COMPUTER NETWORKS

Communication:- Means to convey a message, a picture, speech or an idea that is recieved and understood clearly and correctly by the perion to whom it is conveyed.

Data communication:- containing message, pictures and voice has taken the importance.

Main Factors of data communication are:-

* The tranimission should take place without Error to the reciever.
* The cost of transmission over a large distance should be small.
* The message should be Safe & secure.

Network:- A network consists of two or more computers that are linked in order to share resources, Exchange files, or allow Electronic communication.

Data communication can be uni-directional (or) Bi-directional.

→ In uni-directional communication transfer of data is form source to destination only.

Eg:- Transmission centre and Television

→ In Bi-directional communication transfer of data is from source-destination & vice-versa.

Eg:- communication b/w computers

Goals of CN:-

→ To provide sharing of resources such as information
→ To provide inter-process communication among users.
→ It provides the n/w users with max. performance at min cost

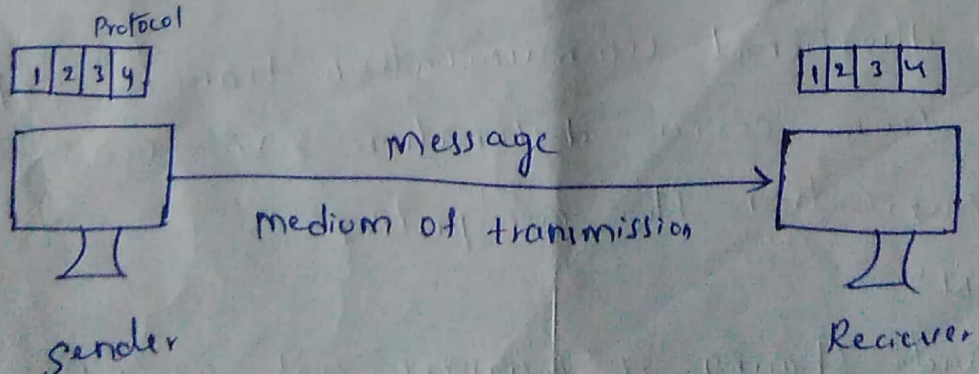
Applications of CN:-

1) Business Application:-
   * Data base resource
   * communication medium
   * Electronic commerce

2) Home Application:-
   * Internet access
   * personal communication
   * Entertainment
   * Electronic commerce

3) Mobile computers:
   * Military application
   * Airports
   * Banking
   * weather Reporting

Overview of Internet:- The Internet is the global system of interconnects computer Networks that uses the internet protocol suite to link device would wide while transfering the data over the Internet it consists of 5 components.



Message:- Data to be communicated

Sender:- It is the device that sends data

Reciever:- It recieves the information

Medium:- It is physical path through which message passes from sender to reciever the transmission medium can be twisted-pair cable, co-axial cable, fiber optic cable.

Protocol:- It is a set of goven rules that govern data communication.

Internet protocol:- A protocol specifies the exact format and meaning of each message. protocol also specifies the condition under which computer should send a given message and how a computer should respond when a message arrives.

For a communication to occur the entities must agree on a protocol.

A protocol defines what is communicated how it is communicated, and when it is communicated

main Element of protocol are:-

* Syntax
* Semantics
* Timing.

syntax:- The term syntax refers to the structure or format of the data, means order in which they are presented.

Ex:- simple protocol might Expect the first 8 bits of data to the adress of sender, second 8 bit to adress

of reciever and rest of the stream to be message itself.

Semantics:- The word semantics refers to the meaning of each section of bits

How a protocol pattren to be interpreted, and what action is to be taken based on interpretation

Ex:- Does an adress identify the route to be taken (or) final destination of message.

Timing:- The term timing refers to 2 charaiterstics

1) When data should be sent and how fast they can be sent

Ex:- If sender produce data at 100mbps but the reciever can process data only at 1mbps then the transmission will overload the reciever and some data will be lost.

Layering scenario:-

A protocol layer can be implemented in software and in hardware or in combination of both

To reduce their design complexity most networks are organized as a stack of layers (or) levels each one built upon the one below it.

The purpose of each layer is to offer certain services to the higher layers.

This concept is actualy a familiar one and used throughout computer science

Layer 'n' on one machine carriers a conversation with layer 'n' on another machine.

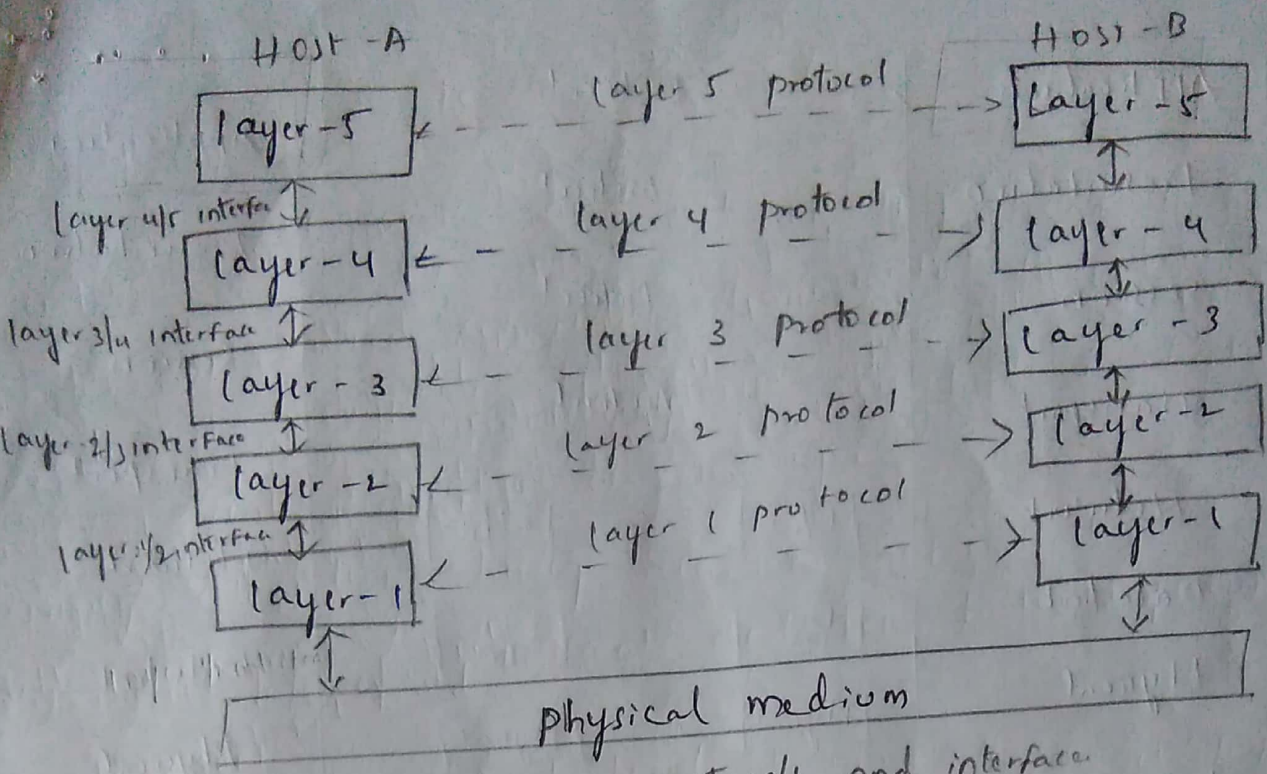
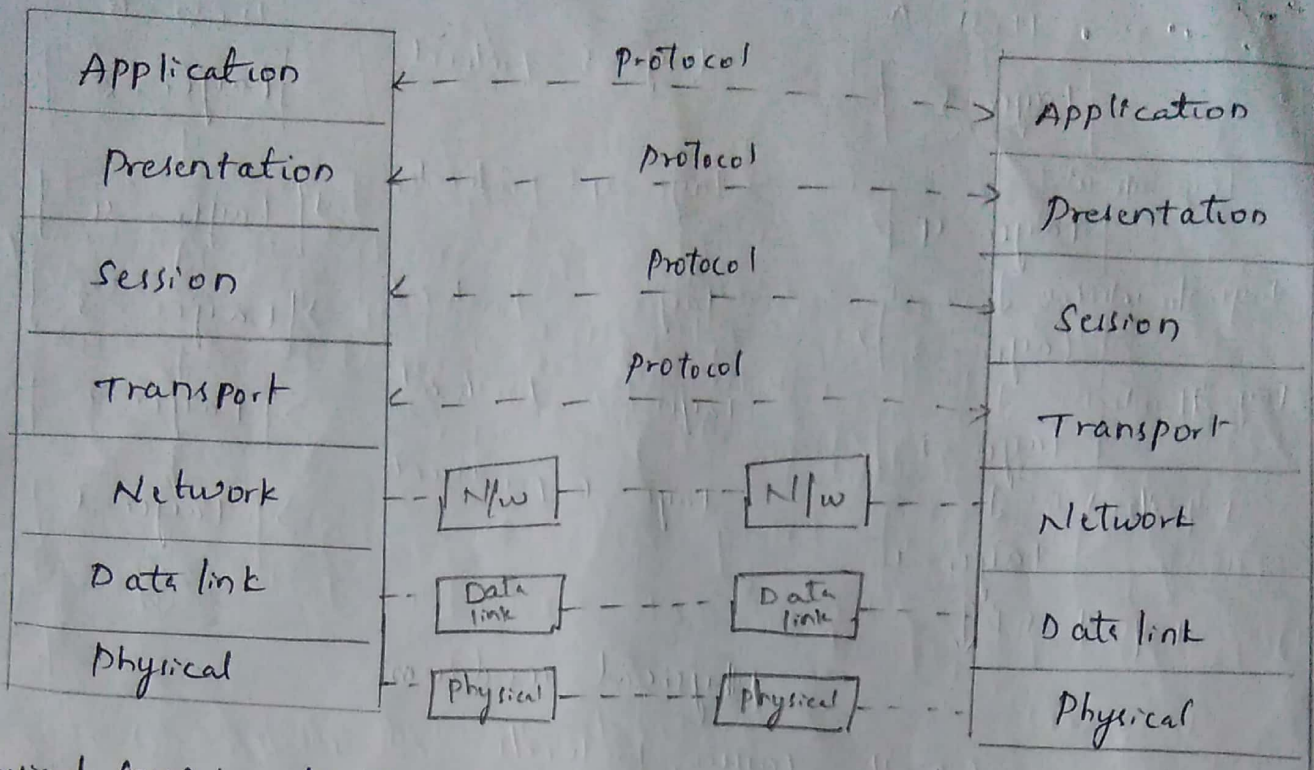


fig:- 1 layer, protocols and interface

corresponding layer on different machine are called peers
Each pair of adjacent layer is called interface it
defines which primitive operation and services the
lower layer offer to upper one.
A set of layers and protocols is called a
network architecture.

ISO - OSI Reference model:-

The international organization for standardization developed the open system interconnection reference model. It has 7- layers used to perform networking task.



Physical layer:- This layer transmits raw bits over a communication channels physical layer consider 4 factor. They are Electrical mechanical, procedural and functional attributes

Electrical attributes describe the voltage level and mechanical attributes describes the connectors & wires of the interface.

Functional attributes describe the function to be performed by the physical interface & the procedural attributes describe the sequence of events required to Effect the actual data transfer

Data link layer:-

It is responsible for the transfer of data over the channels. It groups of 0's and 1's into frames.

A frame is a series of bits that forms a unit of data it detects and correct the transmission Error using Error correction method. It also provides data flow control to Ensure that the data terminal Equipment (DTE) does not become over burdned. identifies device on n/w

Network layers:-

It specifies the intra-network operations & different types of addressing & routing services

logical & service addresing are provided from n/w layer it also provides switching controls & terminal connections

Transport layer:-

It is responsible for reliable end to end data transfer It performs the service of sending and receiving of data to session layer

It also provide flow control, sequence numbering message acknowledgement.

Session Layer:- It adds mechanisms to establish, maintain synchronize and manage communication b/w n/w entities.

This layer has specific primitives & protocol data unit.

Presentation layer:- It is responsible for data compression, data Expansion, data encryption, data decryption.

Application layer:-

It supports end user function like login, password file transfer It supports the virtual terminal and virtual file concept.

It contains service Elements to support application process such as job management & business data exchang

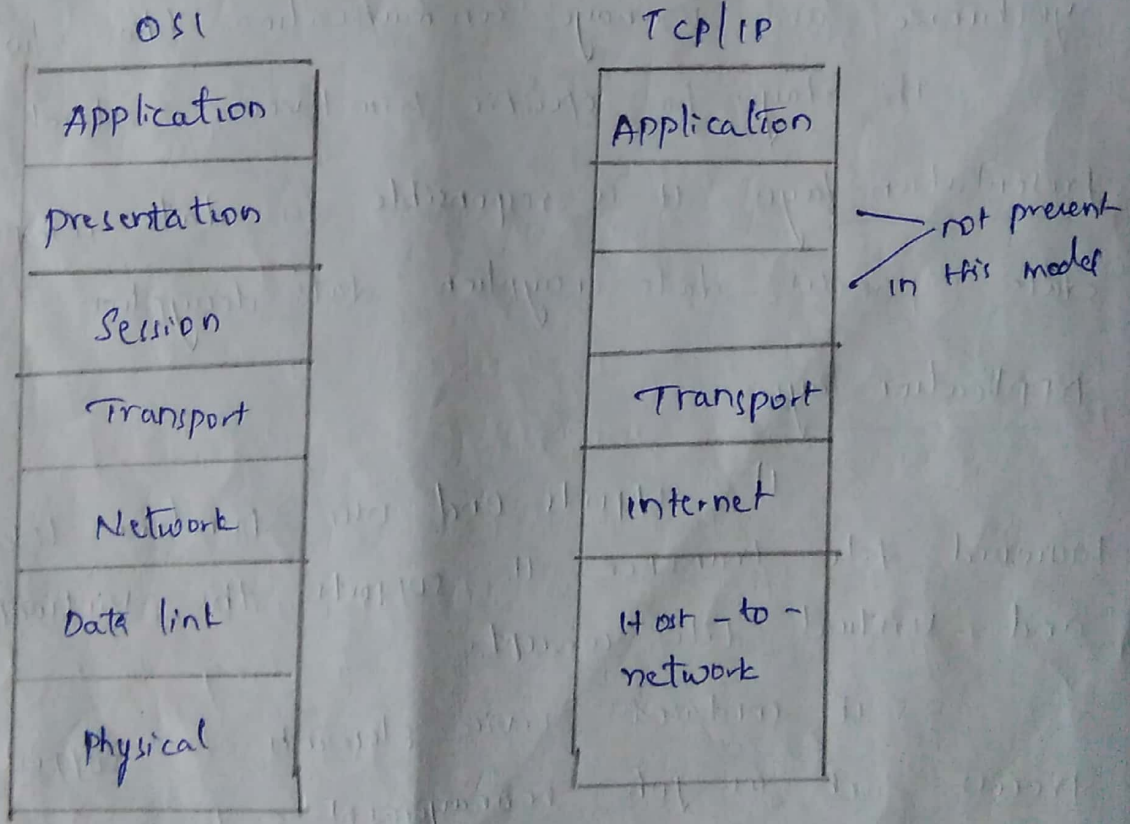
when data is sending, each layer of OSI adds its own header to data Except physical layer.

TCP/IP Reference model:-

Now let us turn from OSI reference model to the reference model used in all wide area networks, ARPANET and its successor, the world wide internet.

When satellite & radio n/w were added later, the existing protocols had trouble interworking with them. So new reference architecture was needed.

Thus the ability to connect multiple n/w in a seamless way was one of the major design goal. The architecture later became known as the TCP/IP reference model.



Internet layer:- Internet layer is equivalent to the n/w layer. The application layer is roughly used in

All these requirment led to choice of Packet switching n/w based on a connectionless internetwork layer. This layer is called internet layer.

The internet layer defines an official Packet format and protocol called IP (Internet protocol)

This layer is to deliver IP packets, where they are supposed to go. Packet routing is the major issue here as is to avoiding congestion. For this reason TCP/IP internet layer is similar in functionality to OSI n/w layer.

Transport layer:

The layer above the internet layer in TCP/IP model is now called as Transport layer. It is designed to allow peer entities on source to destination, a end-end to transport protocols have defined here.

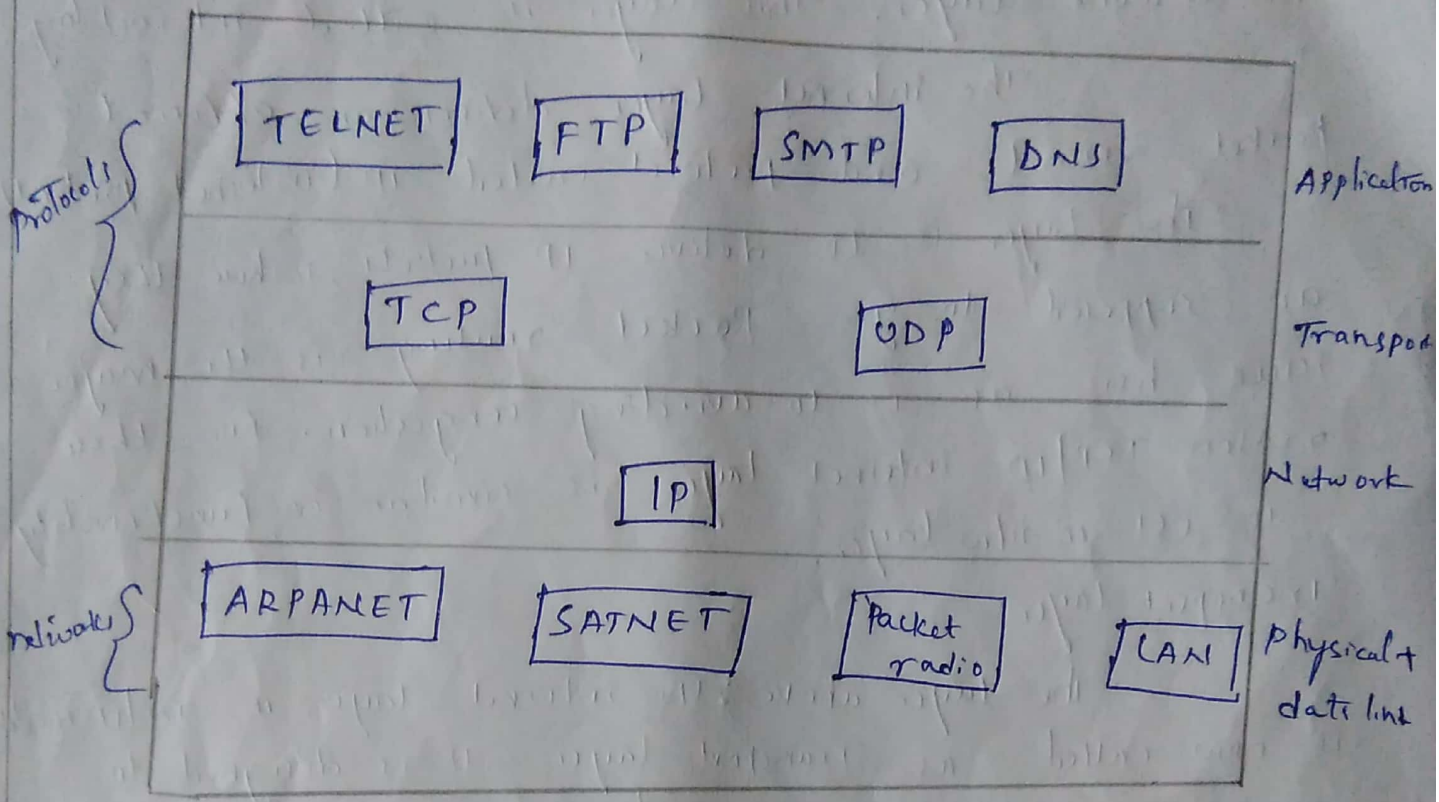
* TCP - Transmission control protocol = connection oriend protocol
* UDP - User datagram protocol = connectionless protocol

TCP:- allows a byte stream orginating on one machine to be delivered without error on any other machine in the internet

It fragments the incoming byte stream into discrete message & passes each one to internet layer. At destination receiving TCP process reassembles the received message into output stream

UDP:- is an ~~xxx~~ro un-reliable connection less protocol for applications do not want TCP's sequencing (or) flow control it is widely used for one shot, client-server-type in which prompt delivery is more important than accurate delivery.

The relation of IP, TCP, UDP is as shown in fig.



Application layer:- (TCP/IP does not have session or presentation layer. on top of the transport layer is application layer. It contains all the higher-level protocols. The early one includ virtual terminal (TELNET), FTP, SMTP. Virtual terminal allows user on one machine to log onto distant machine

FTP:- provides a way to move data efficiently from one machine to another.

DNS:- for mapping host names onto their n/w adresses.

Host to Network layer:- in this host has to connect to network using some protocol so it can send IP packet to it. this protocol is not defined & varies from host-host and Network to Network.

Comparison of OSI and TCP/IP reference model:-

OSI	TCP/IP
1) It is having 7 layer	1) It is having 4 layer
2) It has strict boundaries	2) It does not have strict boundries
3) It developed model and then protocol	3) It developed protocol then model
4) In network layer, OSI supports both connection less and connection-oriented communication	4) In network layer it supports connection less only
5) It is protocol independent	5) It is protocol dependent
6) It provides clear services, interfaces & protocols	6) It will not clearly distinguish b/w services, interfaces & protocols

Internet history and standard adminstration:-

Internet has revolutionized many aspects of our daily lives. It is a communication system that brought a wealth of information to our fingertips.

Brief history:-

In the mid-1960's main frame computer in research organization were standard device. The Advanced Research Project agency (ARPA) in the Department of Defence (DOD) was intrested in finding a way to connect computers so that the researchers they funded could share their findings, there by reducing cost & duplicaton effort.

In 1967, Association of computing machinery (ACM) meeting. ARPA presented ideas for ARPANET, a small n/w of connected computers. The idea was each host computer would attched to a specialized computer called IMP (Interface message Processor), the IMP's in turn connected to one another.

In 1969, ARPANET was a reality. Four nodes at university of California at los angeles (UCLA), university of Utah, were connected via the IMPs to form a n/w software called Network Control Protocol (NCP) provides communication b/w the hosts.

Internet Today:- Internet has come long way since 1960's

i) International Internet service providers:-

At the top of hierarchy are the international service provider that connect nations togather.

ii) National Internet service providers:-

They are backbone n/w maintained by specialized companies some of the most well known are Sprintlink, PSINET, UUNET Technologies, AGIS, and internet mel.

iii) Regional internet service providers:-

These are smaller ISP's connected to regional ISPs one or more national ISP's. They are third level of hirerchy.

iv) local internet service providers:

They provide direct service to end users. local ISP's are connected to regional ISP's (or) directly to national ISP's.

most users are connected to local ISP's.

Guided Transmission media:-

The purpose of physical layer is to transport a raw bit stream from one machine to another. Media are roughly grouped into guided media, such as copper wire, fiber optics

1) **Magnetic media:-** one of the most common way to transport data from one computer to another is to write them onto magnetic tape (or) Removable disk (Eg:- recordable DVD's). physically transport the tape or disk to the destination machine and read them back in again.

Although this method is not so sophisticated as using a geosynchronous communication satelite. It is often more cost effective.

Eg:- For a bank with many gigabytes of data to be backed up daily on second machine, it is likely that no other transmission technology can even begin to approach magnetic tapes for performance.

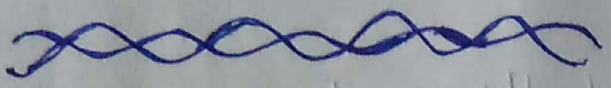
2) **Twisted pair:-**

A Twisted pair consists of two insulated copper wire, typically 1mm thick. The wires are twisted together in a helical form just like DNA molecule. Twisting is done because two parallel wires constitute a fine antenna. when the wires are twisted the waves from different twists cancel out, so the wire radiates less effectively

*) Most common type of application of twisted pair is telephone system. they can run several kilometers without amplification.

* twisted pairs can be used for transmitting either analog or digital signals

* category 3 twisted pair consist of two insulated wires gently twisted together



∴ upto - 16MHz (10MBPS)
3-4 twists per feet

Fig:- category 3 UTP

* category 5 twisted pair having more twists per centimeter

fig:- category 5 UTP.

∴ (100MHz) → 10MBPS
3-4 twists per inch

Coaxial cables:-

co-axial cable has better shielding than twisted pairs, so it can span longer distance at higher speed. Two kinds of co-axial cables widely used

i) 50-ohm cable
ii) 75-ohm cable

50-ohm cable commonly used for digital transmission
75-ohm cable commonly used for analog tranmission

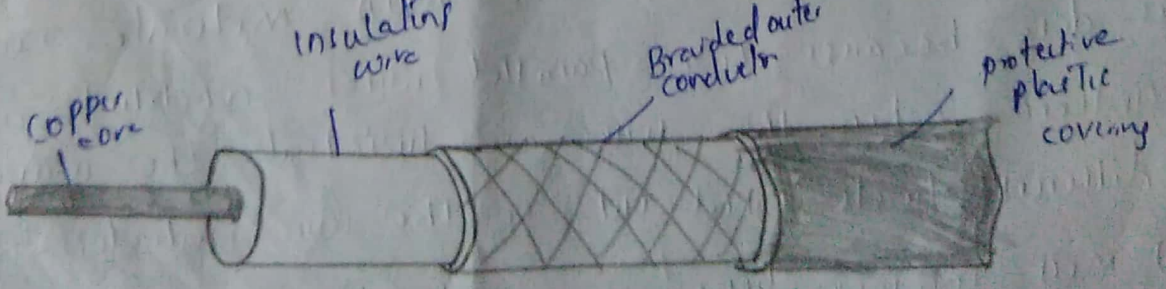


fig:- co-axial cable

Co-axial cable consists of stiff copper wire as the core, surrounded by 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.

