Computer Networks

* Basics of Computer Networking:

Internet was invented by Tim Berners-Lee in 1989.

Open system:

A system which is connected to the network and is ready for communication.

Closed system:

A system which is not connected to the network and can't be communicated with.

Computer Network:

It is the interconnection of multiple devices, generally termed as Hosts connected using multiple paths for the purpose of sending/receiving data or media.

There are also multiple devices or mediums which helps in the communication b/w two different devices which are known as Network devices

Ex: Router, Switch, Hub, Bridge

Topology:

The layout pattern using which devices are interconnect is called as network topology such as bus, star, mesh, ring, daisy chain

OSI (Open Systems Interconnection)

It is a reference model that specifies standards for communications protocols & also the functionalities of each layer.

Protocol:

A protocol is the set of rules or algorithm which define the way how two entities can communicate across the network & there exists diff protocol defined at each layer of the OSI model. Few of such protocols are TCP, IP, UDP, ARP, DHCP, FTP etc

Protocol used for emails → SMTP, IMAP, POP

Q. Differences b/w star, rings, mesh, tree
Adv & Dis Adv

A: Star: less expencive than mesh, easy to install & reconfigure, less cabling

Adv: ~~It is very reliable~~ Robustness - if one cable / device fails then all the others will continue to work.

It is high performing as no data collisions occur.

Disadv: It is expensive

Extra hardware is required (hubs or switches)

depends on hubs — If hub/switch fails, all devices connected will have no network connection

More cabling than other topologies

Rings:

Adv: Can transfer data quickly even for many devices

No data collisions as data flows in only one direction. Easy to install & reconfigure. Easy for fault isolat

Disadv: If any device is faulty, the whole network will fail, can be resolved by dual ring or switch capa

Unidirectional. Expensive & less security. of doing the bre

esh:

Adv: msgs can be received more quickly by short route to recipient.

msgs have many possible ways to travel

multiple connections mean, no node is isolated.
new nodes can be added without interruption to other nodes

Disadv: full mesh networks are impractical to set up.
many connections need lot of maintainence.
big no. of I/O ports & big amt. of cabling.

Tree:

Adv: Scalable as leaf nodes can accommodate more nodes in hierarchial chain.
Other hierarchial networks are not affected if one of them gets damaged.
~~Easy~~ maintainance
Fault finding

Disadv: Huge cabling is needed
Lot of maintenance
Backbone forms the pt of failure

Unit I

Overview of Internet

* Data: refers to info
- presented in any form
- agreed upon by the parties (creating & using)

*Data Communication:

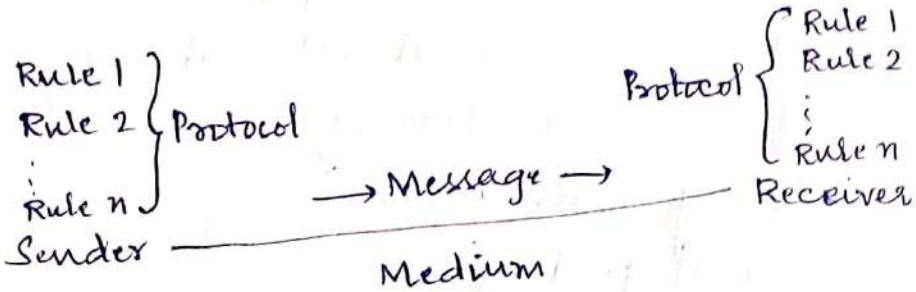
- It is the exchange of data b/w two devices via some form of transmission medium (wire cable)
- Communication system made up of a combination of hardware & software.
- Effectiveness of data communication system depends on

→ Delivery (data should reach correct destination)
→ Accuracy (data shouldn't change during delivery)
→ Timeliness (data should be delivered on time & in sent given order)
→ Jitter (small delay from sender to receiver - uneven quality in video)

* Components:

A data communication system is made up of five components.

- Sender
- Receiver
- Medium
- Protocol
- Message



Q. Difference b/w jitter & delay

A: Delay is the time it takes for data to move from one endpoint on the network to another. It is a complex measurement affected by multiple factors. Jitter, on the other hand, is the difference in delay b/w two packets. Similarly, it may be caused by several factors on the network.

• Message:
The information (data) to be communicated
- consist of txt, nos, pics, audio or video

• Sender:
The device that sends the data msg
- computer, workstation, etc

• Receiver:
The device that receives the data msg
- computer, workstation, etc.

• Medium:
The physical path by which a msg travels from sender to receiver.
- twisted pair, coaxial cable, fibre-optic, radio waves

• Protocol:
A set of rules that govern data communications
- an agreement b/w the communicating devices
- devices may be connected but not communicating (no protocol)
- arabic speaker with japanese speaker.

* Data representation:

• Text:
- sequence of bits (0s or 1s)
- different sets of patterns to represent txt symbols (each set is called: code)
- ASCII : 7 bits (128 symbols)
- common coding system today is:
Unicode uses : 32 bits to represent a symbol or charact

• Numbers:

- represented by bit patterns
- the no. is directly converted to binary no.

• Images:

- represented by bit patterns
- a matrix of
  resolution: size of pixels
- high resolution: more memory is needed
- Each pixel is assigned a bit pattern
  - 1 bit pattern (b x w dots image)
  - 2 bit pattern (4 levels of gray)
  - RGB (color images)

• Audio:

- continuous not discrete
- change to digital signal

• Video:

- Recording / broadcasting of a pic or movie
- change to digital signal.

* Data Flow:

Communication b/w two devices

- Simplex
- Half Duplex
- Full Duplex

* Simplex: (one way street)

The communication is unidirectional.
Only one device on a link can transmit, the other c

only receive.
Use the entire capacity of the channel to send data.
Ex: keyboard, monitor

* Half Duplex: (one lane with two directional traffic)
each station can both transmit & receive but not at the same time.
When one device is sending, the other can only receive & vice versa
The entire capacity of a channel is taken over by the transmitting device
Ex: Walkie-talkies

* Full Duplex: (Duplex) (two way street)
Both stations can transmit & receive at same time.
Signals gng in either direction sharing the capacity of the link
Sharing can occur in two ways:
- Link has two physically separate transmission paths - One for sending & the other for receiving
- The capacity of the channel is divided b/w signals travelling in both directions

Ex: Telephone network

* Networks:
Physical structures:
- Types of connection:
- Network: two or more devices connected through links.
- Link: Communication pathway that transfers data from

one device to another.

- Two devices must be connected in some way to the same link at the same time. Two possible types:
  - Point to point
  - Multi point

* Point to Point

- dedicated link b/w two devices.
- Entire capacity of the link is reserved for transmission between those two devices
- Use an actual length of wire or cable
- other options such as microwave or satellite is possible.

Ex: Television, remote control.

* Multipoint (multidrop):

Spa
More than two devices share a single link
Capacity is shared
Channel is shared either spatially or temporarily.
- Spatially shared: if devices use link at same time.
- Timeshare: if users must take turns

Physical Topology:

Two or more links form a topology
The topology of a network is the geometric representation of the relationship of all the links & linking devices

Topologies: Mesh, star, bus, ring, tree & hybrid.

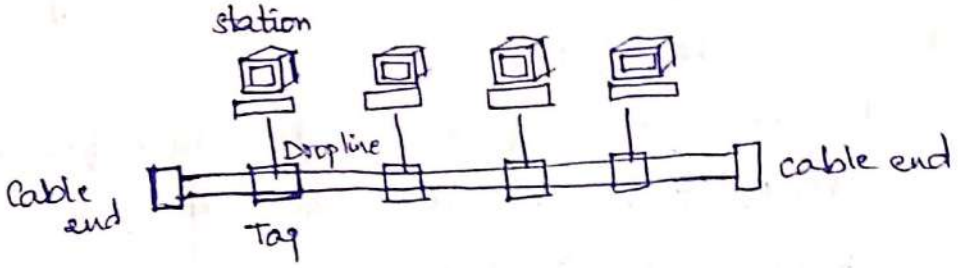
* Bus:

It is multipoint

One long cable acts as a backbone

Used in the design of early LANS, and Ethernet LANs

Based on Address send the data



Adv:

Ease of installation

Less cables than mesh, star

Less expensive

reconfigure is easy

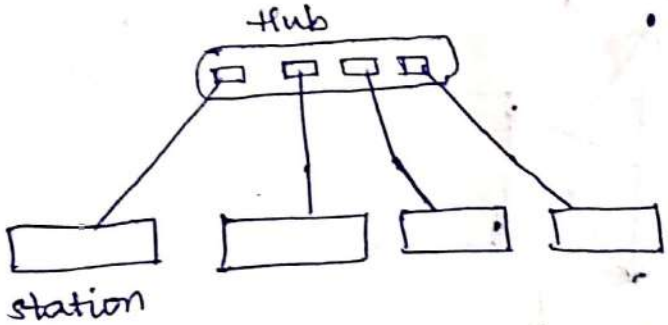
DisAdv:

Difficult, reconnection & fault isolation (limit of taps).

Collisions occus during transmissi of data.

More no. of computers installed then signal strength will be low.

* Star:

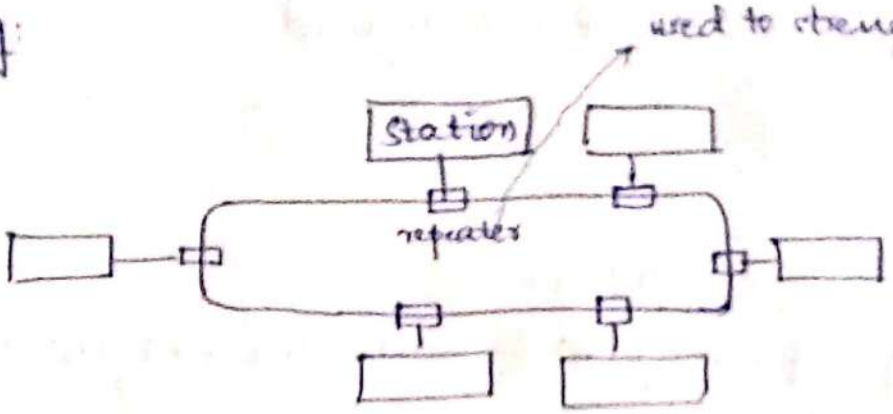


Dedicated pt-to-pt to a central controller (Hub/switch)

No direct traffic b/w devices

The control acts as an exchange.

* Ring:



Each device has dedicated pt-to-pt connection with only the two devices on either side of it

A signal is passed along the ring in one direction from device to device until it reaches its destination.

Each devices incorporates a repeater.

