA (wave length division multiple access):

- Based on frequency we are dividing the total channel into different individual channels, when we are having multiple no of users.
- Applied on fiber optic LAN.
- Each station is assigned two channels.
- A narrow channel is provided so a control channel to signal the station.
- A wide channel is provided so the station can output data frames.
- Narrow channel divided into M time slots.
- Wide channel is divided into n+1 data frame slots.
- The purpose of adding additional bit is used to indicate the status of the slot.
- Status indicates which channel agree on both the channels.
- If A want to communicate with B it must first insert a CONNECTION REQUEST frame in a free slot on B's control channel.
- If B accepts, communication take place on A's data channel.

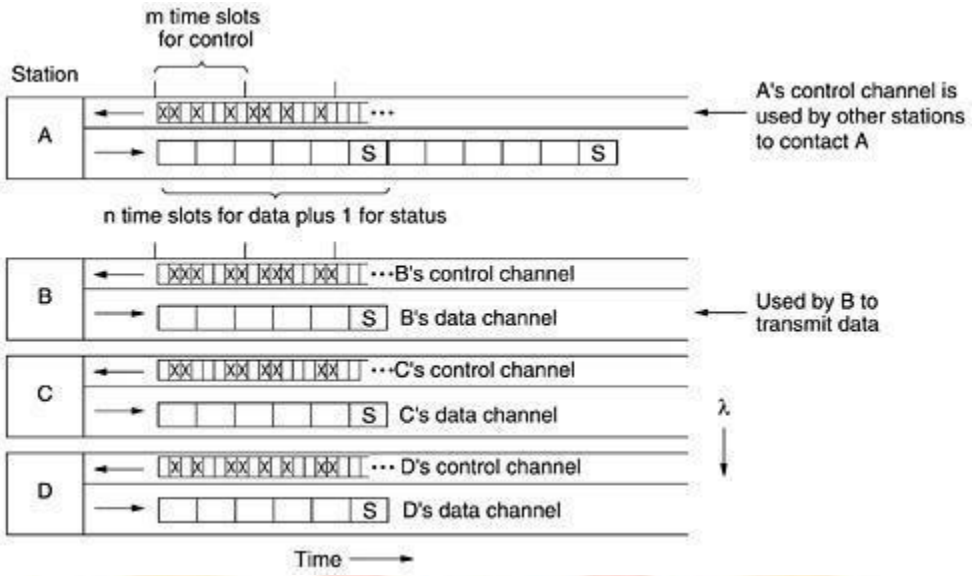


Fig: Wavelength division multiple access.

WDMA applied in 3 different approaches:

1. Constant rate connection oriented data traffic EG: uncompressed media.
2. Variable rate connection oriented data traffic Eg: file transfer
3. Data gram services. Eg: UDP packets.

2.6.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 is called hidden station problem.
- If two stations are out of the range the stations get bad reception the problem is called exposed station 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.

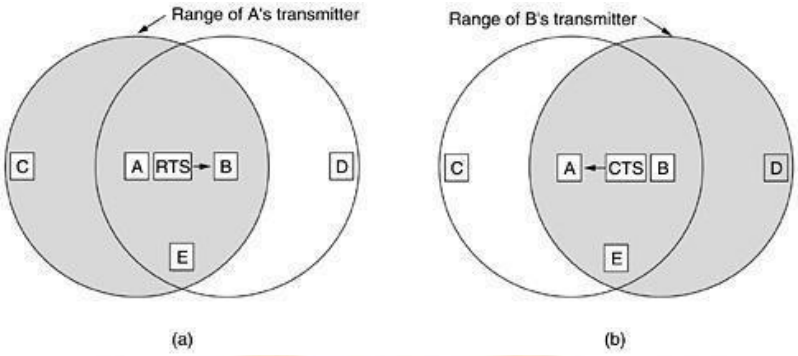


Fig: The MACA protocol. (a) *A* sending an RTS to *B*. (b) *B* responding with a CTS to *A*.

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:

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

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

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 to 500 meters.
- 10Base5, a **transceiver** is clamped securely around the cable its tap makes contact with the inner 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 to ensure that all othertransceivers also realize that a collision has occurred.

- With 10Base5, a **transceiver cable** or **drop cable** connects the transceiver to an interface board in 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, allows the computer to power the transceiver electronics
- The transceiver cable terminates on an interface board inside the computer. The interface board contains 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, rather than using vampire taps.
- With 10 base2, the connection to the cable is just a passive BNC t-junction connector. BNC connectors are easier to use and more reliable.
- Thin Ethernet is much cheaper and easier to install, but it can run for only 185 meters per segment, each of which can handle only 30 machines.
- Detecting cable breaks, excessive length, bad taps, or loose connectors can be a major problem with 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 the cable, 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 detected easily.
- 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.

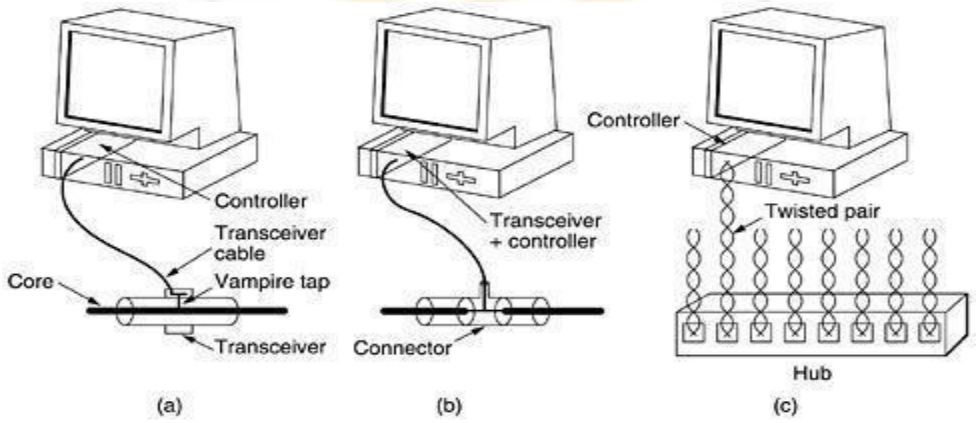


Fig: Three kinds of Ethernet cabling. (a) 10Base5. (b) 10Base2.(c) 10Base-T.

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.

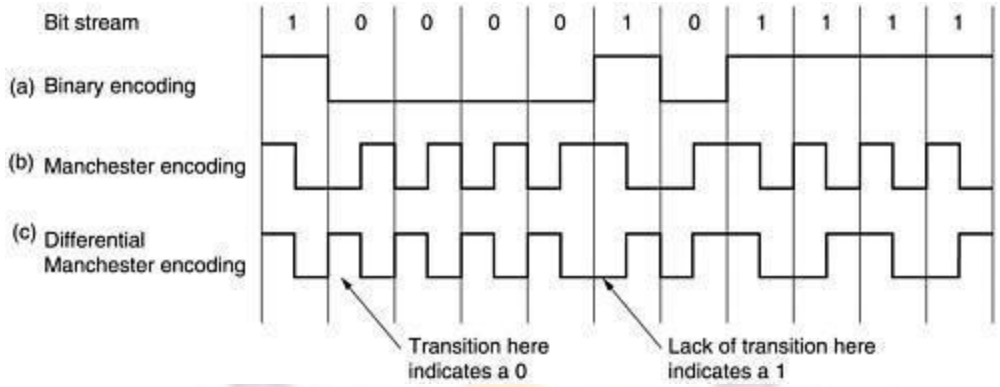


Fig: (a) Binary encoding. (b) Manchester encoding. (c)Differential Manchester encoding.

- 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 max of 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 frame to 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 no of slots is skipped.
- If the randomization interval for all collisions was 1023, the chance of two stations colliding for a second time would be negligible.
- By having the randomization interval grow exponentially as more & more consecutive collision occur.

- The algorithm ensures a low delay when only a few stations collide but also ensures that the 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 the destination station.

performance:

If each station transmits during a contention slot with probability P, the probability A that some stations acquires the channel in the slot is
A= KP(1-P)k-1
K-represents station ready to transmit.
P-represents each station X'mits during a contention slot.
A-represents probability that some station acquires the channel in the slot.
A-is maximum when p=1/k.
1/a-represents mean no of slots per contention.
2t-represents each slot has a duration.
2t/a-represents mean no of slots.
If the mean frame takes P sec to transmit when many stations have frames to send.
Channel efficiency=P/P+2t/a.
If no of stations are increasing, the channel efficiency decrease.

To formulate the channel efficiency, Eg: in terms of the frame length, F, the network bandwidth, B, the cable length, L, & the speed of signal propagation, C, for optional case of e contention slots per frame.
With P=F/B the channel efficiency becomes.
Channel efficiency=1/(1+2BLe/CF).

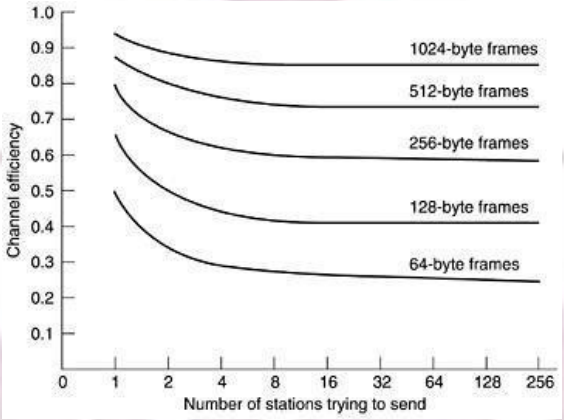


Fig: Efficiency of Ethernet at 10 Mbps with 512-bit slot times.

IEEE 802.4 (Token Bus):

- Ethernet does not provide priorities.
- Here all important and unimportant stations are wait same time.
- In ring topology, if one system fail all the ring will fail.
- physically token bus is a linear or tree shaped cable onto which the stations are attached.
- Logically , the stations are organized into a ring with each station knowing the address of the station to its left & right.
- When the logical ring is initialized , the highest numbered station may send the first frame.

- After it passes permission to its immediate neighbor by sending the neighbor a special control frame called a token.
- The token propagates around the logical ring, with only the token holder being permitted to transmit frames.
- Only one station at a time holds the token, collisions do not occur.

Token bus MAC sublayer protocol:

- Preamble is used to synchronize the receivers clock.
- Start delimiter & end delimiter fields are used to mark the frame boundaries.
- The frame control is used to distinguish data frames from control frames.
- The destination address & source address fields uses either 2 byte or 6 byte size.
- The data field may be up to 8182 bytes long when 2 byte address are used & up to 8174 bytes long when 6 bytes addresses are used.
- Checksum are used to detect the errors.

IEEE 802.5 (Token Ring):

- In a token ring a special bit pattern, called the token, circulates around the ring when ever all stations are idle.
- When a station wants to transmit a frame, it is required to size the token and remove it from the ring before it transmitting.
- Ring interfaces have two operating modes, listen and transmit.
- In listen mode, i/p bits are simply copied to output, with a delay of 1 bit time.
- In transmit mode, which is entered only after the token has been sized, the interface brakes the connection between i/p & o/p entering its own data onto the ring.
- In ring network, if the cable brakes some where the ring dies.
- This problem can be solved by the use of a wire center.
- Physically each station is connected to the wire center by a cable containing at least two twisted pairs, one for the data to the station & one for the data from the station.

Token ring MAC sublayer protocol:

When there is no traffic on the ring, a 3-byte token circuits endlessly, waiting for a station to size it by setting a specific 0 byte to a 1 byte, thus converting the token into the start of frame sequence.

Data frame format:

SD- start delimiter.
AC- access control.
FC- frame control.
ED- end delimiter.
FS- frame status.

- The starting delimiter and ending delimiter mark the beginning and ending of the frame.

- The access control byte contains the token bit & also the monitor bit, priority bits & reservation bits.
- The frame control bytes distinguishes data frames from various possible control frames.
- Destination address & source address fields uses either 2 byte or 6-byte address.
- Data may be as long as necessary.
- Checksum field is used for error detection.
- Frame status byte, it contains A & C bits.
- When the sending station drains the frame from the ring, it examines the A & C bits.
- Three combinations are possible.
- A=0 & C=0; destination not present or not powered up.
- A=1 & C=0; destination present but frame not accepted.
- A=1 & C=1; destination present and frame copied.

IEEE 802.6: (Distributed queue dual bus)

- It is used in MAN.
- Two parallel , unidirectional buses are used, with stations attached to both buses are parallel.
- Each bus has a head-end, which generates a steady stream of 53-byte cells.
- To X'mit a cell, a station has to know whether the destination is also the left of it or to the right of it.
- If the destination is to right, the sender uses bus A, otherwise it uses bus B.
- In all the others, if a station gets the chance to send it will.
- Here, stations queue up in the order they became ready to send & transmit in FIFO order.
- To simulate FIFO queue each station maintains two counters RC & CD.
- RC (request counter) counts the no of downstream requests pending until the station itself has a frame to send.
- At that point, RC is copied to CD, RC is recent to 0 & now counts the no of requests made after the station become ready.
- To send a cell, a station must first make a reservation by setting the request bit in some cell on the reverse bus.
- As this cell propagates down the reverse bus, every station along the way notes it and increments its RC.
- For example after page no.302 in text book.

IEEE 802.2 : (Logical link control)

- The LLC forms the upper half of the data link layer, with the MAC sublayer below it.
  - **Protocol formats:**

- The network layer on the sending m/c passes a packet to LLC using the LLC access primitives.
- The LLC sub layer then adds an LLC header. Containing sequence and acknowledgement numbers.
- The resulting structure is then inserted in the payload field of an 802.x frame & transmitted.
- LLC provides unreliable datagram service, acknowledged datagram service, & reliable connection oriented service.
- For acknowledged datagram or connection oriented service, the data frame contain a source address, a destination address, a sequence number, an acknowledgement number, and a few miscellaneous bits.
- For unreliable datagram service, the sequence number and acknowledgement numbers are omitted.

BRIDGES:

Many organizations have multiple LAN's and wish to connect them,

- LAN's can be connected by devices called bridges, which operate in the data link layer.
- We mention 6 reasons why a single organization may end up with multiple LAN's.
- First, may university & corporate departments have their own lan's, there is a need for interaction between different departments. So bridges are needed.
- Second, the organization may be geographically spread over several buildings separated by considering distances.
- Third, it may be necessary to split a single LAN into separate LAN's to accommodate the load.
- Fourth, the physical distance between the most distant m/c is too great. Using bridges the total physical distance covered can be increased.
- Fifth, reliability, bridge can be programmed to exercise some discretion about what it forwards and what it does not forward.
- Sixth, the bridges can contribute to the organizations security.

Operations of a LAN bridge from 802.3 to 802.4:

- Host A has a packet to send.
- The packet descends into the LLC sub layer & acquires an LLC header.
- Then it passes into the MAC sub layer & an 802.3 header is precedent to it.

- This unit goes out onto the cable & passed up to the MAC sub layer in the bridge, where 802.3 header is stripped off.
- The packet (with LLC header) is then handed off to the LLC sub layer in the bridge.
- In this, the packet is destined for an 802.4 subnet connected to the bridge.
- It works its may down the 802.4 side of the bridge & off it goes.