Co-axial cables used To be widely used within telephone system for long-distance lines but have now replaced by fiber optics on long-haul routes

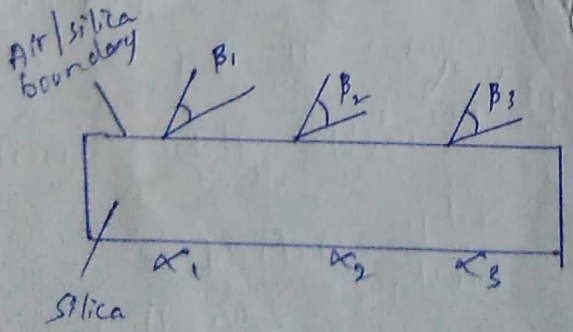
Fiber optics:-

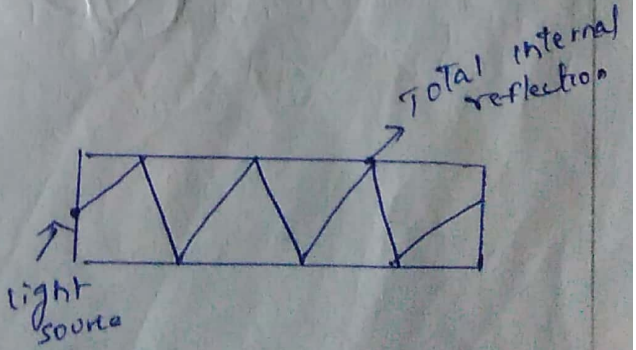
An optical transmission system has three key components: light source, Transmission medium, detector

light source:- A pulse of light indicates a '1' bit and the absence of light indicates '0' bit

Transmission medium:- It is an ultra-thin fiber of glass

detector:- It generates an electrical pulse when light falls on it. By attaching a light source to one end of an optical fiber and detector to other, we have uni-directional data transmission system that accepts an Electrical signal, converts and transmit it by light pulses, and then reconvert the o/p to an Electrical signal at receiving end.

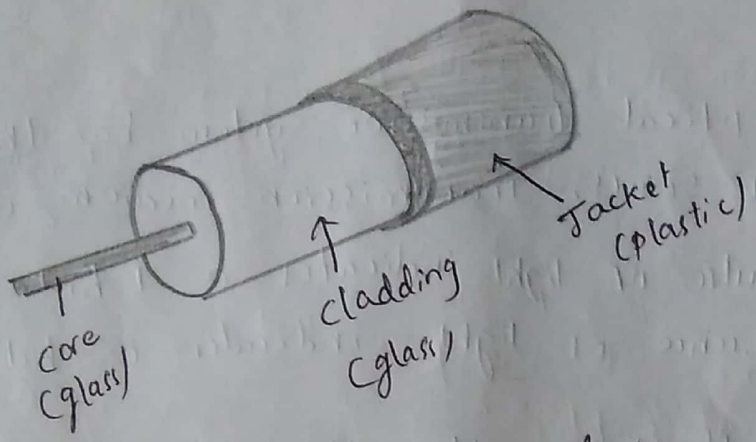




Fiber cables:-

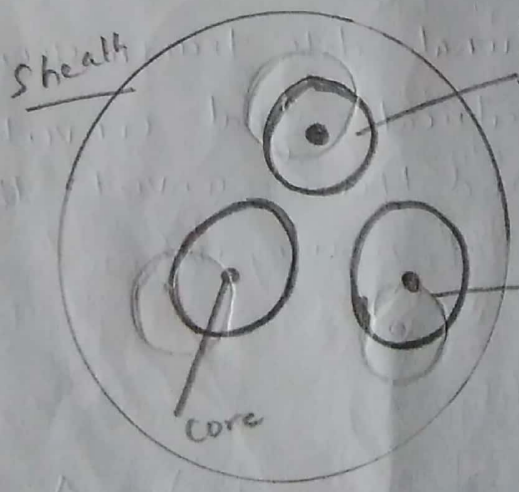
Fiber optic cables are similar to co-ax, except except without braid.

* Single fiber view:- At the centre is the glass core through which the light propogates. In multimode fibers, the core is typically 50 microns in diameter, about the thickness of a human hair. In single mode fiber core is 8 to 10 microns



Sheath with three fibers: End view

Fibers are typically grouped in bundles, protected by an outer sheath.



Wireless Transmission:-

Some people belive that the future holds only two kinds of communication

*) Fiber
* Wireless

All fined computers, telephones, faxes use fiber, all mobile one will use wireless

a) Electro magnetic spectrum:-

When Electron move, they create Electromagnetic waves that can propogate through space. in vacuum Electromagnetic waves travel at the same speed no matter what their frequency. This speed usually called the 'speed of light'. 'c' is approximately 3×10^8 m/sec, or about 1 foot (30 cm) per nanosecond.

The no. of oscillations per second of a wave is called its frequency 'f', and is measured in Hz The distance b/w two consecutive maxima is called wavelength. which is universally designated by the greek letter λ (lambda).

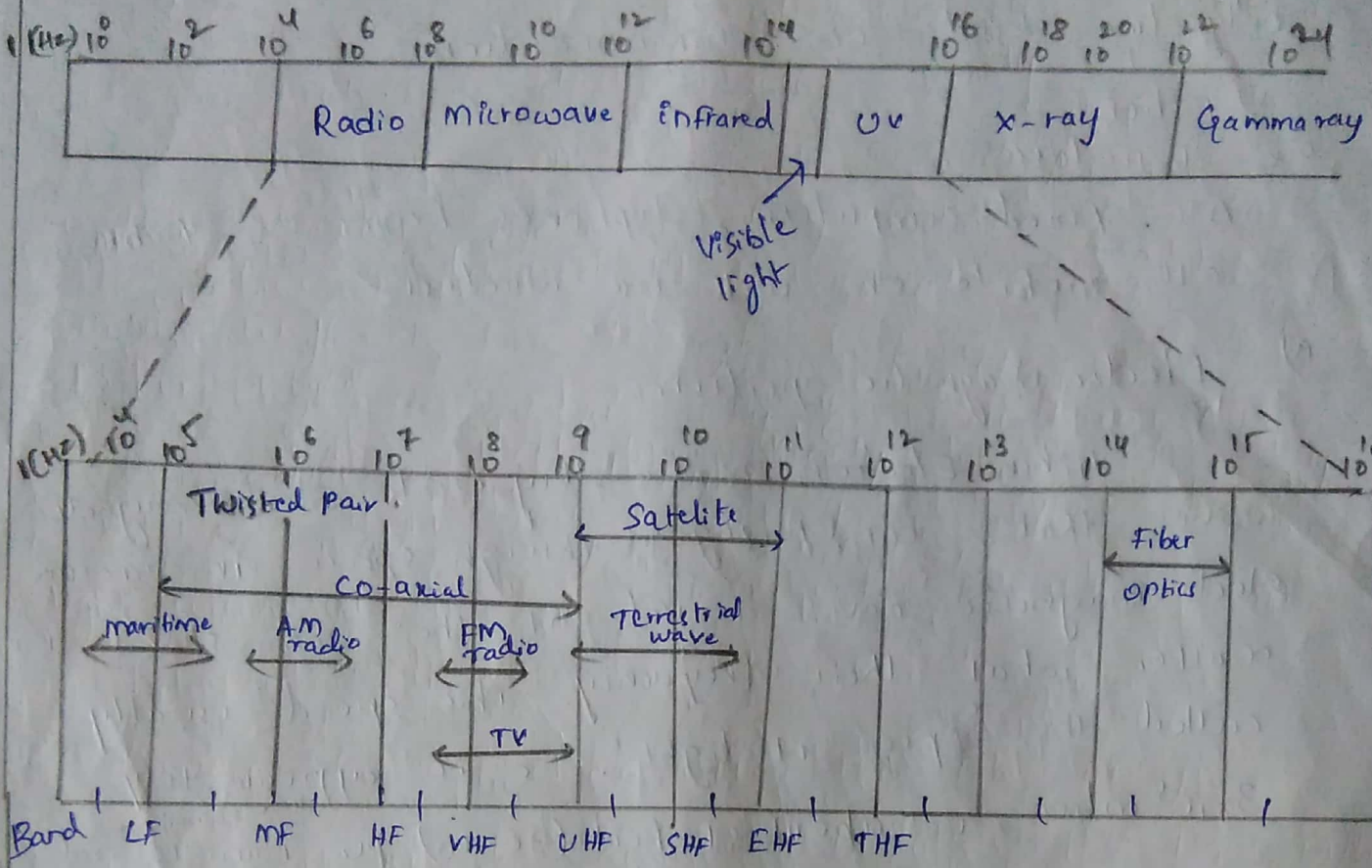
The fundamental relation b/w f, λ, c is

$$\lambda f = c$$

The Electromagnetic spectrum as shown in fig below The radio, microwave, infrared, and visible light portion of spectrum can all be used for transmitting information by modulating the amplitude frequency, or phase of waves.

UV rays, X-rays, gamma rays would even better.

due to their higher frequency's. and are dangerous to living things.



LF band goes from 1 km to 10 km (approximately 30 kHz - 300 k

The term LF, MF, HF refers to low, medium, high frequency. Higher bands later named by Very, ultra, super, extremly, Tremendously high frequency bands.

The amount of information that an Electromagnetic wave can carry is related to its bandwidth. So co-axial cable with 750 MHz bandwidth can carry several gigabits/sec. This is reason why networking people like fiber optics

b) 'Radio transmission':-

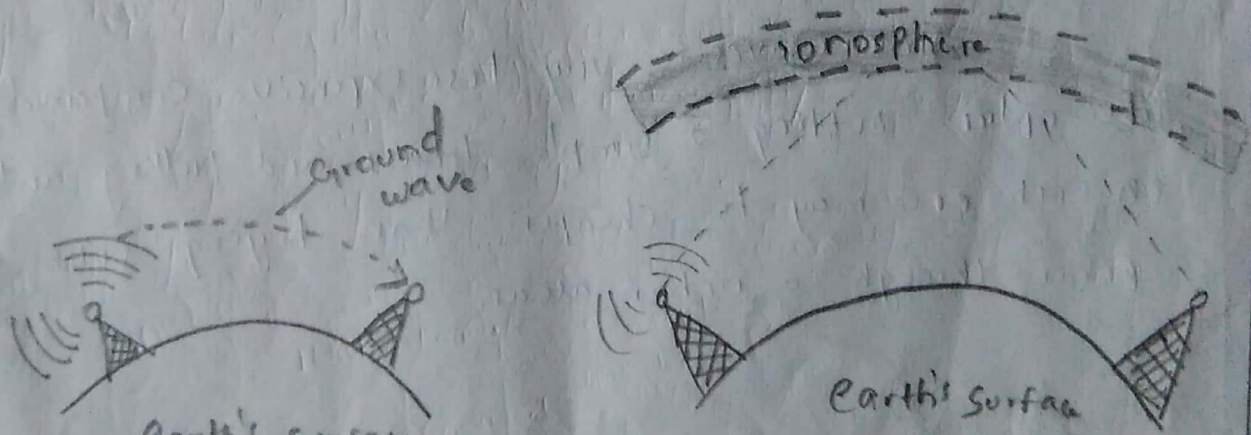
Radio waves are easy to generate; can travel long distance and can penetrate buildings easily, so they are widely used for communication.

Radio waves are omni-directional, meaning that they travel in all directions from the source.

In VLF, LF, MF bands, radio waves follow the ground. These waves can be detected for 1000kms at low frequencies and less at higher ones.

In the HF and VHF bands the ground waves tends to be absorbed by the Earth, However the waves that reach the Inosphere, a layer of charged particles circling the Earth at height of 100 to 500km, are refracted by it and sent back to Earth.

The military also communicate on the HF and VHF bands.



(a) fig: b

fig(a):- VLF, LF and MF bands, radio waves follows the curvature of earth.

fig(b):- in the HF band, they bounce off the inosphere.

9) Micro-wave Transmission:

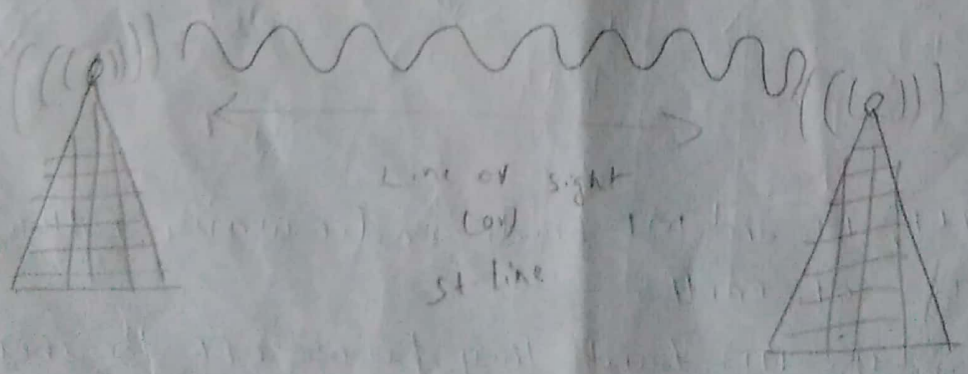
Above 100 MHz, the wave travel is nearly straight line and can therfore be narowly focused. concentrating all the energy into a small beam by means of a parabolic antenna (like TV dish). give higher signal-noise ratio. but tx and Rx antenna must be accurately aligned with each other.

unlike radio waves at lower frequencies, microwaves donot pass through building well. even though the beam may be well focused at transmitter there is still some divergence in space. some waves may be refracted off.

microwave communication is widely used for long distance telephone communication, mobile phones, television distribution.

Before fiber optics for decades these microwaves formed for long-distance telephone transmission system.

microwaves is very less expensive compared to fiber optics. putting 2 simple towers and putting antenna on each one may be cheaper than buying 50km of fiber through a urban areas.



d) Infrared and millimeter waves:-

unguided infrared & millimeter waves are widely used for short-range communication. The remote controls used on TV, VCR's and stereos all use infrared communication. They are relatively directional, cheap and easy to build.

Major drawback is they do not pass through solid object

e) light wave Transmission:-

unguided optical signaling has been in use for centuries. But a modern application is to connect LAN in 2 buildings via laser mounted on rooftops. This scheme offers very high bandwidth & low cost. It is also relatively easy to install.

A disadvantage is that laser cannot penetrate rain (or) thick fog, but they work well in sunny days.

Design issues of Data link layer:-

Service interface to the n/w layer, framing control, error detection & error control, frame formatting sequencing

Service interface to the n/w layer:-

Data link layer provide services to the n/w layer The main service is transferring data from the n/w layer on the source to n/w layer on destination can be done by data link control protocol

Un-acknowledge connectionless service, Acknowledge connectionless service, Acknowledge connection-oriented services are provided by data link layer to the n/w layer

Framing:-

Data link layer break the stream into discrete frames and computes the checksum for each frame, at destination the checksum ~~reco~~ recomputed.

The breaking of bit stream by inserting spaces or time gaps is called framing, it is difficult to count on timing & mark the start & end of each frame

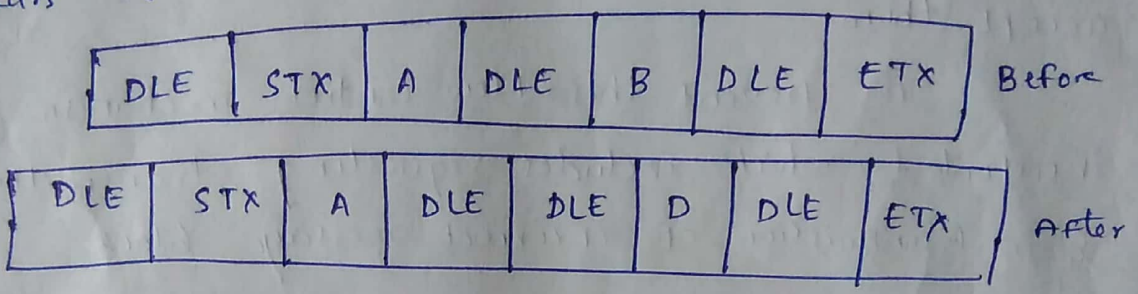
Simple methods used for framing are:-

1) character count
2) starting & ending characters, with character stuffing
3) starting & ending flags, with bit stuffing.

Character count:- This method uses a field in the header of frame to specify the no. of characters in the frame, Such framing for 4 frames of sizes 5, 5, 8, 8 characters

A dis-advantage with this framing is that the count can be garbled by transmission error.

Character stuffing:- The special character Data link escape (DLE) is stuffed infront of control character when it appears as a part of data.



Bit stuffing:- in bit stuffing a specific bit is stuffed into the outgoing character stream

Each frame begins & ends with special bit pattren, 01111110 called flag byte, when 5 consecutive 1's are encountered it stuff as '0'.

Data - 0110 - 1111111111111111 0010

After stuffing - 0110 - 11111011111011111010010

Error control:- To ensure the proper sequencing and safe delivery of frames at the destination, an acknowledgment should be sent by the destination network.

Reciever sends a fram. contains +ve or -ve acknowldge about incoming frame.

If sender recieves +ve ack frame has arrived -ve means frame has not arrived & the frame is to re-transmitted

TO reduce the error control time is introduced & sequence number to the outgoing frames are maintained

Flow control:- when the sender is running on fast machine & reciever is on slow machine the transmitter will transmit frames faster than the reciever can accept them.

To prevent this flow control mechanism is incorporated which includes requesting transmitter & re-transmission of incorrect message block.

Autometic Repeat, Request is the most common re-transmission technique, retransmission of data in 3 cases

i) Damaged Frames
ii) lost Frames
iii) lOst Ack

cyclic redundancy check (CRC):-

A CRC is an error-detecting code commonly used in digital n/w's & storage devices to detect accidental changes to raw data

The theory of CRC & checksums is developed by using algebra & polynomials

Polynomial codes are used with frames transmissio schemes. A single set of check digit is generated fo

each frame transmitted based on the contents of the frame and is appended by the transmitter to the tail of the frame, the reciever then performs a similar computation on a complete frame & check digits

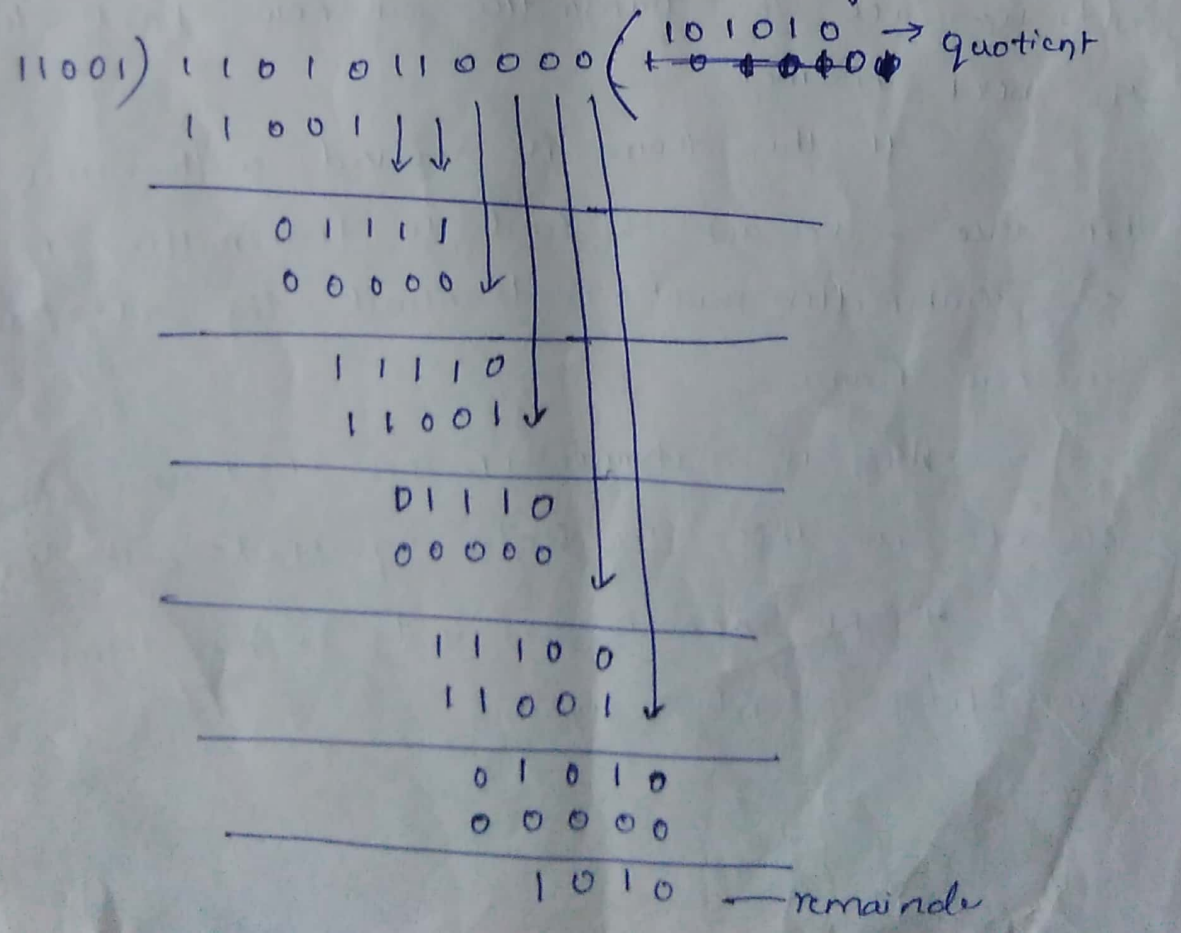
if no errors have been induced answer is found if different answer is found, it indicates error.

CRC remainder is appended to the data unit, so that it is exactly divisble by a second number, if any remainder is generated, it indicates error in the data and is rejected.

Ex:- suppose we want to send the data 1101011 & generator polynomial is $G(x) = x^4+x^3+1$

$G(x) = x^4+x^3+1 = 11001$

Actual data = 1101011 after appending = 11010110000



Data link layer protocols:-

i) simplex protocol

ii) stop & wait protocol

Simplex: In this there is no flow control & error control, it is a uni-directional protocol i,e from sender to recieved

The transmitting & recieving hosts are always ready processing time can be ignored, infinite buffer space available. No sequence number (or) ack are used here.

stop & wait protocol:-

The sender sends one frame & Then waits for an ack before proceeding are called stop & wait

Transmitter sends a frame over the commonication line & then wait for +ve (or) -ve ack from the recieved

If no-error occurs in the transmission Reciever sends +ve ack, the transmitter can now start to send the next frame!

If the frame is Recieved with errors, then ~~+ve~~ - ve ack is send to tranimitter, In This case transmitter must re-transmit the old packets in new frame.

There is a chance of loss of frames/ack, to account for this, The sender equipped with timer.

If no ACK is Recieved when timer expires same frame sends again.

Sliding window protocol:-

It is an error correction method. To increase the data rate, this method allows the sender to transmit a specific number of packets in continuous mode without recieving +ve ack for these packets.

The no. of packets that can be transmitted in this way known as window size.

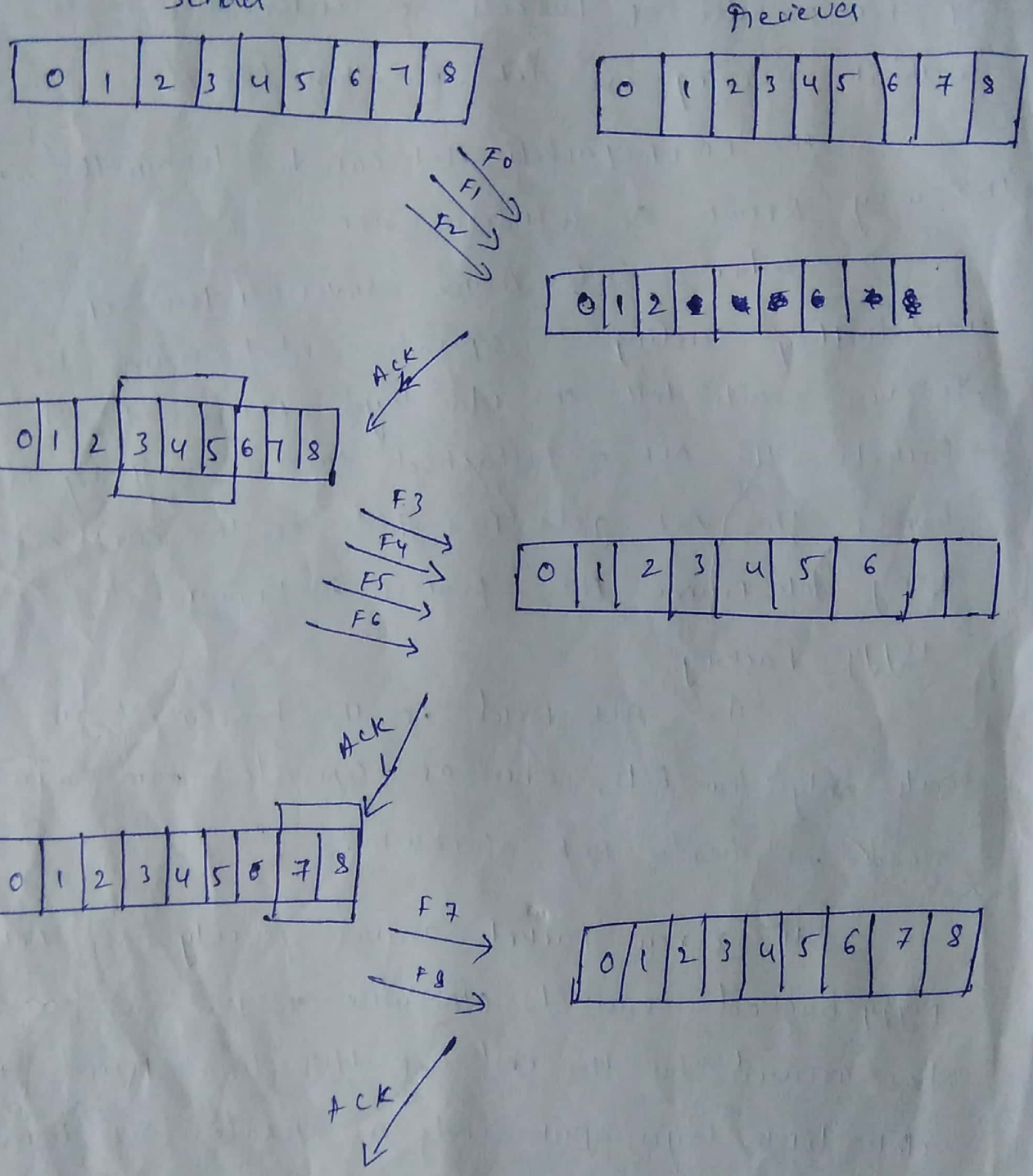
When a data frame arrives, instead of immediatley sending a seperate control frame, the reciever waits till the n/w layer passes it the next packet. The Ack is attached to the outgoing data frames, the Ack gets free ride on the next outgoing data frame this process is known as piggy backing.

The Ack field in the header frame costs only few bits, where as seperate frame would need a header, Ack, checksum.

If a new packet arrives quickly, the Ack is piggy backed onto it, otherwise if no new packet has arrived by the end of this time period, the data link layer just sends a seperate Ack frame.

Each portion of the transmission is assigned a unique consecutive sequence number & the reciever uses the no's to place recieved packets in the correct order discarding duplicate packets and

identifying missing ones. The problem with this is that there is no limit on the size of sequence numbers that can be required.



Unit-II

Multiple Access Protocol:-

Many algorithms for allocating a multiple access channel are known in following section.

ALOHA:- In 1970's Norman Abramson at the university of Hawai devised a new method to solve the channel allocation problem.