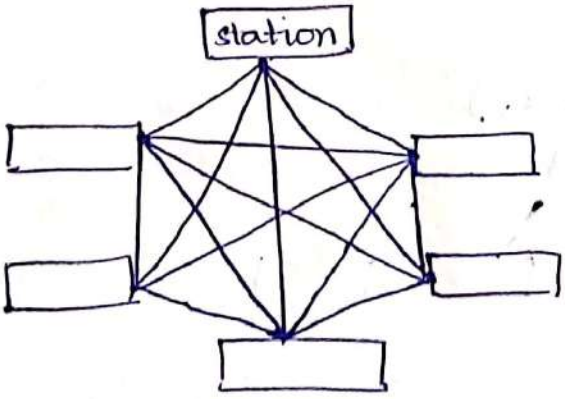
* Mesh:

Every link is dedicated pt-to-pt link.

The term dedicated means that the link carries traffic only between the two devices it connects.

To link n devices fully connected mesh has

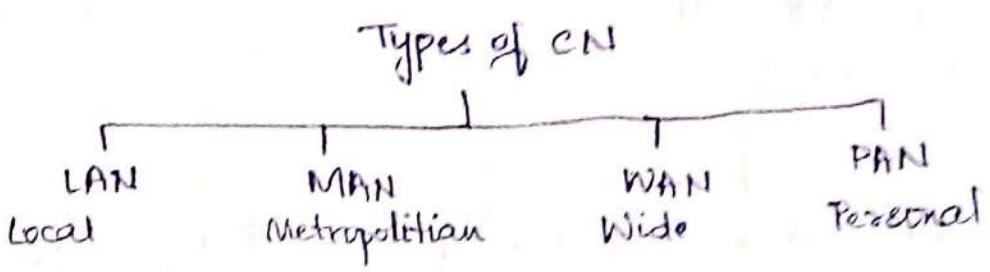
$n(n-1)/2$ physical channels (full duplex)



Every device on the network must have n-1 ports (links)

* Hybrid:

* Categories of Networks:



. size
. transmission technology
. topology

* Personal Area Network:

. It is a CN organized around an individual person within a single building, small office or residence.
. It includes computers, telephones, peripheral devices, video games etc.

* Local Area Network:

. Privately owned
. Links devices in the same building / campus
. Size limited to few kms.
. Simple LAN : 2 PCs & 1 printer
. Allow resources to be shared (hardware, software or data)
. Data rates (speed):

4 to 16 Mbps - early
100 to 1000 Mbps - today

. Lack of privacy
. Limited range
. High security

* Metropolitan Area Network:

- Connection of diff LANs.
- Size b/w LAN & WAN
- Inside a town or city

Ex: DSL (Digital Subscriber Line) provided by telephone company

- Less security
- fibre optics or cables

* Wide Area Network:

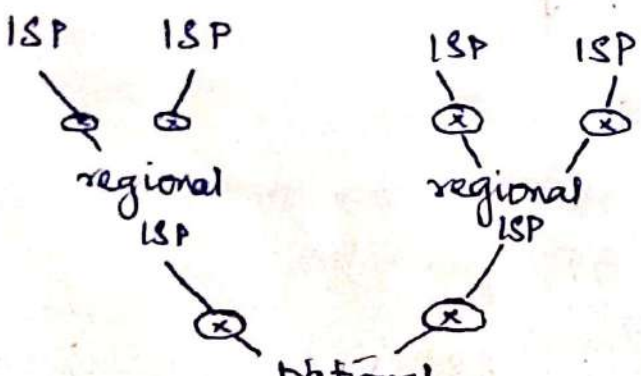
- Provides long distance transmission of data over large geographic areas (country, continent, world)
- Satellite or telephone cables
- connection among MANs
- Data sharing using routers
- Need to have firewalls.

Switched WAN
- backbone of Internet

Dialup line pt to pt WAN (telephone – internet)
- leased line from a telephone company.

* Internetwork:

Two or more networks connected together.



Q. Difference b/w small i & capital i (internet)

A: internet is wide network through which computers are interconnected globally with one another & share data. Internet refers to millions of computer connected in a gigantic network which communicate via TCP/IP protocol.

* Internet History:

It came in 1960. → ARPA (Advanced Research Projects Agency) in DOD wanted to connect research organisations. In 1967, ARPA presented its ideas for ARPANET.

. Host computer connecting to IMP (Interface Message Processor)

. Each IMP communicate with other IMP.

In 1969, four nodes/universities connected via IMPs to form a network.

. NCP (Network Control Protocol) provided communication b/w the hosts.

1972, Vint Cerf & Bob Kahn invented TCP (Transmission).

TCP was split into TCP & IP

→ MILNET

→ CSNET

→ NSFNET

→ ANSNET

* Elements of protocol:

. Syntax: structure or format of data

. Semantics: meaning of each section of bits

. Timing: when data should be sent & how fast they can be sent.

* Standard:

Creating & maintaining an open & competitive market for equipment manufactures.

Providing guidelines to ensure interconnectivity necessary in today's marketplace to vendors, manufacturers etc.

- de facto : not approved by an organised body but adopted as standards through widespread use
- de jure : approved by law.

* Standards are developed through the cooperation of:

- Standards Creation Committees
  - ISO, ITU-T, CCITT, ANSI, IEEE, EIA
- Forums
  - Created by special-interest groups.
  - Present their conclusions to the standard bodies.
- Regulatory Agencies
  - Ministry of Telecommunication & Information Technology (KSA).
  - Purpose: Protecting the public by regulating radio, television & communication

* Internet standards:

- Thoroughly tested specification that is useful to be adhered to by those who work with the Internet.
- Formalized regulation that must be followed
- Specification become Internet standard
  → begins as Internet draft for 6 months
  → Upon recommendation from the Internet authorities draft

→ RFC is edited, assigned a no., & made available to all interested parties.

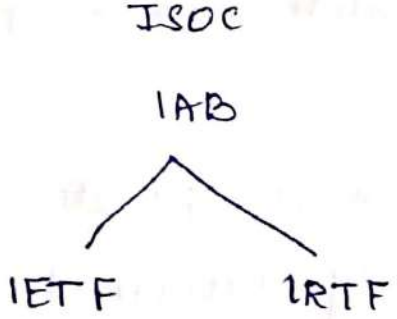
* Maturity level of RFC:

- Proposed standard → specification is tested & implemented by diff grps.
- Draft standard → atleast two successful independent & interoperable implementations.
- Internet standard → after successful implementation.
- Historic → successful / unsuccessful pass of maturity levels to become Internet standard
- Experimental → experiments shouldn't affect operation of Internet
- Informational → contains general, historical or tutorial info.

* Requirement levels of RFC:

- Required → min. conformance. Ex: IP & ICMP
- Recommended → if it is of any usefulness. Ex: FTP & TELNET
- Elective → use it for its own benefit (not req. not recommended)
- Limited Use → RFCs are used in limited situations
- Not Recommended → inappropriate for general use.

* Internet Administration:

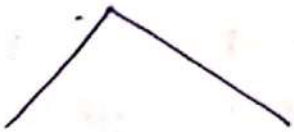


ISOC:

Internet Society is an international, non profit organization formed to provide support for the Internet standards process.

IAB (Internet Advisory)

It is an technical advisor to ISOC. Editorial management of RFC



IETF
Engineering Task Force
(identifies operational problems & proposing sol^n's to these problems)
IESG

IRTF
Research Task Force
(focuses on long term research topics related to Internet protocols, applications)
IRSG

* Purpose of Protocol layering:

- Each layer should offer services to the layer above it.
- Higher layers should be shielded from details of how the service is provided to it by lower layers.
- Modularization eases maintenance & updating of the system.
- Without layering, each new application has to be reimplemented for every network technology.

* OSI Reference Model:

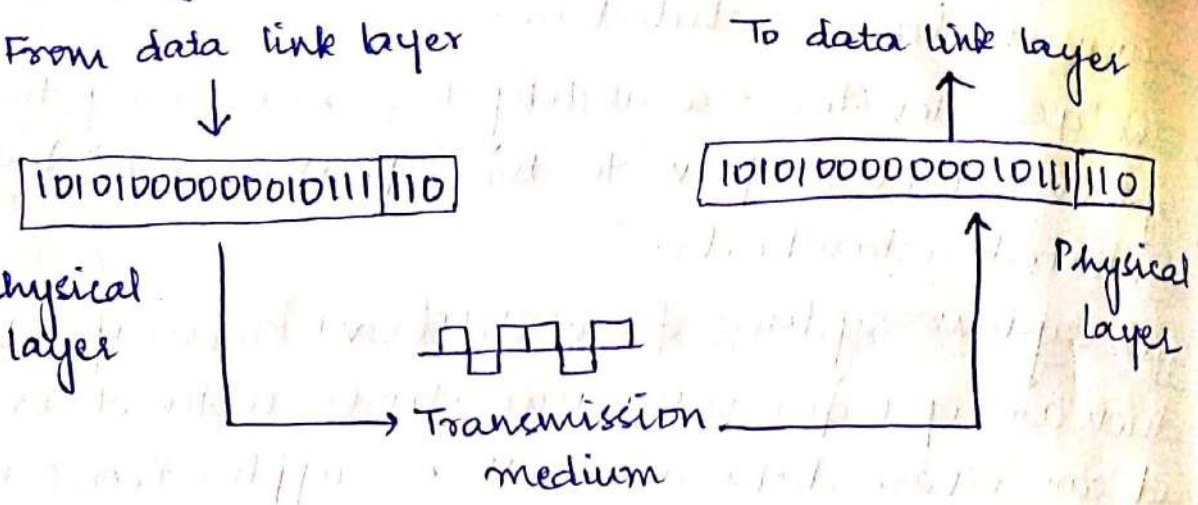
· International standard organisation (ISO) established a committee in 1977 to develop an architecture for computer communication.

- In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.
- Term "open" denotes the ability to connect any two systems which conform to the reference model and associated standards.
- Open system: Systems from different manufactures which are open for communications with other systems and can share data as well as applications with each other.
- The OSI model is now considered the primary Architectural model for inter-computer communications.
- The OSI model describes how information or data makes its way ~~through~~ from application programmes (such as spreadsheets) through a network medium (such as wire) to another application programme located on another network.
- The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller & more manageable problems.
- This separation into smaller more manageable functions is known as layering.

1. Physical layer:

- It coordinates the functions required to transmit bit stream over physical medium.
- Provides physical interface for transmission of information.
- It deals with transmitting raw bits over the

• Covers all - mechanical, electrical, functional & procedural aspects for physical communication.