Transparent bridges:

used only by 802.3 & 802.4

- The bridges maintains tables called hash tables contain information regarding what information is transferred from one LAN to another.
- When all the hash tables are empty it uses a special concept flooding.
- Flooding means broadcasting all the destination information in the form of frame to all the LAN's .when ever there is unknown destination.
- Bridges accepts the frame if it is in the other LAN.
- Discard the frame if it is in the same LAN.
- Flooding used to send the frame if it is unknown destination.
- To avoid the loops we are using spanning trees.
- Purging means removing the entries after reaching the destination. It will purge periodically.
- Backward learning is used in transparent bridges from which particular source the information is coming.

Source routing bridges:

- The routing is done frame source to destination and we can do some hardware and software changes used by 802.5
- It uses discovery frame concept to identify which particular source is going to which destination.
- Source bridge is connection oriented.

Remote bridges:

- The LAN's connected in different distances can be connected using remote bridges.
- We use point to point links in connecting the bridges.
- Various protocols can be used on the point to point lines.
- Standard point to point data link protocol can be used, putting control MAC frames in the payload fields.
- Another option is strip off the Mac header and trailer at the source bridge & put what is left in the payload field of the point to point protocol.

- The disadvantage is the checksum that arrives at the destination host is not the one computed by the source host. So , errors may not be detected.

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 the destination.
- The network layer must know about the topology of the communication subnet in the set of all routers, and choose appropriate paths through it.
- Network layer is the lowest layer that deals with end-to –end transmission.

3.1.Design Issues

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

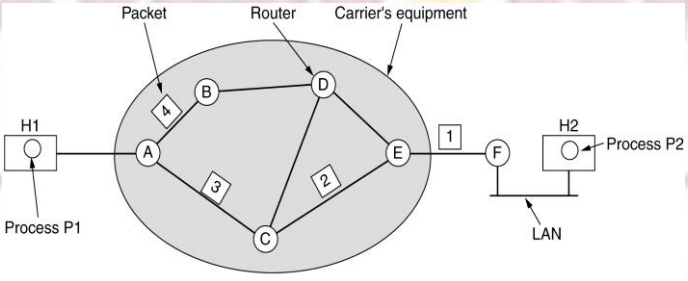
Services provided to the transport layer:

- The network layer provides services to the transport layer at the network layer / transport layer 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 numbering plan, even across LAN'S & mans.

IMPLEMENATION OF CONNECTIONLESS SERVICE:

- If CL service is offered, packets are injected into the subnet individually & routed independently 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 with instructions to deliver it to process p2 on host H2.
- The message is four times longer than the maximum packet size, so the network layer has to 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 of these 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 was then forwarded to E& then to F.
- When the packet reaches F, it was encapsulated in a data link layer frame & sent to H2 over the 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 first three.
- 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 "routing algorithm".



A's table

initially		later	
A	–	A	–
B	B	B	B
C	C	C	C
D	B	D	B
E	C	E	B
F	C	F	B

Dest. Line

C's table

A	A
B	A
C	–
D	D
E	E
F	E

E's table

A	C
B	D
C	C
D	D
E	–
F	F

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 destination router 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 machine is 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 circuit it 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 to router 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. This is called ***Label Switching***.

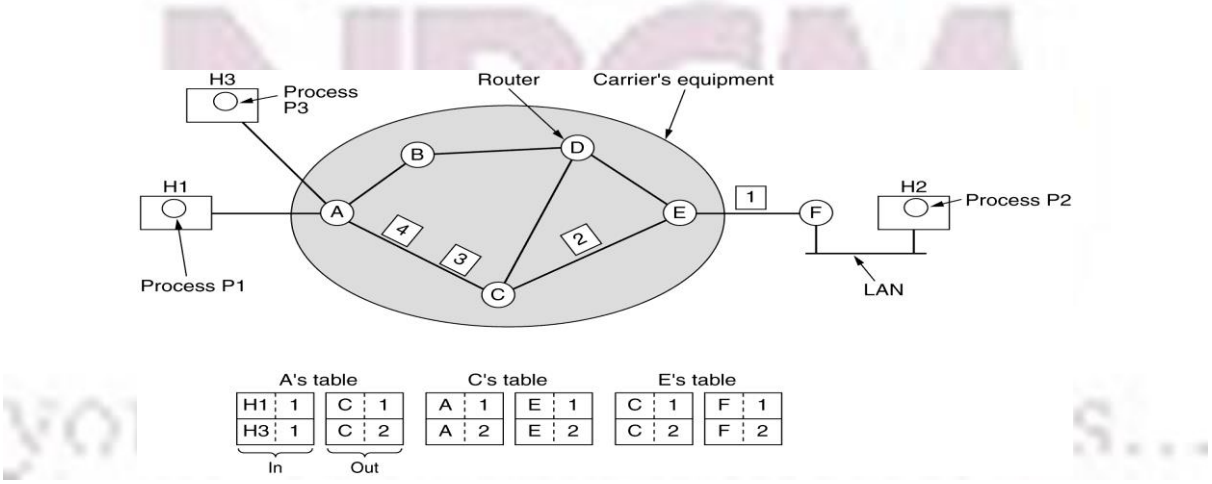


Fig: Routing within a virtual-circuit subnet

Comparison 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 table space 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 lost during 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 can be allocated in advance for each VC.

3.2Routing 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 the subnet uses datagram's internally, this decision must be made a new for every arriving data packet since the best route may have changed since last time.
- 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***.

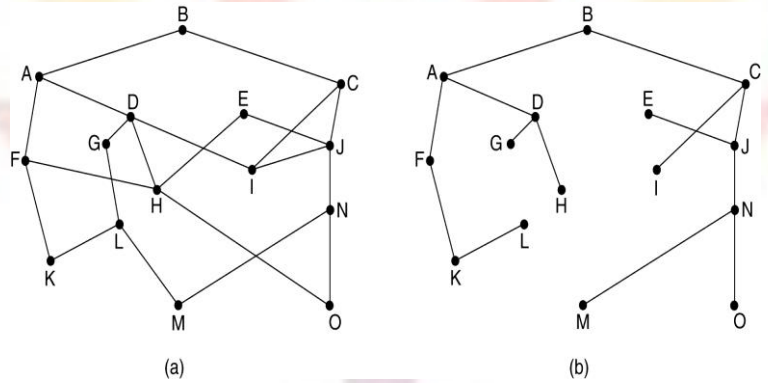
- **Nonadaptive algorithms** do not base their routing decisions on measurements or estimates of the current traffic and topology. This procedure is sometimes called **static routing.**

- **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.***

→link state 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 the destination. Such a tree is called a **sink tree.**



(a) A subnet. (b) A sink tree for router B.

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 path between 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 better paths.
- A label may be either temporary or permanent.
- When it is discovered that a label represents the shortest possible path from the source to that node, it is made permanent & never changes thereafter.

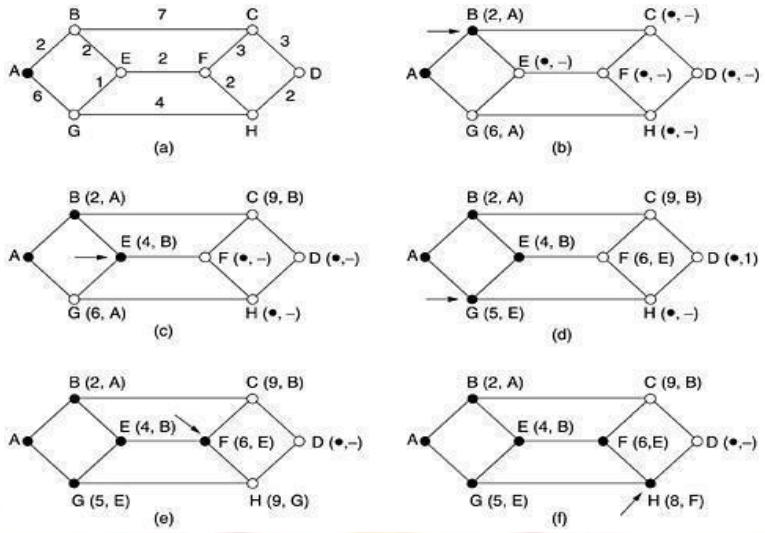


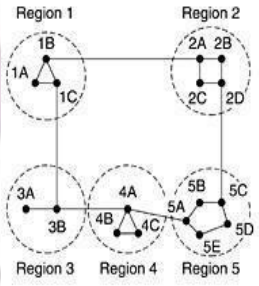
Fig. The first five steps used in computing the shortest path from *A* to *D*. The arrows indicate the working node.

FLOODING:

- Flooding is another static algorithm.
- In flooding, every incoming packet is sent out on every outgoing line except the one it achieved on.
- Flooding generates vast number of duplicate packets, an infinite number we need to take measures to damp the process.
- One such measure is to have a hop counter contained in the header of each packet, which is 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 receives from its hosts.
- Each router needs a list per source router telling which sequence numbers originating at that 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 k have 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 every line.
- Only on those lines that are going approximately in the right direction.
- Flooding can be useful in distributed database applications to update all the databases concurrently.

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 status reports 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 the other 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 all other 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 for most destinations in region 5.



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 method if none of the above methods described below are applicable.
- The problem with flooding is it generates too many packets and consumes too much bandwidth.
- A third algorithm is multi destination routing. In this method, each packet contains a list of all destinations.
- When a packet arrives at a router, the router checks all the destinations to determine the set of output lines that will be needed.
- A fourth broadcast algorithm use the sink tree for the router initiating the broadcast or any other spanning tree.
- A spanning tree is a subset of the subset of the subnet that includes all the routers but contain s no loops.
- If each router knows which of its lines belong to the spanning tree , except the line it arrived on, 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 the job.
- Last broadcast algorithm is to approximate the behavior of the previous one, even when the routers 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 is normally 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 the first 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***.

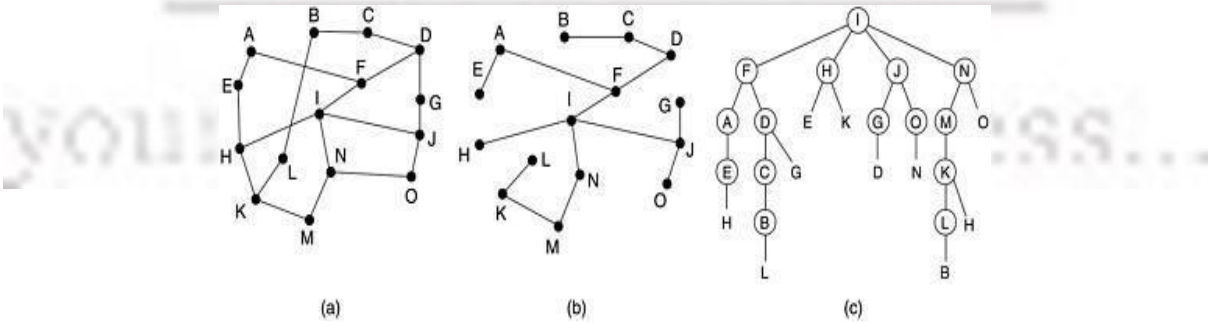


Fig. Reverse path forwarding. (a) A subnet. (b) A sink tree. (c)The tree built by reverse path forwarding.

Multicast Routing:

- Some applications need processes work together in groups, a group of processes implementing a distributed database system.
- It is frequently necessary for one process to send a message to all other members of the group.
- 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 query their hosts periodically.
- In multicast routing, each router computes a spanning tree covering all other routers in the subnet.

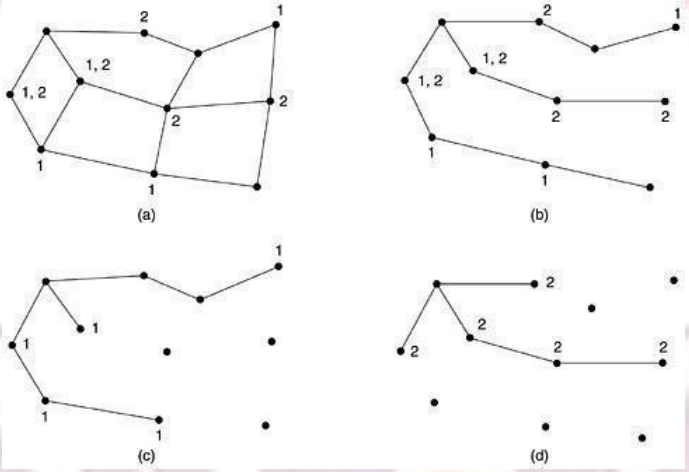


Fig: (a) A network. (b) A spanning tree for the leftmost router.
(c) A multicast tree for group 1. (d) A multicast tree for group 2.

- The above fig shows the subnet with two groups 1 and 2.
- 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 lead to 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 PRUNE message, 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 the best 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 time or 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 each destination. 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 is indicated 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.

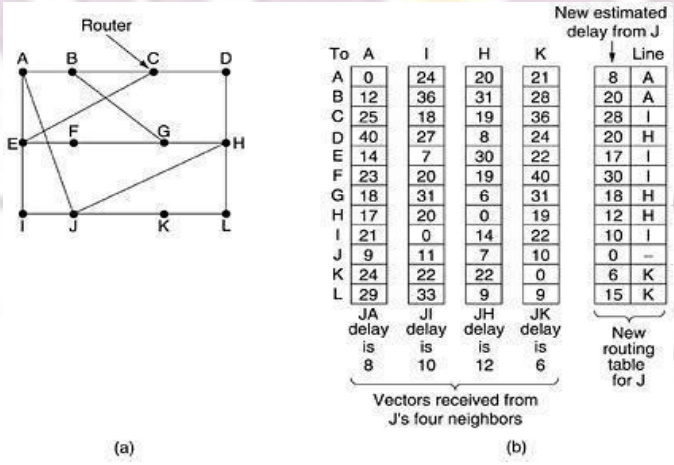


Fig: (a) A subnet. (b) Input from *A, I, H, K,* and the new routing table for *J*.

- 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 msec respectively.
- 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 G is 18 msec. & that the route to use is via H.

COUNT- TO- INFINITY PROBLEM:

- Consider a router whose best route to destination X is large.
- If on the next exchange neighbor A suddenly reports a short delay to X.
- The router just switches over to using the line to A to send traffic to X.
- No router ever has a value more than one higher than the minimum of its entire neighbor.
- All the routers work their way upto infinity, but the number of exchanges required depends on the numerical value used for infinity.
    - SPLIT HORIZON HACK:
- The split horizon algorithm works the same way as distance vector routing, except that the distance to X is not reported on the line that packets for X are sent on.