Although his work called 'ALOHA' system, used ground-based radio broadcasting, the basic idea is applicable to any system

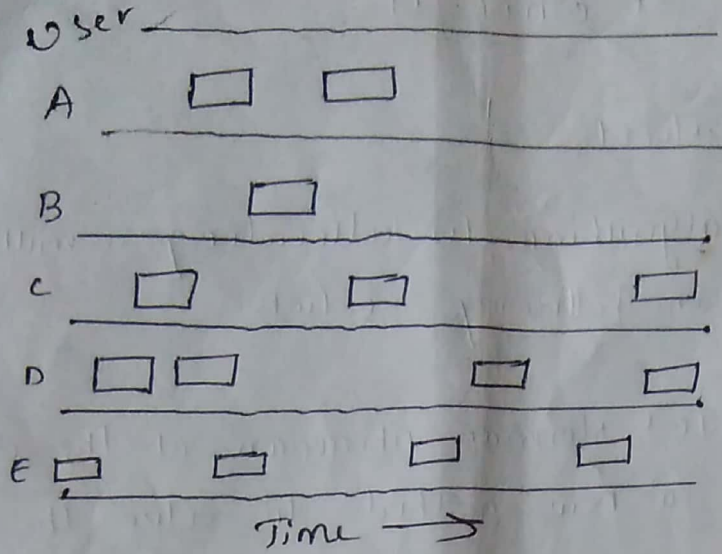
Two versions of ALOHA here are:-

i) Pure ALOHA
ii) Slotted ALOHA

i) **Pure ALOHA:-** Pure ALOHA does not require global time synchronization. let users transmit whenever they have data to be sent. There will be collision of course, & colliding frames will be damaged. However due to feedback a sender can always find out wheather it's frame was destroyed by listening to the channel.

If the frame was destroyed the sender just waits a random amount of time & sends it again.

A sketch of ~~frames~~ generation in an ALOHA system. we have made frames all the same length because the throughput of ALOHA is maximized by having uniform frame size rather than variable length frames.



Whenever two frames try to occupy the channel at the same time there will be collision and both will be garbled. if the first bit of new frame overlaps with just the last bit of frame almost finished. both frames will be destroyed and have to be re-transmitted later.

let the probability of k transmission attempts per frame time. With Mean 'G' per frame

i) Clearly $G \geq N$ At low load (i.e $N \approx 0$) there will be few collisions, and few retransmission. so $G \approx N$.

ii) At high load, they do there will be many collision so $G > N$. under all loads. the throughput 'S' is just the offered load 'G', times the probability P_0

$\therefore S = GP_0$ where P_0 is probability that a frame does not suffer a collision.

probability that 'k' frames are generated given by poisson distribution

$$Pr[k] = \frac{G^k e^{-G}}{k!}$$

The expected number of transmission, E per carriage return typed is then

$$E = \sum_{k=1}^{\infty} k P_k = \sum_{k=1}^{\infty} k e^{-G}(1-e^{-G})^{k-1} = e^{G}.$$

As a result of Exponential dependence of E upon G, small increase in channel load can drastically reduce its performance.

Carries sense multiple Acess protocols:- CSMA

Protocol in which

With slotted ALOHA the best channel utilization that can be achieved is 1/e. This is hardly surprising. since with station transmitting at will, without paying attention to what other stations are doing, they are bound to many collisions, in LAN however it is possible for station to detect what other stations are doing. These nlw can achieve a much better utilization than 1/e.

Protocols in which stations listen for carrier (i,e transmission) and act accordingly are called "Carrier sense protocols".

Two types of CSMA :-

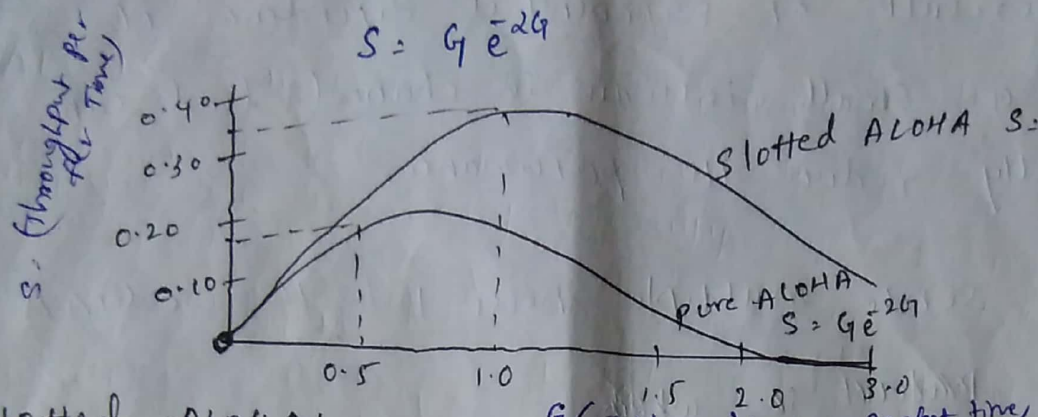
i) Persistent CSMA
ii) Non persistent CSMA
iii) P- Persistent CSMA

Probability of zero Frame is e^{-G}.

Mean number of Frames is $2G$

∴ The probability for entire vulnerable period is given by $P_0 = e^{-2G}$ using $S = GP_0$ we get

$$S = Ge^{-2G}$$



Slotted ALOHA:-

In 1972 Roberts published a method for doubling the capacity of ALOHA system. It requires the users to agree to on slot boundaries.

Roberts method is known as Slotted ALOHA. a computer is not permitted to send whenever a carriage return is typed instead it is required to wait for the begning of the next slot. Thus a continuous Pure ALOHA is turned into discrete one.

∴ The probability of no other traffic during the same slot as our test frame is e^{-G} lead to

$$S = Ge^{-G}$$

Slotted ALOHA peaks at $G = 1$, with throughput of $S = 1/e$ (or) about 0.368, twice that of pure ALOHA.

The probability of collision is $1 - e^{-G}$.

$$\therefore P_k = e^{-G}(1 - e^{-G})^{k-1}$$ [∵ k-1 collisions for one success].

i) 1- Persistent:- The 1-persistent method is simple and straight forward. in this method after the station find the line idle, it sends its frame immediatley (with probability 1). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediatley.

ii) non Persistent method:- in this method, a station that has a frame to send sense the line. if the line is idle it sends immediately, if the line is not idle, it waits a random amount of time and then sense the line again.

* it reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.

* This method reduces the effiency of the n/w because the medium remains idle when there may be stations with frames to send.

iii) P- persistent:- it is used if the channel has time slot with a slot duration equal to or greater than the maximum propogation time.

*) it reduces the chance of collision and improve efficency.

When station becomes ready to send, it senses the channel, if it is idle, it transmit with Probability p, with a probability $q = 1-p$. defers until next slot.

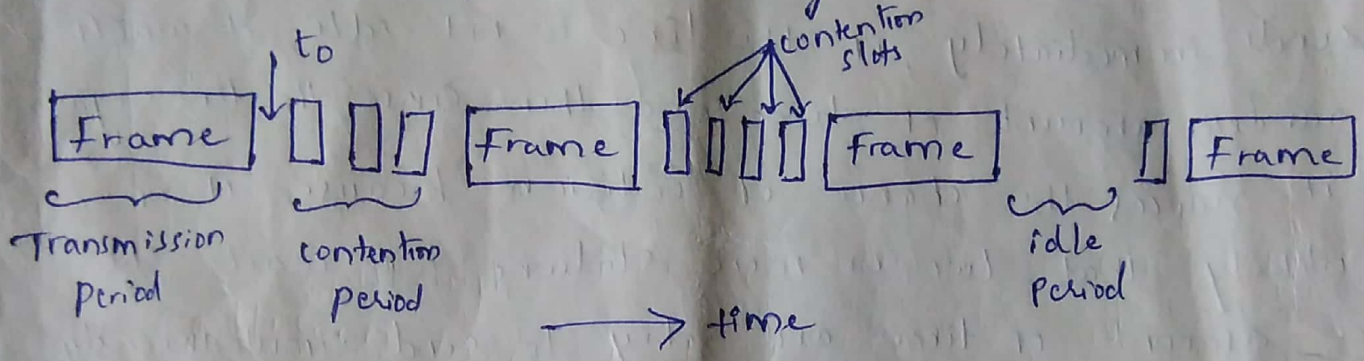
This process is repeated until either the frame has been transmitted or another station has begun transmitting.

CSMA with Collision Detection:- (CSMA+CD)

If 2 stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision immediatley. They stop transmitting as soon as collision is detected.

Quickly terminating damaged frames save time and bandwidth.

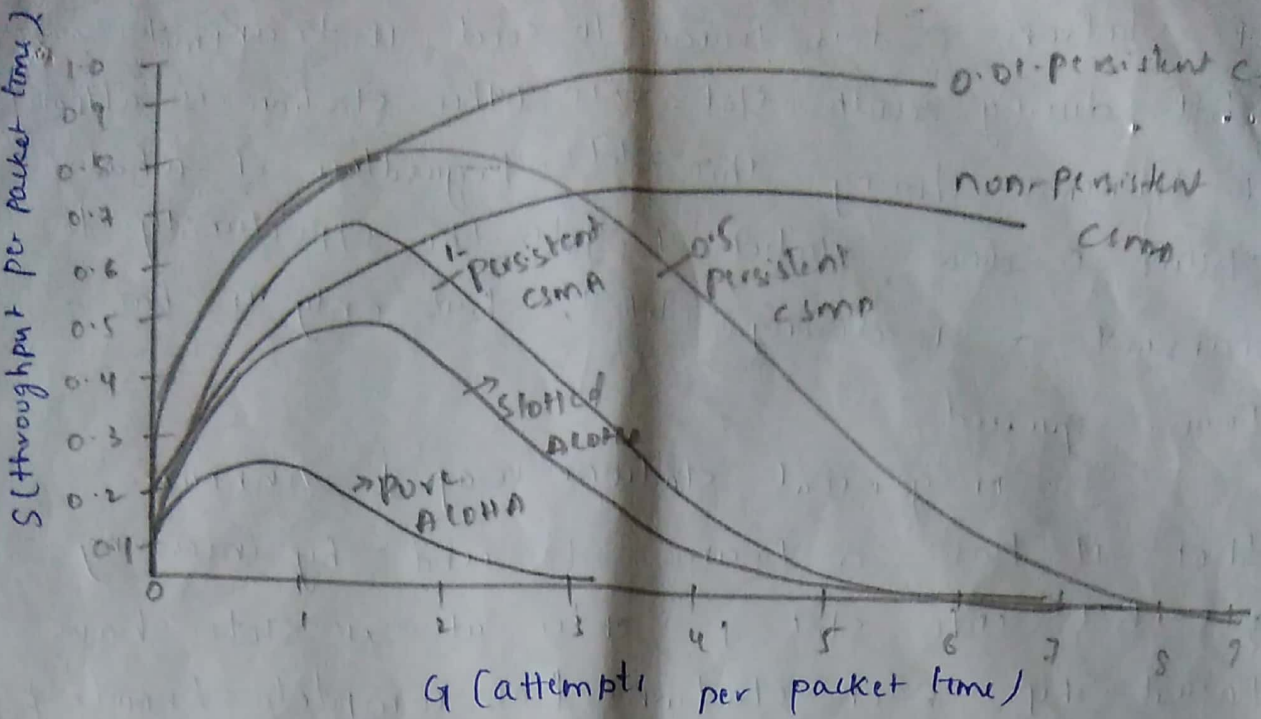
This protocol is known as CSMA/CD. widely used on LAN in MAC sublayer.



At point marked 't_0' a station has finished transmitting its frame. Any other station having a frame to send may now attempt to do so. If 2 or more stations decide to transmit simultaneously, there will be collision. Collision will be detected by looking at the power (or) pulse width of the received signal & comparing it to transmitted signal.

After a station detects a collision, it aborts transmission waits a random period of time, and then tries again. (if no other station has started transmitting in mean time.

∴ CSMA/CD will consist of alternating contention & transmission period, with idle periods occuring when all station are quite.



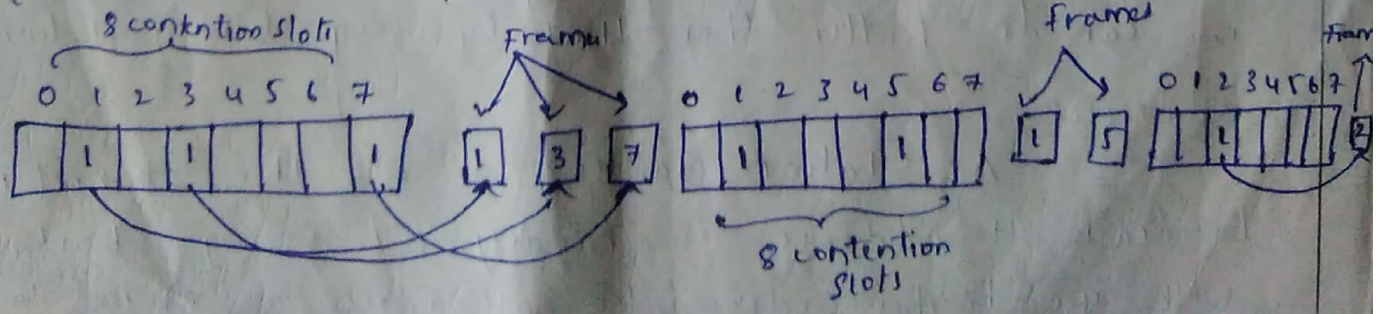
Collision-free protocol:-

Although collision do not occur with CSMA/CD once station has captured the channel. they can still occur during the contention period. These collision adversely effect the system performance. Especialy when the cable is long (or) frames are short

Two types of collision-free-protocols:-

i) A Bit-map protocol
ii) Binary countdown

Bit-map protocol:- First collision free-protocol is the basic bit-map protocol Each contention period consists of Exactly N slots.



If station 0 has frame to send, it transmits a 1 bit during zeroth slot. No other station is allowed to transmit during this slot. Regardless of what station 0 does, station 1 gets the opportunity to transmit a 1 during slot 1, but only if has a frame queued.

In general station 'j' 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 wish to transmit.

Since every one agrees on who goes next, there will never be collisions. After the last ready station has transmitted its frame, all station easily monitor, and another n-bit contention period is begun.

Protocol like this in which the desire to transmit is broadcast before the actual transmission are called "Reservation protocol".

Binary countdown:-

A problem with the basic bit-map protocol is that overhead is 1 bit per-station, so it does not scale well to network with thousands of stations we can do better than that by using binary station addresses.

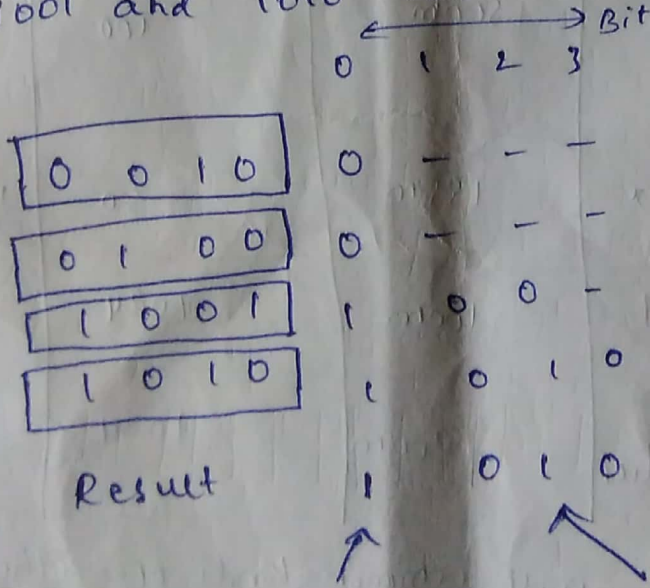
A station wanting to use the channel now broadcast, its address as binary bit string, starting with the higher order bit. All adress are aloned to

be the same length. The bits in each adress position from different stations are BOOLEAN ORed together. We will call this protocol "Binary countdown"

To avoid conflicts, an arbitration rule must be applied: as soon as a station see that the high-order bit position that is '0' in its address has be overwritten with a '1' it gives up.

Eg:- If stations 0010, 0100, 1001, 1010 are all trying to get the channel.

In the first bit time station transmit 0, 0, 1 and 1 respectively. These are ORed together to form a '1'. Stations 0010 and 0100 see the '1' and know that a higher-numbered station is competing for the channel, so they give up for current round. Stations 1001 and 1010 continue.



It has property that higher numbered station have higher priority than lower-numbered station.

Ethernet-Physical layer:-

IEEE has standardized a number of LAN and MAN under the name of IEEE 802. A few has survived but many have not.

most important survivors are

802.3 (Ethernet), 802.11 (Wireless LAN), 802.15 (Bluetooth) 802.16 (wireless MAN).

802.3 and 802.11 have different physical layers and different MAC sublayers. but on the same logical link control sublayer.

Ethernet cabling:-

Since the name "Ethernet" refers to the cable.

Name	cable	max. seg	Nodes/seg	Advantages
10 Base 5	Thick coax	500m	100	orginal cable; now obsolete
10Base2	Thin coax	185m	30	No hub needed
10 Base-T	Twisted Pair	100m	1024	cheapest system
10 Base-F	Fibr optics	2000m	1024	Best- b/w building

fig:- most common kinds of Ethernet cabling.

Four types of cabling commonly used

10Base 5:- Popularly called "thick ethernet". It resembles a yellow garden hose with markings every 2.5 mts to show where the taps go. connections to it are generally made using Vampire taps. in which pin is very carefully forced halfway into co-axial cables core.

Notation:- 10Base 5 means. that it operates at 10 mbps, uses baseband signaling and support segments of upto 500 meters.

10Base 2:- is called as "thin Ethernet." which in contrast to the garden-host-like thick ethernet bends easily. Connections to it are made using BNC connector to form T-Junctions rather that using vampire taps. This is much cheaper and easier to install but it can run only for 185 meters per segment. Can handle only 30 machines.

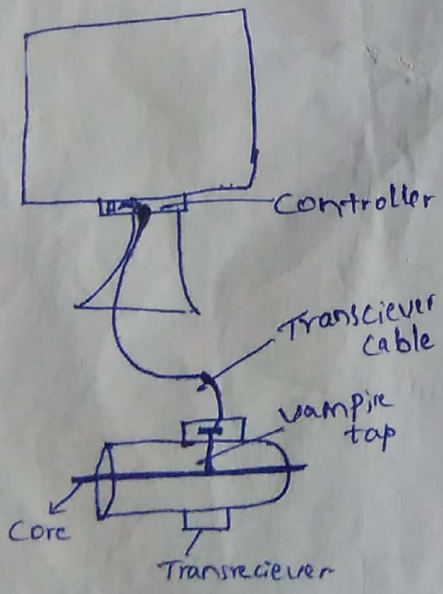


fig:- 10 Base 5

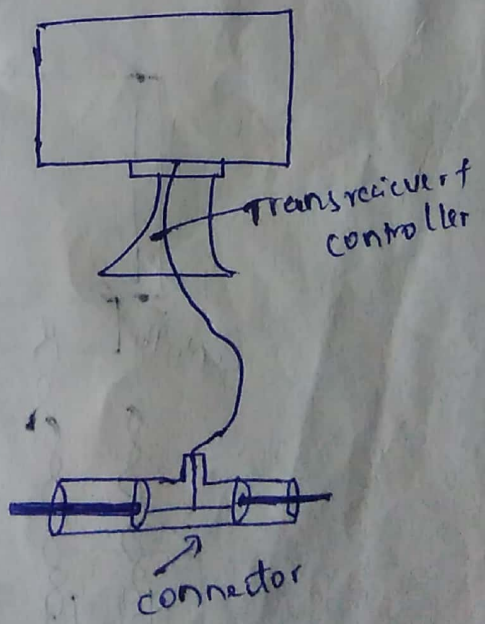


fig:- 10 Base 2

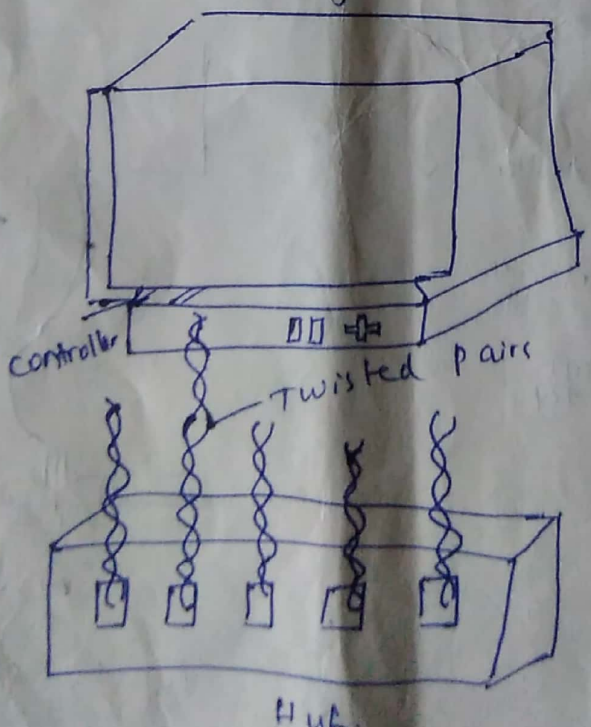
i) 10Base5 is a transciever cable or drop cable connects to transciver to an interface board in computer. this cable is 500mts long contains 5 twisted pairs. 2 for Data in and Data out, Two more for control signal in and out, Fifth pair is not used.

→ controller is responsible for assembling data into proper frame format.

ii) 10Base2 cable is just a passive BNC-T-function connector. The Transciver electronics are on the controller board; each station always has its own Transciver.

iii) 10BaseT :- There is no shared cable at all just the hub to each station is connected by dedicated cable. If cable breaks can be easily detected.

Disadvantage:- max cable run from hub is only 100mts or may be 200mts if very high quality twisted pairs are used. it quickly become dominant



10Base-F:- It uses fiber optics. It is expensive due to cost of connectors and terminators. But it has Excellent noise immunity.

Ethernet MAC sublayer protocol:-

→ The orginal DIX (DEC, Intel, Xerox) fram structure is as shown. Each frame starts with a preamble of 8 bytes, each containing bit pattren 10101010.

→ The Frame contains two addresses, one for the destination and one for the source. The standard allows 2-bytes and 6-bytes adresses.

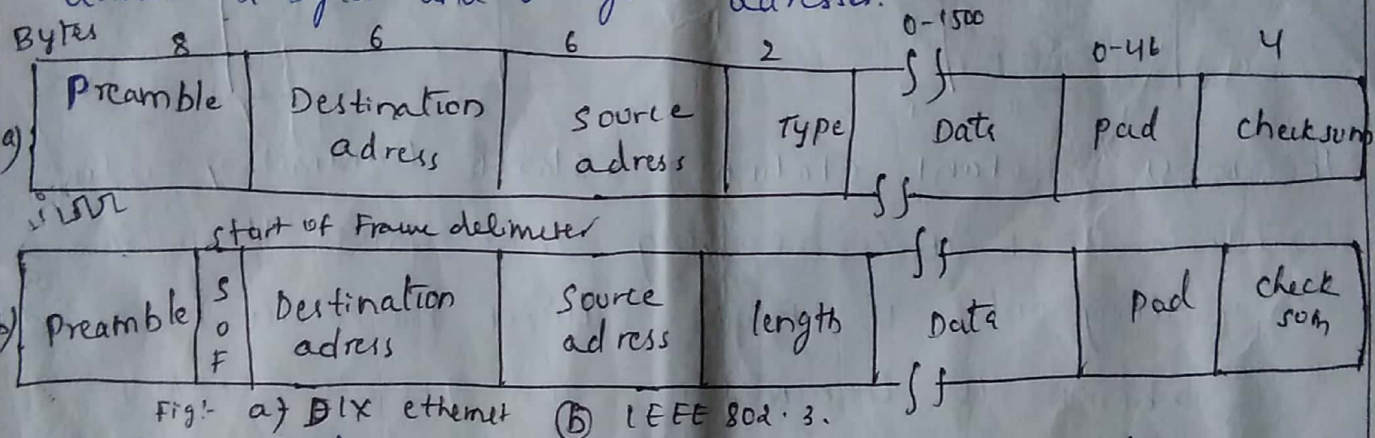


Fig:- a) DIX ethernet (b) IEEE 802.3.

→ Another feature of addresing is use of bit 46 (adjacent to high-order bit) to distinguish local from global addresses

→ Next comes "Type" field, which tells the Reciever what to do with the frame. multiple n/w-layer Protocol may be in use at same time on same machine The "Type" field specifies which Process to give the frame.

→ Next comes the data upto 1500 bytes. This limit was choosen somewhat arbitarily at the time DIX standard.

→ If data portion of frame is less than 46 bytes the pad field is used to fill out the frame to min size.

→ another reason for having minimum length frame is to avoid collision b/w the frames.

At time '0', station A, at one end of the n/w sends off a frame. Propogation time for frame to reach the other end 'τ'. Just before frame gets to the other end (at time $\tau - \varepsilon$).

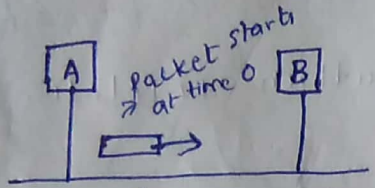


fig-a

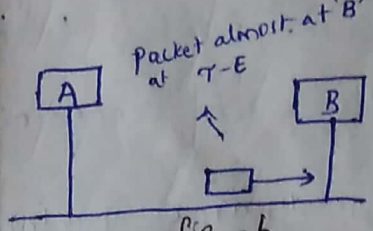


fig-b

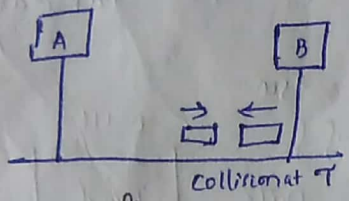


fig-c

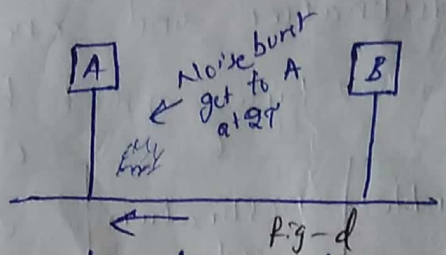


fig-d

The most distant station, B. starts transmitting, when B-detects that it is receiving more power than it is putting out, it knows collision has occured, so it aborts its transmission and generate 48-bit noise burst to warn all other stations.

At about 2τ time sender sees the noise burst and aborts it transmission too. it waits a random time before trying again.

When IEEE Standardized Ethernet, made a changes to DIX format, i) To reduce the preamble to 7 bytes and use the last byte for a "start of frame" ii) To change "Type" field into "length" field.