The physical layer is responsible for the movement of individual bits from one hop (node) to the next.

Functions:

- Physical characteristics of interfaces & medium.
  It also defines the type of transmission medium.
- Representation of bits
  Sequence of 0s or 1s
- Data rate
- Synchronization of bits
  Sender & receiver must be synchronized.
- Physical topology
  Mesh, ring, star, etc
- Transmission mode
  Simplex, half duplex, duplex

What are the physical layer components on my computer?

- NIC (Network Interface Card)

→ Has a unique 12 character hexadecimal no. permanently burned into it at the manufacturer.

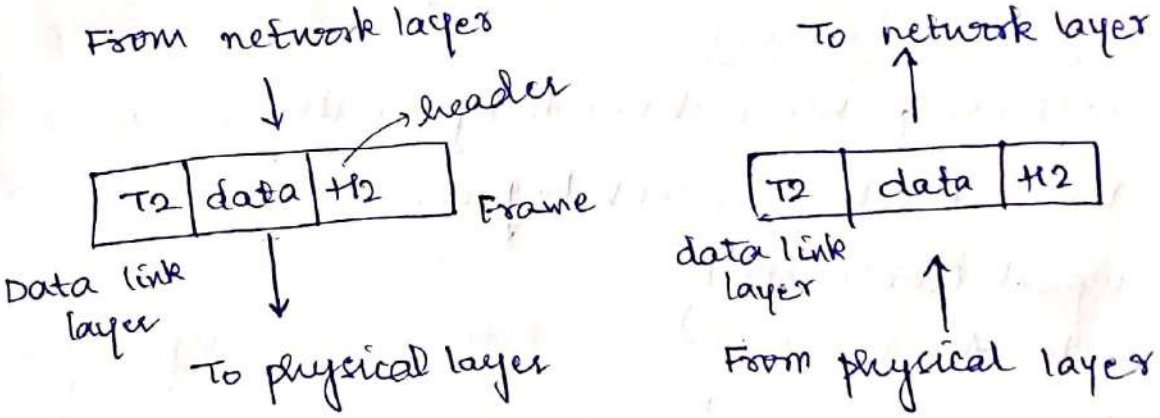
→ The no. is the MAC address / physical address of a

- Cabling.

Twisted Pair
Fibre Optic
Coax Cable.

2 Data Link Layer:

- Data link layer attempts to provide reliable communication over the physical layer interface.
- Breaks the outgoing data into frames & re-assemble the received frames.
- Create & detect frame boundaries.
- Handle errors by implementing an acknowledgement & retransmission scheme.
- Implement flow control.
- Supports pt to pt as well as broadcast communication.
- Supports simplex, half-duplex or full duplex "



The data link layer is responsible for moving frames from one hop(node) to the next

Functions:

- Framing:

divides the stream of bits into manageable data units called frames.

adds a header to the frame to define the sender and/or receiver of the frame

- Flow control:
imposes a flow control mechanism to avoid overwhelming the receiver

- Error control:
adds mechanisms to detect & retransmit damaged/lost frames

- Access control:
determine which device has control over the link at any given time.

- Link establishment & termination:
establishes & terminates the logical link b/w two nodes

- Frame sequencing
transmits/receives frames sequentially

- Frame acknowledgement:
provides/expects frame acknowledgements.

DLL is divided into two sub layers:

- LLC (Logical Link Control)
- MAC (Media Access ")

- LLC:

→ It is the upper portion of DLL

→ performs flow control & management of connection errors

→ Has three types of connections:

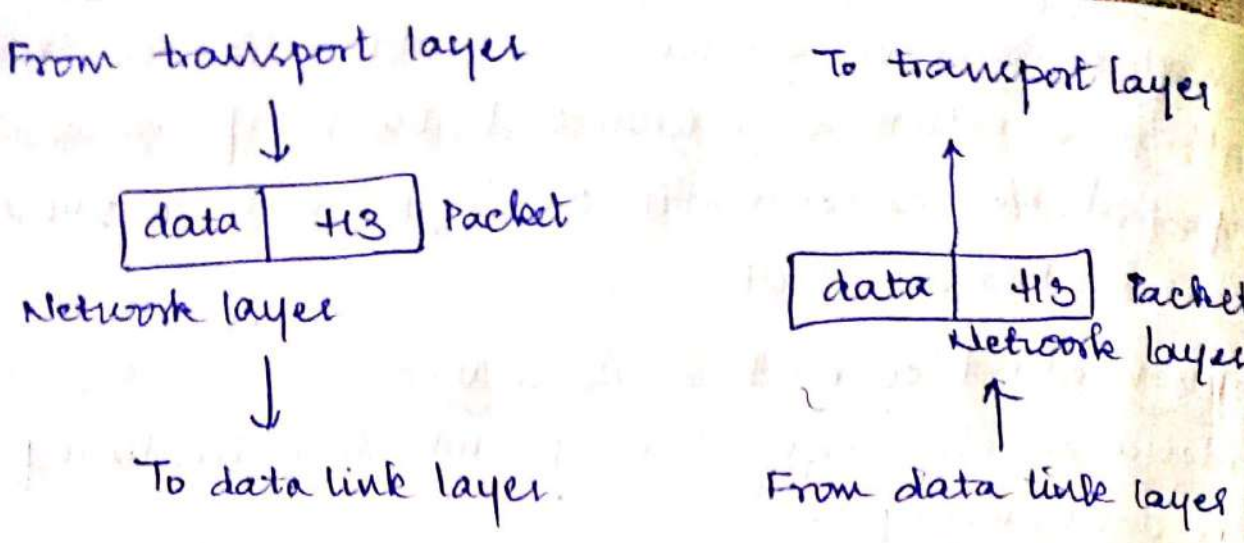
1. Unacknowledged connectionless service:
does not perform reliability checks or maintain a connection

2. Connection oriented service: connectionless : Ex: UDP
once the connection is established, blocks of data can be transferred b/w nodes until one of the node terminates the connection. Ex: TCP

3. Acknowledged connectionless service:
provides a mechanism through which individual frames can be acknowledged.

• MAC:
It contains methods to regulate the timing of data signals & eliminate collisions.
→ ~~The~~ ~~MAC~~ It determines where one frame of data ends & the next one starts - frame synchronisation
→ Four types of
1. Time based
2. Character counting
3. Byte stuffing
4. Bit "

3. Network layer:
• It is responsible for source to destination delivery of individual packets across multiple networks.
• Defines the most optimum path the packet should take from S to D
• Defines logical addressing so that any endpt can be identified. IP addressing
• Handles congestion in the network.
• Facilitates interconnection b/w heterogeneous networks (internetworking)



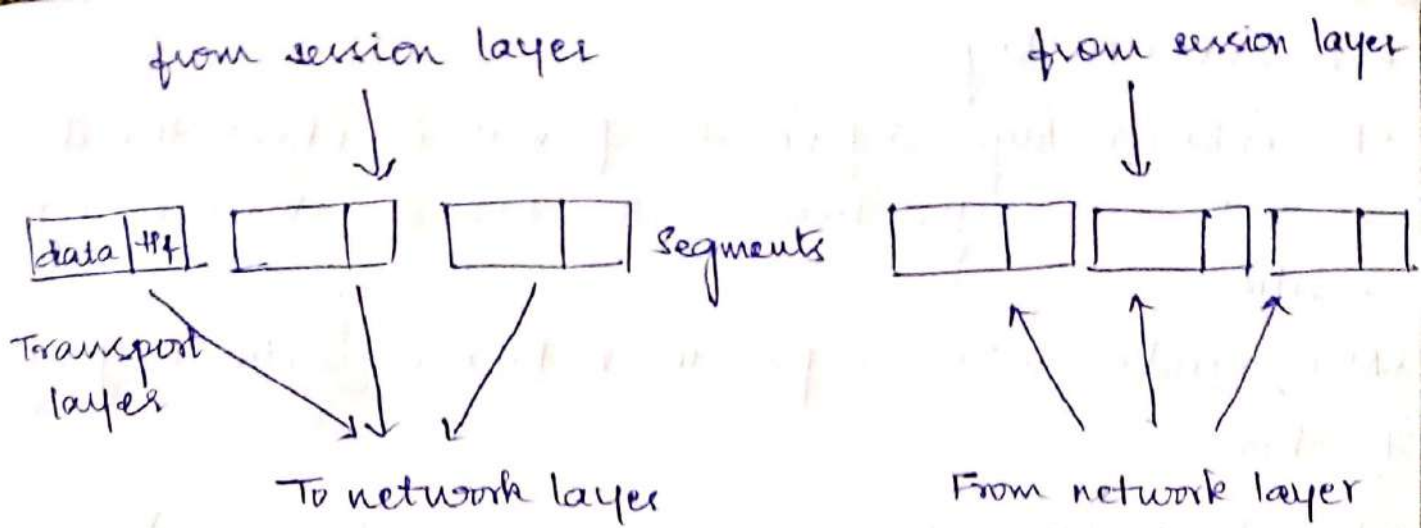
The network layer is responsible for the delivery of individual packets from the source host to the destination host

Functions:

1. Logical addressing
2. Dynamic routing
3. Congestion control
4. Accounting & billing
5. Address transformation
6. Source host to destination host error free delivery of packet.

4. Transport layer:

- Purpose of this layer is to provide a reliable mechanism for the exchange of data b/w two processes in diff computers.
- Ensures that the data units are delivered error free, delivered in sequence.
- Ensures that data units are delivered in sequence.
- Ensures that there is no loss or duplication of data units.
- Provides connectionless or connection oriented services.



The transport layer is responsible for the delivery of message from one process to another

Functions:

1. Service pt addressing
2. Segmentation & reassembly
3. Connection control
4. flow control (end to end)
5. error control.

5. Session layer:

- Session layer provides mechanism for controlling the dialogue b/w the two end systems.
- It defines how to start, control & end conversations (called sessions) b/w applications.
- This layer requests for a logical connection to be established on an end-user's request.
- Any necessary log-on or password validation is also handled by this layer.