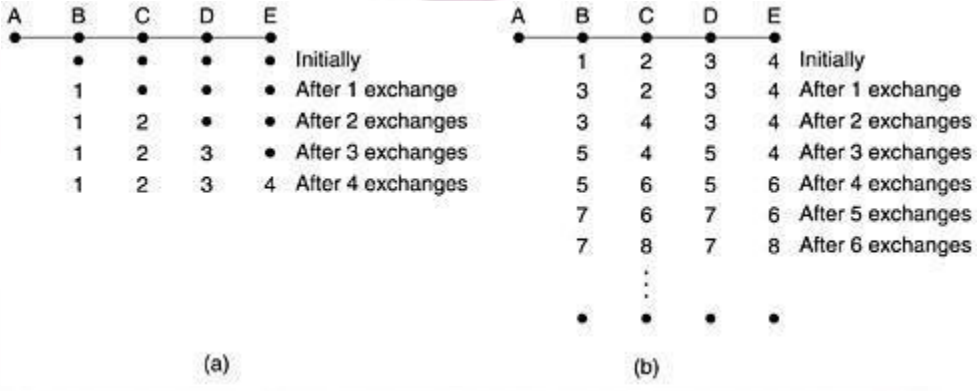


Fig: The count-to-infinity problem.

DYNAMIC ROUTING ALGORITHMS OR ADAPTIVE ALGORITHMS

These algorithms change their routing decisions to reflect changes in the topology & the traffic.

- Adaptive algorithms differ in where they get their information, when they change the routers &what metric is used for optimization.
- Dynamic algorithms are of two types:

1. Distance vector routing algorithm.

2. Link state routing algorithm.

Link state routing algorithm: this algorithm is simple and can be stated as five parts. Each router must

1. Discover its neighbors &learn their network address.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

Learning about the neighbors:

- Routers know who its neighbors are by sending a special hello packet on each point –to – point line.
- The router on the other end is expected to send back a reply telling who it is.
- The names must be globally unique.
- Here N is the artificial node.

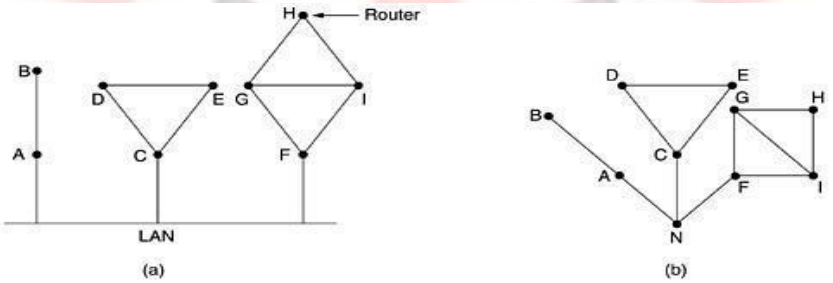


Fig: (a) Nine routers and a LAN. (b) A graph model of (a)

Measuring line cost:

- The router requires knowing or at least estimate of the delay to each of its neigh bours.
- To determine this delay it sends a special ECHO packet over the line that the other side is required to send back immediately.
- By measuring the round trip time & dividing it by two.
- The sending router can get a reasonable estimate of the delay. when measuring the delay. To factor the load in, the round-trip timer must be started when the ECHO packet is queued. To ignore the load, the timer should be started when the ECHO packet reaches the front of the queue.
- Heavy load takes more time.
- Low load takes less time.
- If load ignore, bandwidth consider problems does nor occur.
- To over come this problems, load spread both lines, then problems does not occur.

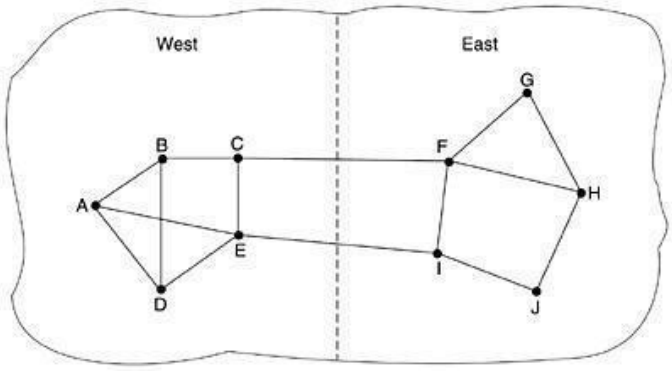


Fig: A subnet in which the East and West parts are connected by two lines.

Building link state packets:

- Once the information is collected the router has to build a packet containing all the data.
- The packet starts with the identity of the sender, followed by a sequence number & age & a list of neighbors.
- The packets can be building periodically at regular intervals or when some significant event occurs.

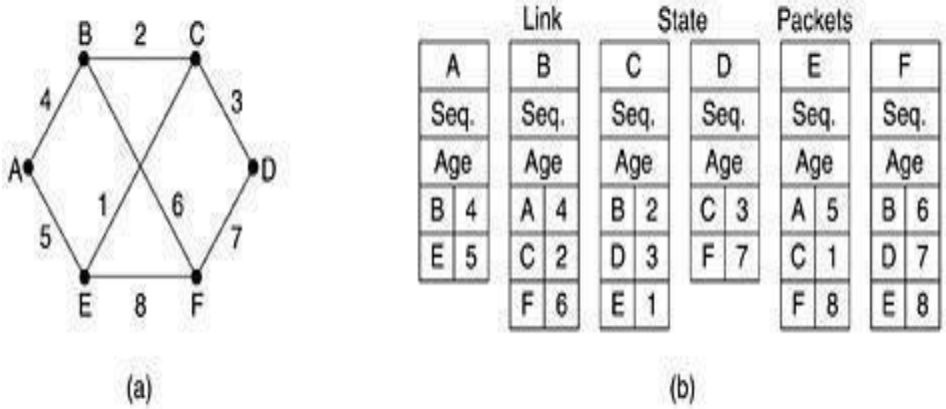


Fig: (a) A subnet. (b) The link state packets for this subnet.

Distributing the link state packets:

- To avoid inconsistencies, loops& other problem. Flooding is used to distribute the link state packets.
- To keep the flood in check, each packet contains a sequence number that is incremented for each new packet sent.
- Routers keep track of all the pairs they see.
- When a new link state packet comes in, it is checked against the list of packets already seen.
- If it is new, it is forwarded on all lines except the one it arrived on.
- If it is duplicate, it is discarded.

Computing the new routers:

- Once a router has a full set of link state packets.
- It can construct the entire subnet graph because every link is represented.
- Every link is represented twice, once for each direction.

Routing for mobile hosts:

- To route a packet to a mobile host, the network first has to find it.
- We have 3 types of hosts.
- Users who never move are said to be stationary.
- Migratory host moves at fixed interval sites with fixed time intervals.
- Roaming uses actually compute on the run& want to maintain their connections as they move around all users who are away from home are called "mobile users".
- All hosts are assumed to have a permanent home location that never changes.
- Hosts also have a permanent home address that can be used to determine their home locations, analogous to the way the telephone number.

- The world is divided up (geographically) into small units. Let us call them areas, where an area is typically a LAN or wireless cell.
- Each area has one or more foreign agents, which are processes that keep track of all mobile hosts visiting the area.
- In addition, each area has a home agent, which keeps track of hosts whose home is in the area,
- When a packet is sent to a mobile user, it is routed to the users home LAN.
- Packet is sent to the mobile host's home address.
- The home agent encapsulates packet, the foreign agent removes the original packet from the payload field & send it to the mobile user as a data link frame.
- Home agent tells the sender to send packets to the mobile host by encapsulating them in the payload of packets addressed to the foreign agent.
- Subsequent packets can now be routes directly to the user via the foreign agent.

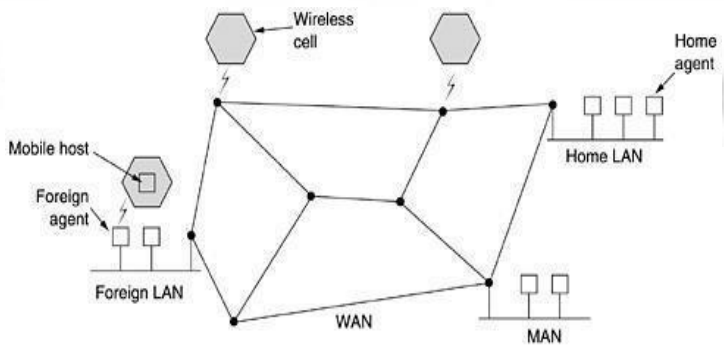


Fig: A WAN to which LANs, MANs, and wireless cells are attached.

3.3Congestion control algorithms

- When too many packets are present in the subnet, performance degrades. This situation is called congestion.
- Congestion ctrl occurs if move no .of packets are transmitted with in the maximum range of carrying 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 processing with 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 can absorb it.
- Flow control involves some direct feedback from the receiver to the sender.

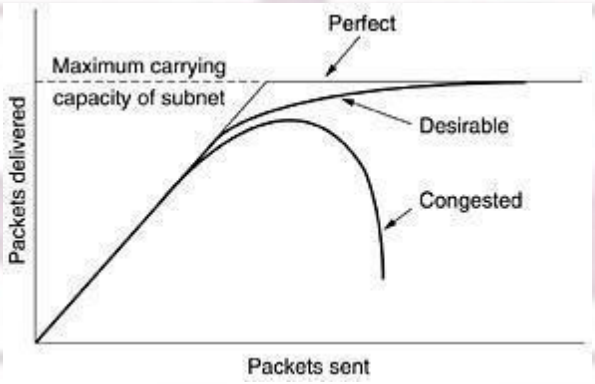


Fig: When too much traffic is offered, congestion sets in and performance degrades sharply.

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 going on. 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 any water 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 finite internal 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 into an 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 one packet.
- If the byte count is too low, the next packet must wait until the next tick.

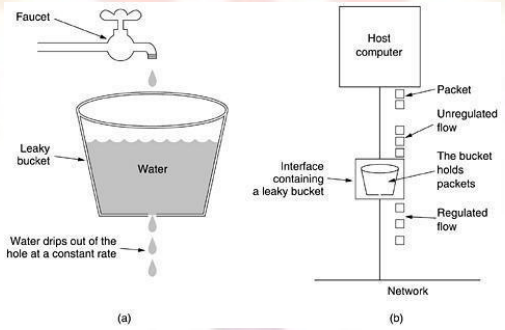


Fig: (a) A leaky bucket with water. (b) A leaky bucket with packets.

Token bucket algorithm:

In this algorithm, the leaky bucket holds tokens, generated by a clock at the rate of one token every delta 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 be generated.
- Token bucket algorithm provides a different kind of traffic shaping than the leaky bucket algorithm.
- The difference between two algorithms is token bucket algorithm throws away tokens when the bucket 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 is sent.
- 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.

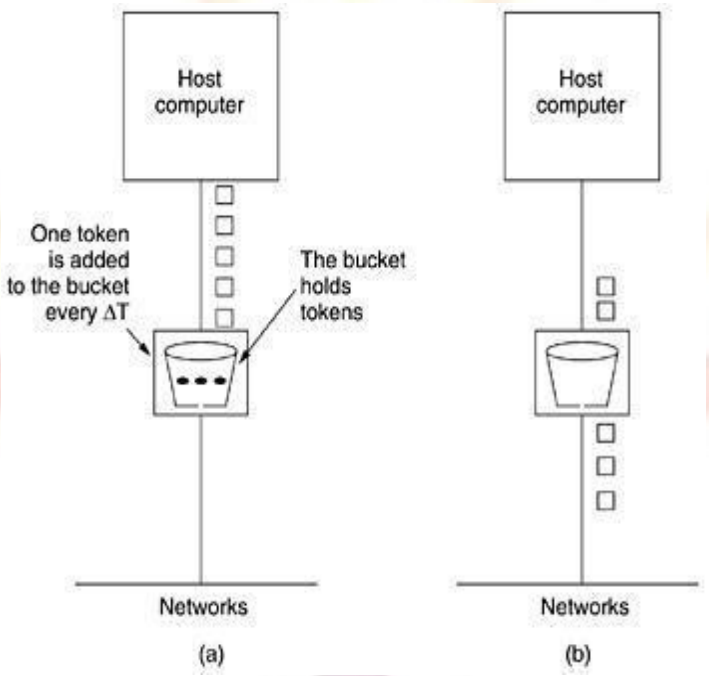


Fig: The token bucket algorithm. (a) Before. (b) After.

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 is set up.
- This agreement specifies the volume & shape of the traffic, quality of service required, & other parameters.

- In this way, congestion is unlikely to occur on the new virtual circuits because all the necessary resources 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 its transmission 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 the specified destination by x percent.
- Other packets aimed at the same destination generate more choke packets. The host should ignore 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 host reduces 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 the reaction 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 or ahead of its schedule.
- The packets that are ahead of schedule get slowed down & packets that are behind schedule get speeded up.

Congestion control for multicasting:

- In multicasting we need to send messages to a group. There are multiple senders and multiple receivers.
- 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 the tree 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 receive from.
- The routers use this information to optimize band width planning.

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 connections are normally established.
- The subnet builds a virtual circuit to the router nearest the destination network as the destination 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 more gateways to the destination.
- This works better when all the networks have the same properties.

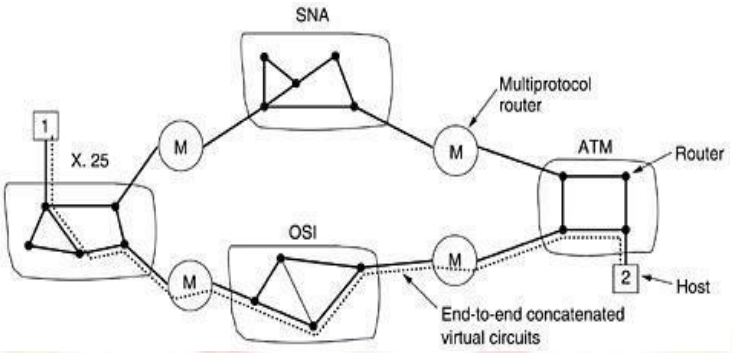


Fig: Internetworking using concatenated virtual circuits.

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.

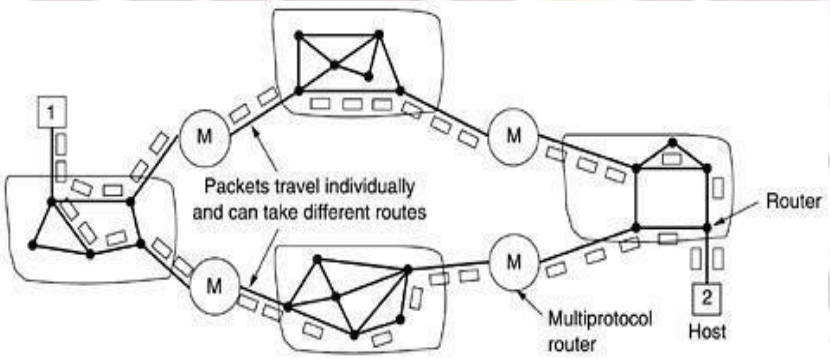


Fig: A connectionless internet.

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

Tunneling:

- Source & destination hosts are on the same type of network, but in between source & destination there is a different network.
- A technique called 'tunneling' is used as a solution to this problem.
- Host1 wants to send an ip packet to host 2.
- Host 1 constructs the packet containing the ip address of host 2 & inserts it into an Ethernet frame addressed to multiprotocol router & puts it on the Ethernet.
- When the multi protocol router gets the frame. It removes the ip packet, insects it in the payload field of wan n/w layer packet & address to the multiprotocol router.
- The router removes the ip packet sends it to host 2 inside an Ethernet frame.
- WAN can be seen as a big tunnel extending from one multiprotocol router to the other
- IP packets just travel from one 7end of the tunnel to the other.
- Only the multiprotocol routers has to understand IP &wan packet
- The distance from the middle of one multiprotocol router to the middle of the other acts like a serial line.