Data link layer switching & use of bridges:-

Many organizations have multiple LAN's and wish to connect them. LAN's can be connected by a device called bridges. which operate in the data link layer

Bridges Examine the data layer link addresses to do routing but they are not to Examine the payload field of the frame they route.

They can transport IPv4 (used in internet now) and IPv6 (used in internet future), Apple talk, ATM, OSI or any other kinds of packets in contrast routers Examine the addresses in packets and route based on them.

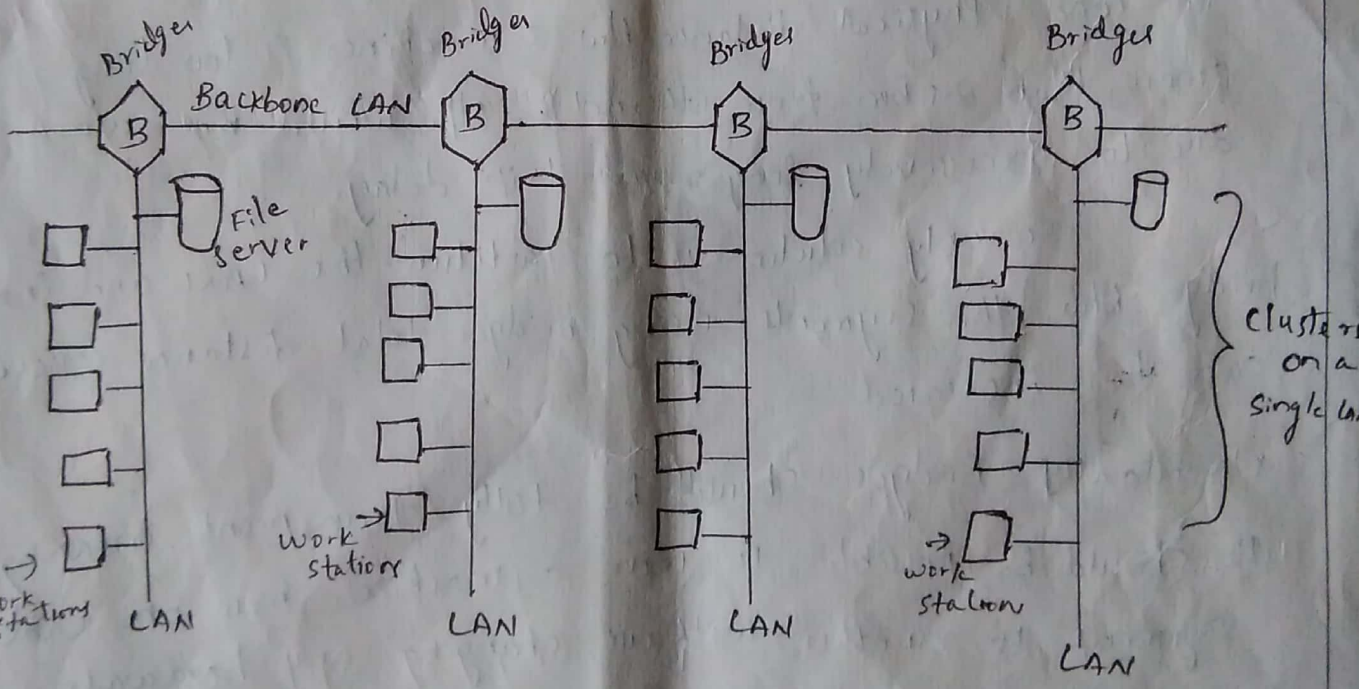


fig:- multiple LAN's connected by a backbone to handle a total load higher than a capacity of a single LAN

*) Many departments have their own LANs primarily to connect their own pc's, workstations and servers. different departments use different LAN's. so bridges are needed.

*) The organizations may be spread over several buildings seperated by considerable distance. It may be cheaper to have seperate LAN's in each building and connect them with bridges and laser links than to run a single cable over the entire site.

*) It is necessary to split single LAN into seperate LAN to accomodate the load. Instead multiple LAN's connected by bridges as shown in fig:-1. each LAN contains a cluster of work stations with its own file server so that most traffic is restricted to single LAN and does not add load to the backbone.

*) In some situations single LAN would be adequate in terms of load. Physical distance blw 2 machines is too long. (more than 2-5 km from ethernet). Nlw would not work due to excessively long round-trip delay.

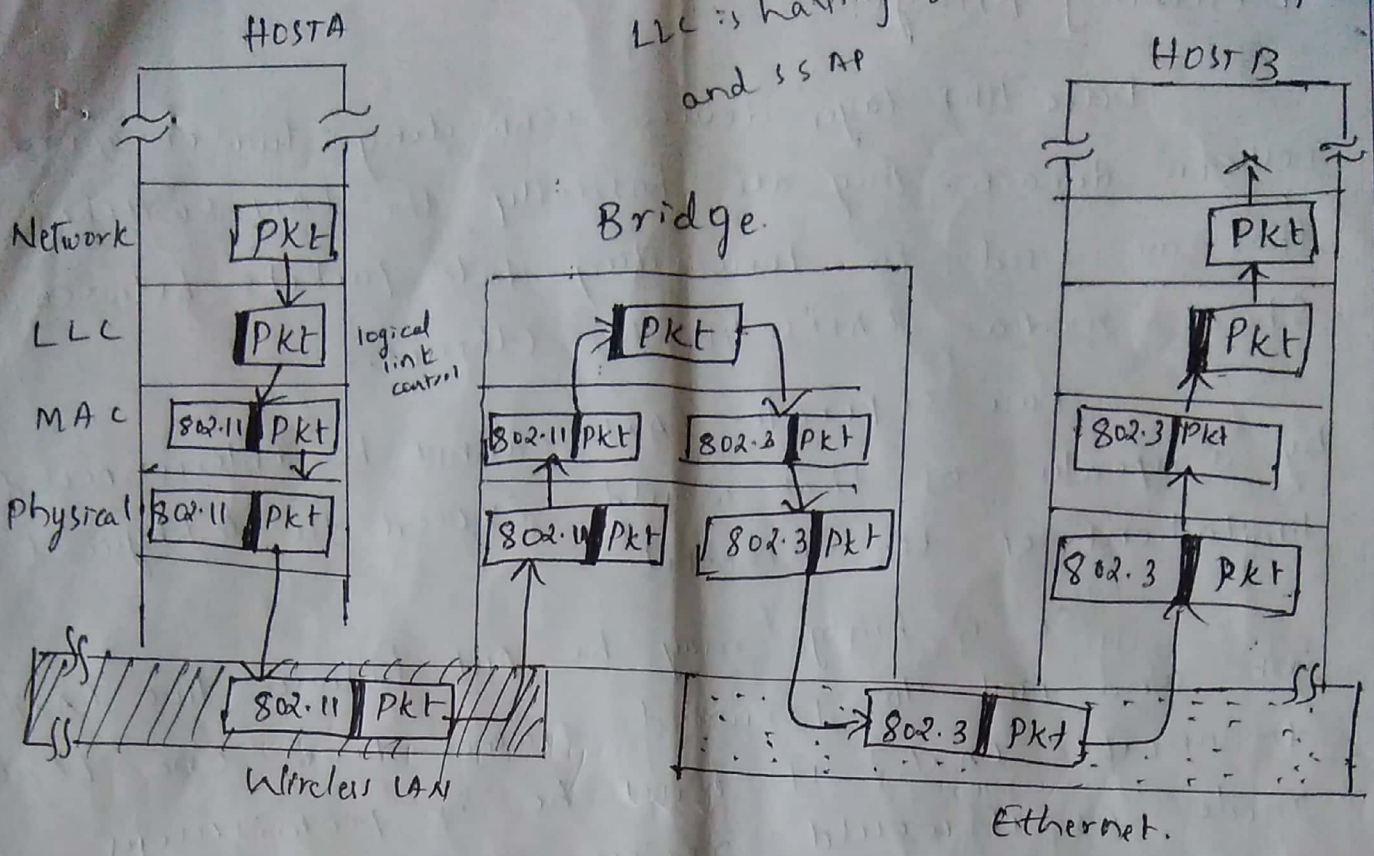
So only solution is to partition the LAN and install bridges blw the segments. Using bridges total distance covered can be increased.

*) Ideally bridges should be fully transprent, meaning it should be possible to move a machine from one cable segment to another without changing any hardware, software (or) configuration table.

Use of bridges from 802.x to 802.y :-

illustrate the operation of simple 2-port bridge Host A on a wireless (802.11) LAN has a packet to send to fixed host B on a (802.3) Ethernet to which the wireless LAN is connected.

LLC is having destination service Access point and SS AP



(802.11) wireless LAN

The packet descends into the LLC sublayer and acquires an LLC header (shown in black in the Fig). Then it passes into the MAC layer and an 802.11 header is prepended. When it hits the bridge connecting 802.11 network to the 802.3 nlw. it starts in the physical layer and works its way upward.

Now in the MAC sublayer in the bridge the 802.11 header is stripped off. The bare packet (with LLC header) is then handed off to the LLC sublayer in the bridge and packet is destinated for an 802.3 LAN, so it works its way down the 802.3 side of the bridge and goes on the Ethernet.

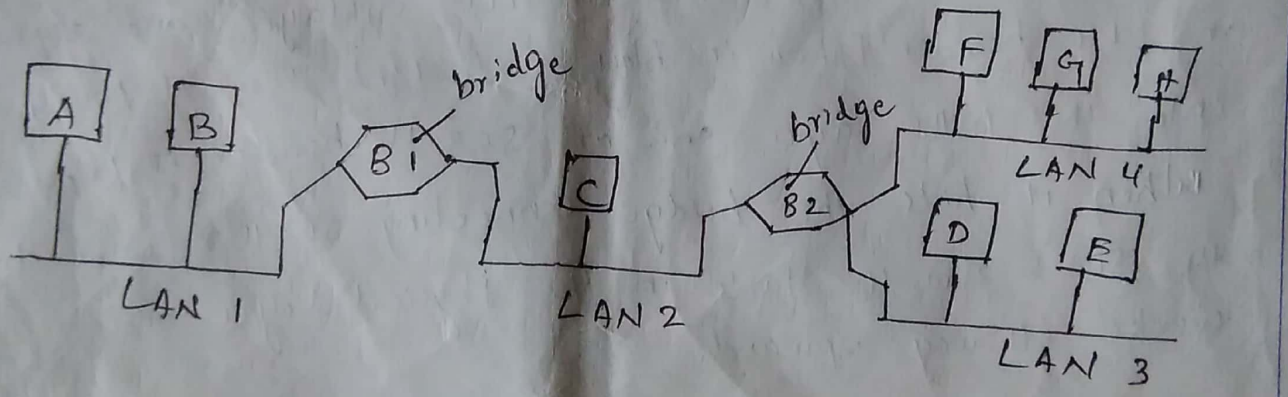
Ethernet has no concept of quality of service,

Learning bridge:-

Data link layer device connecting two or more collision domain. They are basically the LAN switches that are used for forwarding data packets between shared media. LAN's like the Ethernet.

Two seperate LAN cannot be interconnected by a repeater as that would exceed the physical limitations of the Ethernet.

So a bridge may be put between two LAN's link and used to forward frames from one LAN to another LAN. It must be in promiscuous mode as it would recieve all frames transmitted on either of LAN's and forward them to other.



In its simplest form Transparent bridges operates in promiscuous mode. accepting every frame transmitted on all the LAN to which it is attached.

→ Consider the above fig:- 1) Bridge B_1 is connected to LAN1 and LAN2, Bridge B_2 is connected to LAN 2, 3, 4.

→ A frame arriving at bridge B_1 on LAN 1 destinated for A can be discarded immediatley

because it is already on correct LAN, but a frame arriving on LAN 1 for 'C (or) 'F' must be Forwarded.

→ When a frame arrives, a bridge must decide wheather to discard or forward it. and if later on which LAN to put the frame.

→ This decision is made by looking up the destination addres in big (hash) table inside the bridge.

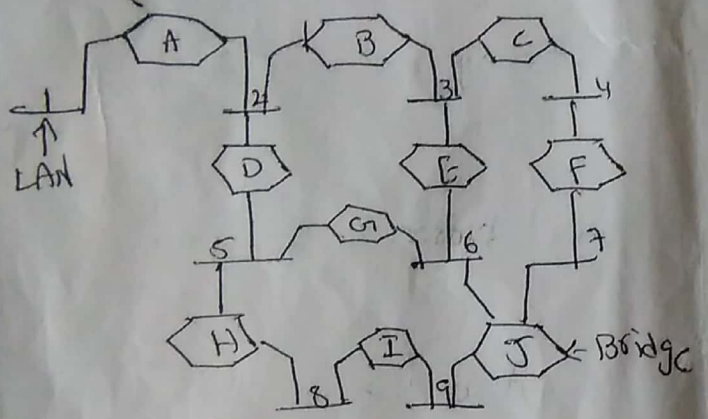
→ This table can list each possible destination and tell which o/p line (LAN) is belongs on.

There should be a forwarding table maintained by a bridge that will help it to forward packets over the LAN. This is known as the "learning Bridge".

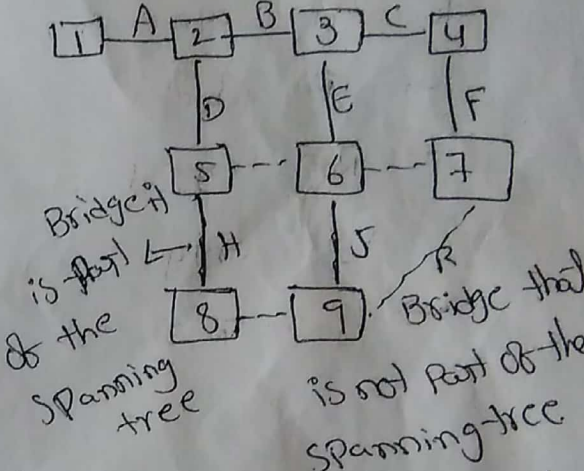
Spanning Tree Bridges:

To increase reliability some sites uses 2 or more bridges in Parallel b/w pair of LANS. This arrangement creates problems because it forms a loop whenever we send a packet from one LAN to another LAN if we have 2 bridges the packet goes to 2 Bridges at the destination side we receive the same frame 2 times By Providing comm b/w the bridges we can avoid this Problems.

→ Spanning tree bridges are used to avoid the Problems.



Fig(a): Interconnected LAN's



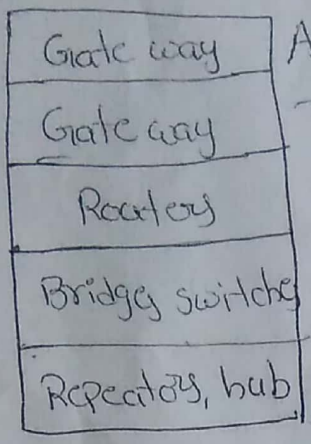
fig(b): Spanning tree covering the LAN's

→ To built spanning tree first, choose 1 bridge to be the root of the tree. They make this choice by having each one it is serial no

→ They broadcast it's serial number, that installed by name factories it is a unique number in world wide. The bridge with lowest numbe becomes the root afterwards a tree of shortest path from root to every bridge and LAN is constructed.

→ If a bridge / LAN fails a new one computed.

→ The distributed algorithm used for constructing the spanning tr



Repeaters:- Repeaters are Analog devices that are used to connect to cable segments. A signal appearing on one of them is amplified and putout on the other

→ Repeaters doesn't Understand frames / packets they understand 'Volts" only

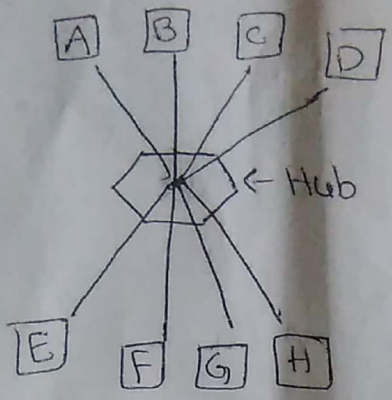
→ By using repeaters we can extend the length of Nlw

Hubs:- A HUB has no of input lines that it joins electrically.

→ frames arriving on any of the lines are sent to all the lines except which it came

→ If 2 frames arrive at the same time they will collide so, retransmission of data occurs.

→ All lines coming into HUB must operate at same speed



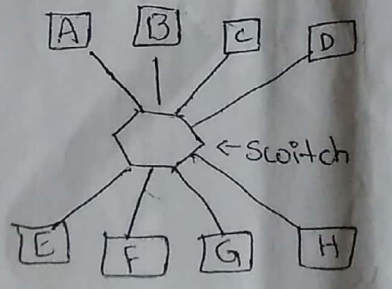
Switches:- These are similar to bridges in that, both rest on the frame address.

→ The main difference is bridges are used to connect LAN's where switches are used to connect individual computers.

→ when we send a frame within the LAN Bridge discards the Packet switch forwards the Packet to the particular node.

→ Each computer has its lineguard when a frame arrives it stores the frame into that lineguard.

→ whenever faster transmission take place if buffer space is fulled then it discards the Packet's then retransmission require



Routers:- when a packet comes to router. It removes the header & trailer & actual Packet forwarded to the routing software. This software uses the Packet header to choose the op line

→ In Packet header we have IP address of Packet we have IPV4 & IPV6.

IPV4 - 32 bit

IPV6 - 128 bit

Gateway:- Gateways are used to connect to computer that users Connection Oriented Transport Protocol.

→ The Transport Gateway. Copy the Packets from one Connection to other which are using 2 different Protocols & reformats the Packets as the System needed

Application gateways:- These understand the format & contents of data & translate messages from one format to another.

Difference between Pure ALOHA and slotted ALOHA.

S. No	Pure ALOHA	slotted ALOHA
1	frames are transmitted at arbitrary time	1. Time is divided up into discrete slot, the frame is sent at the start of a slot
2.	Throughput (S) = G x e^{-2G}	2. Throughput (S) = G x e^{-G}
3.	Vulnerable time is 2 times the frame transmission time	3. Vulnerable time is one half that of Pure ALOHA
4.	The maximum utilization is about 18.4%	4. The maximum utilization is about 36.8%.
5.	Global time is not requir	5. It requires global time for synchronization, as it is divided up into discrete slot
6.	Simple to implement	6. Implementation is complex due to the synchronization of all nodes.
7.	Cannot used for satellite, due to very low utilization	7. It is used in broadcast satellite.

UNIT-III

Network Layer

etwork Layer:

In network Layer the data is send from source to destination. i.e the data is divided into Packets. The Packets contain the data with source and destination address due to the communication from source to destination Packet loss may be occur overloaded.

To send that from source to destination we have to choose appropriate path by using the network topology.

Network Layer design issues

1. store and forward Packet switching.
2. Services Provided to the transport Layer
3. Implementation of connectionless service
4. Implementation of connection oriented service
5. Comparison of virtual-circuit and datagram subnet.

1. store & forward Packet switching:

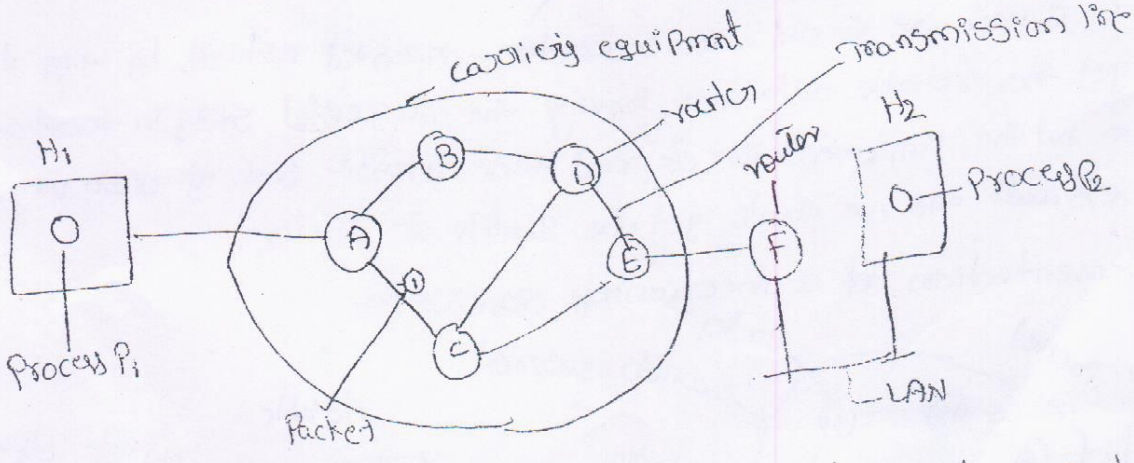


fig: The environment of the nlw Layer Protocols

→ Host H_1 is connected to the nearest router 'A' by using transmission line that present in carrying equipment. In contrast H_2 host is connected through LAN with router F.

Process P_1 sends the Packet to the nearest router through the LAN Point-to-Point link to the carrier

→ The last hop finished finished its processing by verifying the checksum.
→ Then it is forwarded to the next router along the Path until it reache the destination host. This mechanism is store-and forward Packet Switchi

Services Provided to the Transport Layer

The network layer providing service to the transport layer at the N/w layer / Transport Layer interface. The services are

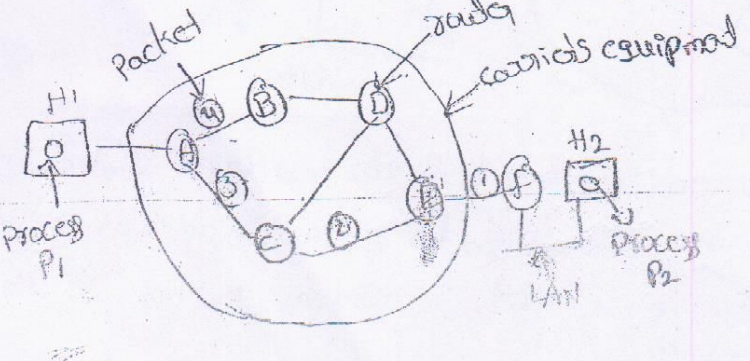
1. The Service should be independent of the router technology.
2. The Transport Layer should be shielded from the number, type, and topology of the routers present.
3. The network addresses available in transport layer.

By Providing these services the designer of the n/w layer have a lot of freedom to writing detailed specification of Service to be offered to transport layer, and this can be done through the connection oriented / connection le services.

If you are going to consider the connection less n/w, the information of data transfering is very easy. like data send in the form of packets those can contain the Sender & Reciver address and it is very usefu in real time traffic.

If you are consider the connection-oriented network, by using this w can get the reliable data & it having the successful story in telephone system but the implementation of real time traffic such as audio, video is very difficult and we can't get the quality of Service

Implementation of connectionless service:-



A's table

A	-
B	B
C	C
D	B
E	C
F	C

A	-
B	B
C	C
D	C
E	B
F	B

A	A
B	B
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 datagram Subnet

→ The Packets

→ In datagram subnet process P_1 has send a message to P_2 on host H_2.

→ Let us assume the message is divided into 4 Packets & same size that Packets are stored in router 'A' using Point-to-Point Protocol by using A's initial table the Packet is delivered to B or C. router and the same way 'c' router having two paths c&D & c-to-E and the same way Packets 1,2,3,4 initially stored in 'A'. next it send to F router through the carrier equipment And routing table will be designed by using routing algorithm.

Implementation of connection-oriented services:

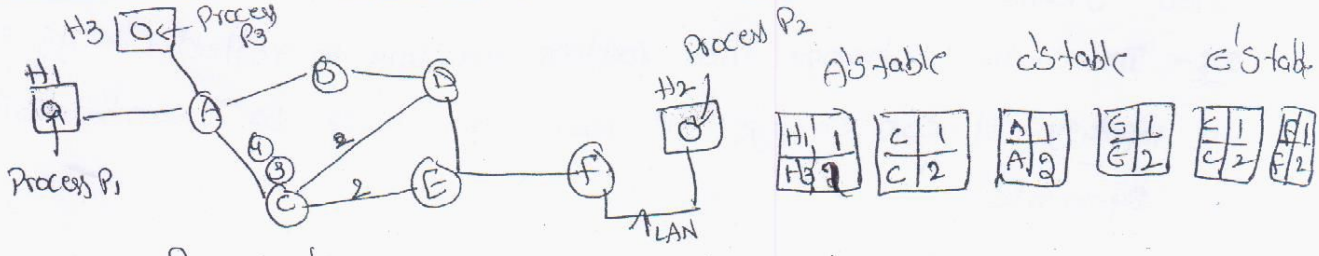


fig: Routing within virtual circuit subnet

To implement connection-oriented service is n/w layer to transport layer we need virtual circuit subnet. means before sending the packet we need to establish the path between the sender to receiver then only data can be transfered in connection oriented services that is nothing but virtual circuit n/w.

In this service if you are establish the connection then it takes i.e it establish the connection b/w H_1 to H_2 then transfer the data each connection identifies by 1. next consider the H_3 host & establish the connection H_3 to H_2. In this we can avoid the conflicts

Routing Algorithms:

Routing Algorithm is nothing but it is responsible for deciding the Path to transfer the data from source to destination

→ If the subnet uses virtual circuits internally, routing decisions are made only when a new virtual circuit is being set up. Therefore, data packets just follow the previously established route. The latter case is sometimes called session routing

* (virtual circuit means before the packet connection is established).

→ Routing are chosen independently for each packet. or only when new connections are established, certain Properties are desirable in a routing alg. correctness, simplicity, robustness, stability, fairness, & optimality.

Routing alg's can be grouped into 2 major classes.

1. Non adaptive Alg.
2. Adaptive Alg.

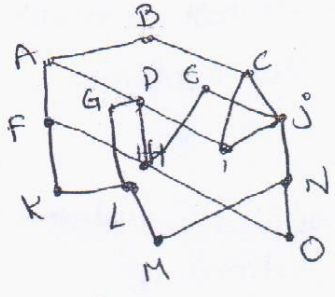
1°- It do not base on their routing decisions on measurements or estimate the current traffic & topology this procedure is sometimes called Static Routing.

2°- In contrast, change their routing decisions to reflect changes in the topology. It can change the route dynamically so it can be called as "Dynamic".

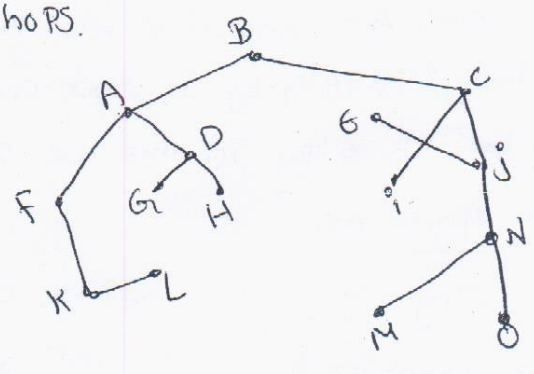
The optimality Principle: optimality principle is reading the optimal routes without knowledge of topology or traffic. It states that if router 'j' is on the optimal path from router 'i' to router 'k', then the optimal Path from 'j' to 'k' also fally along the same route.