1. dialog control
2. synchronization, session & sub session
3. Session closure

6. Presentation layer:

- Presentation layer defines the format in which the data is to be exchanged between the two communicating entities.
- Also handles data compression & data encryption (cryptography)

Functions:

- Translation (converting formats into required formats)
- Encryption (security)
- Compression & Decompression: more than 25 MB data is compressed

7. Application layer:

- Application layer interacts with application programs & is the highest level of OSI model.
- Application layer is to allow access to network resources, it contains management functions to support distributed applications.
- Ex: file transfer
  electronic mail
  remote login etc

Functions:

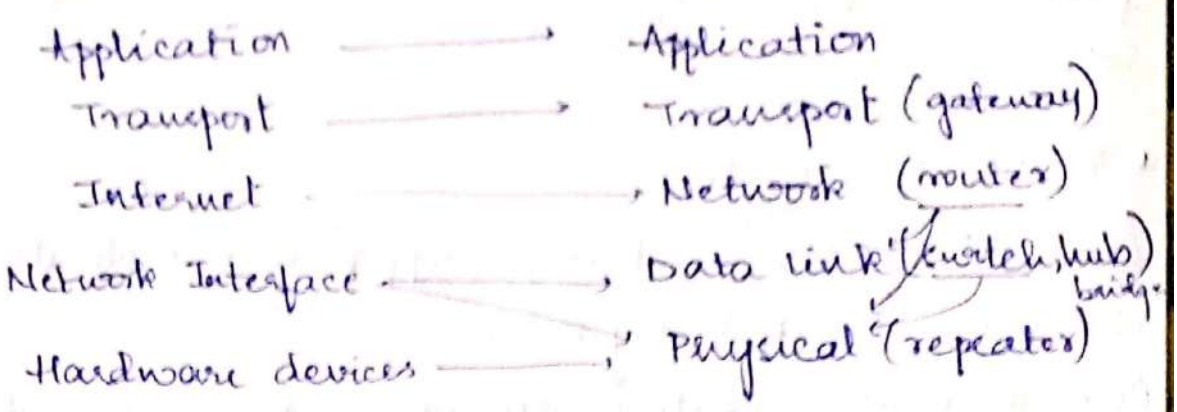
- Network virtual terminal
- File transfer access & management
- Mail services & directory services.

* TCP/IP Protocol:

- The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not match exactly with those in the OSI model.
- The original TCP/IP protocol suite was defined as four

. Today, however, TCP/IP is thought of as a five-layer model with the layers named similarly to the ones in the OSI model.

Layers in TCP/IP protocol



* Similarities b/w OSI reference model & TCP/IP RM:

- Both have layered architecture
- Layers provide similar functionalities
- Both are protocol stack
- Both are reference models.

* Transmission media: (cable (wired) or air (wireless))

The pathway through which individual systems are connected in a network are called transmission media.

Makes electronic signals possible from one computer to other

Characteristics:

- Cost of media
- Installation requirement
- Bandwidth (two or more use communication channel) — Baseband: one person uses CC
- Band usage
- Attenuation (signal gets weakened when sending info from sender to receiver) → need to strengthen repeater is used. How much is weakened is attenuation

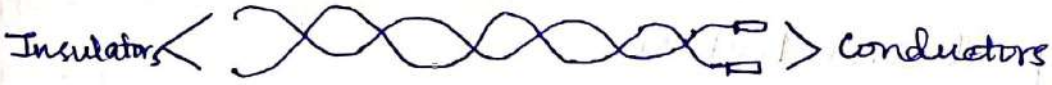
Transmission media

- Guided (wired)
  - Twisted pair cable
  - Coaxial cable
  - Fibre optic cable
- Unguided (wireless)
  - Free space

* Twisted pair cable:

Consists of two conductors (copper) each with its own plastic insulation twisted together.

One wire is used to carry signals to receiver, the other is used as ground reference

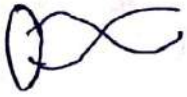


Issues:

- Interference due to unwanted electrical coupling of two copper wires (reduce noise)
- " " " " " b/w the neighbouring twisted pairs.

Twisted pair (TP)

- UTP Unshielded



- STP Shielded

It has a metal foil or braided mesh covering that encases each pair of insulated conductors. (to prevent penetration of

• UTP:

- ordinary telephone wire
- less expensive
- weak immunity against noise & interference
- suffers from external EM interference

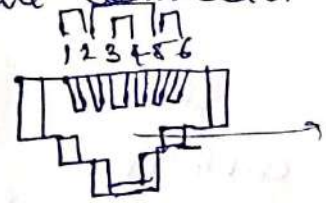
• STP:

- An extra metallic sheath on each pair
- relatively more expensive
- provide better performance than UTP
  - Increased data rate
  - " bandwidth.

• UTP Categories:

Cat 3 (16 MHz)
Cat 4 (20)
Cat 5 (100) (more wider cable) (clg)
Cat 5E (enhanced)
Cat 6
Cat 7 (most wider)

* RJ stands for registered jack. The RJ45 is a keyed connector, meaning the connector can be inserted in only one way



RJ-45 female

→ the one inserted in this is RJ-45 male

• Advantages:

less expensive
easy to work

• Disadvantages:

low data rate
short range

* Coaxial Cable: (coax)

Carries signals of higher frequency ranges than twisted cable.

Coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath (noise shouldn't penetrate), which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.

Applications:

- Television signals distribution
  - Ariel to TV
  - Cable TV
- Long distance telephone transmission
  - Can carry 10,000 voice calls simultaneously
  - Being replaced by fibre optic
- Short distance computer systems links
  - Local area network
  - Metropolitan area network.

The outer metallic wrapping serves both as a shield against noise & as the second conductor which completes the circuit.

	Category	Impedence	Use
Radio Guide	RG 59	75 Ω	Cable TV
	RG 58	50 Ω	Thin Ethernet
	RG 11	50 Ω	Thick Ethernet

Coaxial Cable Connectors:

The most common type of connector used today is Bayonet Neill-Concelman (BNC).

- BNC connetor - used to connect the end of cable to device (TV)
- BNC T " - " in Ethernet networks
- BNC terminator - used at the end of cable to prevent

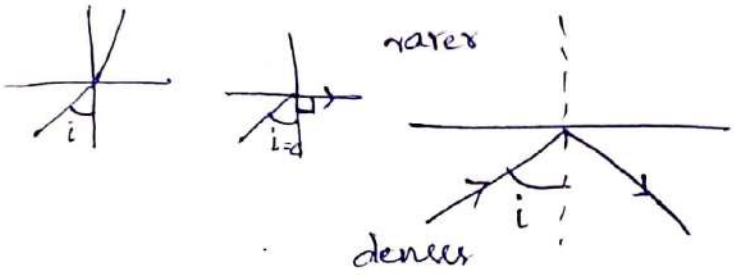
Issues (Performance)

Coaxial cable has much higher bandwidth the signal weakens rapidly and requires the frequent use of repeaters (attenuation)

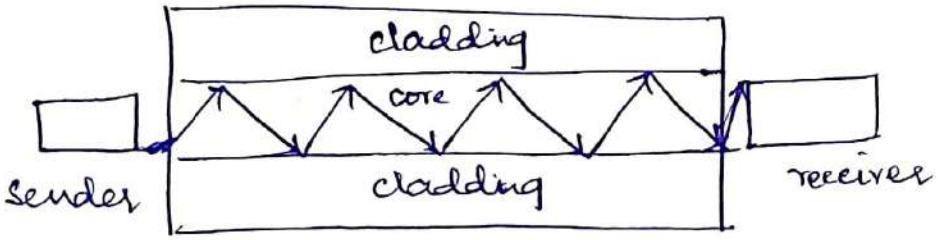
* fibre optics cable: (TIR)

. Made of glass / plastic & transmits signals in the form of light.

. If a ray of light travelling through one substance suddenly enters another substance, the ray changes direction.



$i > C$, TIR (reflection)



+ glass / plastic is covered by cladding of less dense glass / plastic so that light doesn't penetrate out.

Path (Modes)

Single mode | multimode

Multimode:

multiple beams from a light source move through the core in different paths.

. step index

sudden change in light beam which contributes to distortion

. graded index

varying densities. Density is high at core & decreases to its lowest at the edge.

Connectors

- SC (Subscriber channel) ⟶ TV
- ST (Straight-tip) ⟶ Networks
- MT-RJ (RJ 45)

Benefits:

- Greater capacity (hundreds of Gbps)
- Smaller size & weight (thin fibres)
- Lower attenuation
- Greater repeater spacing

Drawback:

- Costly
- Can be used for shorter dist.

*Unguided Media (Wireless):

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.

- Radio waves:

Frequencies b/w 3kHz & 1 GHz are normally called radio waves. Radio waves, particularly those waves that propagate in the sky mode can travel long distances. This makes radio waves a good candidate for long distance broadcasting such as AM radio.

*Note: Radio waves are used for multicast communications such as radio & television & paging systems. They can penetrate through walls. Highly regulated. Use omni directional antennas.

Advantage:

An AM radio can receive signals inside a building

Disadvantage:

It cannot isolate a communication to just inside/outside a building

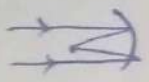
Applications

. Multicasting: There is one sender & many receivers

Ex: AM & FM radio, television, cordless phones.

. Micro waves:

Two types of antennas are used.

. Dish antenna 

. Horn " 

Types:

. Satellite pt to pt (one sender → satellite → receiver)

. Broadcast link (multiple senders → satellite → multiple receivers)

. Infrared waves:

Frequency 300 GHz to 400 THz (wavelength from 1mm to 770 nm) can be used for short range communication.

*Note: Can be used for ✓ in a closed area using line of sight propagation.

Applications:

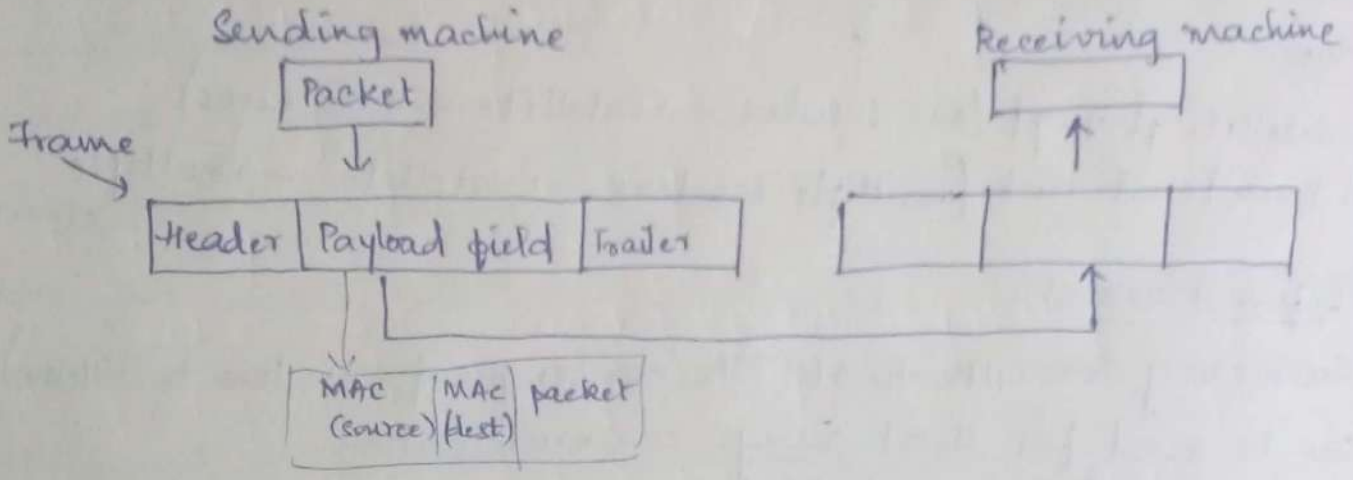
IR signals defined by IrDA transmit through line of sight, the IrDA port on the keyboard needs to pt to the PC for transmission to occur

2. Data Link Layer

* Data Link Layer Design Issues:

- Services provided to Network layer (sends packets without worries)
- Framing / packetizing
- Error Control (CRC)
- Flow Control
- Addressing (MAC)
- ~~Media~~ access control (overcome collision)

* Functions of Data Link layer:



* Services provided to Network layer:

Transferring data from N/w layer on the source machine to N/w layer on the destination machine.