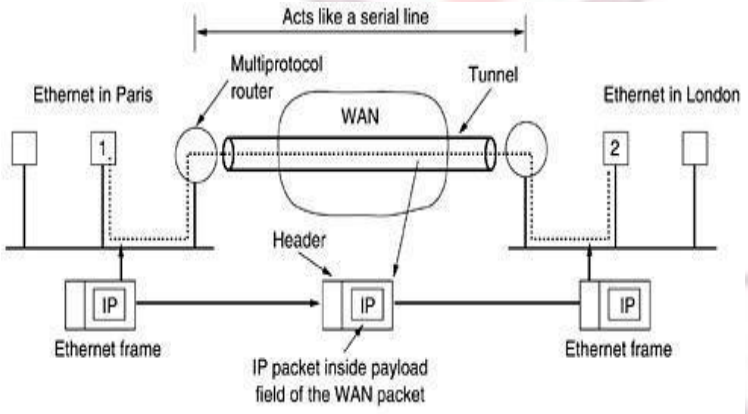


Fig: Tunneling a packet

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 any network to which it is connected

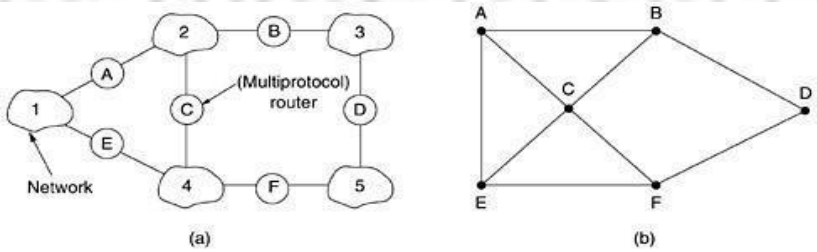


Fig: (a) An internetwork. (b) A graph of the internetwork.

- 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 packets sizes 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 designation is reached
- In Non Transparent fragmentation we reassemble the fragments only at the digestion

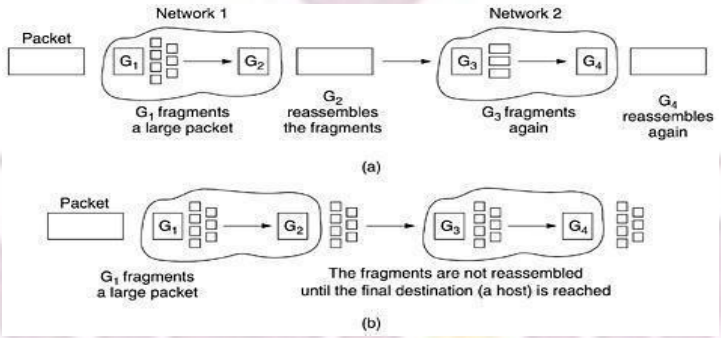


Fig: (a) Transparent fragmentation. (b) Nontransparent fragmentation

Network layer in the internet

IP protocol :

- At the network layer, the internet can viewed as a collection of sub network or autonomous systems (AS) that are inter connected
- an IP datagram consists off a header part and a test part
- the header has 20 bits fixed part and variable length optional part

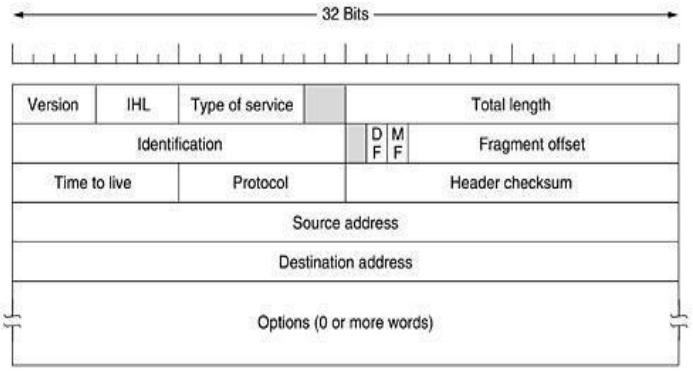


Fig: The IPv4 (Internet Protocol) header.

- 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.

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

Fig: Some of the IP options.

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 Corporation for 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

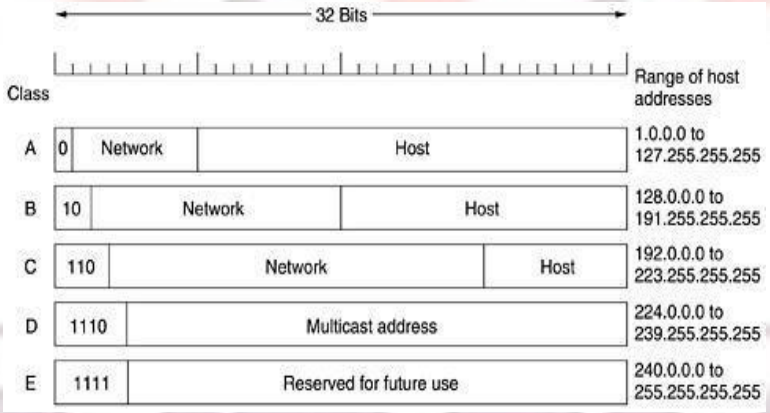


Fig: IP address formats.

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

SUBNETS:-

- The parts of the network are called subnets.
- Subnet means the set of all routers and communication lines in a network.
- We can connect the same IP address of different numbers.
- The host is sub divided & added to the IP address.

Internet control protocols:-

The internet control protocols are:

➔ ICMP –Internet Control Message Protocol

➔ ARP – Address Resolution Protocol.
➔ RARP-Reverse Address Resolution Protocol.

ICMP:-

- The operations of the internet is monitored closely by the routers.
- If an unexpected event happens during transmission the ICMP is used to report.
- It is also used to test the Internet.
- Each ICMP message type is encapsulated in an IP packet.
- The ICMP messages used are

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

Fig: The principal ICMP message types.

ARP: address resolution protocol

- Every machine on the internet has one or more ip address.
- By identifying IP address we can reach destination.
- Ip addresses are not used for sending packets because the data link layer hardware does not understand internet addresses.
- In Arp the Ethernet address is added to ip address & the request is send to ARP server.
- By using Ethernet address we can recognize & communicate with original system.
- ARP find out which Ethernet address corresponds to a given ip address.

RARP: (Reverse Address Resolution Protocol).

- In RARP, an Ethernet address is given; we have to find corresponding IP address.
- An Ethernet address is sent & asks the corresponding ip address.
- RARP servers sees the request, it looks up to the Ethernet address in its configuration files& sends back the corresponding ip address.

OSPF: (open shortest path first):

- The open shortest path first protocol is a hierarchical interior gateway protocol for routing in internet protocol using a link-state in the individual areas that makeup the hierarchical.

- OSPF is the most widely used IGP in large networks.
- BGP is the most widely used EGP in large networks.
- OSPF protocol can operate security.
- An OSPF network can be broken up into small networks.
- A special area called the backbone area forms the core of networks and other areas are connected to it.
- Different types of links: OSPF supports 4 types of links.
  - point-to-point

    Transient
    Stub
    Virtual

Point-to-point: it is used to establish a connection between two routers. No host or other router is present between them.

Transient link: it is a network which several routers are connected.

Stub link: it is a network that is connected to a single router.

Virtual link: if no direct connection is possible, a virtual link may be established. A virtual link must have a least one end-point in the backbone. Virtual links with both end-points in the backbone can be defined to restore failures that make the backbone discontinuous.

BGP: (Border Gateway Protocol):

- BGP is an inter autonomous system routing protocol.
- An autonomous system is a network or group os networks under common administration and with common routing policies.
- BGP is used to exchange routing information for the internet and is the protocol used between ISP (internet service protocol).
- ISP's user BGP to exchange information, with other networks.
- When BGP is used autonomous systems the protocol is referred to as External BGP (EBGP).
- If BGP is used to exchange information within as AS, then the protocol is referred to as Internal BGP(IBGP).
- BGP categorizes the network into 3 types.

Stub n/w: there is only one connection b/w the n/w OR b/w the AS. The host on one side can send data to other as, while the receiving AS cannot send data back to source AS.

Multiconnected n/w : using this n/w , data traffic can be sent or received from both sides. It has more than one connection with other n/w.

Transient n/w: a transient n/w is a multiconnected n/w that allow transient data traffic.

BGP neighbors exchange full routing information when the TCP connection b/w neighbors' is

first established. When changes are made to routing table, the BGP routers send their neighbors' only those routes that have changed.

IPV6: ipv6 has longer address than ipv4. It provides an unlimited supply of internet address.

- IPV6 simplifies the header format, it contains only seven fields.
- IPV6 gives better support for options.
- IPV6 provides security.

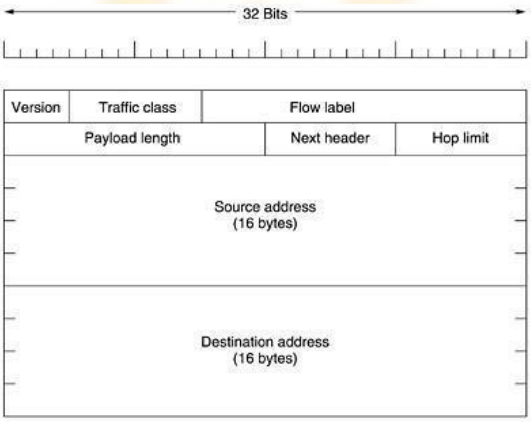


Fig: The IPv6 fixed header (required).

- Version field is 6 for IPV6 & 4 for IPV4.
- Traffic class field is used to distinguish packets with different real time delivery requirements.
- Flow label field used to allow a source & destination to set up a connection with particular properties & requirements.
- Payload length field tells how many bytes follow the 40- byte header.
- Next header field tells which of the currently extension headers. It tells which transport handler to pass the packet to.
- Hop limit field used to keep packets from living forever.
- The source address & destination address fields specify the source & destination address each of 16 bytes length.

NETWORK LAYER IN ATM NETWORKS:

- The ATM layer deals with moving cells from source to destination & involves routing algorithm and protocols with in the ATM switches.
- It deals with global addressing.
- The ATM layer is connection oriented, both in terms of the service offers & the way it operates internally. The basic element is virtual circuit.
- Virtual circuit is a connection from one source to one destination.
- Virtual circuits are unidirectional, but a pair of circuits can be created at same time.
- The ATM layer does not provide any acknowledgement.

- The cells sent along a virtual circuit will never arrive out of order.
- The ATM subnet discards cells if congestion occurs.

Cell formats:

- In the ATM layer, two interfaces are distinguishes

UNI: user network interface.

NNI: network interface.

- UNI defines the boundary between a host & an ATM network.
- NNI defines the boundary between two ATM switches.
- In both UNI &NNI cell consist of a 5- byte header followed by a 48 – byte payload. But the headers are slightly different.
-

GFC	VPI	VIC	PTI	CLP	HEC

Fig: ATM layer header at UNI

VPI	VIC	PTI	CLP	HEC

Fig: ATM layer header at NNI

- GFC: General flow control field is present only in cells between a host &the network
- VPI: Virtual path identifier field selects a particular virtual path.
- VCI: virtual channel identification field selects a particular virtual circuit within the chosen virtual path
- PTI: payload type field defines the type of payload the cell contains in accordance with the values 000, 001, 010, 011,100, 101, 110, 111.
- CLP: cell loss priority bit is set by a host to differentiate between high priority traffic &low priority traffic
- HEC: Header error check field checks the header checksum it does not check the payload
- NNI format is same as UNI format the GFC field is not present in NNI format.
- The 4 bits are used to make VPI fld 12 bits instead of 8 bits.

Connection setup:

- ATM supports both permanent virtual circuits &switched virtual circuits.
- Permanent virtual circuits are always present &can be used at will, like leased lines.
- Switched visual circuits have to be established each time they are used , like making phone calls.
- Virtual circuits establishment uses the six message types:

SETUP,
CALLPROCEEDING
CONNECT
CONNECT ACK
RELEASE
RELEASE COMPLETE

- The normal procedure for establishing a call is for a host to send a SETUP message on a special virtual circuit.

- The network responds with CALL PROCEEDING to acknowledge receipt of the request.
- when the SETUP message finally arrives, the designation host respond with CONNECT accept the care.
- The network sends a CONNECT ack. Msg. to indicate that it has received the CONNECT message
- The virtual circuit termination is simple
- The host wishing to stop just sends a RELEASE message , which propagates to the other end &causes the circuit to be released.

Routing and switching:

- When a virtual circuit is setup ,the setup message passes through the N/W from source to destination
- ATM layer designed to make efficient routing possible, VPI field is used to route, but not VCI.
- Using only VPI's has many advantages.
- Once a virtual path has been established from source to destination other virtual circuits along the path just follow the existing path.
- Routing of individual cells is easier when all virtual circuits for a given path all always in the same bundle.
- All routing on virtual paths makes it easier to switch a whole group of virtual circuits.
- Virtual paths make it easier for carries to offer closed user groups to corporate customers.

Congestion control:

- ATM networks must deal with both long term congestion, caused by more traffic coming in than the system can handle, short-term congestion, caused by burstiness in the traffic.
- We use three different strategies to control the congestion
  -Admission control
  -Resource Reservation
  -Rate Based Congestion Control

Admission control:

- In low-speed net works, it wait for congestion to occur & then react telling the source to slow down.
- In high speed networks, this approach works poorly, because thousands of additional packets may arrive in the interval between sending the notification & notification arriving at the source.
- A major tool for preventing congestion is admission control.
- When a host wants a new virtual circuit, it must describe the traffic to be offered &the service expected.

- The network then check is it possible to handle this connection without affecting existing connections.
- If no route can be located, the call is rejected.

Resource Reservation:

- At call setup time , resources are reserved in advance
- The traffic descriptor gives the peak cell rate
- To handle that rate, the network has the possibility of reserving enough bandwidth along the path.

Rate Based Congestion Control:

- In rate based congestion control after every `k' data cells sent, each sender transmits a special RM(resource management)cell
- This cell travels along the same path as the data cells.
- But, this RM cell is specially treated by the switches along the way.
- When the RM cell reaches the destination, it is examined, updated, and sent back to the sender the full path for RM cells is as shown below.

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.

The services provided by the transport layer protocols can be divided into five categories:

- 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-end delivery 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.

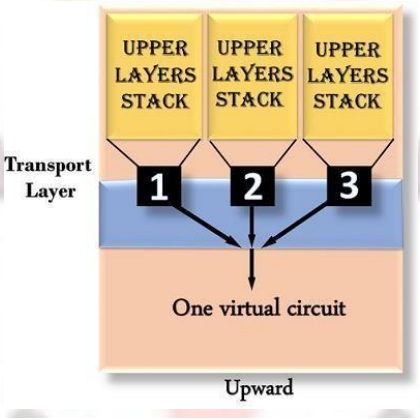
Multiplexing

The transport layer uses the multiplexing to improve transmission efficiency.