A tree is rooted at the destination such tree is called a sink tree

→ A sink tree doesn't contain any loops. so each packet will be delivered within a finite & bounded no. of hops.



(a) Subnet



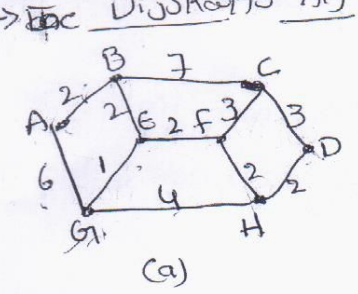
(b) A Sink tree for router B.

Shortest path Routing

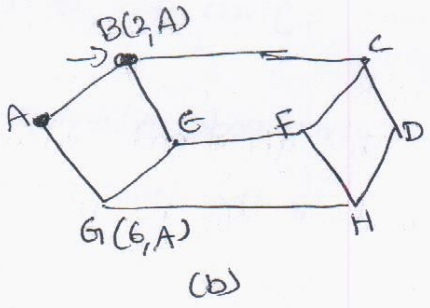
- It is simplest and easy to understand and it is static routing alg. This can builds a graph of the subnet. where each node rep

between two routers

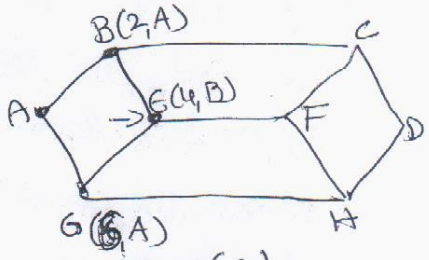
→ Dijkstra's Alg



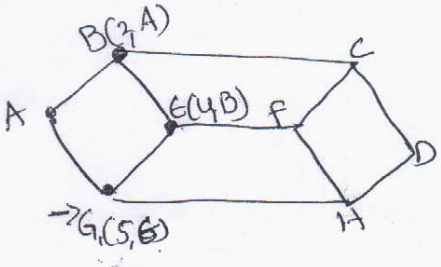
(a)



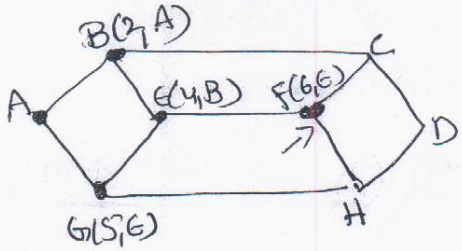
(b)



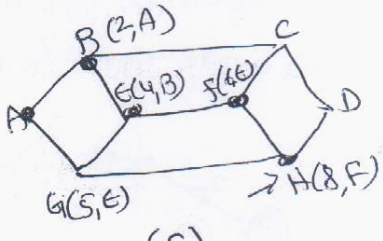
(c)



(d)



(e)



(f)

Shortest path from A

→ The alg chooses a route between a pair of nodes by finding the shortest path between them.

→ Shortest path can be measured by using two techniques.

1. Path – Path length is no. of hops.
2. Geographic distance – Kilometers

→ The labels on the arcs could be computed as a function of the distance, bandwidth, average traffic, communication cost, mean queue length, measured delay, and other factors. Shortest path can be measured by using any one of the factor.

2 types of shortest path Alg's.

1. Dijkstra's Alg. 2. Bellman-Ford Alg.

1:- It computes the shortest path b/w a pair of routers of a graph

→ 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 infin

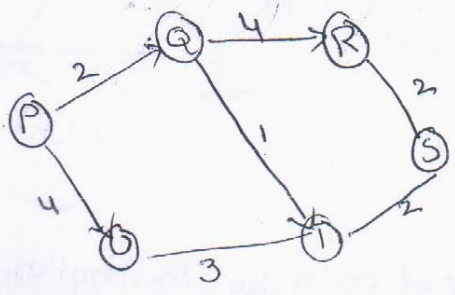
Paths are found the labels may change, reflecting b/w paths

label may be either tentative or permanent.

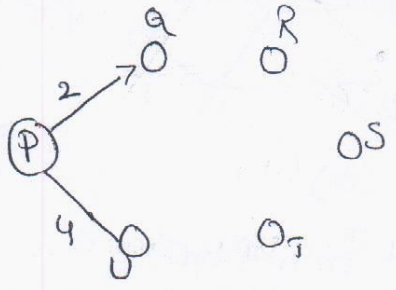
Bellman ford Alg:- Bellman-ford Alg is some what similar to Dijkstra Alg. The shortest Path from a given node is computed such that the Path has at most one link.

-> At each step from the given node, atleast path with max links are determined. The completion of the least Path cost to each node & the cost of that path is done.

Eg:- Consider the graph given below to compute the shortest path b/w nodes P & S are computed.

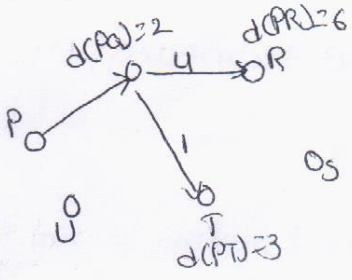


STEP 1:-



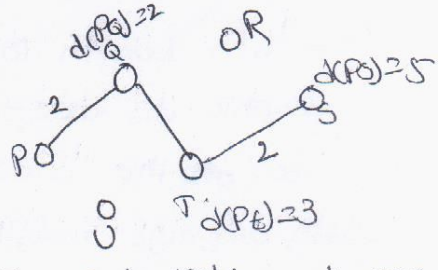
Distance of PQ is shorter than the distance of PU. So route PQ is select

Step 2:



Distance of PT is less than the distance of PR. Hence Route PQT is selected.

STEP 3:



Since node 'T' has only one link i.e Ts' Route TS is selected therefore the shortest path is PQTS

Flooding

It is a routing alg. In this alg every incoming Packet is sent on all outgoing ling expect the line on which it has arrived.

one of the major problem in this alg is that it generates a large number of duplicate Packets on the n/w. to stop their duplication

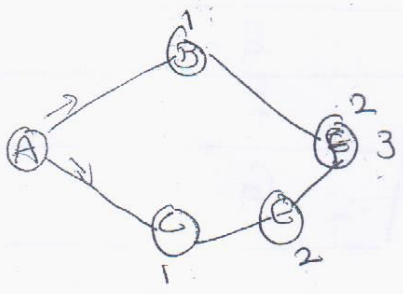
-> It include the hop counter (hop is nothing but path from source to destination, hop count is intermediate node(s) in the header of r Packet, and their counter is decremented at each hop along.

and finally at the destination hop counter will be zero & it represent the exact hop information without duplicate.

→ and second solution Packet is flooded to avoid sending them a second time

→ Another solution is to use selective flooding. in this routers do not send every incoming packet out on every output line.

Instead Packet is sent only on those line which are ~~Approximately~~ going on the right direction.



Applications:-

- Military
- Database
- wireless nlw

Drawbacks

- Duplication of data
- bandwidth

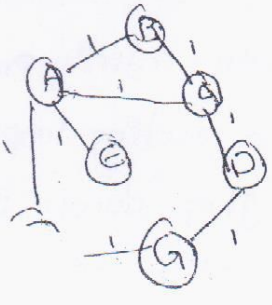
Distance Vector Routing / Bellman-ford / ford fulkerson :-

In distance vector routing alg each router maintain a table. It contain information about distance. and these table are updated by exchanging information with the neighbore nodes.

Distance vector routing also known as Bellman ford routing & Ford fulkerson. (Bellman - 1957 & ford & fulkerson 1962)

In distance vector routing each router maintain a routing table indexed by and containing one entry for each router in the subnet.

This entry contains 2 parts the prefered outgoing line to use for that destination & an estimate of the time or distance to that destination



Initial distance stored at each node.

Information stored at node	Distance To Reach node						
	A	B	C	D	E	F	G
A	0	1	1	?	1	1	?
B	1	0	1	?	?	?	?
C	1	1	0	1	?	?	?
D	?	?	1	0	?	?	1
E	1	?	?	?	0	?	?
F	1	?	?	?	?	0	1

Final distance stored at each node

Information stored at node	Distance to Reach node						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

Routing table maintained at node B.

Destination	cost	Next hop.
A	1	A
C	1	C
~~E~~	1	~~E~~
D	2	~~E~~
E	2	A
F	2	A
G	3	A.

The count-to-Infinity Problem.

Distance vector Routing has a issue ~~is~~ count-to-infinity Problem. Counting to infinity is just another name for a routing loop. Routing loops usually occur when an interface goes down. It can also occur when two routers send updates to each other at the same time.

consider a router whose best rout to destination 'x' is large if on the next exchange neighbour a suddenly report a short delay to 'x'. The route just switches over to using the line to a to send traffic to X.

A	B	C	D	E	
∞	∞	∞	∞		initially
1	∞	∞	∞		After 1 exchange
1	2	∞	∞		After 2 exchange
1	2	3	∞		After 3 exchange
1	2	3	4		After 4 exchange

(a)

A	B	C	D	E	
1	2	3	4		Initially [dis-brac]
3	2	3	4		After 1 exchange
3	4	3	4		After 2 Exchange
5	4	5	4		After 3 exchange
5	6	5	6		After 4 exchange
7	6	7	6		After 5 exchange
7	8	7	8		After 6 exchange
⋮					
∘	∘	∘	∘		

(b)

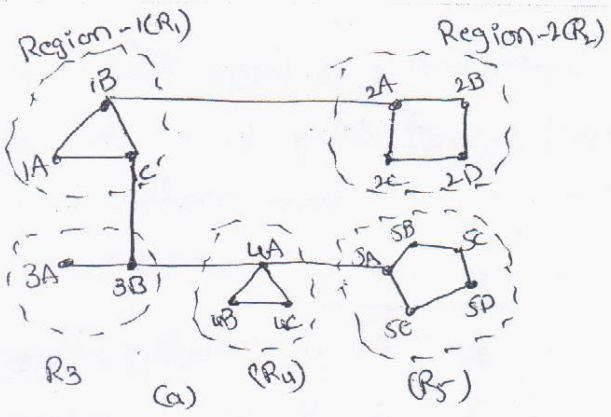
In Situation-1 initially their is no values assigned to routers, after that we are going to perform the exchange by that we get value 1,2,3,4 after 4 exchange.

In situation-2 initially each router having the some distance 1,2,3,4 and after that we have to exchange the router B with router D value. like that we can exchange 1st in place of 1 to 3 next in the place of 2 with 4, after 4 we get the values. so exchange the 3 with 5 and so on.

Hierarchical Routing :-

Normally if n/w size grows then routing tables grow proportionally & CPU time is needed to scan them and more bandwidth is needed to send status reports about them.

In hierarchical routing, routers are divided into regions, and contain the information about packets with destination address. for huge n/w's two-level hierarchy may be insufficient, it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups.



Full table for 1A

Destination	Line	Hop
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)

In above example 1st the routers are divided into Regions. each region contain the information about Packets.

And next step we are going to prepare the table for 1A (i.e region 1) and the table contain Destination, notify but nodes into line and hops. line is nothing but the communication between 1A to that particular destination. next hops is nothing but communication ling between Source to destination.

In third step hierarchical table contain the same three fields i.e Destination, line & hop. here in destination only region-1 can consider the all nodes remaining it contain the regions number in hops less number hops can be considered

Congestion Control Algorithms

Congestion is a situation in communication n/w's in which too many Packets are present in Part of the subnet, Performance degrades. Congestion in a n/w may occur when the load on the n/w (i.e number of Packets sent to the n/w) is greater than the capacity of the n/w (i.e the number of Packets a n/w can handle).

The various causes of congestion in a subnet are.

1. The inputs streams of Packet begin arriving on 3 or 4 i/p lines and all need the same o/p line.
2. The routers buffer space is too limited
3. The routers are Too slow. To Perform book keeping tasks (queuing buffers, updating tables).
4. Slow speed CPU at routers will Perform the routine task such as queuing buffers updating tables slowly.

General Principle of congestion control:-

Congestion control refers to techniques and mechanisms that can either Prevent congestion before it happens or Remove congestion after it has happened.

This approach leads to dividing all solutions into 2 groups

1. open loop (congestion Prevention)
2. close Loop (congestion control)

i:- open loop solutions attemp to solve the Problem by good design to make sure it doesnot occur in the first place. In this method ↓ cies are used to Prevent the congestion before it happens. ↓ ngestion control is handled either by source or either by destin

The various methods used for open loop congestion control are:

1. Re Transmision Policy :- The reTransmission Policy is concerned with how fast a sender time out and what it transmit upon time out.
→ The retransmission Policy & the retransmission timer need to be designed to optimise efficiency and at the same time Prevent the congestion.

2. Acknowledgement Policy :- If each Packet Ack immediately the Ack Packet generate extra traffic. If Acknoledgements are saved upto Piggyback onto reverse traffic extra time out and retransmission may result.

3. : A good routing alg can help avoid congestion by spreading the traffic overall the ling.

4. Discard Policy is the rule telling which Packet is drop when thar is no space.

5. Packet queuing and service Policy relates to whether the routers have one queue per i/p line one queue per o/p line or both.

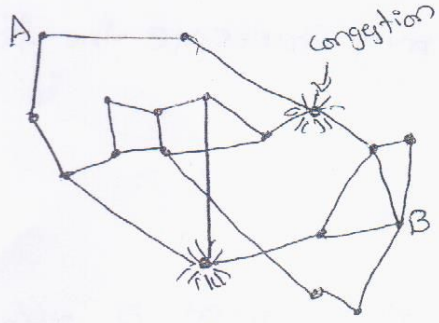
6. Packet lifetime management deals with how long a Packet may lived before being discarded.

Congestion Control:-

Admission Control (Virtual circuits) :-

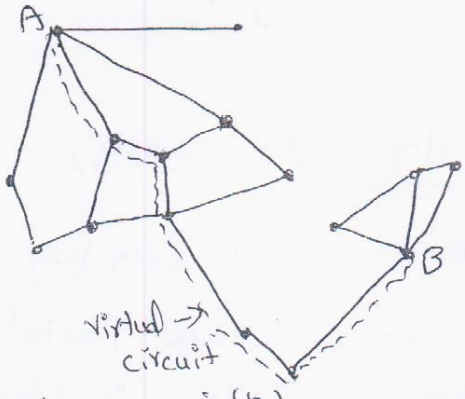
once congestion has been signled no more Virtual circuits are setup untill the Problem gone away. This attempt to steup new transport layer connections failed.

An alternative approach is to allow new virtual circ but carefully route all new virtual circuits around Proble



(a)

A congested subnet



(b)

A redrawn subnet that eliminates the congestion. A vc from A to B.

Datagram Subnet:-

Warning Bit:- In this its signals the warning state by setting a special bit in the packets header. When the packet arrived at its destination the transport entity copied the bit into next Ack sent back to the source.

As long as the router was in the warning state it continued to set the warning bit which meant that the source continued to get Ack with its set.

As long as the warning bits continued to flowing the source continued to decrease its transmission rate.

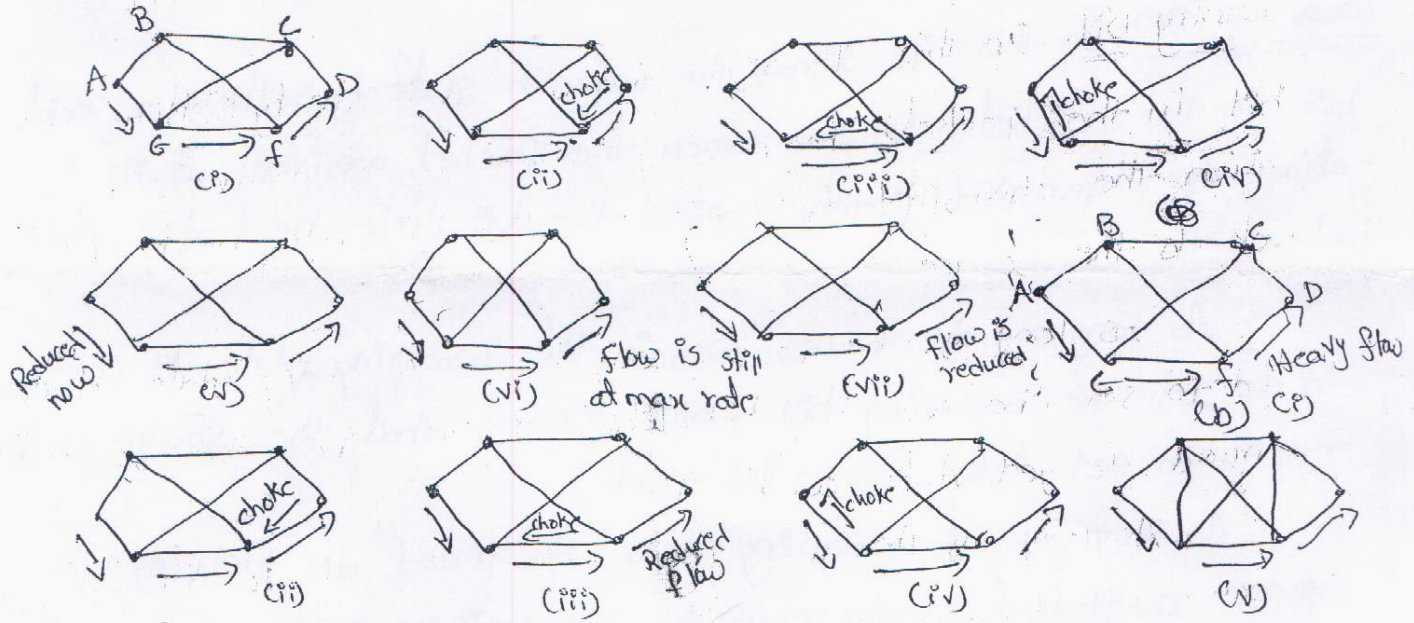
Choke Packet:- In this approach the router sends A choke packet to the source host giving at the destination found in the packet. When the source host get's the choke packet it is required to reduce the traffic sent to the specified destination.

If other packets aimed at the same destination are probably already under way and will generate at more choke packets the host should ignore choke packets refering to that destination for a fixed time intervels. After that the period hay expire the host listens for more choke packets for another interval. If one arrives [illegible]

So that host reduces the flow. If know choke packet occurs during the lisening period. the host may increase the flow again

Hop-by-Hop choke Pakets:

→ At high speeds are over long distance at high speed & over long distance sending a choke packets to the source hosts does not work well. because the reaction is slow. An alternative approach is to have the choke packet take effect at every hop it passes through



→ fig (a) :- A choke packet that affects only the source.

(b) : A choke packet that affects each hop it passes through.

UNIT-IV

Internetworking

Internetworking: Internetworking is the practice of connecting a computer network with other networks through the use of gateways that provide a common meth & routing information Packets between the networks. The resulting system of interconnected networks are called an internetwork

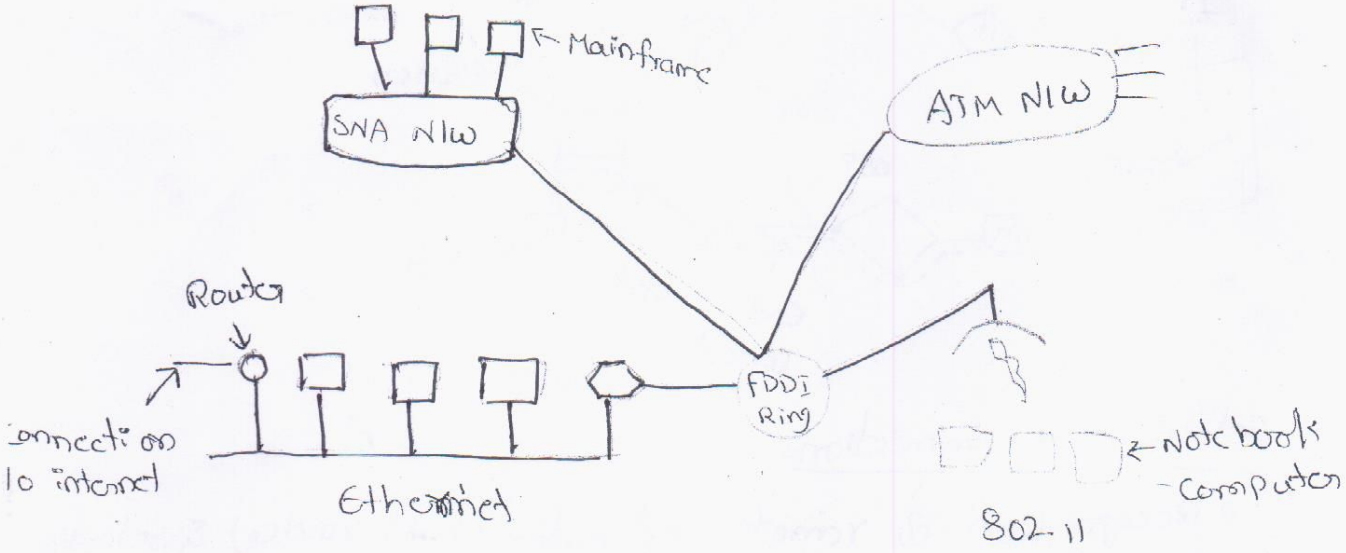
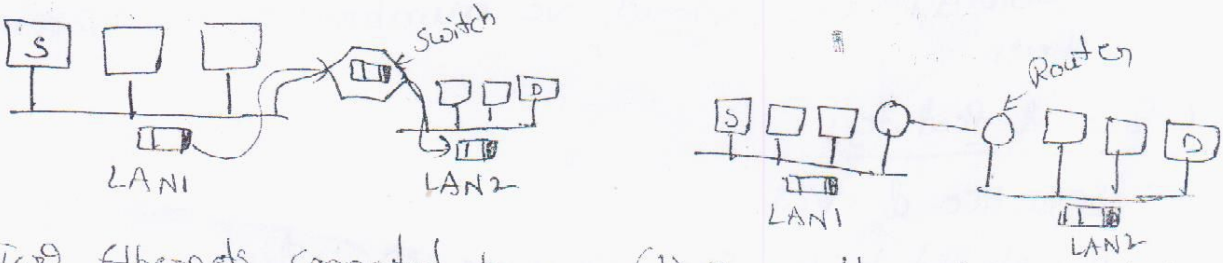


fig: A collection of interconnected networks.

~~we are using the netw~~

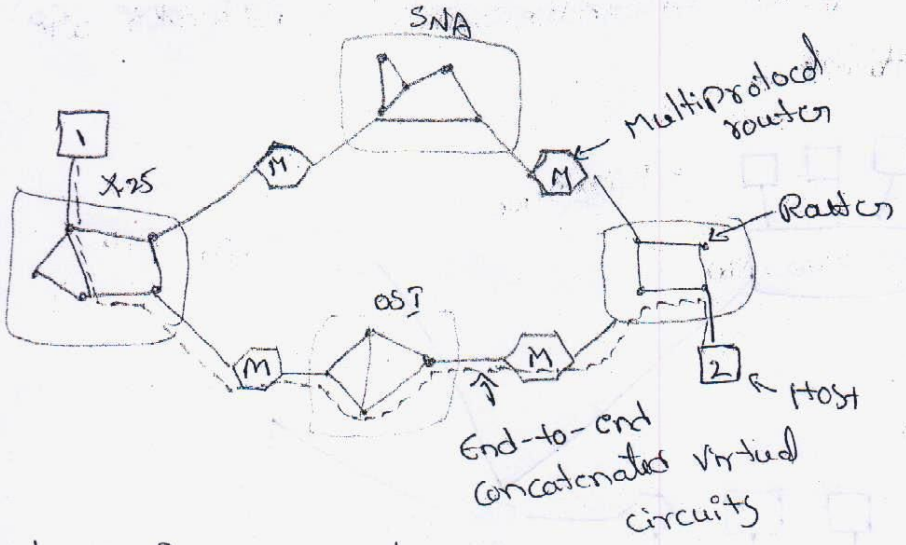
we are connected by the network in different ways like Switching, Routers etc...



(a) Two Ethernets connected by (b)

The source machine S. wants to send a packet to the destination machine, D. These machines are on different Ethernets connected by a switch. S encapsulates the packet in a frame & sends it on its way. The frame arrives at the switch. The frame has to go the LAN2 by looking at its MAC address. The switch just removes the frame from LAN1 & deposits it on LAN2.

Concatenated Virtual Circuits



Set-up of a connection:

→ Recognition of remote destination (host, router) & selection of multiprotocol router for first virtual circuit.

→ Multiprotocol router extends VC towards.

Data Transfer:

→ Same path of all packets.

→ Conversions (Packet format, VC numbers) in multiprotocol routers.

Essential Features:

→ Sequence of VCs

→ NW should have same/similar Properties

where the source and destination hosts are on the same type of network, but there is a different nw in between.

Eg:- International bank with a TCP/IP-based Ethernet in Paris, and a TCP/IP-based Ethernet in London.

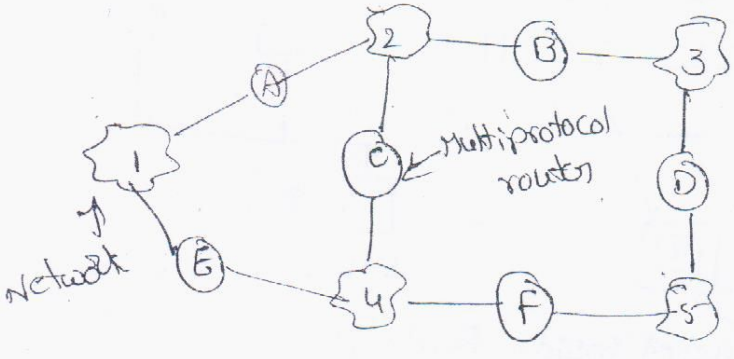
→ To send an IP Packet to host2, host1 constructs the Packet containing the IP address of host2, inserts it into an Ethernet frame addressed to the Paris multiprotocol router & puts it on the Ethernet.

→ when the multiprotocol router gets the frame, it removes the IP Packet.

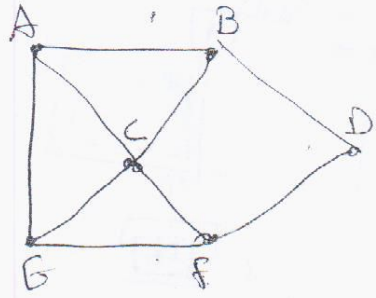
→ insert in the Payload field of the WAN NW layer Packet and addresses the latter to the WAN address of the London multiprotocol router

Internetwork Routing:

Routing:- Routing is the process of moving Packets across a network from one host to another. It is usually performed by dedicated devices called routers.