- Unacknowledged Connectionless Service (no confirmation) (no logical connection) LANs (less errors → reliable) (S → R)
- Acknowledged (confirmation) " "
- " Connection-oriented " (sends data & waits for confirmation).

* Framing:

- DLL translates the physical layer's raw bit stream into discrete units (messages) called frames.
- Character count:

uses a field in the header to specify the no. of characters in the frame. When the data link layer at the destination sees the character count, it knows how many characters follow & hence where the end of the frame.

. The trouble with this algorithm is that the count can be be garbled by a transmission error.

. Framing - Byte Stuffing:

. We use two character sequence DLE STX (Data link Escape, Start of Text) to signal the beginning of a frame & DLE ETX (End of Text) to flag the frame's end.

. The second framing method, starting & ending character stuffing, gets around the problem of resynchronization after an error by having each frame start with the ASCII character sequence DLE STX & end with the sequence DLE ETX.

. If ~~two~~ DLE ETX happens to appear in the frame itself, use character stuffing, within the frame, replace every occurence of DLE with the two character sequence DLE DLE. The receiver reverses the process, replacing every occurence of DLE DLE with a single DLE.

Ex: If the frame contained "A B DLE D E DLE", the characters transmitted over the channel would be "DLE STX A B DLE DLE D E DLE DLE DLE ETX".

character stuffing
DLE
ESC
FLAG

. | DLE | STX | A | DLE | B | DLE | ETX |

| DLE | STX | A | DLE | DLE | B | DLE | ETX |

stuffed DLE

| DLE | STX | A | DLE | B | DLE | [redacted] | ETX |

- Framing - Bit Stuffing:

Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream.

Each frame begins & ends with a special bit pattern, 01111110 (in fact, a flag byte)

01111101
↓ ← bit stuff
011111001
↓

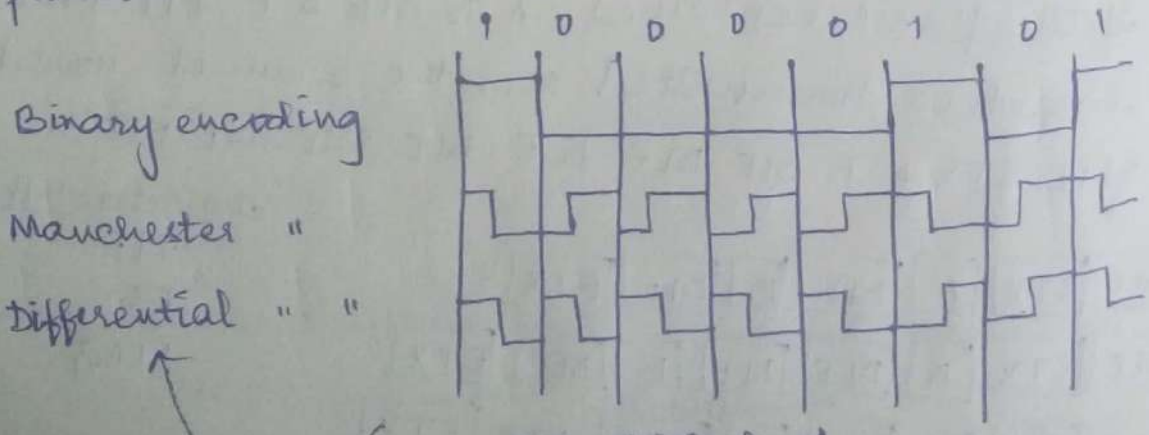
** Physical Layer Coding Violations / Line coding:

- This framing method is used only in those networks in which encoding on the physical medium contains some redundancy.
- Some LANs encode each bit of data by using two physical bits i.e Manchester coding is used.

Bit 1 ⟶ ⌐¬ high-low
Bit 0 ⟶ ⌐¬ low-high
} two signal (T/2) elements.

time →

- The scheme means that every data bit has a transition in the middle, making it easy for the receiver to locate the bit boundaries. The combinations high-high & low-low are not used for data but are used for delimiting frames in some protocols.



Digital-to-digit conversion:

- Line coding
- Block coding
- Scrambling

- digital data represented in 0's & 1's
- These are converted into signals.
- High (+ve) voltage = 1
- Low (-ve) " = 0
- Data symbol can consist of no. of data bits.
- Data symbol can be coded into a single signal / multiple signal elements.

(bps)

- No. of bits sent per sec → bit rate
- No. of signal elements per sec → baud rate

↑ bit ↓ baud

Schemes:

→ Unipolar — NRZ (Non Return to Zero) (only +ve) (signal levels either above/below)

→ Polar — NRZ, RZ & biphase (manchester & diff. manchester)

NRZ: +ve & -ve

RZ: +ve, -ve, 0

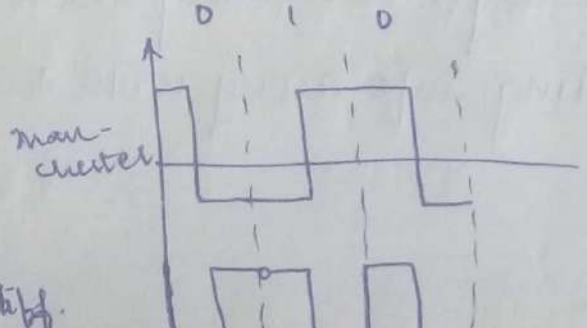
Level: NRZ-L + RZ

NRZ-I & RZ

Diff. manchester

0 → presence of transition

1 → absence " "



* Error Control:

Frames received properly or not

- Acknowledgement - Receiver sends a special acknowledgement frame (-ve or +ve) to sender. (i received it time)
- Timers - If ack. is lost, then sender schedules a timer to expire after a while after the ack. should have been (resending frames - timers) returned
- Sequence Numbers - retransmissions introduce possibility of duplicate frames, add sequence no. to each frame.

* Flow control:

Matching the speed of sender to receiver

- feedback based - sending feedback to sender to send more data or how receiver is.
- rate based - limits the rate at which senders may transmit data

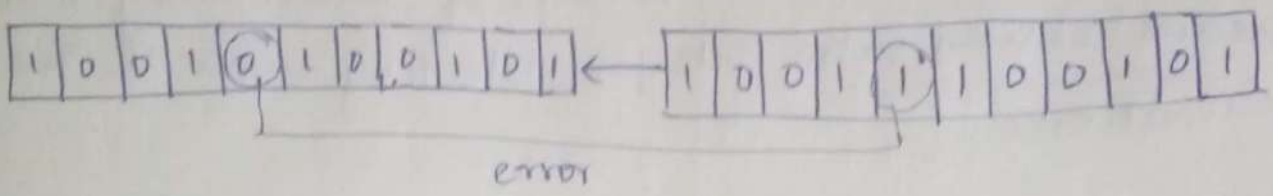
* Error correction & detection:

- It is physically impossible for any data recording or transmission medium to be 100% perfect 100% of the time over its entire expected useful ~~file~~ life.
- As more bits are packed onto a square cm. of disk storage as communications transmission speeds increase, the likelihood of error increases - sometimes geometrically
- Detecting & correcting error requires redundancy - sending info along with the data.

* Types of Errors:

• Single bit error:

It means only one bit of data unit is changed from 1 to 0 or from 0 to 1.



• Burst error:

It means two or more bits in data unit are changed from 1 to 0 from 0 to 1. In burst error, it is not necessary that only consecutive bits are changed. The length of burst error is measured from first changed bit to last changed bit

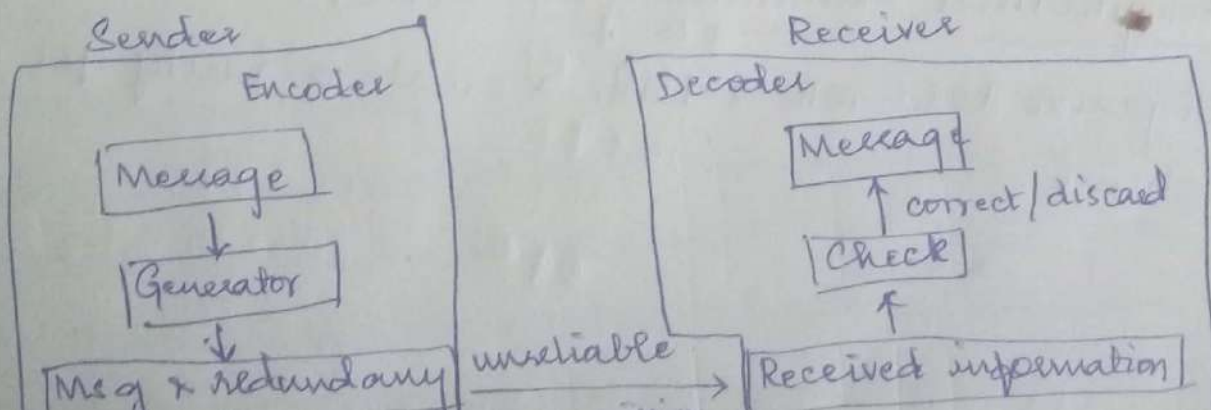
* Error Detection vs Error Correction:

• Error detecting codes:

Include enough redundancy bits to detect errors & use ACKs & retransmissions to recover from the errors.