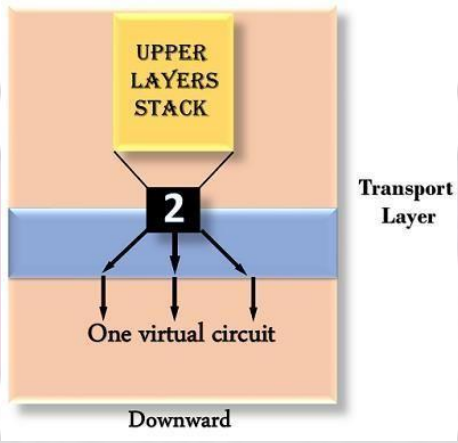
Multiplexing can occur in two ways:

- **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 when networks have a low or slow capacity.

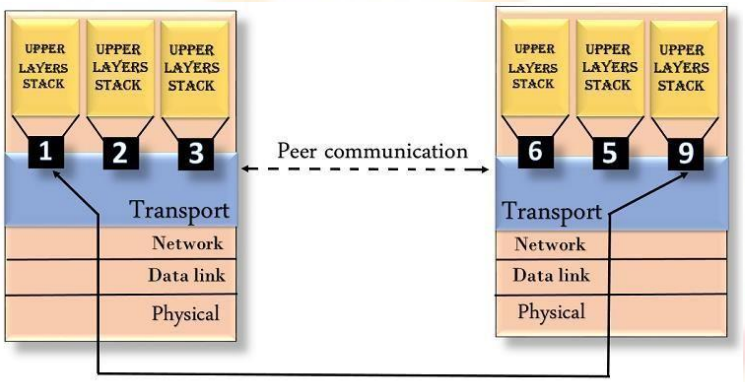


Addressing

- 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.



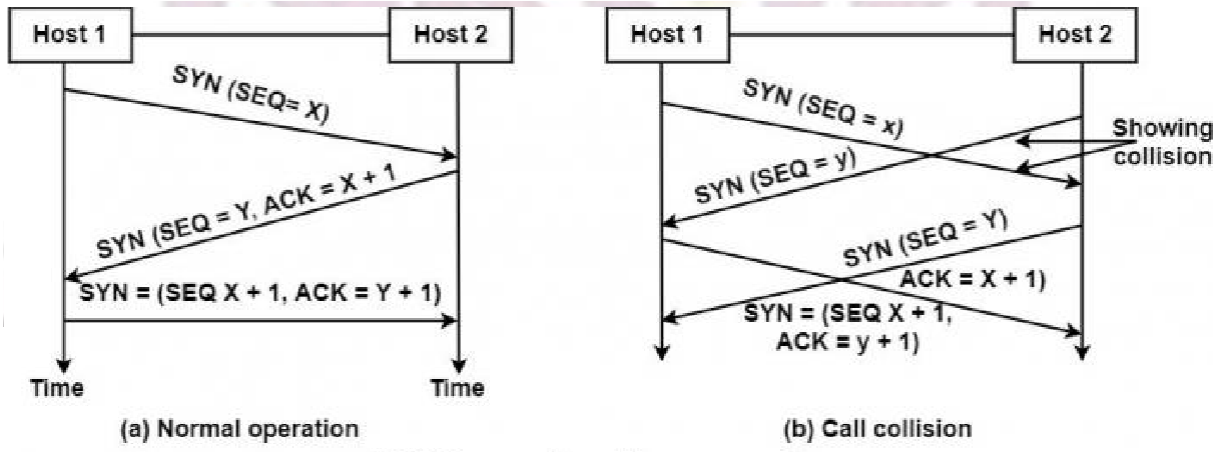
Connection Management

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.

The other side performs a connect primitive specifying the I/O 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.

Call Collision

If two hosts try to establish a connection simultaneously between the same two sockets, then the events sequence is demonstrated in the figure under such circumstances. Only one connection is established. It cannot select both the links because their endpoints identify connections.

Suppose the first set up results in a connection identified by (x, y) and the second connection are also released up. In that case, only tail enter will be made, i.e., for (x, y) for the initial sequence number, a clock-based scheme is used, with a clock pulse coming after every 4 microseconds. For ensuring additional safety when a host crashes, it may not reboot for sec, which is the maximum packet lifetime. This is to make sure that no packets from previous connections are roaming around.

TCP is a connection-oriented protocol and every connection-oriented protocol needs to establish a connection in order to reserve resources at both the communicating ends.

Connection Establishment –

1. Sender starts the process with the following:

- **Sequence number (Seq=521):** contains the random initial sequence number generated at the sender side.
- **Syn flag (Syn=1):** request the receiver to synchronize its sequence number with the above-provided sequence number.
- **Maximum segment size (MSS=1460 B):** sender tells its maximum segment size, so that receiver sends datagram which won't require any fragmentation. MSS field is present inside **Option** field in TCP header.
- **Window size (window=14600 B):** sender tells about his buffer capacity in which he has to store messages from the receiver.

2. TCP is a full-duplex protocol so both sender and receiver require a window for receiving messages from one another.

- **Sequence number (Seq=2000):** contains the random initial sequence number generated at the receiver side.
- **Syn flag (Syn=1):** request the sender to synchronize its sequence number with the above-provided sequence number.
- **Maximum segment size (MSS=500 B):** receiver tells its maximum segment size, so that sender sends datagram which won't require any fragmentation. MSS field is present inside **Option** field in TCP header.
  Since $MSS_{receiver} < MSS_{sender}$, both parties agree for minimum MSS i.e., 500 B to avoid fragmentation of packets at both ends.

Therefore, receiver can send maximum of 14600/500 = 29 packets.

This is the receiver's sending window size.

- **Window size (window=10000 B):** receiver tells about his buffer capacity in which he has to store messages from the sender.

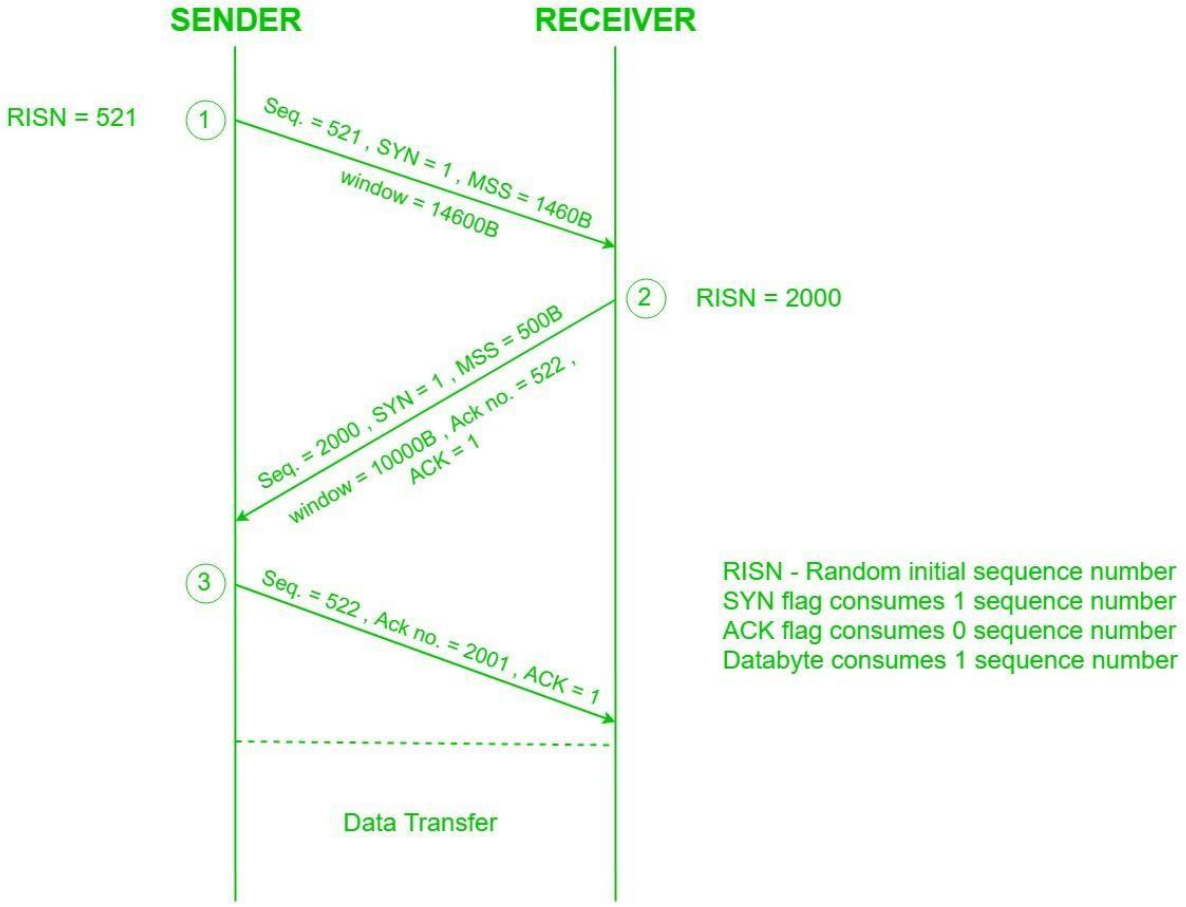
Therefore, sender can send a maximum of 10000/500 = 20 packets.

This is the sender's sending window size.

- **Acknowledgement Number (Ack no.=522):** Since sequence number 521 is received by the receiver so, it makes a request for the next sequence number with Ack no.=522 which is the next packet expected by the receiver since Syn flag consumes 1 sequence no.
- **ACK flag (ACk=1):** tells that the acknowledgement number field contains the next sequence expected by the receiver.

3. Sender makes the final reply for connection establishment in the following way:

- **Sequence number (Seq=522):** since sequence number = 521 in 1st step and SYN flag consumes one sequence number hence, the next sequence number will be 522.
- **Acknowledgement Number (Ack no.=2001):** since the sender is acknowledging SYN=1 packet from the receiver with sequence number 2000 so, the next sequence number expected is 2001.
- **ACK flag (ACK=1):** tells that the acknowledgement number field contains the next sequence expected by the sender.



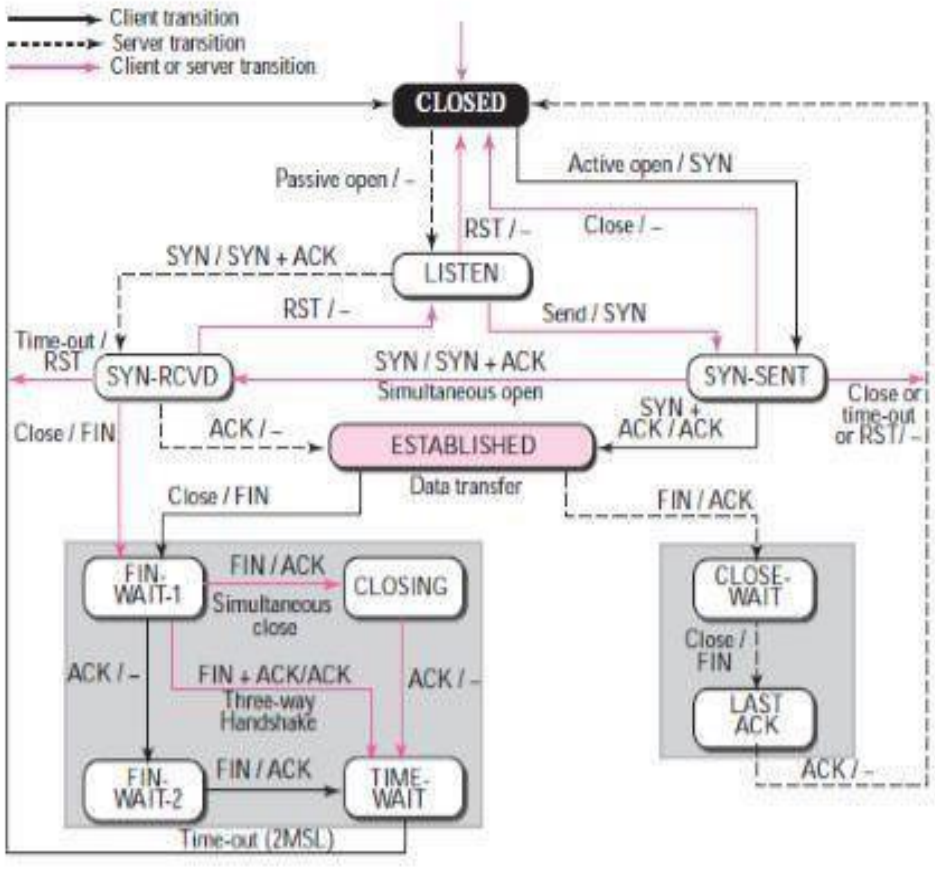
Since the connection establishment phase of TCP makes use of 3 packets, it is also known as 3-way Handshaking **(SYN, SYN + ACK, ACK).**

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.

The client side of the connection is responsible for the connection performs an active connection (active open) while the server performs a passive connection (passive open).

In the event that a connection request arrives on the server and that no application is listening on the requested port, a segment with flag RST (reset) is sent to the client by the server, the connection attempt is immediately terminated.

Principle termination of a TCP connection state diagram

The termination of a TCP connection requires four exchanges of TCP segments.

As a TCP connection is bidirectional (full duplex) , connection termination process should be made in both directions of the communication. The client as the server can send a segment with FIN flag, this mean an end to sending data. Receiving a segment with FIN indicates that the other end will not send more data. The term used then is half closed, the connection is half closed.

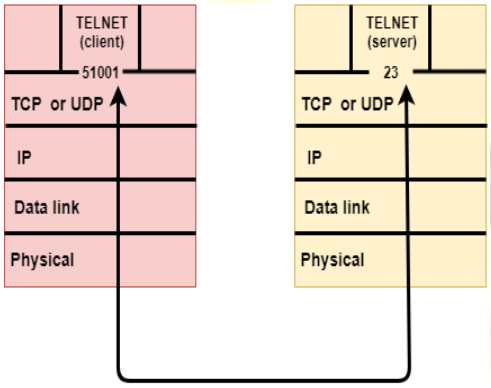
Typically, the client generates the transmission segment with a FIN flag, he made a closing force (active close), the server receives the segment realizes a passive close. The server acknowledge the FIN with ACK, informs the application for the release of this connection and when done then sends a FIN segment to the customer which in turn, acknowledge it with an ACK flag.

4.3Transport Layer protocols

- The transport layer is represented by two protocols: TCP and UDP.
- The IP protocol in the network layer delivers a datagram from a source host to the destination host.
- Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process. When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.
- 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.

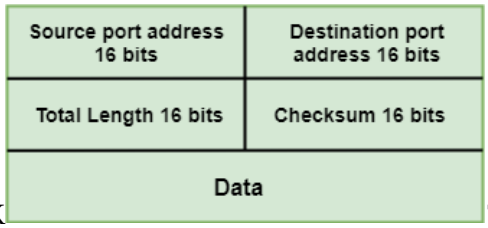


UDP

- 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

Where,

- **Source port address:** It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.
- **Destination port address:** It defines the address of the application process that will receive the message. 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.

Disadvantages of UDP protocol

- 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.