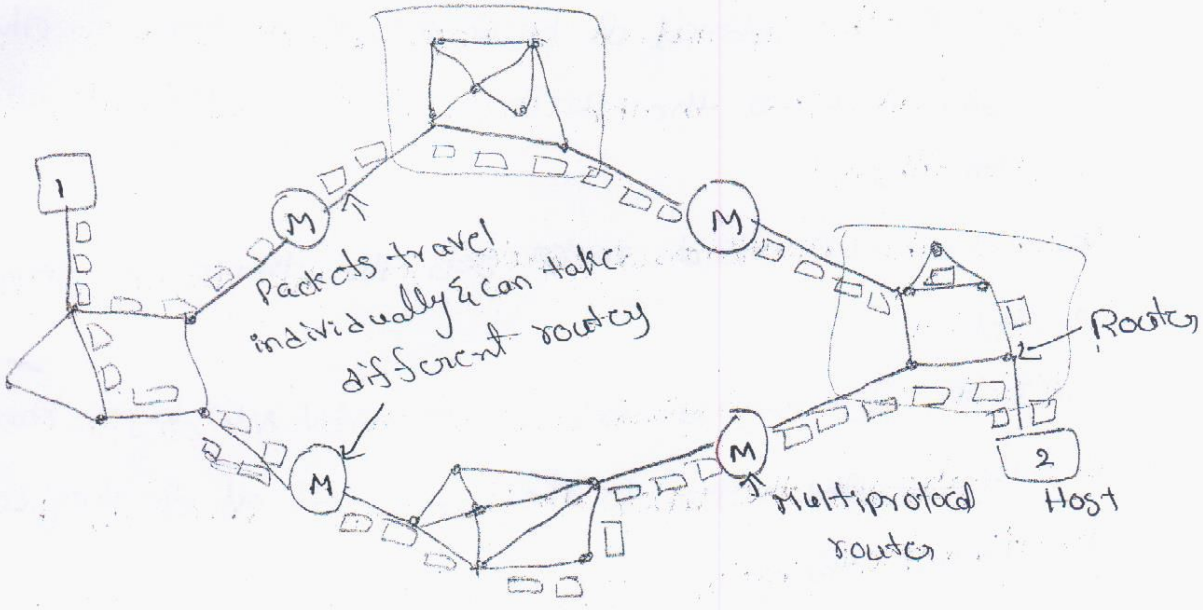
An internetwork



A graph of the internetwork

Connection less internetworking

Connectionless network Protocol. Both operate over IP. The physical, data link, and n/w layer protocols have been used to implement guaranteed data delivery.



Connectionless internet.

Tunneling :-

The solution to this problem is a technique called Tunneli

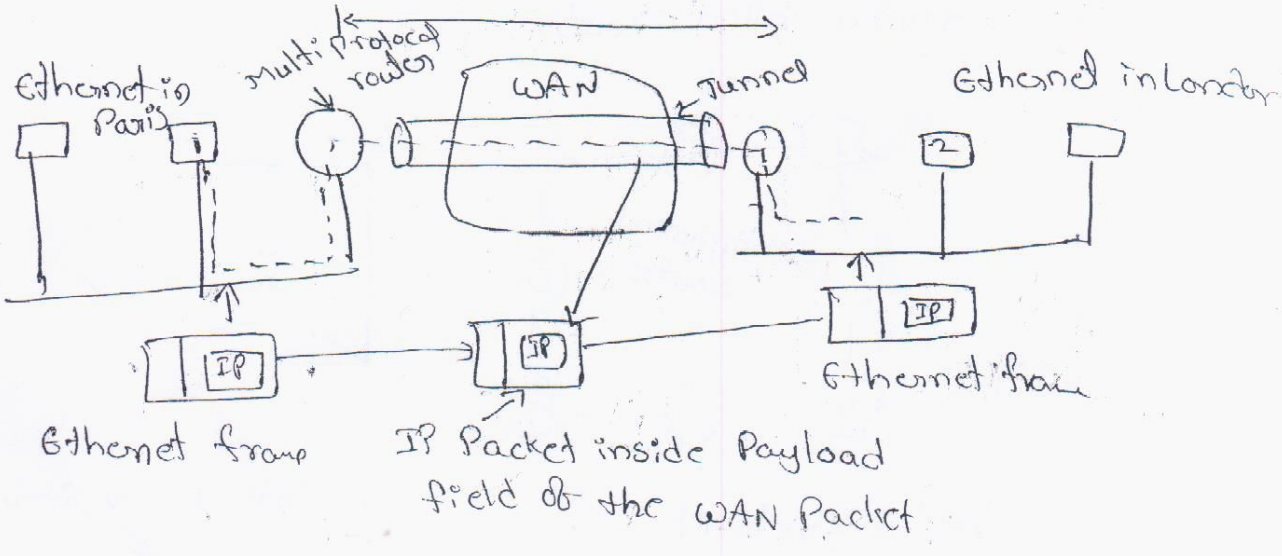


fig: Tunneling a Packet from Paris to London

Here 5 networks are connected by six routers, making a graph model of this situation is complicated by the fact that every router can directly access every other router connected to any network to which it is connected.

~~Eg: 'B' in fig(a) can directly access A and C via network 2 & also D via nw 3.~~

→ A graph of the internetwork is shown in fig. where every router can directly access every other router connected to any network to which it is connected.

→ A Router B can directly access A and C via network 2 and also D via network 3.

→ After the construction of the graph, distance vector or link state routing algorithm is applied to the set of multiprotocol routers. It gives a two level routing alg.

Fragmentation:

Fragmentation means the division of a Packet into smaller units to accommodate a Protocols.

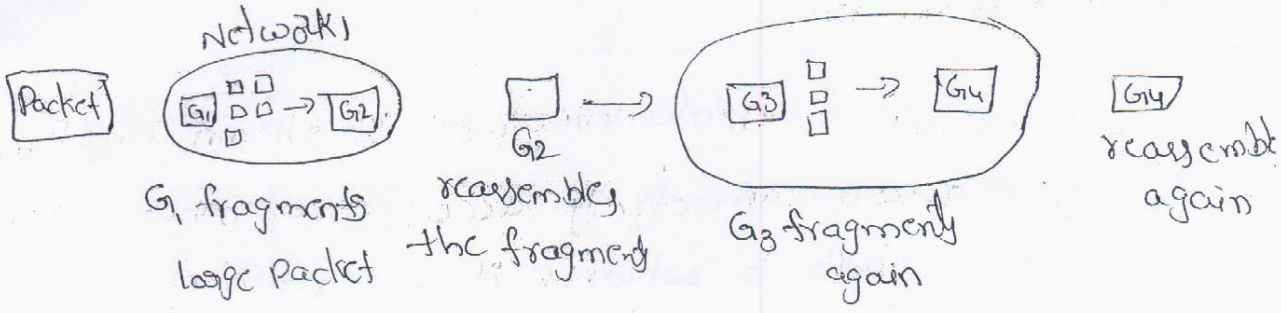
→ Maximum Packet Size may vary from one nw to another. fragmentation are of two type: 1. Transparent

2. nonfragmentation.

1. Transparent fragmentation:-

→ The first strategy is to make fragmentation caused by a small Packet network transparent to

must pass on its way to the ultimate destination.
→ when an oversized packet arrives at a gateway, the gateway breaks it up to fragments.
→ Each fragment is addressed to the same exit gateway, where the pieces are recombined.



(a). Transparent fragmentation

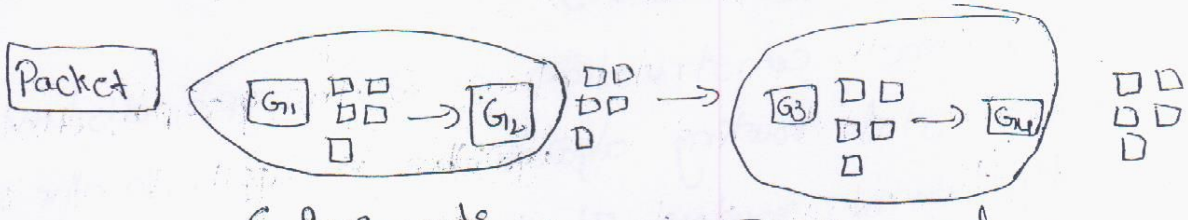


fig: Nontransparent fragmentation

Problems of Transparent fragmentation

1. The exit gateway must know when it has received all the pieces, so either a count field or an end of packet bit must be provided.
2. All packets must exit via the same gateway.
3. ~~overhead~~ Nontransparent fragmentation:-
1. Once a packet has been fragmented, each fragme

IPV4:- Internet Protocol taking a layer-3 Protocol (OSI) takes data segments from layer-4 (Transport) and divides it into a Packet IP Packet encapsulating data unit received from above layer and add to its own header information.

(IP Encapsulation)

The encapsulated data is referred to as Ip payload. IP header contains all the necessary information to deliver the Packet at the other end

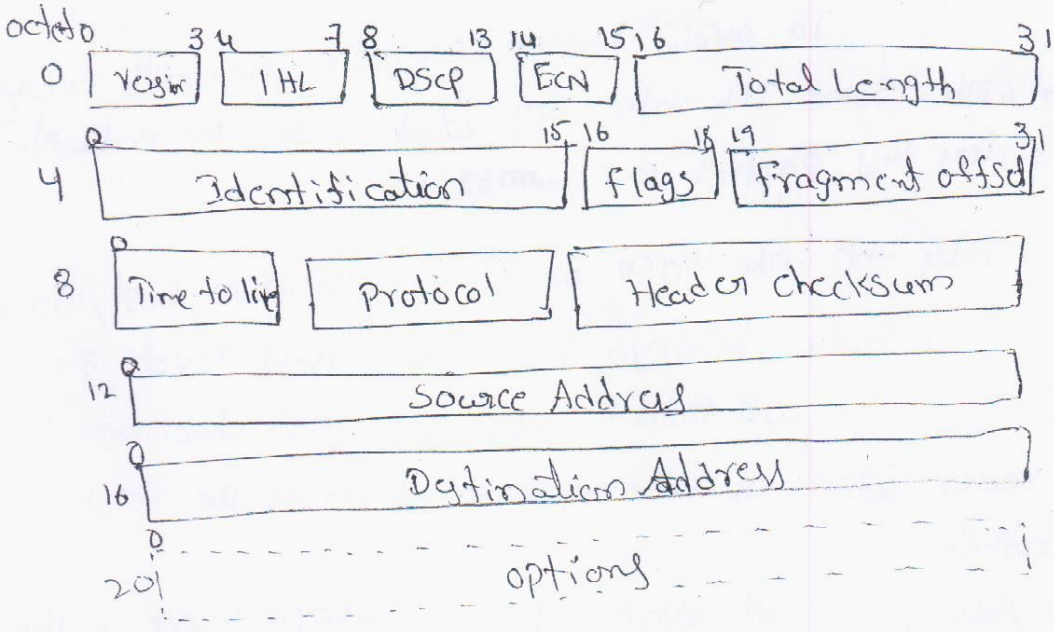


fig: IP Header

IP header includes many relevant information including version number, which in this context is 4.

1. Version: Version no. of internet Protocol used (eg. IPV4)
2. IHL: Internet header Length; Length of entire IP header
3. DSCP: Differentiated Service code point; This is Type of Servic
4. ECN: Explicit Congestion Notification: It carries information about

5. Total length :- Length of entire IP Packet (including IP header & IP payload).

6. Identification :- If IP Packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP Packet.

7. flags :- If IP packet is too large to handle, these 'flags' tell if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.

8. Fragment offset :- The offset tells the exact position of the fragment in the original IP Packet.

9. Time to leave :- To avoid looping in the network every packet is sent with some TTL value set, which tells the network how many routers this packet can cross.

10. Protocol :- Tells the nw layer at the destination host, to which Protocol this Packet belongs to, i.e the next level protocol

11. Header checksum :- This field is used to keep checksum value of entire header which is then used to check if the Packet is received error-free.

12. Source Address :- 32-bit address of the sender (or source) of the packet

13. Destination Address :- 32-bit address of the receiver (or destination) of the Packet.

14. options :- This is optional field, which is used if the value of IHL is greater than 5. This option may contain values for option such as security, Record Route Time stamp etc.

IPV6:-

Features:-

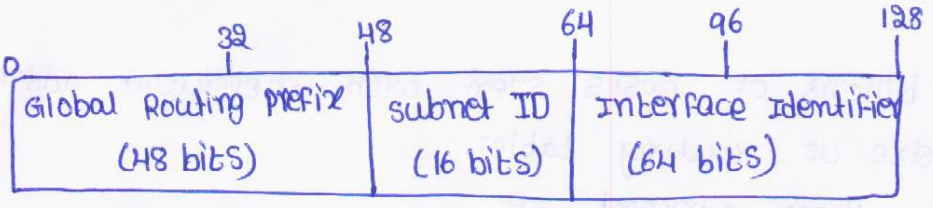
→ It supports billions of hosts, even with inefficient address alloca
→ Reduces the size of routing tables.
→ More security than current IP.
→ Tries to accommodate better Quality-of-service (QOS)
→ Allows old and new protocols to coexist.
→ Allows the host to roam without changing its address.
→ Assists multicasting by specifying scopes.
→ Allows the protocol to evolve in future.

- The addresses in IPV6 are 16 bytes long. Even without efficient utilization, we can get 1500 addresses per square foot.
- IPV6 addresses do not have classes, but the adress space is still sub divided into various ways based on the leading bits, like based on leading bits, like based on prefix, we can resource it either for local use or multicast or broadcast or also for host address.

Address prefix Assignments for IPV6.

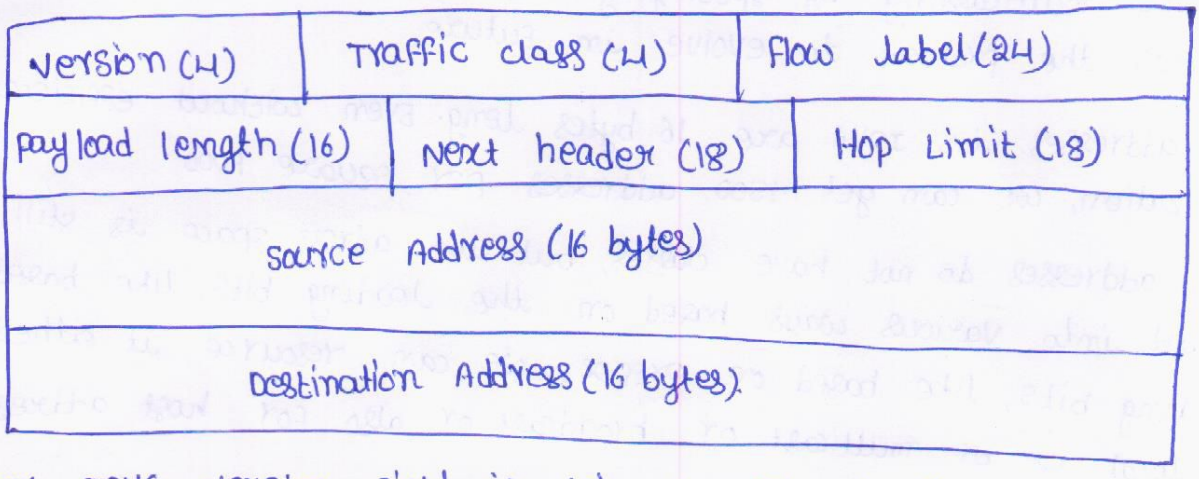
prefix	use
00 ..... 0 (128 bits)	Unspecified
00 ..... 1 (128 bits)	Loopback
1111 1111	multicast addresses
1111 1110 10	List Local unicast
1111 1110 11	site Local unicast
Everything else	Global unicast

IPV6 Global unicast Address format



→ Each address is represented as x:x:x:x:x:x:x:x ('x 8-times') with e "x" representing a hexadecimal notation of 16-bit piece of address.

The IPV6 header format is shown in below fig:-



→ FOR IPV6 version field is '6'. "Traffic class" is to differen between packets with different real-time delivery requirements.

→ Flow label enables source and destination to setup a pseudo c with particular properities

→ payload length field tells us how many bytes will follow the 40 byte header.

→ Next header field enables additional or optional extension headers.

→ Hop limit keeps maximum limit on number of routers that process the packet.

* The two techniques used for the transition from IP4 to IPV6 are a) Dual-stack operations

b) Tunneling.

(9)

Classless Interdomain Routing (CIDR):-

→ To accomodate an arbitary prefix length to a network number, we are using CIDR.

→ The entries in CIDR routing table contain a 32-bit address and 32-bit mask.

→ CIDR routes packet according to the higher-order bits of the IP packets CIDR uses a technique, called super netting so, that single routing entry covers a block of classful addresses.

→ The world was partitioned into four zones, each one given a portion of the class c address.

→ The allocation was described by RFC 1518 and is as follows.

- Addresses 194.0.0.0 to 195.255.255.255 are for Europe.
- Addresses 198.0.0.0 to 199.255.255.255 are for North America.
- Addresses 200.0.0.0 to 210.255.255.255 are for central & south America
- Addresses 202.0.0.0 to 203.255.255.255 are for Asia and the pacific.

→ The routing tables all over Asia are now updated with three entries, each one contains bars and mask addresses.

The entries are.

Addresses			Masks.	
11001010	00011000	00000000	11111111	11111111
			11110000	00000000
11001010	00011000	00010000	11111111	11111111
			11110000	00000000
11001010	00011000	00001000	11111111	11111111
			11111100	00000000

→ Sometimes CIDR is called as "classless routing".

Address Resolution protocol (ARP):-

→ARP maps the IP Addresses and MAC addresses, which IP address belongs to which MAC address. This mapping can be done statically or dynamically.

→ Dynamic mapping is done by ARP and RARP protocols. ARP maps IP addresses to MAC addresses and RARP does the reverse.

→ Suppose a host 'A' wants to know MAC address of host 'B' for which IP address of 'B' is known to 'A'. So 'A' sends ARP packet containing MAC address, IP address of A and B. This packet will be broadcasted in the N/W.

→All the hosts in the N/W take that packet. They compare IP address in packet with their IP address. All except 'B' will discard the packet.

→Only 'B' identifies the IP address & fills its MAC address & forms ARP reply packets. It sends it directly to 'A'. Since 'B' can know MAC address of 'A' from ARP request packet.

Hardware Type		protocol Type.
Hardware Length	protocol Length	operation Request 1 Reply 2.
sender Hardware Address (For example. 6 bytes for Ethernet)		
sender protocol Address (For example, 4 bytes for IP)		
Target Hardware Address (For example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol Address. (For example, 4 bytes for IP)		

* Typical ARP Packet.

Hardware Type:- This is a 16-bit field defining the type of network on which ARP is running.

Protocol Type:- This is a 16-bit field defining the protocol using ARP

Hardware length:- This is an 8-bit field defining the length of th Physical address in bytes.

Protocol length:- This is an 8-bit field defining the length of the Ip address in bytes.

Operation:- This is a 16-bit field defining the type of packet. Two Packet types are defined, ARP request and ARP reply.

Sender Hardware Address:- This is a variable-length field defining the physical address of the sender.

Sender protocol Address:- This is a variable-length field defining the logical address of the sender.

Target Hardware Address:- This is a variable-length field defining th physical address of the target.

Target protocol Address:- This is a variable-length field defining the logical address of the target.

Reverse Address Resolution protocol (RARP):-

→RARP assigns IP address to a known MAC address. RARP server sees this MAC address and finds its IP address from local configuration files and gives reply.

→ However, IP address can be coded into boot image itself. But, since, several clients get boot image from some servers, all may get the same IP address.

→ RARP demands the presence of RARP server on each network. Such RARP requests cannot be broadcasted onto other LANs. To avoid this problem Bootstrap protocol was designed.

→ RARP uses Ethernet broadcast messages, whereas BOOTP uses UDP messages.

Dynamic Host configuration protocol:-

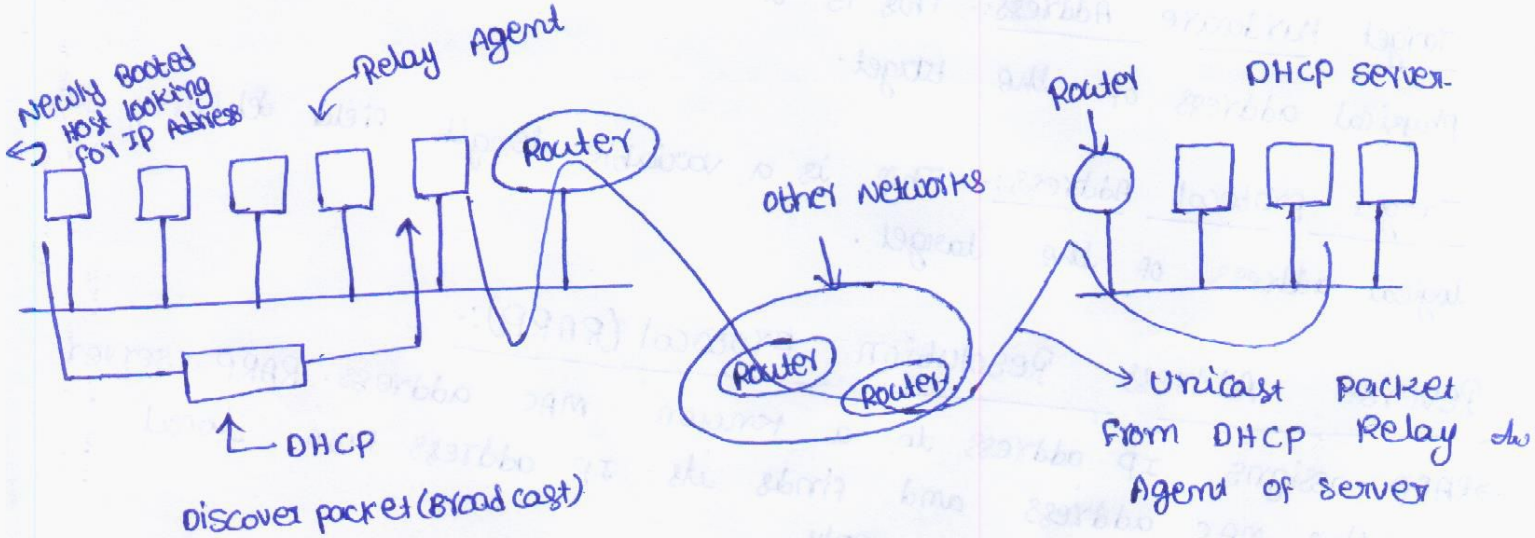
→ when a new host is added, it can't use BOOTP until administrator assigns IP address to it and enters entry into BOOTP configuration tasks. To avoid it, BOOTP was extended to DHCP.

→ DHCP supports both manual and automatic addressing assignment.

→ DHCP will have DHCP server, one for several LANs and a DHCP relay agent ~~sent~~ receives such broadcasts & get the information from DHCP server via a unicast connection.

→ All that needed by DHCP relay agent is IP address of DHCP server. However, IP addresses are assigned to hosts only on a 'lease' basis.

→ If renewal request is denied, it has to try again with DHCP request.



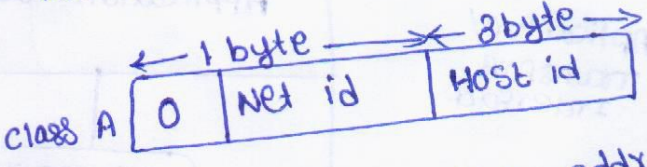
* DHCP Representation.

→ The main difference between the transport and network layer is that the transport layer resides in the local machine whereas the network layer is spread across the network.

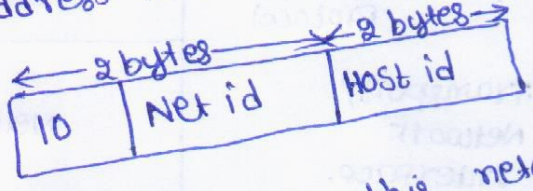
IP Addresses:-

→IP protocol uses 32-bit address (4-bytes) for the network addressing, depending on applications the network addresses are classified into 5 types. class A, class B, class C, class D, class E.

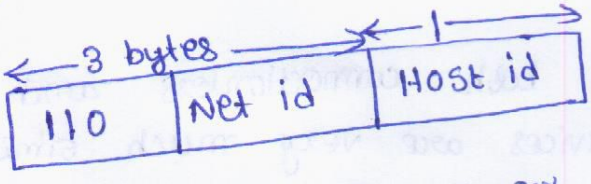
class A Network Address:- In class A, 1 byte is used for network address and 3 bytes are used for host address. The first bit is always '0' for class A network.



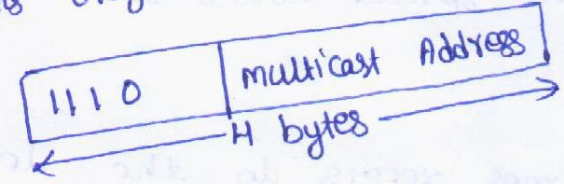
Class B Network Address:- In this addressing 2 bytes are reserved for a network address and 2 bytes are reserved for a host address.



Class C Network Address:- In this network address, 3 bytes are reserved for net id and 1 byte for host id. The first 3 bits are reserved as 110.



Class D Network Address:- It is used for multicasting and indicating the multicast group address. It doesn't contain any net id or host id. It contains only a group id.

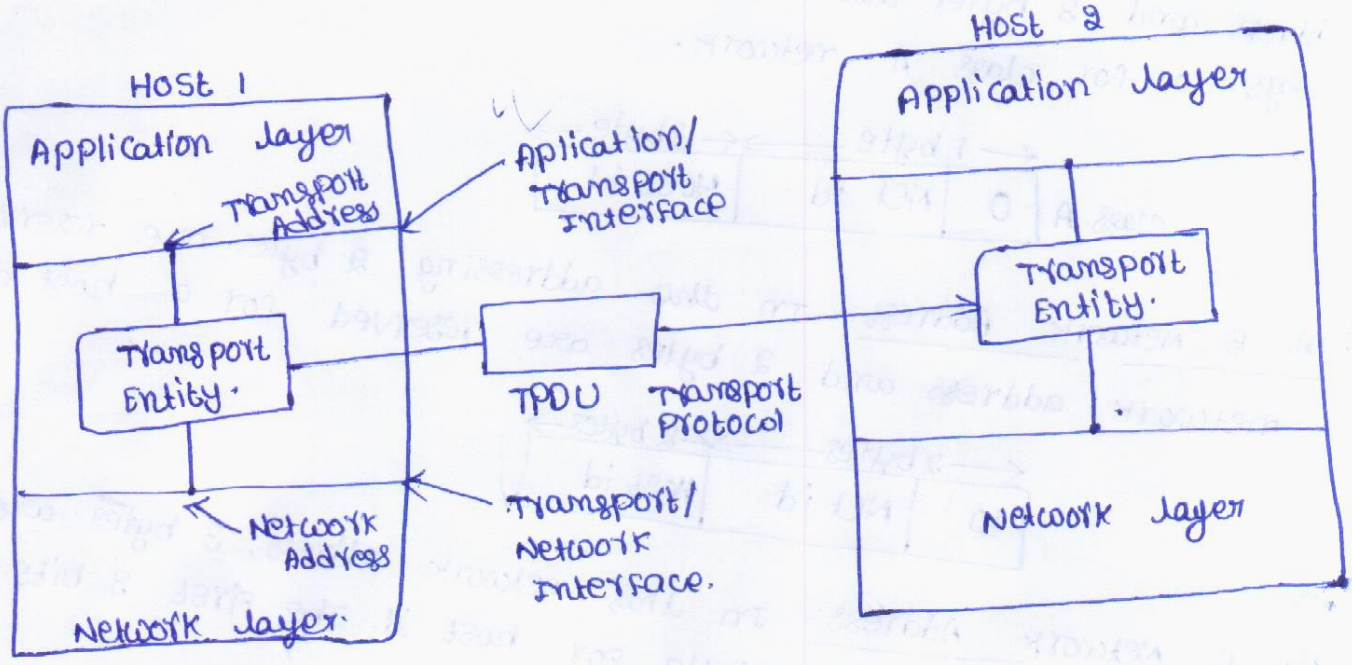


Class E Network Address:- Class E address is reserved for future use. The first byte bits are reserved as 1110.