• Error correcting codes: (forward error correction)

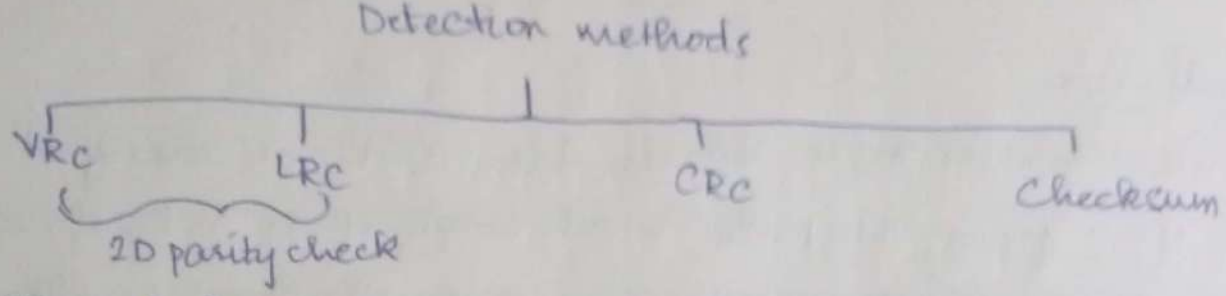
Include enough redundancy to detect & correct errors.



* Error Detection:

Error detection means to decide whether the received data is correct or not without having a copy of the original message.

Error detection uses the concept of redundancy, which means adding extra bits for detecting errors at the destination.



• Vertical Redundancy Check (VRC)/Parity Check:

Append a single bit at the end of data block such that the no. of ones is even

Even parity (odd parity is similar)

0110011 ⟶ 01100110

0110001 ⟶ 01100011

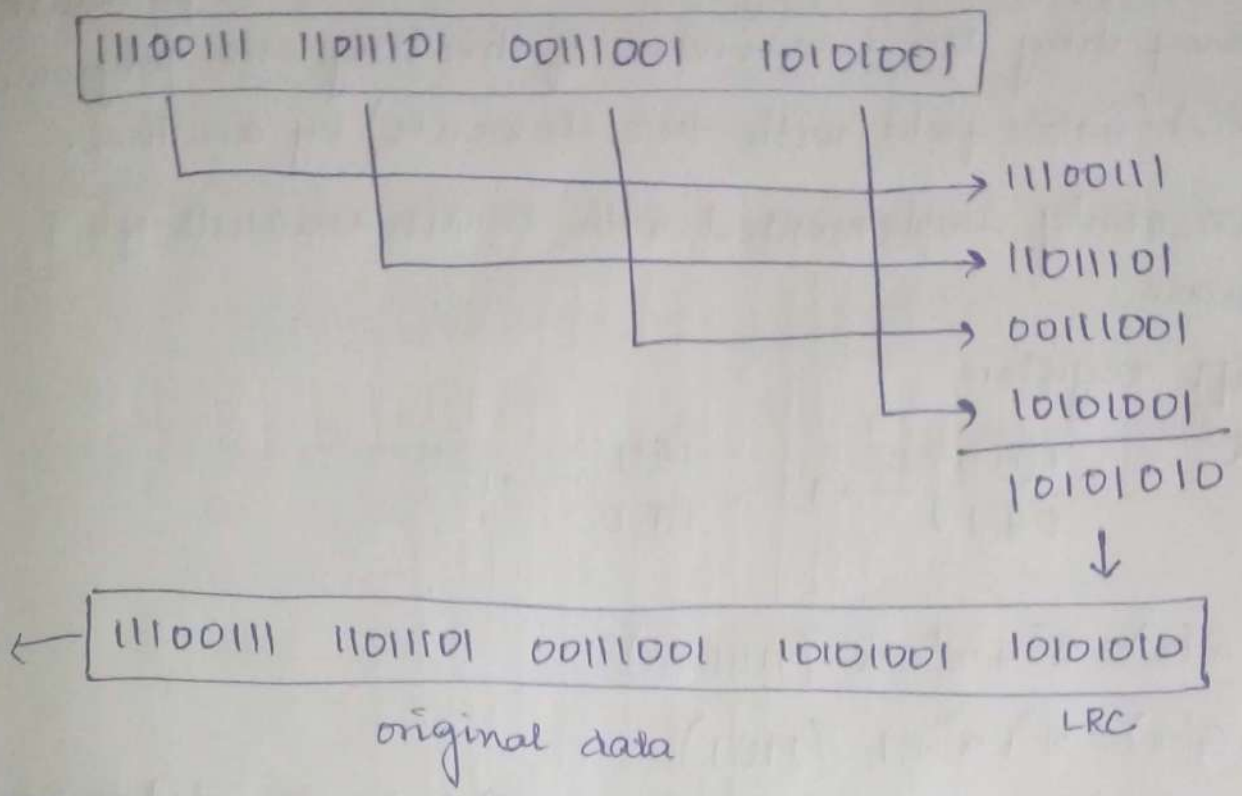
Performance:

Detects all odd no. errors in a data block.

• Longitudinal Redundancy Check (LRC):

Organize data into a table & create a parity for each column.

→



Performance:

- Detects all burst errors up to length n (no. of columns)
- Misses burst errors of length n+1 if there are n-1 uninverted bits b/w the first & last bit.
- If the block is badly garbled, the probability of acceptance is $(1/2)^n$.

- Cyclic Redundancy Check (CRC):

- The cyclic redundancy check is a technique for detecting errors in digital data, but not for making corrections when errors are detected. It is used primarily in data transmission.
- In CRC method, a certain no. of check bits (checksum) are appended to the message being transmitted. The receiver can determine whether or not the check bits agree with the data to ascertain with a certain degree of probability whether or not an error occurred in transmission.

- The CRC is based on polynomial arithmetic in particular, on computing the remainder of dividing one polynomial in GF(2) (Galois field with two elements) by another.
- Can be easily implemented with small amount of hardware
  → shift registers
  → XOR

$1 \oplus 0\}, 0 \oplus 1\} \longrightarrow 1$ $\quad$ $1 \oplus 1\}, 0 \oplus 0\} \longrightarrow 0$

Ex: $M(x) = x^5 + x^4 + x \quad (110010)$

$G(x) = x^3 + x^2 + 1 \quad (1101)$

used to generate 3 bit CRC = C(x) to be appended to M(x)

3 is highest degree → add 3 zeroes to M(x) (checksum)

→ M(x) = 110010000

G(x) = 1101

```
1101 ) 110010000 ( 100 = 10
       1101
       -----
        0011
        0000
        -----
         0110
         0000
         -----
          1100
          0000
          -----
           1000
           0000
           -----
            0000
            0000
            -----
               00 → Remainder
```

It will remain same for (ii) part too

---

* CRC standard Polynomials:

CRC-8	x^8+x^2+x+1	ATM header
CRC-10	$x^{10}+x^9+x^5+x^4+x^2+1$	ATM AAL
CRC-16	$x^{16}+x^{12}+x^5+1$	HDLC
CRC-32	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$	LANs

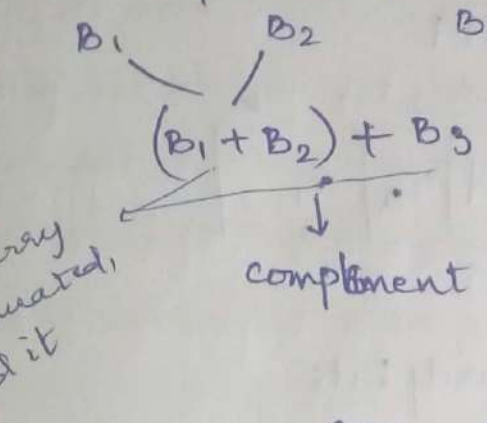
* CRC performance:

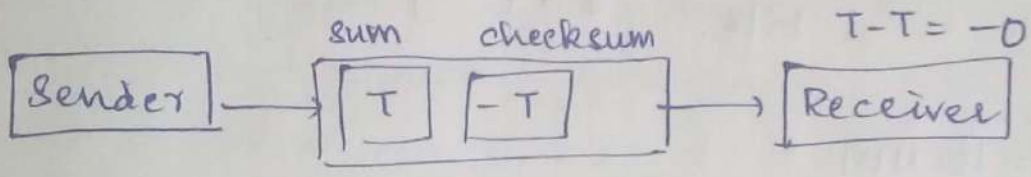
CRC is a very effective error detection technique. If the divisor is chosen according to the previously mentioned rules, its performance can be summarized as follows:

- CRC can detect all single bit errors
- double bit errors (three 1's)
- any odd no. of errors (x+1)
- all burst errors of less than the degree of the polynomial.
- most of the larger burst errors with a slight prob.

• Checksum: (used in IP, TCP & UDP)

Ex: 110111 | 100110 | 001011 (divide into m segments)





At receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented. If the result is zero, it is accepted.

* Error Correction:

Once deleted, the errors must be corrected.

• Retransmission (Backward error correction) (Automatic Repeat Request (ARQ))

→ Simplest, effective & mostly used
→ retransmission of data by sender

• Forward Error Correction (FEC):

→ Receiving device can correct errors by itself

* Hamming code: $(2^r \geq m+r+1)$

No. of Data bits k	No. of Redundant bits r	Total bits k+r
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10

If value of $m = 7$

$2^0 = 1; 2^1 = 2$

$2^2 = 4; 2^3 = 8; 2^4 = 16 > 7+4+1$ → $16 > 12$ ✓

11	10	9	8	7	6	5	4	3	2	1	•
d	d	d	r_8	d	d	d	r_4	d	r_2	r_1	

error correcting bits or parity bits

Ex: Data = 1001101

11	10	9	8	7	6	5	4	3	2	1
1	0	0		1	1	0		1		

$r_1 = 1, 3, 5, 7, 9, 11$

1 0 1 0 1 → odd (1)

$r_2 = 2, 3, 6, 7, 10, 11$

$r_4 = 4, 5, 6, 7$

$r_8 = 8, 9, 10, 11$

	11	10	9	8	7	6	5	4	3	2	1
Adding r_1	1	0	0		1	1	0		1		1
Adding r_2	1	0	0		1	1	0		1	0	1
Adding r_4	1	0	0		1	1	0	0	1	0	1
Adding r_8	1	0	0	1	1	1	0	0	1	0	1

Suppose receiver gets 10010100101

	1	0	0	1	0	1	0	0	1	0	1
1, 3, 5, 7, 9, 11	1	0	0	1	0	1	0	0	1	0	1
2, 3, 6, 7, 10, 11	1	0	0	1	0	1	0	0	1	0	1
4, 5, 6, 7	1	0	0	1	0	1	0	0	1	0	1
8, 9, 10, 11	1	0	0	1	0	1	0	0	1	0	1
							0	1	1	1	

* functions & requirements of the data link protocols:

The basic function of the layer is to transmit frames over a physical communication link. Transmission may be half duplex or full duplex. To ensure the frames are delivered free of errors to the destination station (IMP) a no. of requirements are placed in data link protocol.