TCP

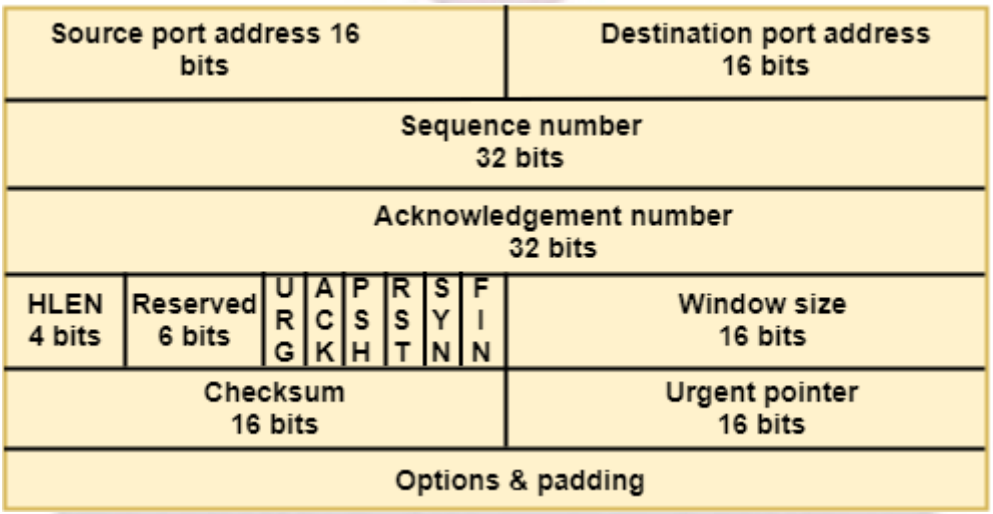
- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and 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, then the data is retransmitted to the destination. 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.
- **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
- **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:
  - Establish a connection between two TCPs.
  - Data is exchanged in both the directions.
  - The Connection is terminated.

TCP Segment Format



Where,

- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
- **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-bit sequence number field represents the position of the data in an original data stream.
- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
- **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
- **Reserved:** It is a six-bit field which is reserved for future use.
- **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

There are total six types of flags in control field:

- **URG:** The URG field indicates that the data in a segment is urgent.
- **ACK:** When ACK field is set, then it validates the acknowledgement number.
- **PSH:** The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.
- **RST:** The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers.
- **SYN:** The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation (with the ACK bit set), and confirmation acknowledgement.
- **FIN:** The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination confirmation.
    - **Window Size:** The window is a 16-bit field that defines the size of the window.
    - **Checksum:** The checksum is a 16-bit field used in error detection.
    - **Urgent pointer:** If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
    - **Options and padding:** It defines the optional fields that convey the additional information to the receiver.

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-Oriented protocol	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 the acknowledgement of data and has the ability to resend the lost packets.	It neither takes the acknowledgement, nor it retransmits the damaged frame.

UNIT-V

Application Layer –Domain name system, SNMP, Electronic Mail; the World WEB, HTTP, Streaming audio and video.

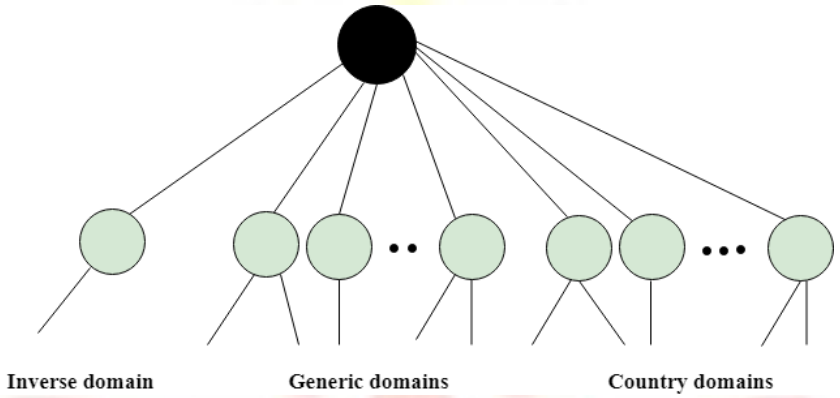
An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

5.1Domain name system

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.

- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.

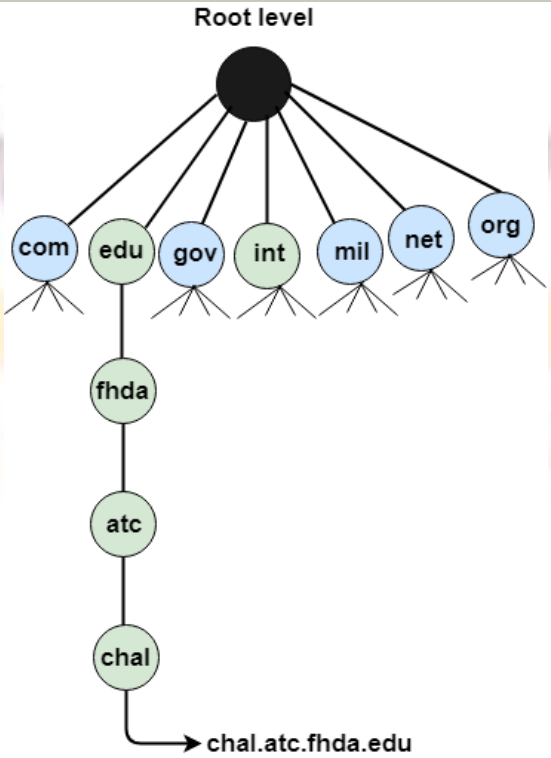


Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Label	Description
Aero	Airlines and aerospace companies
Biz	Businesses or firms
Com	Commercial Organizations
Coop	Cooperative business Organizations
Edu	Educational institutions
Gov	Government institutions
Info	Information service providers
Int	International Organizations
Mil	Military groups
Museum	Museum & other nonprofit organizations

Name	Personal names
Net	Network Support centers
Org	Nonprofit Organizations
Pro	Professional individual Organizations



Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain

The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

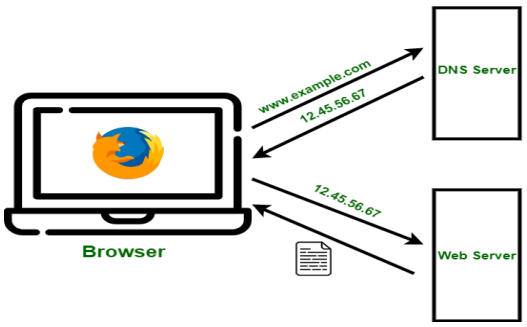
Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.

- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

Example for working of DNS

DNS resolves names to numbers, to be more specific it resolves domain names to IP addresses. So if you type in a web address in your web browser, DNS will resolve the name to a number because the only thing computers know are numbers.



Working: If you wanted to go to a certain website you would open up your web browser and type in domain name of that website. Let us use google.com. Now technically you really do not have to type in google.com to retrieve Google web page, you can just type in IP address instead if you already know what google's IP address is, but since we are not accustomed to memorizing and dealing with numbers, especially when there are millions of websites on Internet, we can just type in domain name instead and let DNS convert it to an IP address for us.

So back to our example, when you type google.com on your web browser DNS server will search through its cache to find a matching IP address for that domain name, and when it finds it it will resolve that domain name to IP address of Google web site, and once that is done then your computer is able to communicate with a Google web server and retrieve the webpage.

So DNS basically works like a phone book, when you want to find a number, you do not look up number first, you look up name first then it will give you the number. So to break this down into further detail, let us examine the steps that DNS takes. So when you type in google.com in your web browser and if your web browser or operating system cannot find IP address in its own cache memory, it will send a query to next level to what is called resolver server. Resolver server is basically your ISP or Internet service provider, so when resolver receives this query, it will check its own cache memory to find an IP address for google.com,

and if it cannot find it it will send query to next level which is root server. The root servers are the topmost server in the DNS hierarchy.

There are 13 sets of these root servers from a.root-servers.net to m.root-servers.net and they are strategically placed around world, and they are operated by 12 different organizations and each set of these root servers has their own unique IP address. So when root server receives query for IP address for google.com, root server is not going to know what IP address is, but root server does know where to send resolver to help it find IP address. So root server will direct resolver to TLD or top-level domain server for .com domain. So resolver will now ask TLD server for IP address for google.com.

The top-level domain server stores address information for top-level domains such as .com and .net, .org, and so on. This particular TLD server manages .com domain which google.com is a part of. So when a TLD server receives query for IP address for google.com, TLD server is not going to know what IP addresses for google.com. So the TLD will direct resolver to next and final level, which are authoritative name servers. So once again the resolver will now ask authoritative name server for IP address for google.com. Authoritative name server or servers are responsible for knowing everything about domain which includes IP address.

They are final authority.

So when the authoritative name server receives query from resolver, name server will respond with IP address for google.com. And finally, resolver will tell your computer IP address for google.com and then your computer can now retrieve google web page. It is important to note that once resolver receives IP address, it will store it in its cache memory in case it receives another query for google.com. So it does not have to go through all those steps again.

DNS servers has different types of records to manage resolution efficiently and provide important information about a domain. These records are the details which are cached by DNS servers. Each records have a TTL(Time To Live) value in seconds associated with it, these values set time for the expiration of cached record in DNS server which ranges to 60 to 86400 depending on the DNS provider.

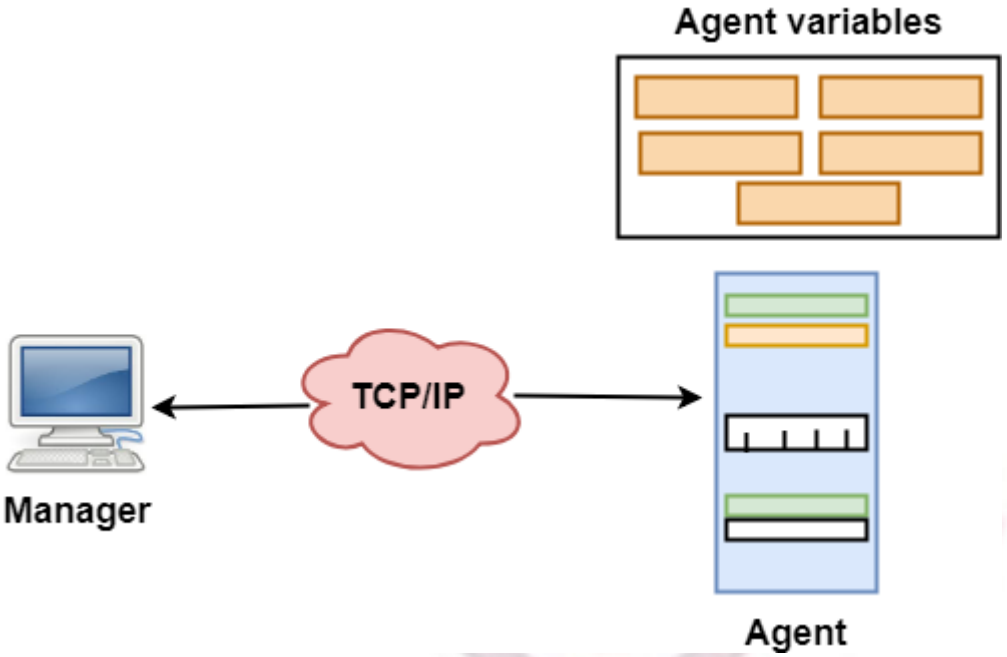
- A records – points to IPv4 address of machine where website is hosted
- AAAA records – points to IPv6 address of machine where website is hosted
- MX – points to email servers
- CNAME – canonical name for alias points hostname to hostname
- ANAME – Auto resolved alias, works like cname but points hostname to IP of hostname
- NS – nameservers for subdomains
- PTR – IP address to hostname
- SOA – containing administrative information about the DNS zone
- SRV – service record for other services
- TXT – Text records mostly used for verification, SPF, DKIM, DMARC and more
- CAA – certificate authority record for SSL/TLS certificate
-

5.2 SNMP

- SNMP stands for **Simple Network Management Protocol**.
- SNMP is a framework used for managing devices on the internet.

- It provides a set of operations for monitoring and managing the internet.

SNMP Concept



- SNMP has two components Manager and agent.
- The manager is a host that controls and monitors a set of agents such as routers.
- It is an application layer protocol in which a few manager stations can handle a set of agents.
- The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.
- It is used in a heterogeneous network made of different LANs and WANs connected by routers or gateways.

Managers & Agents

- A manager is a host that runs the SNMP client program while the agent is a router that runs the SNMP server program.
- Management of the internet is achieved through simple interaction between a manager and agent.
- The agent is used to keep the information in a database while the manager is used to access the values in the database. For example, a router can store the appropriate variables such as a number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.

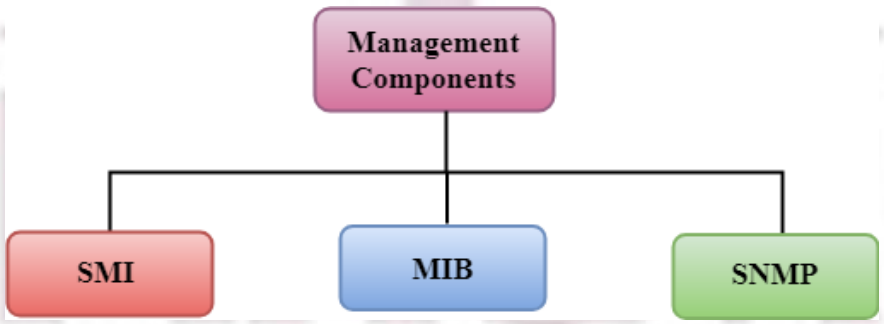
- Agents can also contribute to the management process. A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manager.

Management with SNMP has three basic ideas:

- A manager checks the agent by requesting the information that reflects the behavior of the agent.
- A manager also forces the agent to perform a certain function by resetting values in the agent database.
- An agent also contributes to the management process by warning the manager regarding an unusual condition.

Management Components

- Management is not achieved only through the SNMP protocol but also the use of other protocols that can cooperate with the SNMP protocol. Management is achieved through the use of the other two protocols: SMI (Structure of management information) and MIB(management information base).
- Management is a combination of SMI, MIB, and SNMP. All these three protocols such as abstract syntax notation 1 (ASN.1) and basic encoding rules (BER).



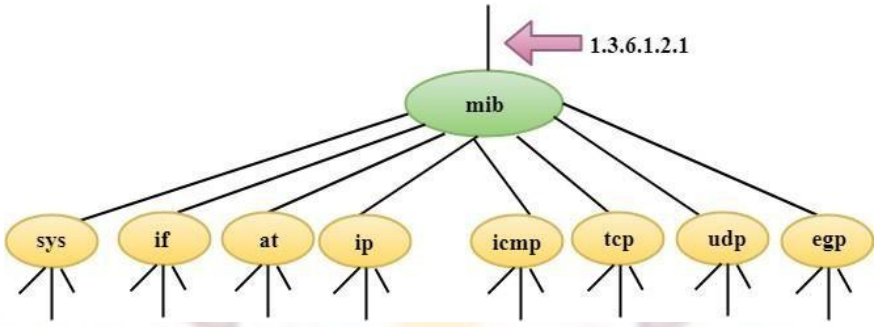
SMI

The SMI (Structure of management information) is a component used in network management. Its main function is to define the type of data that can be stored in an object and to show how to encode the data for the transmission over a network.