Transport layer :-

Services provided to the upper layers:

→ The main goal of the transport layer is to provide reliable, cost effective and efficient data transport to the application layer and hide the underlying network details from users and the application layer.



→ The elements of the transport layer are combinedly called the "transport entity".

→ Transport layer offers both connectionless and connection oriented services. These services are very much similar to the services provided by the network layer.

→ The main difference between the transport and Network layer is that the transport layer resides in the local machine whereas the network layer is spread across the network.

Quality of Service :- (QoS)

→ Quality of service sometimes refers to the level of quality provided i.e., the guaranteed service quality.

→ High quality of service is often confused with a high level of performance or achieved service quality. For example, high rate, low latency and low bit error probability.

Various quality of service parameters are as follows.

a) connection establishment delay.
b) Throughput
c) Transit Delay
d) protection
e) priority
f) Resilience
g) Residual error ratio.
h) connection establishment failure probability.

Connection establishment Delay:- The amount of time taken for requesting a connection & its acknowledgement

Throughput:- Time taken to measure the no. of bytes of user data that is transferred per second.

Transit Delay:- Time taken for transmitting the message by source and receipt at destination.

Protection:- provides ways for protecting the data against unauthorized reading & modifying

Priority:- provides a way to give priority to connections & specifies which connection is more important than the other.

Resilience:- specifies the probability of transport layer.

Residual error Ratio:- counts the no. of missed or scrambled messages as a fraction of total no. of messages transmitted.

Connection establishment failure probability:- This specifies the probability of a connection not getting established within the specified time due to congestion or hardware malfunctioning.

Transport layer service primitives:-

The transport layer service primitives are

LISTEN :- server is waiting for connection request.

CONNECT : client sends the connection request TPDU, requesting for connection.

SEND : Transfer the data.

RECEIVE : Receive the data.

DISCONNECT : Terminates the connection using DISCONNECT TPDU.

ADDRESSING CONNECTION ESTABLISHMENT:-

Addressing:-

-> The transport entity can be addressed to TSAP A Transport entity can have multiple TSAPs. (Transport service Access point).

-> Transport address is usually a hierarchical address & uniquely identifies a transport entity. A true universal transport address may have the following format.

Transport address = <galaxy><star><plane><country><network><host><port>

connection Establishment:-

connection establishment may simply sending CONNECTION REQUEST TPDU to the remote machine. Many problems occur when these TPDUs are lost, stored somewhere in the network & sent after a long delay.

Duplicate TPDUs are created and original TPDUs and its duplicates arrive at the destination. Thus a congestion will be caused.

Crash Recovery:-

→ The transport layer can recover from the crashes in the network and router by retransmission or by setting up a new virtual circuit. But the problem arises when the host itself crashes.

→ one technique of recovery from host crashes is that the clients continue to work even after the server crashes.

→ server will broadcast a TPDU to all clients after restart, about the status of the connection.

→ Based on the information received from the clients, server identifies its previous state and takes the necessary action.

→ After receiving a message, the events that can occur at the client are aknowledging (A), writing the message onto upper layer(W) and crash(C).

→ A, W, C can occur in any order based on the strategy implemented at the client.

→ server may take the following actions for recovery of always retransmit, never retransmit, retransmit when no message are outstanding (S0), or retransmit when

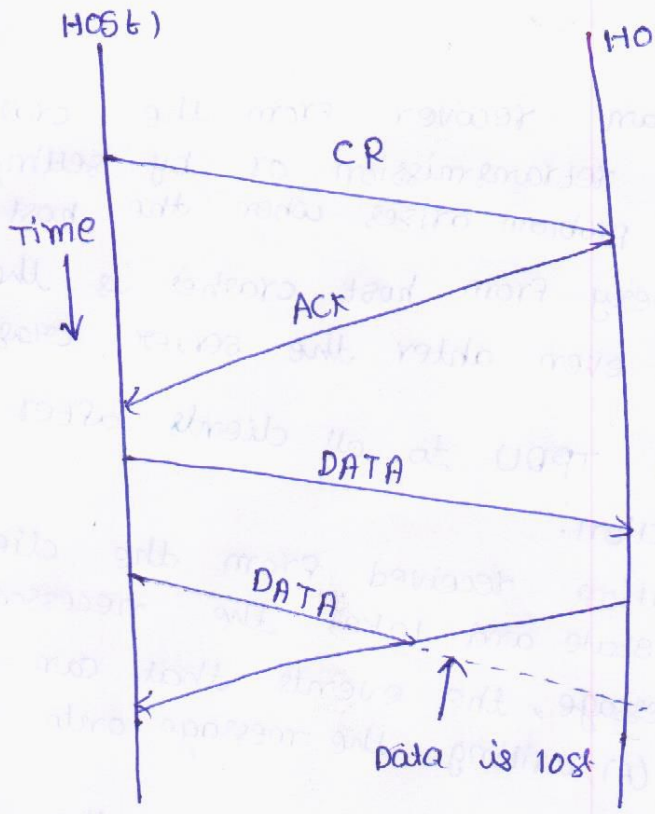
→ In general, crashing at any layer can be hidden from the upper layer. Recovery for a layer N crash can be done by layer N+1 provided it maintains enough information.

CONNECTION RELEASE

connection can be released in two ways 1) Asynchronous and 2) synchronous.

Asynchronous disconnection:-

In Asynchronous style of releasing connection is terminated when either party hangs up by sending of DISCONNECT TPDU. This is similar to how telphone system works. This type of terminating a connection is abrupt and can lead to loss of data.



Synchronous Disconnection:- In a synchronous release, there will not be any data loss. In this case, connection will be terminated when each direction releases it. But, it does not work always and may lead to famous problem called "two-army problem".

UNIT - V

THE INTERNET TRANSPORT PROTOCOLS: UDP

The Internet has two main protocols in the Transport Layer, a connectionless protocol and a connection-Oriented one. In the following The connectionless protocol is UDP. The connection oriented protocol is TCP. Because UDP is basically just IP with a short header added we will start with it. We will also look at two Applications of UDP.

Introduction to UDP:-

The Internet protocol suite supports a Connectionless transport (layer) protocol, UDP (User datagram protocol). UDP provides a way for applications to send encapsulated IP datagrams and send them without having to Establish a Connection. UDP transmits segments Consisting of an 8 bytes followed by the payload. the header is as shown in the below figures.

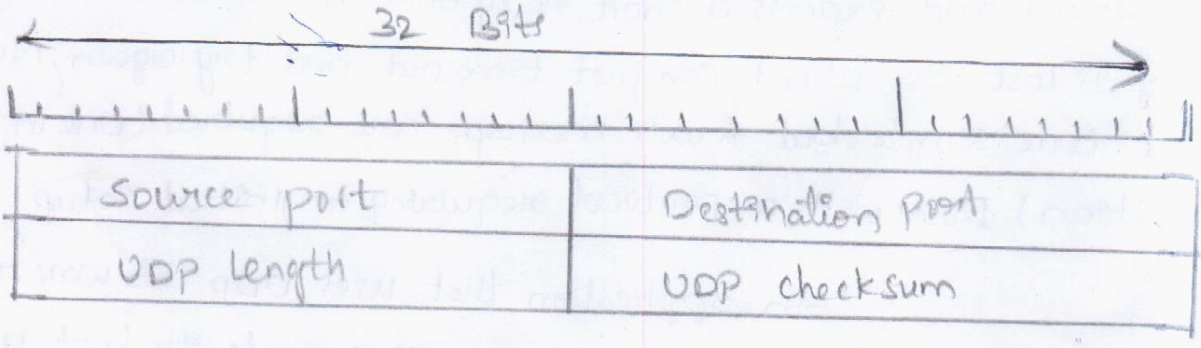


Fig: The UDP header.

The two ports serve to identify the End points within the Source and destination machines. When a UDP packet arrives, its payload is handed to the process attached to the destination port. this attachment occurs when BIND primitive or Something Similar is used as we saw in TCP.

(The binding process is the same for UDP). In fact the main value of having UDP over just using raw IP is the addition of the source and destination ports. Without the port fields, the trans-port layer would not know what to do with that packet. With them it delivers segments correctly. the source port is primarily needed when a reply must be sent back to the source. By copying the source port field from the incoming segment into the destination port field of the outgoing segment, the process sending the reply can specify which process on the sending machine is to get it.

The UDP length field includes the 8-bytes header and the data. the UDP checksum is optional and stored as "0" if not computed (a true computed "0" is used to stored as all "1"s). (It is off is for) the UDP is provides an interface to the IP protocol with the added feature of demultiplexing multiple processes using the ports. For applications that need to have precise control over the packet flow, error control, or timing, UDP provides just what the doctor ordered. one area where UDP is especially useful is in client-server situations. often, the client sends a short request to the server and expects a short reply back. If either the request or reply is lost, the client can just time out and try again. Not only is the code simple, but fewer messages are required (one in each direction) than with a protocol requiring an initial setup.

An application that uses UDP this way is DNS (the domain Name System). a program that needs to look up the IP address of some host name. for Example. www.cs.berkeley.edu can send a UDP packet containing the host name to DNS server. the server replies with a UDP packet containing the host's IP address. No setup is needed in advance and no release is needed just two messages govern the Network.

Remote procedure call :- (RPC)

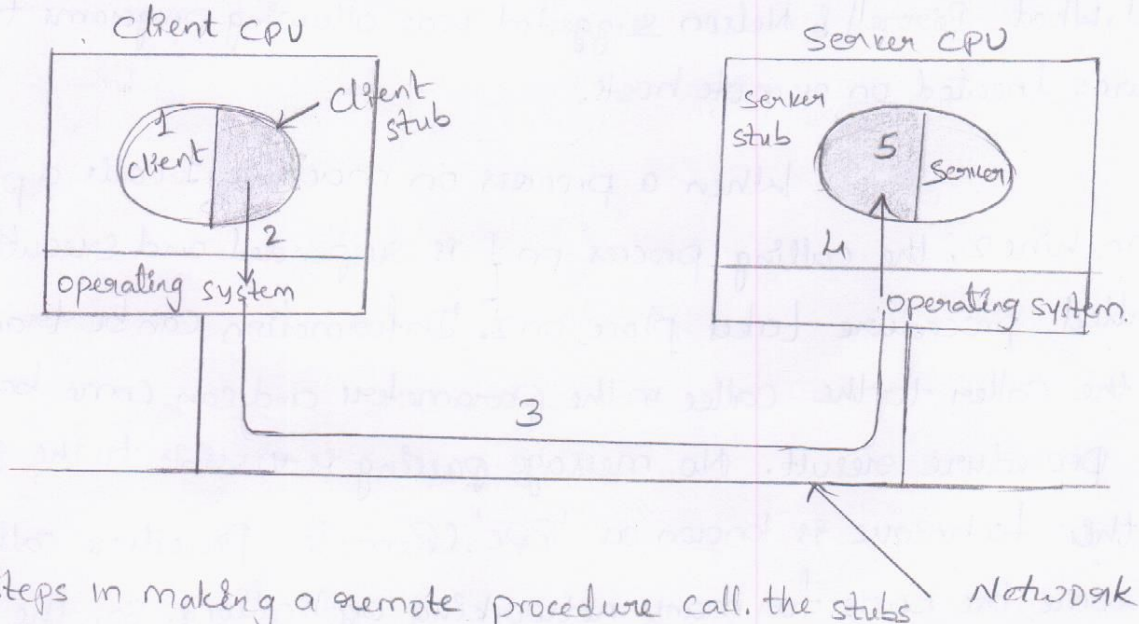
In a certain sense, sending a message to a remote host and getting a reply back is a lot like making a function call in a programming language. In both cases you start with one or more parameters and you get back a result. this observation led people to try to arrange request reply interactions on Nlws to be cast in the form of procedure calls. Such an arrangement makes Nlw applications much Easier to program and more familiar to deal with. For Example Just imagine a procedure named get_IP_address (host name) that works by sending a UDP packet to DNS server and waiting for the reply, timing again if one is not forthcoming quickly Enough. In this way all the details of Nlw can be hidden from the programmer. The key work in this area was done by Birrell and Nelson (1984). In a nutshell, what Birrell & Nelson suggested was allowing programs to call procedures located on remote hosts.

When a process on machine 1 calls a procedure on machine 2, the calling process on 1 is suspended and Execution of the called procedure takes place on 2. Information can be transported from the caller to the callee in the parameters and can come back in the procedure result. No message passing is visible to the programmer. this technique is known as "RPC" (Remote Procedure call) and has become the basis for many networking applications. So, the Calling procedure is known as the client and the called procedure is known as the server. In the simplest form to call a remote

~~The Real-time Transport Protocol~~ :-

procedure the client program must be bound with a small library procedure, called the client stub, that represents the server procedure in the client's address space. Similarly the server is bound with a

Procedure called the server hub. these procedures hide the fact that the procedure call from the client to the server is not local. the actuall steps in making an RPC are shown in below figures. step 1 is the client calling the client stub. this call is a local procedure call, with the parameters pushed onto the stack in the normal way. step 2. is the client stub packing the parameters into a message and making a system call to send the message. packing the parameters is called marshaling. step 3. is the kernel sending the message from the client machine to the server machine. step 4 is kernel passing the incoming packet to the server stub. Finally step 5. is the server stub calling the server procedure with unmarshaled parameters. the reply traces the same path in the other direction.



Steps in making a remote procedure call. the stubs are shaded.

The Real time transport protocol:-

Client-server RPC is one area in which UDP is widely used. Another one is real-time multimedia applications. In particular, as Internet radio, Internet telephony, music-on-demand, videoconferencing, video-on-demand, and other multimedia applications

The Real-Time Transport protocol:-

Became more commonplace, people discovered that each application was reinventing more or less the same real-time transport protocol. the protocol stack for this situation is shown in below figure (packet nesting also).

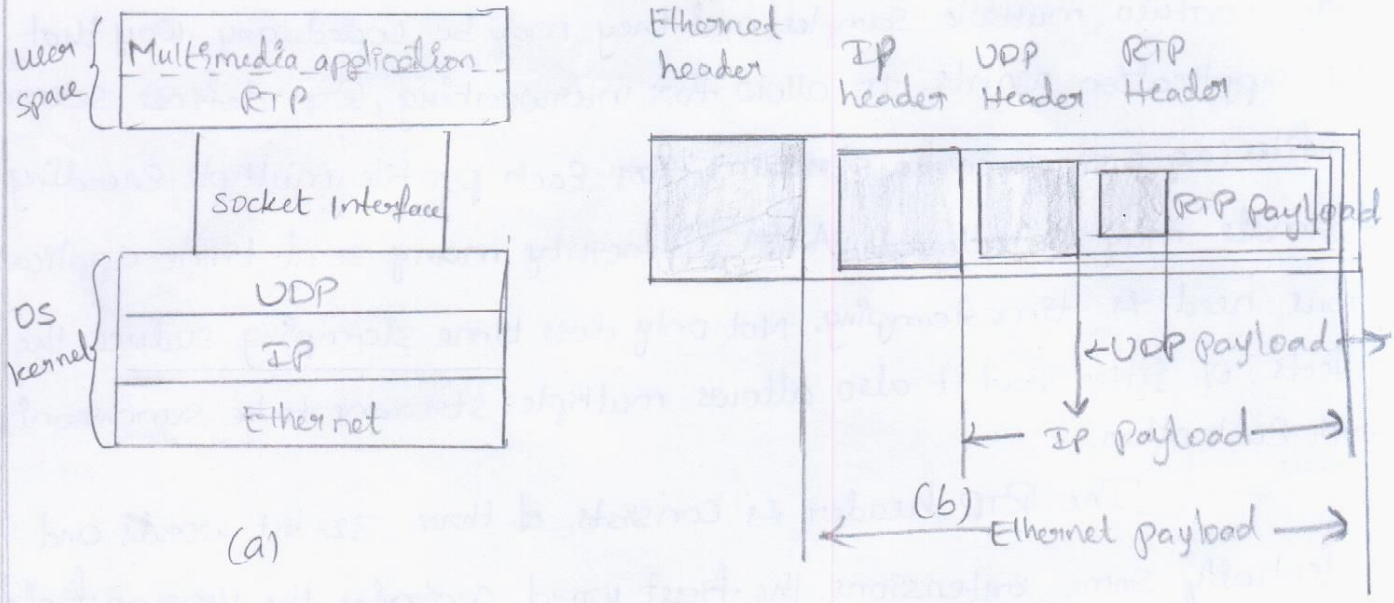


Fig:- (a) The position of RTP in the protocol stack b) packet nesting

the position of RTP in the protocol stack is somewhat strange. It was decided to put RTP in user space and have it (normally) run over UDP. the multimedia application consists of multiple audio, video, text and possibly other streams. these are fed into the RTP library, which is in user space along with the application. this library then multiplexes the streams and encodes them in RTP packets, which it then stuffs into a stocks. At the other End of the socket, UDP packets are generated and Embedded in IP packets. the basic function RTP is to multiplex several real-time data streams onto the single stream of UDP packets the UDP stream can be sent to a single destination (unicasting) or to multiple destinations (multicasting). Because RTP just uses normal UDP its packets are not treated specially by the routers unless some normal IP quality-of-service features are Enabled.

Each packet sent in an RTP stream is given a number one higher than its predecessor. Retransmission is not a practical option since the Re-transmitted packet would probably arrive too late to be useful. As a consequence, RTP has no flow control, no error control, no acknowledge-ments, and no mechanism to request retransmissions. Each RTP payload may contain multiple samples, and they may be coded any way that the application wants. To allow for interworking, RTP defines several profiles (e.g. a single audio stream), for each profile, multiple Encoding formats may be allowed. Another facility many real-time applicat-ions need is timestamping. Not only does time stamping reduce the effects of jitter, but it also allows multiple streams to be synchronized with each other.

The RTP header is consists of three 32-bit words and potentially some extensions. the first word contains the version field, which is already at 2. let us hope this version is very close to the ulti-mate version since there is only one code point left. the P bit indicat that the packet has been padded to a multiple of 4 bytes. the last padding byte tells how many bytes were added. the X bit indicates that an Extension header is present. the format and meaning of the Extension header are not defined. the only thing that is defined is that the first word of the Extension gives the length. this is an Escape hatch for any unforeseen requirements.

The CC field tells how many contributing sources are present, from 0 to 15. the M bit is an (Escape hatch for any unforeseen) application-specific marker bit. It can be used to mark the start of a video frame, the start of a word in an audio channel, or something else that the application under-stands. the payload type field tells which Encoding algorithm has been used.

Since every packet carries this field, the encoding can change during transmission. the sequence number is just a counter that is incremented on each RTP packet sent. It is used to detect lost packets. the timestamp is produced by the stream's source to note when the first sample in the packet was made. this value can help reduce jitter at the receiver - by decoupling the playback from the packet arrival time. the synchronization source identifier tells which stream the packet belongs to. It is the method used to multiplex and demultiplex multiple data streams onto a single stream of UDP packets. Finally the contributing source identifiers, if any, are used when mixers are present in the studio. In the mixer is the synchronizing source, and the streams being mixed are listed here.

RTP has a little sister protocol called RTCP (Real time Transport control protocol). It handles feedback, synchronization, and the user interface but does not transport any data. RTCP also handles inter stream synchronization, & RTCP provides away for naming various sources like ASCII.

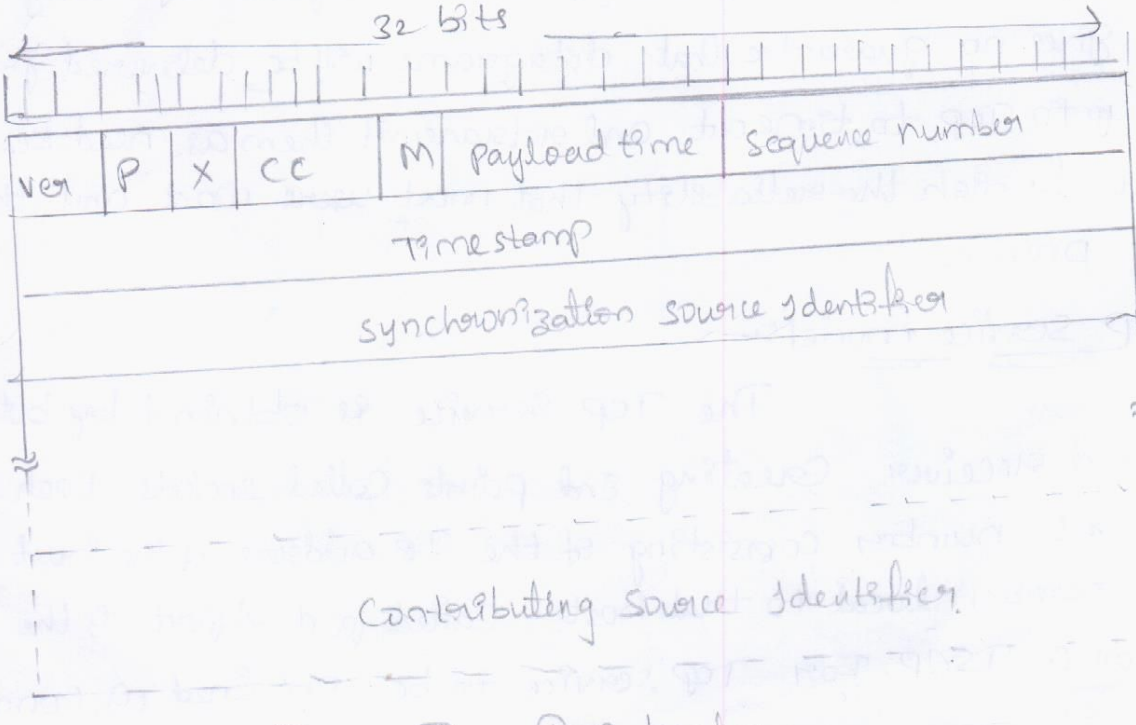


Fig:- The RTP header

The internet transport protocols: TCP :-

UDP is a simple protocol and it has some niche uses, such as client-server interactions and multimedia, but for most internet applications, reliable, sequenced delivery is needed. UDP cannot provided this. So another protocol is required. It is called TCP and is the main workhorse of the internet. Let us now study it in detail.

Introduction to TCP :⇒

TCP (Transmission control protocol) was specifically designed to provide a reliable end to end byte stream over an unreliable internetwork. An internetwork differs from a single network because different parts may have wildly different topologies, bandwidths, delays, packets sizes, and other parameters. Each machine supporting TCP has a TCP transport entity, either a library procedure, a user process, or part of the kernel. In all cases. It manges TCP streams and Interfaces to the IP layer. A TCP entity accepts user data streams from local processes, breaks them up into pieces not exceeding 64KB (1460 data bytes in order to fit in a single Ethernet frame with the IP the TCP headers) and sends each (Packet) piece as a separate IP datagram. IP layer gives no guarantee that datagrams will be delivered properly so it is up to TCP to time out and retransmit them as need be. the TCP must furnish the reliability that most users want and that IP does not provide.

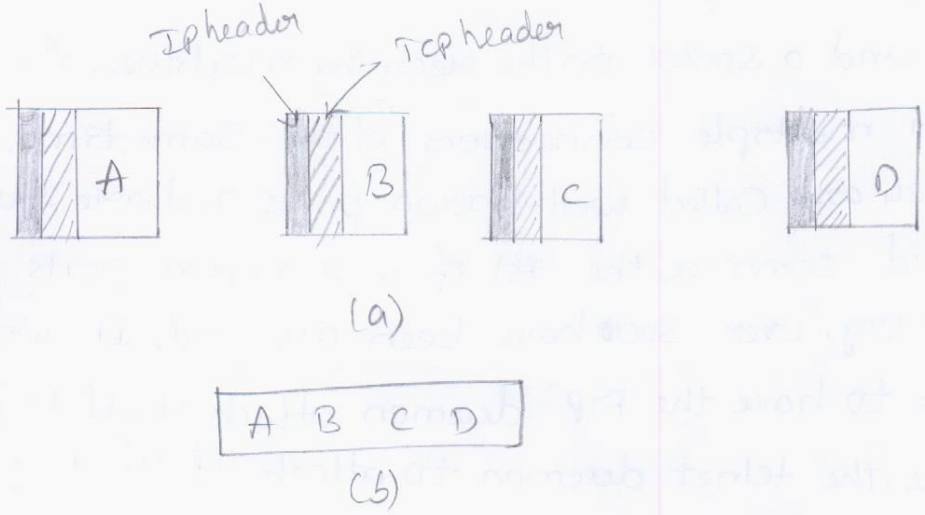
The TCP service model :-

The TCP service is obtained by both the sender and receiver creating end points called sockets. Each socket has a socket number consisting of the IP address of the host and a 16 bit number local to that host called port. A port is the TCP name for a TSAP. For TCP service to be obtained, a connection

must be explicitly established between a socket on the sending machine and a socket on the receiving machine. A socket may be used for multiple connections at the same time. port numbers below 1024 are called well-known ports and are reserved for standard services. the list of well-known ports is given at www.iana.org. over 3000 have been assigned. It would certainly be possible to have the FTP deamon attach itself to port 21 at boot time, the telnet daemon to attach itself to port 23 at boot time, and so on... However, doing so would clutter up memory with daemons that were idle most of the time. All TCP connections are full duplex and point to point full duplex means that traffic can go in both directions at the same time. point-to point means that each connection has exactly two end points. TCP does not support multicasting or broadcasting.

Port	protocol	uses
21	FTP	File transfer
23	Telnet	Remote login
25	SMTP	E-mail
69	TFTP	Trivial file transfer protocol
~~79~~ 79	Finger	Lookup information about a user
80	HTTP	World wide web
110	POP-3	Remote email access
119	NNTP	USENET news

Fig:- Some assigned ports.