- Identification of a frame
- Transmission of frames of any length up to a given maximum. Any bit pattern is permitted in a frame.
- Detection of transmission errors
- Retransmission of frames which were damaged by errors.
- Assurance that no frames were lost.
- In a multidrop configuration → some mechanism must be used for preventing conflicts caused by simultaneous transmission by many stations.
- The detection of failure or abnormal situations for control & monitoring purposes.

* Elementary Data Link Protocols:

The protocols are normally implemented in software by using one of the common programming languages.

- An Unrestricted simplex protocol (sender is not restricted while sending any amt of data)
- A simplex stop-and-wait " (receiver will process info at a finite rate)
- A simplex protocol for a noisy channel

frames may be damaged, if frame is correct → ack sent (or retransmit) if frame incorrect → ignore

errors → duplicate frames

flooding

S ⇉ R

feedback is sent from receiver until then sender will wait

protocols

- For noiseless channel
  - simplest
- For noisy channel
  - stop and wait ARQ
  - Go back N ARQ

To overcome duplicate frames, it is required that the receiver be able to distinguish a frame that it is seeing for the first time from a retransmission. One way to achieve this is to have sender put a sequence no. in the header of each frame it sends. The receiver then can check the sequence no. of each arriving frame to see if it is a new frame or a duplicate to be discarded.

* Sliding Window Protocol:

Data frame transmission:

- Unidirectional assumption in previous elementary protocols

  ⇒ Not general

- Full-duplex-approach 1

  Two seperate communication channels (physical circuits)

  - Forward channel for data
  - Reverse channel for acknowledgement

  Problems: 1. reverse channel bandwidth wasted

  2. cost

- Full duplex approach 2

  Same circuit for both direction.

  Data and acknowledgement are intermixed

- Approach 3

  Attaching acknowledgement to outgoing data frames

PIGGYBACKING

* Piggybacking:

. Temporarily delaying transmission of outgoing ack so that they can be hooked onto the next outgoing data frame.

. Adv: Higher channel bandwidth utilization

. Complication: If wait is longer than sender timeout period then sender retransmits

→ Purpose of acknowledgement is lost

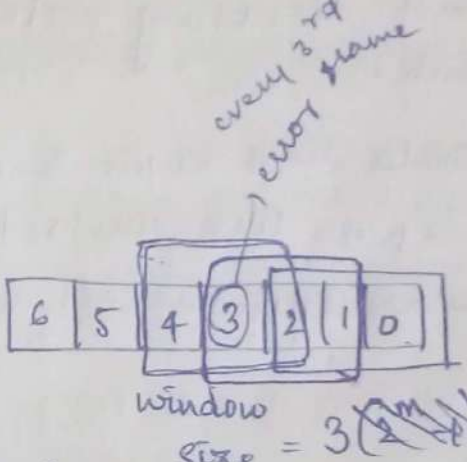
. Sol: If new packet arrives quickly

→ Piggybacking

If not

→ Sending separate ack frame.

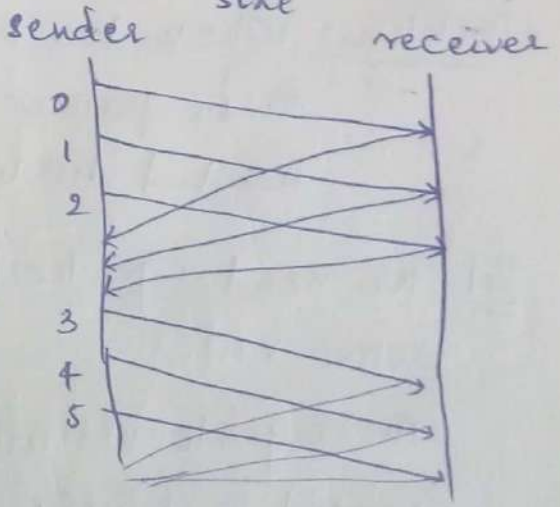
* Sliding Window protocol:



- One bit sliding window protocol
- Go back N protocol
- Selective repeat protocol

→ after the first frame is sent, it will wait for next frame

→ No need to wait, continuous frames are sent & discarded if error occurs (in transmission frame errors are discarded)



If 0,1,2 is sent & 2 has error then 3,4,5 are sent and again 2 is corrected & sent with 3,4,5 again. The duplicate ones will be discarded.

→

* Multi Access Protocols:

- If there is a dedicated link b/w the sender & the receiver then data link control layer is sufficient, however if there is no dedication link present then multiple stations can access the channel simultaneously.

Hence multiple access protocols are required to decrease collision & avoid crosstalk. Thus protocols are required for sharing data on non dedicated channel.

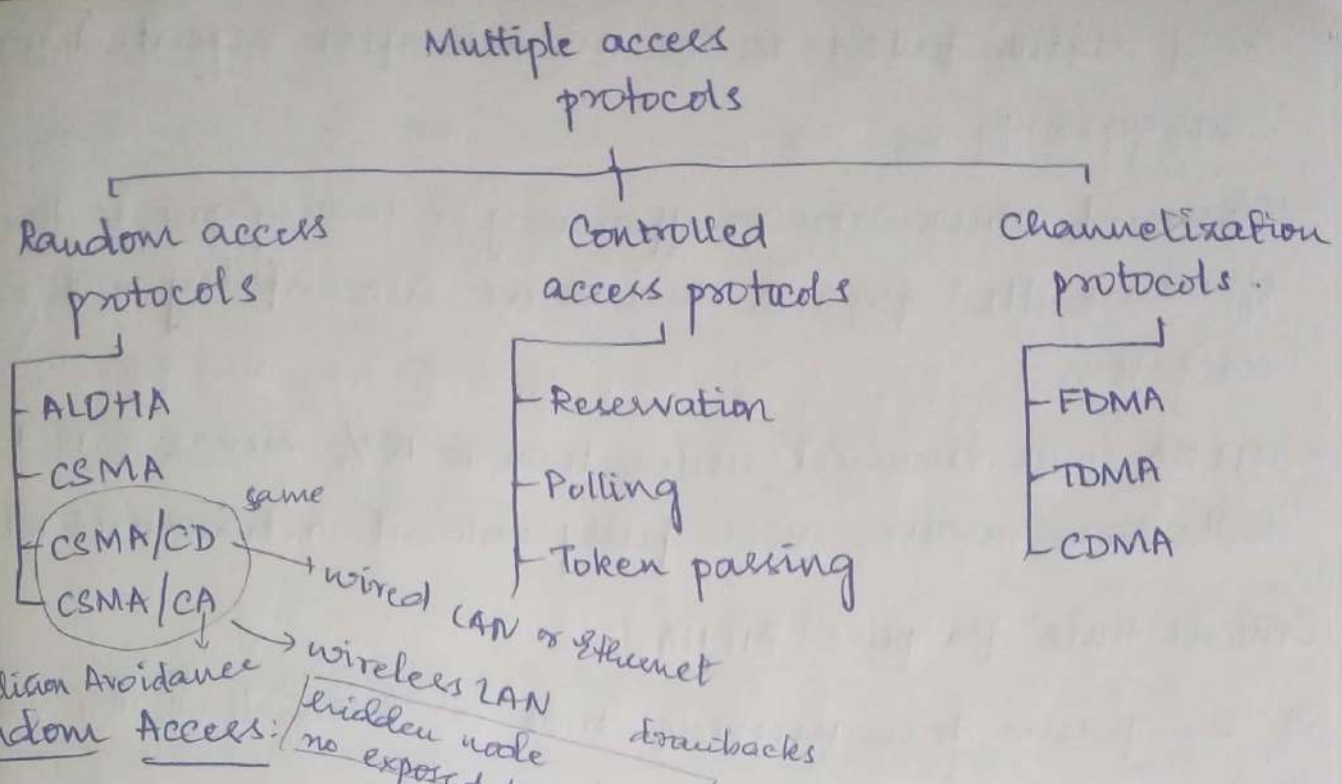
- Broadcast link used in LAN consists of multiple sending and receiving nodes connected to or use a single shared link.
- Data link layer has two functionality oriented sublayers
  → Data link control (LLC) (responsible for error & flow control)
  → Multiple access control (responsible framing & MAC address & multiple access control)
- Problem: When two or more nodes transmit at same time, their frames will collide & link bandwidth is wasted during collision.

Sol: We need a protocol to coordinate the transmission of the active nodes

These protocols are called Medium / Multiple Access Control Protocols.

Their main task is to minimize collisions to utilize bandwidth by:

→ determining when a station can use the link
→ what a station should do when the link is busy
→ what the station should do when it is involved



drawbacks
hidden node
no exposed terminal

* Random Access:

- No station is superior over another station & none is assigned control over another.
- A station with frame to be transmitted can use the link directly based on a procedure defined by the the protocol to make a decision on whether or not to send.

- ALOHA:

→ was designed for wireless LAN & can be used for any shared medium.

→ Pure ALOHA protocol description:

- All frames from any station are of fixed length.
- Stations transmit at equal transmission time
- After transmission, sender waits for ack equal to the max. round trip propogation delay = $2 * t_{prop}$

time taken for a bit of frame to travel b/w two most widely separated stations

- If no ack received, it resends frame as it tells ks the

- If station fails to receive an ack after repeated transmi
it gives up.

→ Channel utilization or efficiency or throughput is the % of transmitted frames that arrive successfully without collisions.