MIB

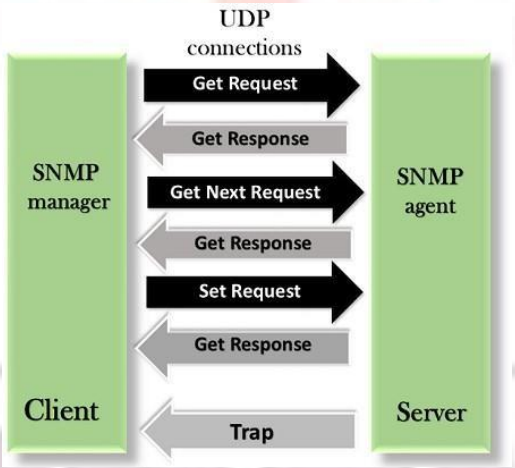
- The MIB (Management information base) is a second component for the network management.

- Each agent has its own MIB, which is a collection of all the objects that the manager can manage. MIB is categorized into eight groups: system, interface, address translation, ip, icmp, tcp, udp, and egp. These groups are under the mib object.



SNMP

SNMP defines five types of messages: GetRequest, GetNextRequest, SetRequest, GetResponse, and Trap.



GetRequest: The GetRequest message is sent from a manager (client) to the agent (server) to retrieve the value of a variable.

GetNextRequest: The GetNextRequest message is sent from the manager to agent to retrieve the value of a variable. This type of message is used to retrieve the values of the entries in a table. If the manager does not know the indexes of the entries, then it will not be able to retrieve the values. In such situations, GetNextRequest message is used to define an object.

GetResponse: The GetResponse message is sent from an agent to the manager in response to the GetRequest and GetNextRequest message. This message contains the value of a variable requested by the manager.

SetRequest: The SetRequest message is sent from a manager to the agent to set a value in a variable.

Trap: The Trap message is sent from an agent to the manager to report an event. For example, if the agent is rebooted, then it informs the manager as well as sends the time of rebooting.

5.3.E-MAIL

Electronic mail, commonly known as email, is a method of exchanging messages over the internet. Here are the basics of email:

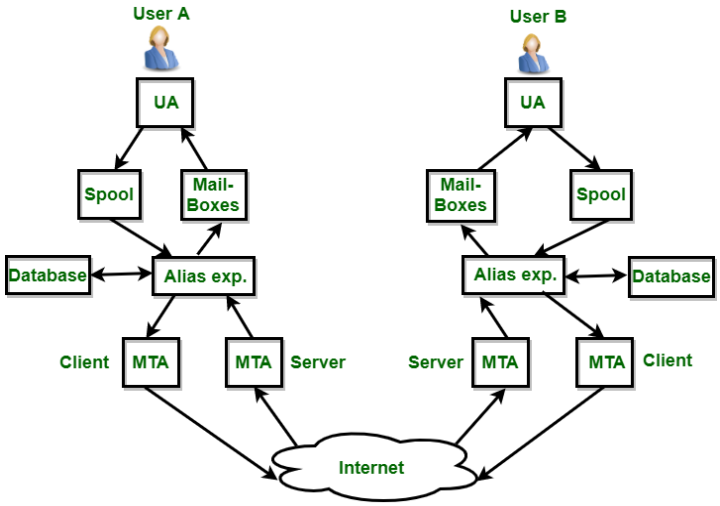
1. An email address: This is a unique identifier for each user, typically in the format of name@domain.com.
2. An email client: This is a software program used to send, receive and manage emails, such as Gmail, Outlook, or Apple Mail.
3. An email server: This is a computer system responsible for storing and forwarding emails to their intended recipients.

To send an email:

1. Compose a new message in your email client.
2. Enter the recipient's email address in the "To" field.
3. Add a subject line to summarize the content of the message.
4. Write the body of the message.
5. Attach any relevant files if needed.
6. Click "Send" to deliver the message to the recipient's email server.
7. Emails can also include features such as cc (carbon copy) and bcc (blind carbon copy) to send copies of the message to multiple recipients, and reply, reply all, and forward options to manage the conversation.

Electronic Mail (e-mail) is one of most widely used services of Internet. This service allows an Internet user to send a **message in formatted manner (mail)** to the other Internet user in any part of world. Message in mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called **sender** and person who receives mail is called **recipient**. It is just like postal mail service. **Components of E-Mail System :** The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

1. **User Agent (UA) :** The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.
2. **Message Transfer Agent (MTA) :** MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfer mail to mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done



3. **Mailbox :** It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox . Access to mailbox is only to owner of mailbox.
4. **Spool file :** This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an **alias**, to represent several different e-mail addresses. It is known as **mailing list**, Whenever user have to sent a message, system checks recipient's name against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

Services provided by E-mail system :

- **Composition –** The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.
- **Transfer –** Transfer means sending procedure of mail i.e. from the sender to recipient.
- **Reporting –** Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.
- **Displaying –** It refers to present mail in form that is understand by the user.
- **Disposition –** This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

Advantages of email:

1. Convenient and fast communication with individuals or groups globally.
2. Easy to store and search for past messages.
3. Ability to send and receive attachments such as documents, images, and videos.
4. Cost-effective compared to traditional mail and fax.
5. Available 24/7.

Disadvantages of email:

1. Risk of spam and phishing attacks.
2. Overwhelming amount of emails can lead to information overload.
3. Can lead to decreased face-to-face communication and loss of personal touch.
4. Potential for miscommunication due to lack of tone and body language in written messages.

5. Technical issues, such as server outages, can disrupt email service.
6. It is important to use email responsibly and effectively, for example, by keeping the subject line clear and concise, using proper etiquette, and protecting against security threats.

5.4 World Wide Web

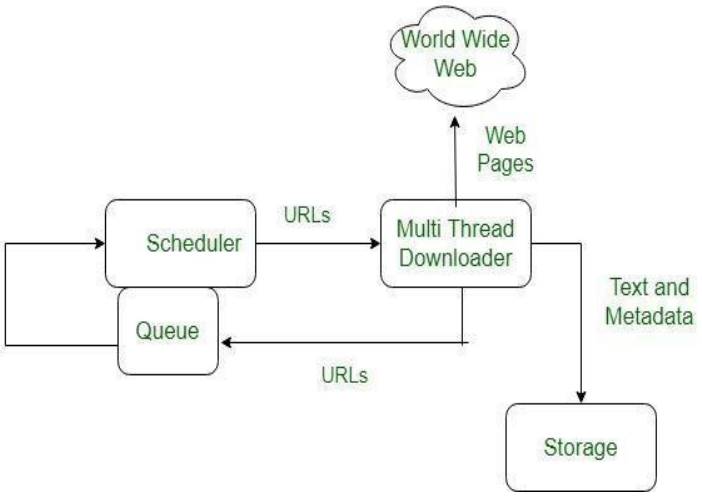
The **World Wide Web** is abbreviated as WWW and is commonly known as the web. The WWW was initiated by CERN (European library for Nuclear Research) in 1989.
WWW can be defined as the collection of different websites around the world, containing different information shared via local servers(or computers).

History:
It is a project created, by Timothy Berner Lee in 1989, for researchers to work together effectively at CERN. is an organization, named the World Wide Web Consortium (W3C), which was developed for further development of the web. This organization is directed by Tim Berner's Lee, aka the father of the web.

System Architecture:

From the user's point of view, the web consists of a vast, worldwide connection of documents or web pages. Each page may contain links to other pages anywhere in the world. The pages can be retrieved and viewed by using browsers of which internet explorer, Netscape Navigator, Google Chrome, etc are the popular ones. The browser fetches the page requested interprets the text and formatting commands on it, and displays the page, properly formatted, on the screen.

The basic model of how the web works are shown in the figure below. Here the browser is displaying a web page on the client machine. When the user clicks on a line of text that is linked to a page on the abd.com server, the browser follows the hyperlink by sending a message to the abd.com server asking it for the page.



Here the browser displays a web page on the client machine when the user clicks on a line of text that is linked to a page on abd.com, the browser follows the hyperlink by sending a message to the abd.com server asking for the page.

Working of WWW:

The World Wide Web is based on several different technologies: Web browsers, Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP).
A Web browser is used to access web pages. Web browsers can be defined as programs which display text, data, pictures, animation and video on the Internet. Hyperlinked resources on the World Wide Web can be accessed using software interfaces provided by Web browsers. Initially, Web browsers were used only for surfing the Web but now they have become more universal. Web browsers can be used for several tasks including conducting searches, mailing, transferring files, and much more. Some of the commonly used browsers are Internet Explorer, Opera Mini, and Google Chrome.

Features of WWW:

- HyperText Information System
- Cross-Platform
- Distributed
- Open Standards and Open Source
- Uses Web Browsers to provide a single interface for many services
- Dynamic, Interactive and Evolving.
- "Web 2.0"

Components of the Web: There are 3 components of the web:

1. **Uniform Resource Locator (URL):** serves as a system for resources on the web.
2. **HyperText Transfer Protocol (HTTP):** specifies communication of browser and server.
3. **Hyper Text Markup Language (HTML):** defines the structure, organisation and content of a webpage.

5.5 HTTP

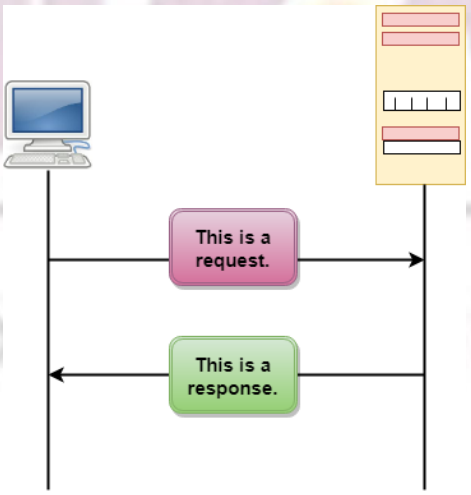
- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.

- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

Features of HTTP:

- **Connectionless protocol:** HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

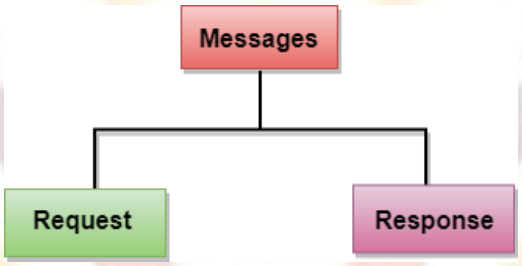
HTTP Transactions



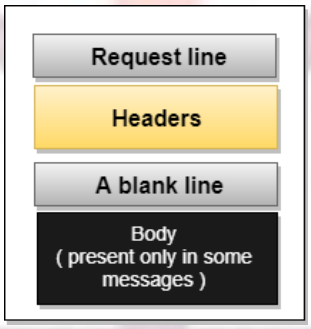
The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

Messages

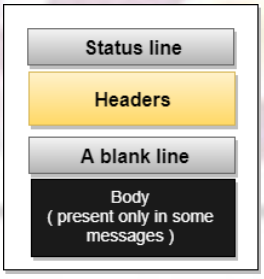
HTTP messages are of two types: request and response. Both the message types follow the same message format.



Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.



Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.



Uniform Resource Locator (URL)

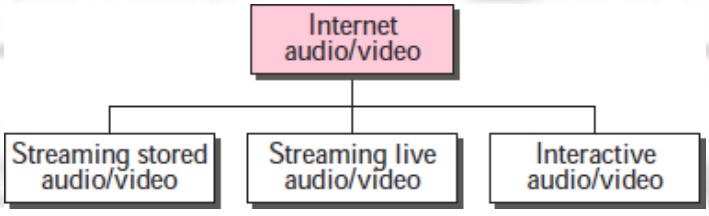
- A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).

- The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.
- The URL defines four parts: method, host computer, port, and path.

- **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.
- **Host:** The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
- **Port:** The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.
- **Path:** Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

5.6 Streaming of audio/video

We can divide audio and video services into three broad categories: streaming stored audio/video, streaming live audio/video, and interactive audio/video. Streaming means a user can listen (or watch) the file after the downloading has started.



In the first category, streaming stored audio/video, the files are compressed and stored on a server. A client downloads the files through the Internet. This is sometimes referred to as on-

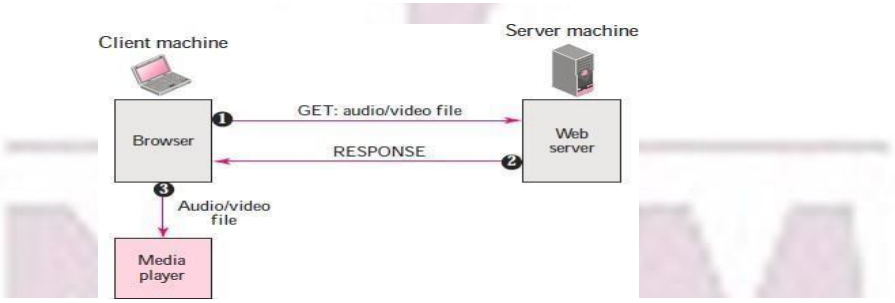
demand audio/video. In the second category, streaming live audio/video refers to the broadcasting of radio and TV programs through the Internet. In the third category, interactive audio/video refers to the use of the Internet for interactive audio/video applications. A good example of this application is Internet telephony and Internet teleconferencing.

STREAMING STORED AUDIO/VIDEO

Downloading these types of files from a server can be different from downloading other types of files.

First Approach: Using a Web Server

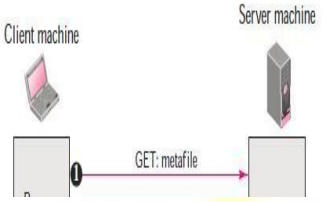
A compressed audio/video file can be downloaded as a text file. The client (browser) can use the services of HTTP and send a GET message to download the file. The Web server can send the compressed file to the browser. The browser can then use a help application, normally called a media player, to play the file. The file needs to download completely before it can be played.



Second Approach: Using a Web Server with Metafile

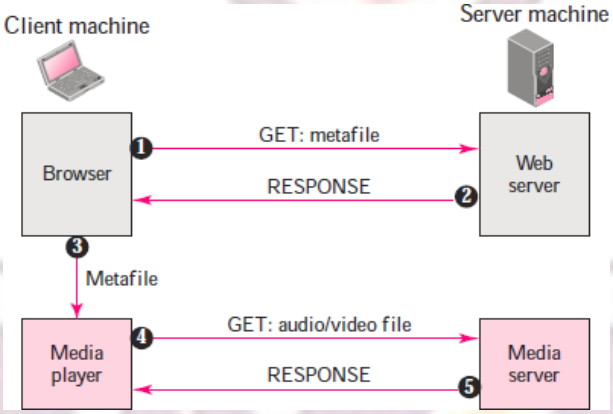
In another approach, the media player is directly connected to the Web server for downloading the audio/video file. The Web server stores two files: the actual audio/video file and a metafile that holds information about the audio/video file.