(a) Four 512 bytes segments sent as separate IP datagrams.
(b) The 2048 bytes of data delivered to the application in a single READ call.

A TCP connection is a byte stream, not a message stream. Message boundaries are not preserved end to end. Some early applications used the PUSH flag as a kind of marker to delineate messages boundaries. When an application passes data to TCP, TCP may send it immediately or buffer it, at its discretion. However, sometimes, the application really wants the data to be sent immediately. One last feature of the TCP service that is worth mentioning here is urgent data. When an interactive user hits the DEL or CTRL-C key to break off a remote computation that has already begun. When the urgent data are received at the destination the receiving application is interrupted. So it can stop whatever it was doing and read the data stream to find the urgent data.

The TCP segment Header:⇒

In the TCP segment Every segment begins with a fixed format, 20 byte header. the fixed header may be followed by header options. After the options, if any up to 65,535-20-20 = 65,495 data bytes may follow, where the first 20 refer to the IP header and the second to the TCP header segments without any data are legal and are commonly used for acknowledgements and control messages.

the source port and destination port fields identify the local end points of the connection. the well-known ports are defined at www.iana.org but each host can allocate the others as it wishes. A port plus its host's IP address forms a 48-bit unique end point. the source and destination end points together, identify the connection. the sequence number and Acknowledgement number fields perform their usual functions. Note that the latter specifies the next byte expected, not the last byte correctly received. Both are 32 bits long because every byte of data is numbered in a TCP stream.

the TCP header length tells how many 32 bit words are contained in the TCP header. this information is needed bcz the options field is of variable length so the header is, too. Technically, this field really indicates the start of the data within the segment, measured in 32-bit words. but that number is just the header length in the words, so the effect is the same. URG is set to 1 if the urgent pointer is in use. the Ack bit is set to 1 to indicate that the Acknowledgement number is valid if Ack is 0, the segment does not contain an acknowledgement so the Acknowledgement number field is ignored. the PSH bit indicates pushed data. the RST bit is used to reset a connection that has become confused due to a host crash or some other reason. the SYN bit is used to establish the connections. the connection request has SYN=1 and ACK=0 to indicate that the piggyback acknowledgement field is not in use. the FIN bit is used to release a connection. It specifies that the sender has more data to transmit. Both SYN and FIN segments have sequence numbers and are thus guaranteed to be processed in the correct order. A window size field of 0 is legal and says that the bytes up to and including Acknowledgement number - 1 have been

Received, but that the receiver is currently badly in need of a rest and would like no more data for the moment. the receiver can later grant permission to send by transmitting a segment with the same Acknowledgement number and a nonzero window size field.

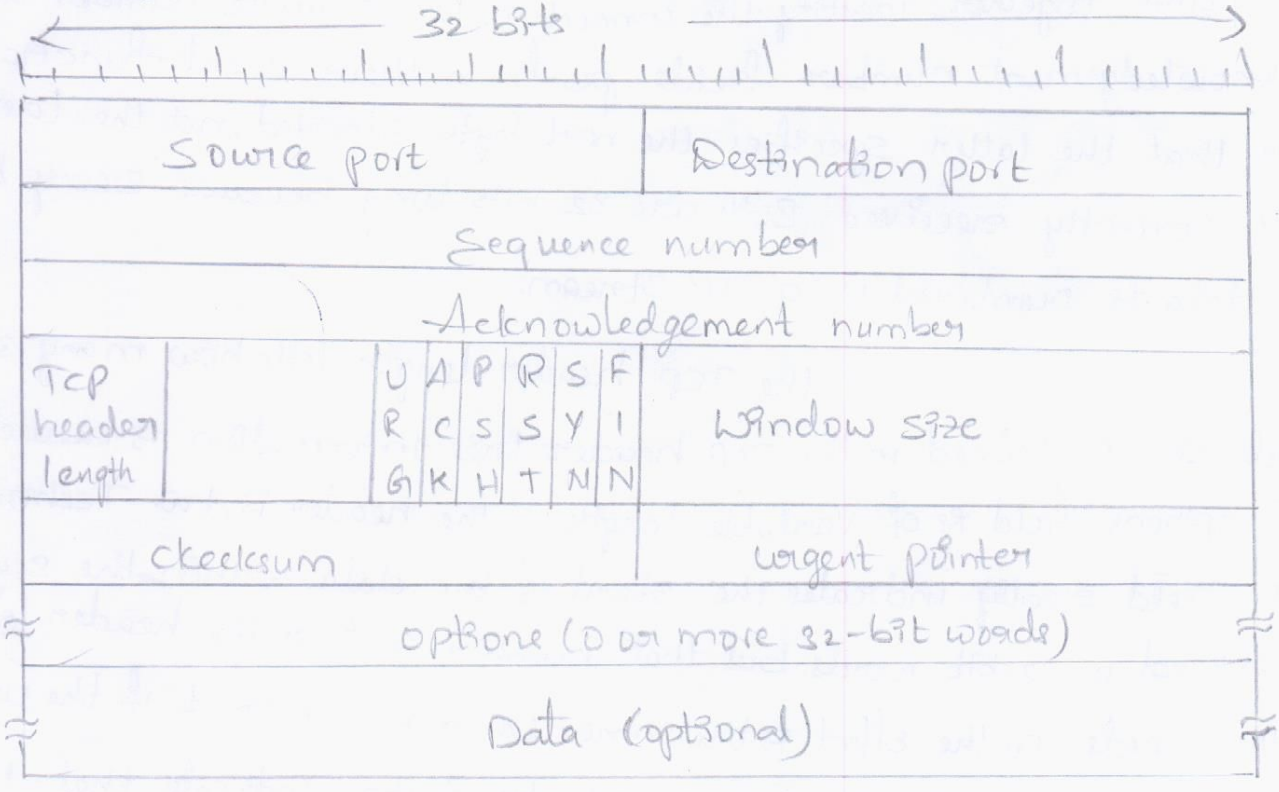


Fig:- The TCP header

Application layer :-

(MIME : multi purpose internet mail Extensions)

Standard client-server applications :-

HTTP :- Hyper text transfer protocol :-

The transfer protocol used throughout the world wide web is HTTP ~~servers~~ and. It specifies what message clients may send to servers and what response they get back in return. Each interaction consists of one ASCII request, followed by one RFC 822 MIME-like ~~res~~ response. All clients and all servers must obey this protocol.

HTTP functions as combination of FTP & SMTP. HTTP is like SMTP because the data transfered b/w client & server looks like SMTP message. In addition the format of message is controled by MIME-like header, HTTP ~~server~~ message are not destinaled to be read by humans; they are read by and interpreted by HTTP server and HTTP client (browser). HTTP delivers messages immidately.

HTTP uses the services of TCP on well-known port 80. on the server machine.

Connections :-

In HTTP 1.0 after the connection was established a single request was sent over and singk response was sent back. The TCP connection was released. Typical web page consisted of HTML text. consisting of large number of icons, images. so establishing TCP connection to transport a single icon became a very Expensive way to operate

This observation led to HTTP 1.1; which supports "persistent connections" with them it is possible to establish a TCP connection. send a request and get a response, and then send additional requests and get additional responces. By amortizing the TCP setup and release over multiple requests.

Methods:- In HTTP the opertions called 'method' other than just requesting a webpage are supported. Each request consists of one or more lines of ASCII text with the first word on the first line being the name of method requested. The names are case sensitive, so GET is a legal method but get is not.

Method	Description
GET	request to read a web page
HEAD	Request to read a web page's header
PUT	Request to store a web page
POST	Append to a named resources (e.g: a web pag
DELETE	Remove the web page
TRACE	Echo the incoming request
CONNECT	Reserved for future use
OPTIONS	Query certain option

Example HTTP Usage:-

Because HTTP is an Ascii protocol. It is quite easy for a person at a terminal to directly talk to web servers. All that need is a TCP connection port 80 on the server.

The following command sequence For UNIX systems)

```
telnet www.ietf.org 80 > log
GET /rfc.html HTTP/1.1
HOST : www.ietf.org

close.
```

* This sequence of command starts up a telnet (i.e TCP) connection to port 80 on IETF's web server, www.ietf.org. The result of the session is re-directed to File log for later inspection.
* Then comes to GET command naming the file and the protocol.
* Next line is the mandatory HOST header
* close command instruct the telnet program to break the connection.

The first 3 lines are o/p from the telnet program the line begining HTTP/1.1 is IETF's response saying that it is willing to talk HTTP/1.1 with you.

FTP:- File transfer protocol:-

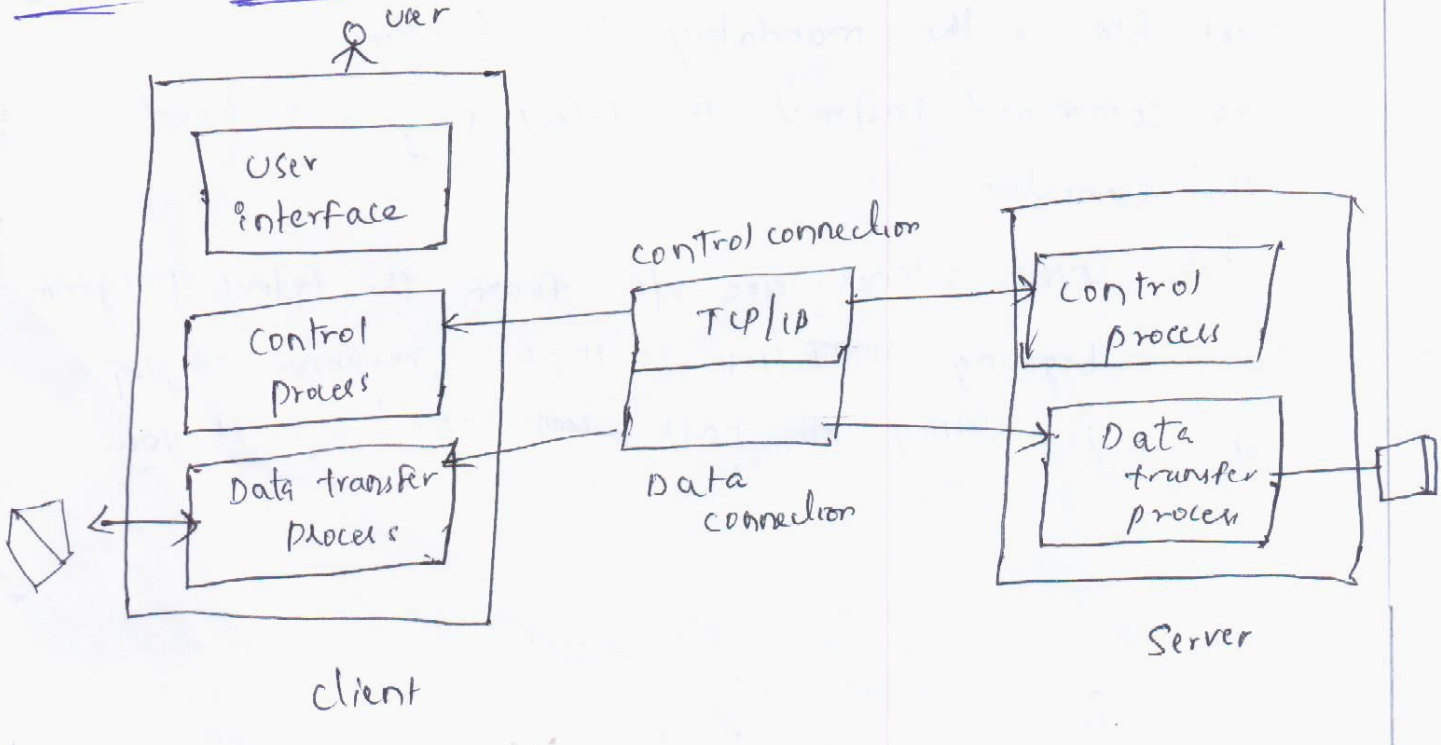
File transfer protocol (FTP) is the standard mechanism provided by TCP/IP for copying a file from one host to another. Although transfering files from one system to another seems simple & straight forward, some problems must be dealt with first. for eg: 2 systems may use different file name conventions. 2 systems may have different way to represent text and data. All these problems have been solved by FTP in a very simple and elegant approch

FTP differs from other client/server application in that it establishes two connections between the hosts.

* one connection is used for data transfer
* another for control information (command & response).

Seperation of command and data transfer makes FTP more efficient. FTP uses two well-known TCP ports :- Port 21 is used for control connection, Port 20 is for data connection

Basic model of FTP:-



* The client has 3 components :- user interface, client control process, and client data transfer process.

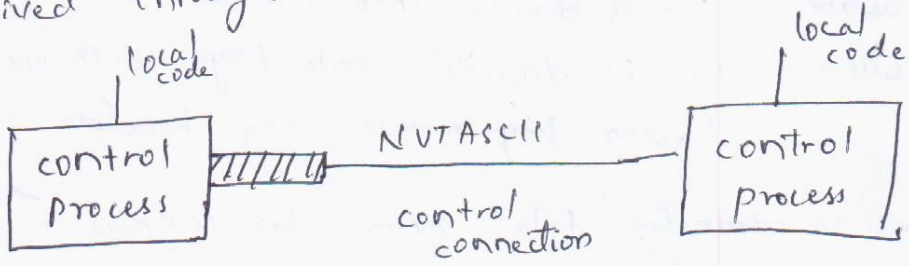
* The server has 2 components :- server control process and server data process.

* The control connection is made b/w the control processes.

* The data connection is made b/w the data transfer process. It remains opened and closed for each file transfer.

communication over control connection :-

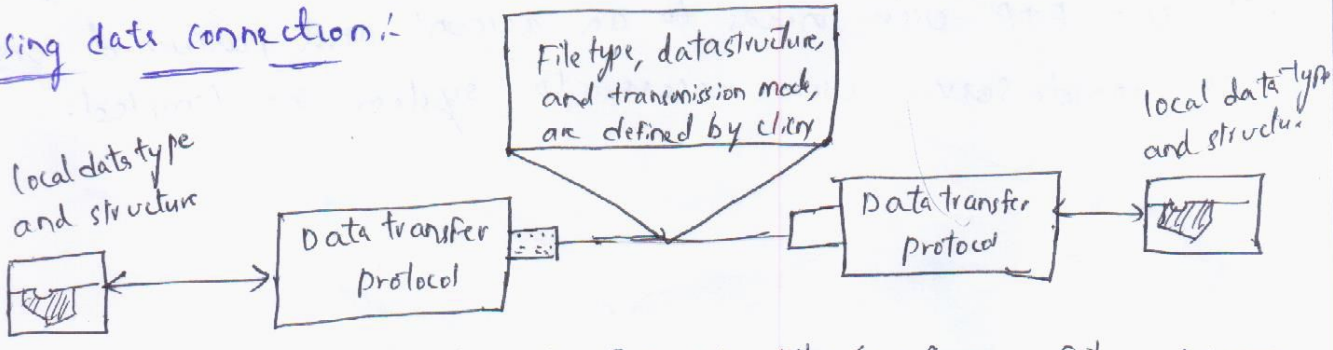
FTP uses 7-bit ASCII character set - communication is achived through command and response.



This simple method is adequate because we send one command or response at a time - Each command or response is only one short line, so we need not worry about file format or structure.

Each line is terminated with a two character (carriage return and line feed) end-of line token.

Using data connection :-



FTP can transfer ASCII File, EBCDIC Files (or) Images File across the data connection.

In ASCII each character is encoded using 7-bit ASCII

* If one or both ends using EBCDIC encoding (the file format used by IBM), the file can be transfered using EBCDIC encoding

The file is sent as continuous streams of bits without any interpretations or encoding.

This is mostly used to transfer binary files such as compiled programs.

Data structure:-

FTP transfer file across data connection by using following interpretation about structure of data:-

i) File structure :- continuous stream of bytes

ii) record structure :- File is divided into records

iii) page structure :- File is divided into pages with each page having page number, page header.

Transmission mode:- FTP transfer file across data connection by using 3 transmission modes

i) Stream mode:- Stream of bytes in default mode

ii) Block mode:- Data delivered from FTP to TCP in blocks havin 3 bytes hea

iii) compressed mode:- If the file is big data can be compressed.

* in text file this is usually space (Blanks)
* In binary file, Null characters are usually compressed.

To use FTP user needs to an account and password on the remote server. User access to system is limited.

Electronic mail (E-Mail):-

Before 1990's it was mostly used in academia. During the 1990's it become known to public at large and grew exponentially to point where no of email's sent per day now is vastly more than no of snail-mail (i.e paper) letters.

Emails like most other forms of communication has its own convention and style.

In 1982, the ARPANET e-mail proposal were published as RFC 821 (Transmission control) and RFC 822 (message format).

Architecture and services:-

In this section we will provide an overview of what e-mail can do and how they are organized. It consists of 2 subsystems

i) user agent:- which allow people to read and send e-mail

ii) message transfer:- which move the message from source to the destination

Typically e-mail systems support 5-basic functions

composition:- Refers to the process of creating message and answer

Transfer:- moving message from the orginator to the recipient

Reporting:- It tells the orginator what happened to the message, is delivered, was it rejected was

Displaying:- incoming message is needed so people can read their e-mail. sometimes conversion is required.

Disposition:- is the final step and concern what the recipient does with the message after recieving it.

The user Agent:-

User agent is normally a program that accepts a variety of commands for composing, receiving and replying to messages.

i) Sending E-mail:- To send an e-mail message, a user must provide the message, the destination adress, and possibly some other parameters. most e-mail system support mailing list, so that a user can send the same message to a list of people with single command.

ii) Reading E-mail:- Typically, when a user agent is started up, it looks at the user's mailbox for incoming e-mail before displaying anything on screen.

Each line of the display contains several field Extracted from the envelope or header of the corresponding message. In a more sophisticated system, the user can specify which fields are to be displayed a 'user profile'.

E-mail has come a long way from the day when it was just File transfer. Sophisticated user agent make managing a large volume of e-mail possible.

Message transfer:- The message transfer system is concerned with relaying message from the orginator to the recipient.

SMTP:- Simple mail transfer Protocol:-

With in the internet e-mail is delivered by having the source machine establish a TCP-connection to port 25 of the destination machine.

In general, getting a second-level domain, such as name-of-company.com, is easy. It merely requires going to a registar for corresponding top-level domain (com in case)

Each domain is named by the path upward from it to the root. Domain names can be either absolute or relative. An absolute domain name always ends with a period (eng.sun.com.) whereas relative one does not.

Domain names are case insensitive, so edu, Edu, EDU mean the same thing.

Eg:- i) cs.yale.edu (yale university in united state)

ii) cs.vu.nl (vrije university, in netherlands)

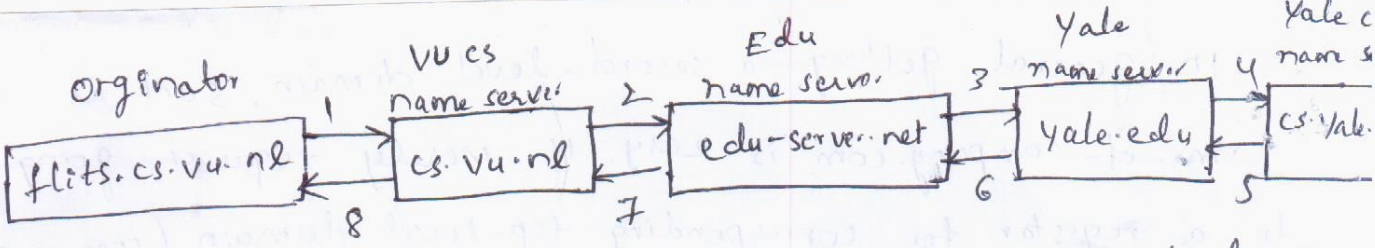
Name servers:-

In theory single name server could contain the entire DNS database and respond to all queries

To avoid the problem associated with having only a single source of information, the DNS name space is divided into non-overlapping zones.

Where the zone boundaries are placed within a zone is up to that zone's administrator.

When a resolver has query about domain name it passes the query to one local name server. An authoritative record is one that comes from the authority that manages the record and is thus always correct.



let us suppose the local name server has never had a query for this domain on there record in this one forward the request cs.yale.edu since each request from client-server the resource record request work It way back to Step 5 through 8.

once these record get back to cs.vu.nl name Server they will be entered into cache there. This is the reason that Time-to-live field is included in resource record.

While DNS is Extremely important to correct functioning of the internet all it really does is map symoblic names for machine in IP address It does not help locate people, resource, Service or object in general.

SMTP is a simple ASCII protocol. After establishing the TCP connection to port 25, the sending machine, operating as the client, waits for the receiving machine.

If the server is willing to accept e-mail the client announces whom the e-mail is coming from and whom it is going to. If such a recipient exist at the destination, the server gives the client go-ahead to send the message. Thus the client sends the message and the server acknowledges it.

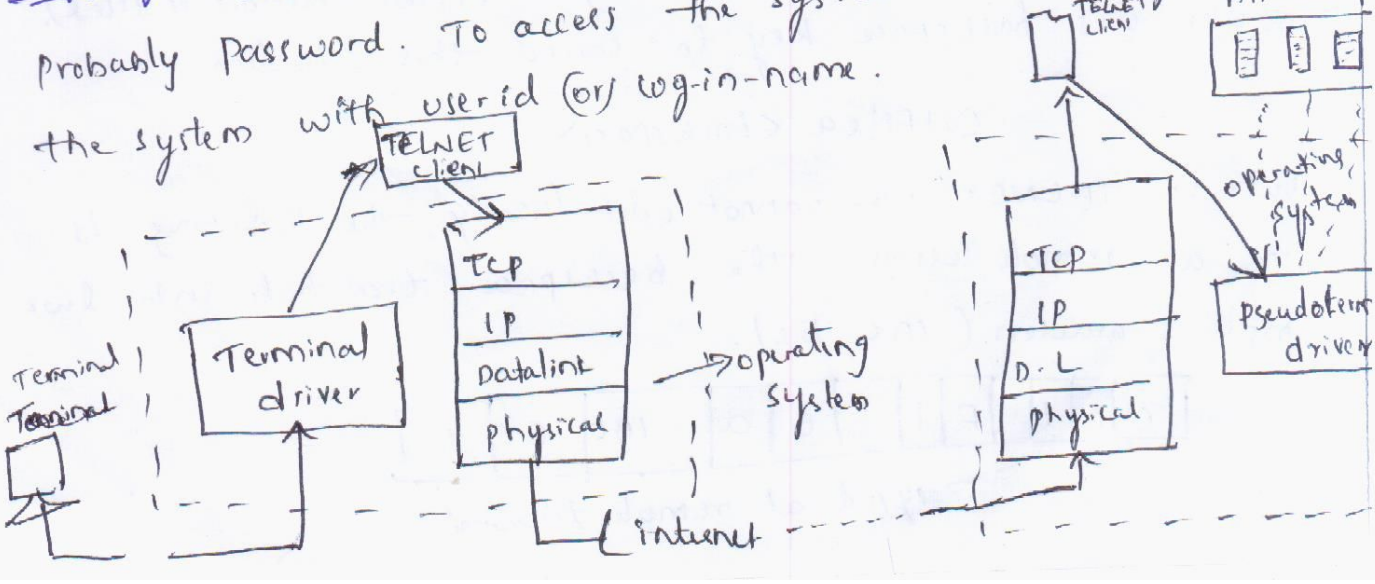
TELNET:-

Telnet is a client-server application program. TELNET is an abbreviation for Terminal NETWORK. It is standard TCP/IP protocol for virtual terminal service as proposed by the international organization for standard (ISO). TELNET enables the establishment of a connection to a remote system such as a way as remote systems

Time sharing environment:-

TELNET was designed at a time when most operating systems, such as UNIX were operating in a time sharing environment.

Logging:- Each authorized user has an identification and probably password. To access the system the user logs into the system with user id (or) log-in-name.



When a user wants to access an application program (or utility) located on remote machine. Here TELNET client and server programs come in use. The user send the keystrokes to terminal driver, where the local OS accepts the character but not interpret them. The characters are sent to TELNET client, which transforms the characters to universal set called "Network virtual terminal" (NVT) characters and delivers them to local TCP/IP protocol stack.

The text in NVT form, travels through internet and arrive at the TCP/IP stack at machine. these characters are passed to O.S and TELNET server. which changes the characters to the ~~correspoince~~ corresponding understandable characters. The Solution is added to piece of software called pseudo terminal dr. The O.S then passes the characters to appropriate application program

Embedding:-

* TELNET use only one TCP connection. The servers uses the well known port 23. and client use an ephemeral port. The same connection is used for sending both data and control char

Eg:- user wants a server to display a file (file1) on a remote server, & we can type

~~catfiel~~ catfiel

catfile1

Suppose name of file has been mistyped (file1 instead of file1). The user uses backspace key to correct this situation

catfile1 <backspace>

Howerver in TELNET user cannot edit locally, the editing is done at remote server. The backspace translate into two remote characters (IAC, EC).

c	a	t		f	i	l	e	1	IAC	EC	1

typed at remote terminal

Mode of operation of TELNET:-

Most TELNET operates in 3 modes

i) Default mode
ii) Character mode
iii) line mode

Default mode:- It is used if no other modes are invoked through option. In this mode echoing is done by the client [echo means data Recieved on one side to other).

Character mode:- each character typed is sent to client to the server. The server normally echoes the character back to be displayed on client screen.

line mode:- A new mode has been compensated for the deficiencies of default mode and character mode. In line mode, line editing (echoing, charater erasing, line erasing...) is done by client. The client then sends the whole line to the server.

Domain Name system (DNS) :-

DNS is a hierarchical, distributed method of organizing the name space of the internet. it is primarily used for mapping host name and e-mail destination to IP addresses but can also be used for other purpose

To map a name onto an IP-address, an application program calls a library procedure called the 'resolver', passing it the name as a parameter.

The resolver sends an UDP packet to a local DNS Server, which then looks up the name and returns the IP-adress to the resolver. which the returns it to the caller.

to the caller. Armed with IP address, the program can then establish a TCP connection with the destination (or) send it UDP packets

The DNS name space:-

Managing a large & constantly changing set of names is a non-trivial problem.

Conceptually, the Internet is divided into over 200 top-level domains, where each domain covers many hosts. and each is partioned into sub-domains, all these domains are represented by Tree, as shown in fig (1) below. The leaves of the tree represents domain that have no sub-domains. leaf domain may contains single host (or) it may represent a company and contain thousands of hosts.

The top-level domain comes in 2 types i) generic ii) countries. The orginal generic domains were com (commercial), edu (educational, institution), gov (U.S federal government), int (International organizations), mil (U.S army force), net (network providers), org (non-Profit organizations). The country domains include one entry for every country.