1. The HTTP client accesses the Web server using the GET message.
2. The information about the metafile comes in the response.
3. The metafile is passed to the media player.
4. The media player uses the URL in the metafile to access the audio/video file.
5. The Web server responds.



Third Approach: Using a Media Server:The problem with the second approach is that the browser and the media player both use the services of HTTP. HTTP is designed to run over TCP. This is appropriate for retrieving the metafile, but not for retrieving the audio/video file. The reason is that TCP retransmits a lost or damaged segment, which is counter to the philosophy of streaming. We need to dismiss TCP and its error control; we need to use UDP. However, HTTP, which accesses the Web server, and the Web server itself are designed for TCP; we need another server, a media server.

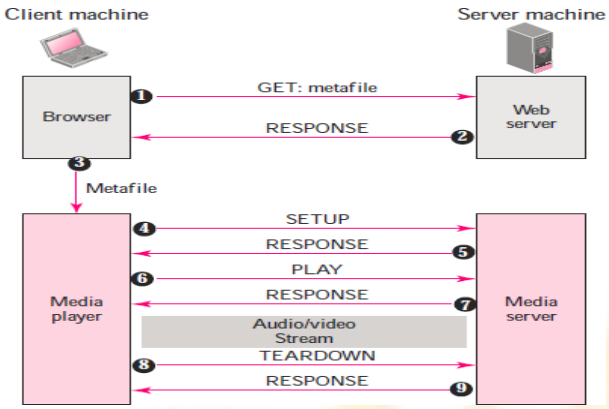
1. The HTTP client accesses the Web server using a GET message.



2. The information about the metafile comes in the response.
3. The metafile is passed to the media player.
4. The media player uses the URL in the metafile to access the media server to download the file.Downloading can take place by any protocol that uses UDP.
5. The media server responds.

Fourth Approach: Using a Media Server and RTSP

The **Real-Time Streaming Protocol (RTSP)** is a control protocol designed to add more functionalities to the streaming process. Using RTSP, we can control the playing of audio/video. Figure5 shows a media server and RTSP.



6. The HTTP client accesses the Web server using a GET message.
7. The information about the metafile comes in the response.
8. The metafile is passed to the media player.
9. The media player sends a SETUP message to create a connection with the media server.
10. The media server responds.
11. The media player sends a PLAY message to start playing (downloading).
12. The audio/video file is downloaded using another protocol that runs over UDP.
13. The connection is broken using the TEARDOWN message.
14. The media server responds.

2. STREAMING LIVE AUDIO/VIDEO

Streaming live audio/video is similar to the broadcasting of audio and video by radio and TV stations. Instead of broadcasting to the air, the stations broadcast through the Internet. There are several similarities between streaming stored audio/video and streaming live audio/video. They are both sensitive to delay; neither can accept retransmission. However, there is a difference. In the first application, the communication is unicast and on-demand. In the second, the communication is multicast and live. Live streaming is better suited to the multicast services of IP and the use of protocols such as UDP and RTP.

Examples: Internet Radio, Internet Television (ITV), Internet protocol television (IPTV)

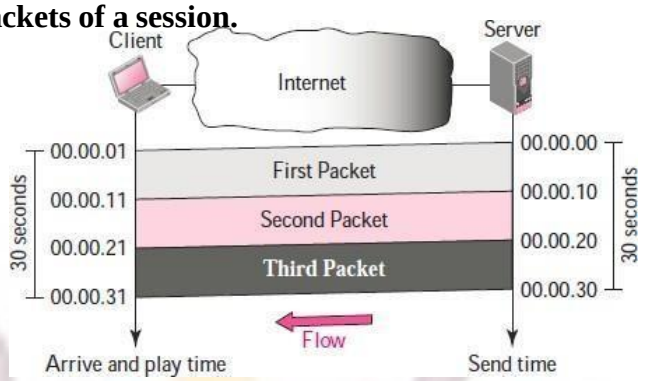
3. REAL-TIME INTERACTIVE AUDIO/VIDEO

In real-time interactive audio/video, people communicate with one another in real time. The Internet phone or voice over IP is an example of this type of application. Video conferencing is another example that allows people to communicate visually and orally.

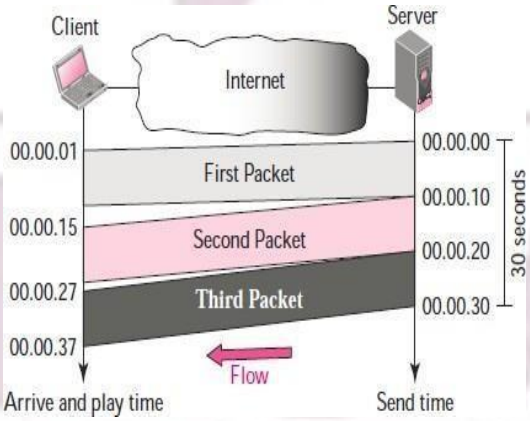
Before discussing the protocols used in this class of applications, we discuss some characteristics of real-time audio/video communication.

- **Time Relationship**

Real-time data on a packet-switched network **require the preservation of the time relationship between packets of a session.**



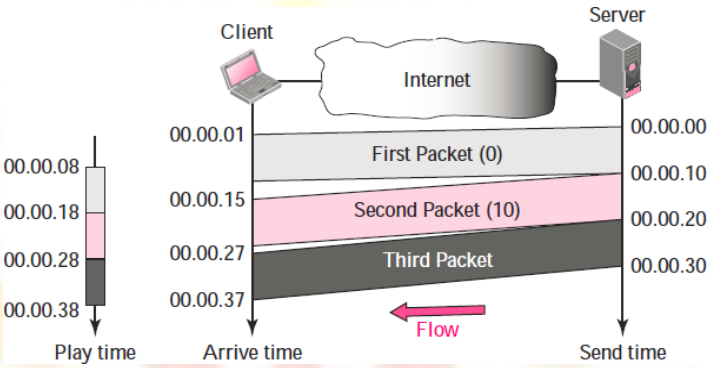
But what happens if the packets arrive with different delays? For example, the first packet arrives at 00:00:01 (1-s delay), the second arrives at 00:00:15 (5-s delay), and the third arrives at 00:00:27 (7-s delay). If the receiver starts playing the first packet at 00:00:01, it will finish at 00:00:11. However, the next packet has not yet arrived; it arrives 4 s later. There is a gap between the first and second packets and between the second and the third as the video is viewed at the remote site. This phenomenon is called



jitter. **Jitter is introduced in real-time data by the delay between packets.**

- **Timestamp**

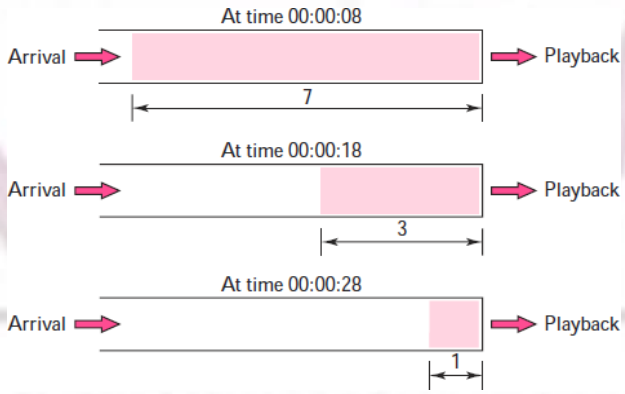
One solution to **jitter** is the use of a **timestamp. If each packet has a timestamp that shows the time it was produced relative to the first (or previous) packet**, **then the receiver can add this timeto the time at which it starts the playback.** Imagine the first packet in the previous example has a timestamp of 0, the second has a timestamp of 10, and the third a timestamp of 20. If the receiver starts playing back the first packet at 00:00:08, the second will be played at 00:00:18, and the third at 00:00:28. There are



no gaps between the packets.

- **Playback Buffer**

To be able **to separate** the **arrival time** from the **playback time**, we need a buffer to store the data until they are played back. The buffer is referred to as a **playback buffer.** In the previous example, the first bit of the first packet arrives at 00:00:01; the threshold is 7 s, and the playback time is 00:00:08. The threshold is measured in time units of data. The replay does not start until the time units of data are equal to the threshold value.



- **Ordering**

We need a ***sequence number*** for each packet. The timestamp alone cannot inform the receiver if a packet is lost.

- **Multicasting**

Multimedia play a primary role in audio and video conferencing. The traffic can be heavy, and the data are distributed using **multicasting** methods. Conferencing requires two-way communication between receivers and senders.

- **Mixing**

If there is more than one source that can send data at the same time (as in a video or audio conference), the traffic is made of multiple streams. **Mixing means combining several streams of traffic into one stream.**

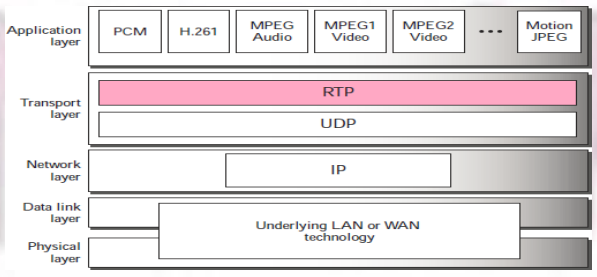
- ***Support from Transport Layer Protocol***

TCP is not suitable for interactive traffic. It has no provision for timestamping, and it does not support multicasting. However, it does provide ordering (sequence numbers). One feature of TCP that makes it particularly unsuitable for interactive traffic **is its error control mechanism**.

UDP is more suitable for interactive multimedia traffic. UDP supports multicasting and has no retransmission strategy. However, UDP has no provision for timestamping, sequencing, or mixing. A new transport protocol, **Real-Time Transport Protocol (RTP),** provides these missing features.

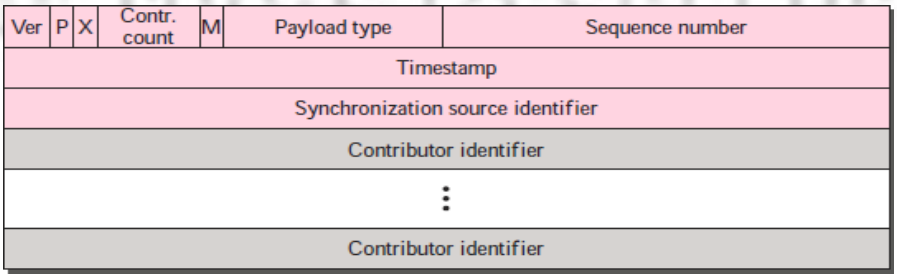
4. Real-time Transport Protocol (RTP)

Real-time Transport Protocol (RTP) is the protocol designed to handle real-time traffic on the Internet. RTP does not have a delivery mechanism (multicasting, port numbers, and so on); it must be used with UDP. RTP stands between UDP and the application program. The main contributions of RTP are timestamping, sequencing, and mixing facilities.



RTP Packet Format

The format is very simple and general enough to cover all real-time applications. An



application that needs more information adds it to the beginning of its payload. A description of each field follows.

- **Ver.** This 2-bit field defines the version number.
- **P.** This 1-bit field, if set to 1, indicates the presence of padding at the end of the packet. There is no paddingif the value of the P field is 0.
- **X.** This 1-bit field, if set to 1, indicates an extra extension header between the basic header and the data.There is no extra extension header if the value of this field is 0.
- **Contributor count.** This 4-bit field indicates the number of contributors. Note that we can have a maximumof 15 contributors because a 4-bit field only allows a number between 0 and 15.
- **M.** This 1-bit field is a marker used by the application to indicate, for example, the end of its data.
- **Payload type.** This 7-bit field indicates the type of the payload. Several payload types have been defined so far.
- **Sequence number.** This field is 16 bits in length. It is used to number the RTP packets. The sequence number of the first packet is chosen randomly; it is incremented by 1 for each subsequent packet. The sequence number is used by the receiver to detect lost or out of order packets.
- **Timestamp.** This is a 32-bit field that indicates the time relationship between packets.
- **Synchronization source identifier.** If there is only one source, this 32-bit field defines the source. However, if there are several sources, the mixer is the synchronization source and the other sources are contributors. The value of the source identifier is a random number chosen by the source. The protocol provides astrategy in case of conflict (two sources start with the same sequence number).
- **Contributor identifier.** Each of these 32-bit identifiers (a maximum of 15) defines a source. When there is more than one source in a session, the mixer is the synchronization source and the remaining sources arethe contributors.

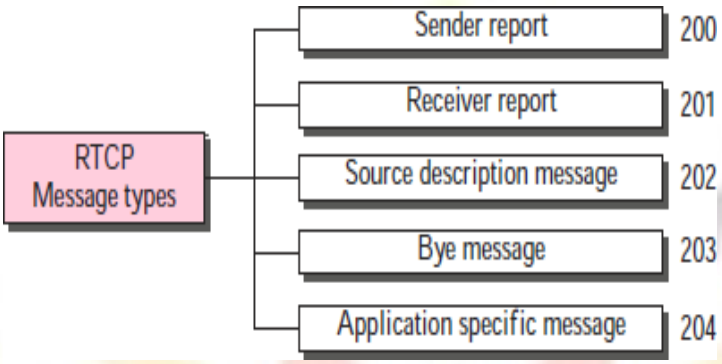
UDP Port

Although RTP is itself a transport layer protocol, the RTP packet is not encapsulated directly in an IP datagram. Instead, RTP is treated like an application program and is encapsulated in a UDP user datagram. However, unlike other application programs, **no well-known port is assigned to RTP**. The port can be selected on demand with only one restriction: The port number must be an even number. The next number (an odd number) is used by the companion of RTP, Real-Time Transport Control Protocol (RTCP).

5. Real-Time Transport Control Protocol (RTCP)

RTP allows only one type of message, one that carries data from the source to the destination. In many cases, there is a need for other messages in a session. **These**

messages control the flow and quality of data and allow the recipient to send feedback to the source or sources. **Real-Time Transport Control Protocol (RTCP)** is a protocol designed for this purpose. RTCP has five types of messages, as shown in the following Figure. The number next to each box defines the type of the message.



Types of messages

- Sender Report:
  The sender report is sent periodically by the active senders in a conference to report transmission and receptionstatistics for all RTP packets sent during the interval.
- Receiver Report:
  The receiver report is for passive participants, those that do not send RTP packets. The report informs the senderand other receivers about the quality of service.
- Source Description Message:
  The source periodically sends a source description message to give additional information about itself.
- Bye Message:
  A source sends a bye message to shut down a stream. It allows the source to announce that it is leaving theconference.
- Application-Specific Message
  The application-specific message is a packet for an application that wants to use new applications (not defined inthe standard). It allows the definition of a new message type.

UDP Port

RTCP, like RTP, does not use a well-known UDP port. It uses a temporary port. The UDP port chosen must be the number immediately following the UDP port selected for RTP, which makes it an odd-numbered port.

6. VOICE OVER IP (Real-time interactive audio/video application**)**

The idea is to use the Internet as a telephone network with some additional capabilities. Instead ofcommunicating over a circuit-switched network, this application allows communication between two parties over the packet-switched Internet. Two protocols have been designed to handle this type of communication: SIP(Session Initiation Protocol) and H.323.