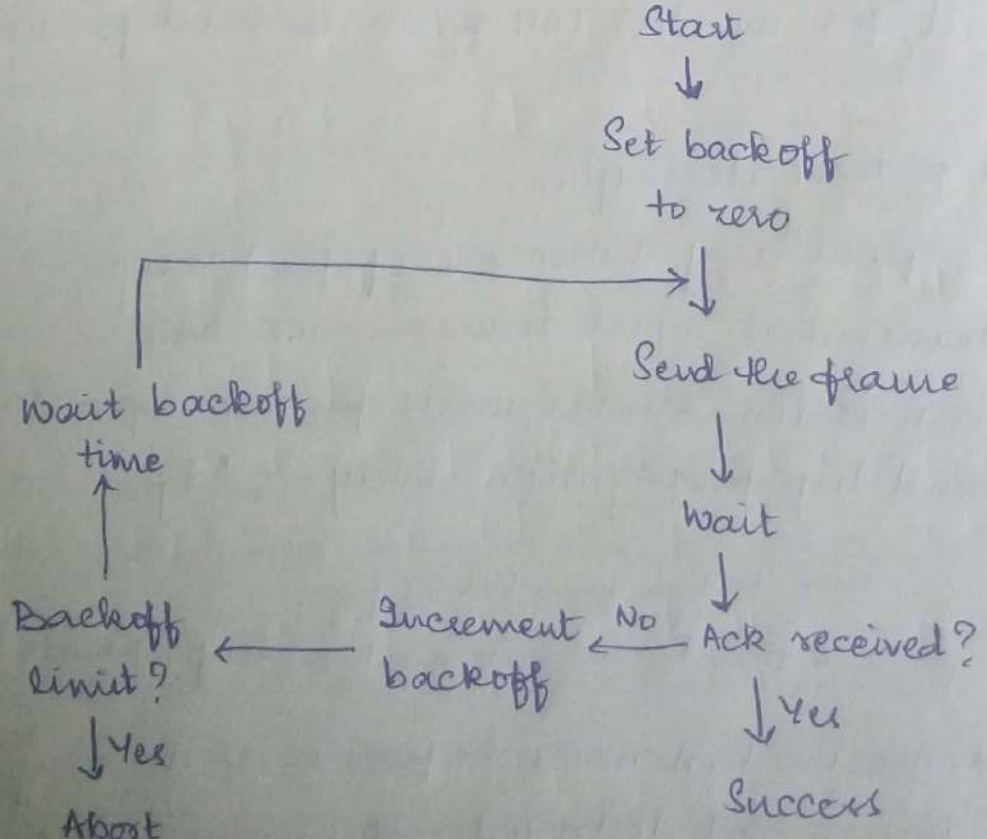
→ ALOHA max. channel utilization is 18% means 0.18 # n fra will ~~arrive~~ arrive successfully without retransmission.

Critical time for pure ALOHA:

If the frame transmission time is T sec, then the vulnerab time is = 2T sec.

This means no station should send during the T-sec befor this station starts transmission & no station should start sending during the T-sec period that the current station is sending.

Procedure for ALOHA protocol:



*Note:

Throughput for pure ALOHA is $S = G * e^{2G}$ → avg no. of all stations frames during one frame transmission time

Max. throughput $S_{max} = 0.184$ when $G = 1/2$

37%

Pure ALOHA

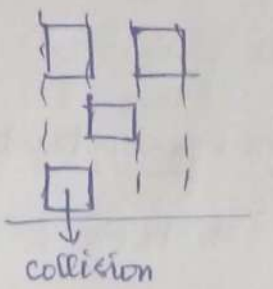
/ \

complete collision | partial collision

Slotted ALOHA

|

complete collision



• CSMA: (Carrier Sense Multiple Access)

→ To improve performance, avoid transmissions that are certain to cause collisions.

→ Based on the fact that in LAN propogation time is very small

→ If a frame was sent by a station, All stations knows immediately so they can wait before start sending.

→ A sender station should sense the medium for another carrier (transmission) before it starts its own transmission (idle)

→ If busy, don't send

→ This can reduce the possibility of collision but it cannot eliminate it.

→ Collision can only happen when more than one station begin transmitting within a short time.

→ The longer the propagation delay, the worse the performance of the protocol.

Types of CSMA:

1. Non-persistent CSMA
2. 1 " "
3. P " "
4. O (order is given to transmit frames)

• Non-persistent CSMA:

→ A station with frames to be sent, should sense the medium
  • If medium is idle, transmit; otherwise
  • If medium is busy, (backoff) wait a random amt. of time & repeat

→ Non-persistent stations are deferential (w.r.t respect others)

→ Performance:
  • random delays reduces probability of collisions
  • bandwidth is wasted if waiting time is more.

• 1-persistent CSMA: (selfish) (2-or more stations collision)
Continuously senses for idle medium & transmits. If not idle, continously listen until medium becomes idle.

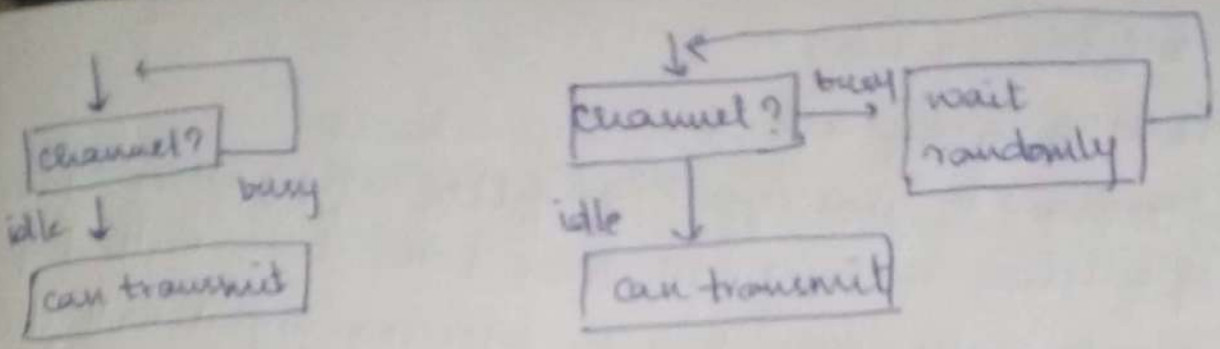
• P-persistent CSMA:

→ Time is divided to slots where each time unit typically equals max. propogation delay.

→ If idle, transmit with prob. (p) or wait one time unit (slot) with prob (1-p) then repeat

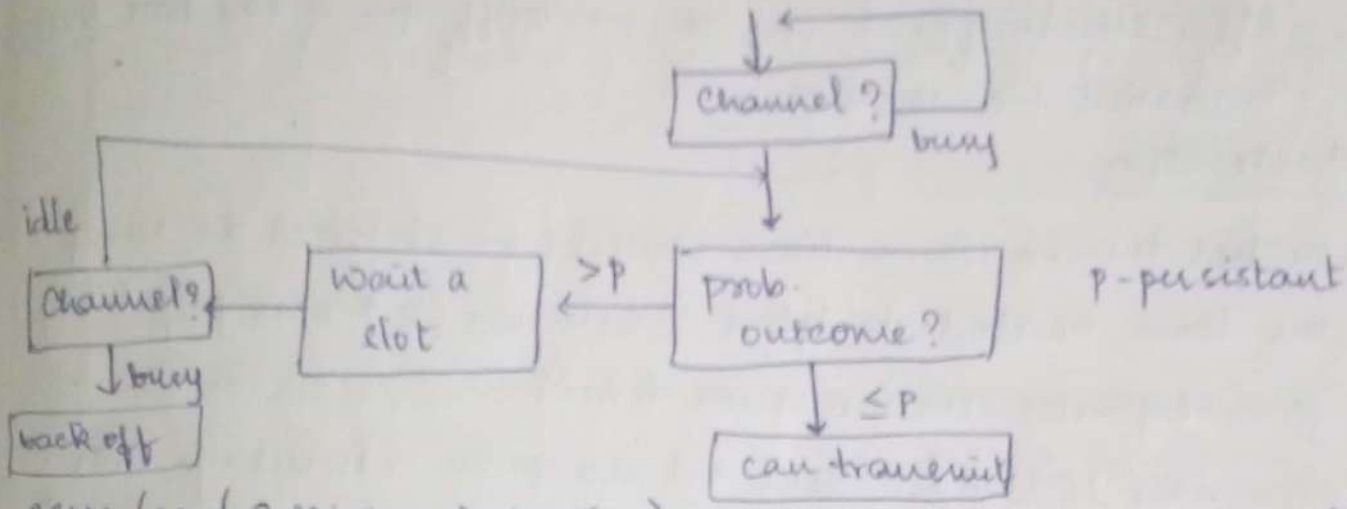
→ If busy, continuously listen until idle & repeat

→ Performance:
  • reduces collisions like non persistent



1 - persistent

non persistant



- CSMA/CD (Collision Detection): (twice the max. propagation delay = detect collision)

→ while transmitting, the sender is listening to medium for collisions

→ Sender stops transmission if collision has occured reducing channel wastage.

→ CSMA/CD is widely used for bus topology LANs (IEEE 802.3, Ethernet)

How does a node detect collision:

Transceiver: A node monitors the media while transmitting. If the observed power is more than transmitted power of its own signal, it means collision occured.

Hub: If I/p occurs simultaneously on two ports, it indicates a collision. Hub sends a collision presence signal to all ports.

→ If collision occurs:

- Abort transmission ✗
- Transmit a jam signal (48 bit) to notify other stations of collision so they will discard the transmitted frame also to make sure that the collision signal will stay until detected by the furthest station
- After sending jam signal, backoff for a random time then
- Transmit frame again

→ Restrictions:

- Packet transmission time should be at least as long as the time needed to detect a collision (2 * max prop delay + jam sequence transmission time)
- Otherwise, CSMA/CD does not have an advantage over CSMA.

* CSMA/CD with binary exponential backoff algorithm:

(Collision resolution mec

- This algorithm is generally used in Ethernet to schedule re-transmissions after collisions.
- After collision takes place b/w 2 stations, if the data is retransmitted soon after it, again collision may occur.

$$\text{Waiting time} = k * T_{slot}$$

$k \in [0, 2^n - 1]$, where n = no. of collisions

- The stations will take random integer from set k i.e $\{0,1\}$ ($n = 1$)

↓ Contention window

waiting time for both stations for $K = 0$ $= 0 * T_{slot} = 0$ (collision)

retransmit < 00 = 0, 01, 10 (Collision)

* Collision free protocol: ← almost same → Control free access protocol
provides in order access to shared medium so every station has chance

* Bit map method to transfer

- All stations will send bits to indicate whether it has frame to send or not.
- At the end of the control frame, every station knows all the station that want to send, the station can send in order
- Protocols like this in which the desire to transmit is broadcasting for the actual transmission are called Reservation Protocols.

- Ex:

0 1 2 3
0 1 0 1 frame 1 frame 3

0 1 2 3
1 0 0 0 frame 0

- Performance:
- $d/(d+1)$ channel utilization rate for high load.
- N bits delay for low load (d is the frame size)

(system)

* binary countdown:

Ex: station 2 (0010) (give up)
4 (0100) (give up)
9 (1001)
10 (1010)

→ this address is sent as 1 is more
9 will give up

- Eventually only one station (with largest station no. among all the competitors) gets the channel.
- Performance:
- Channel utilization rate: $d/(d+\log(N))$ for high load
- $\log(N)$ bits delay for low load

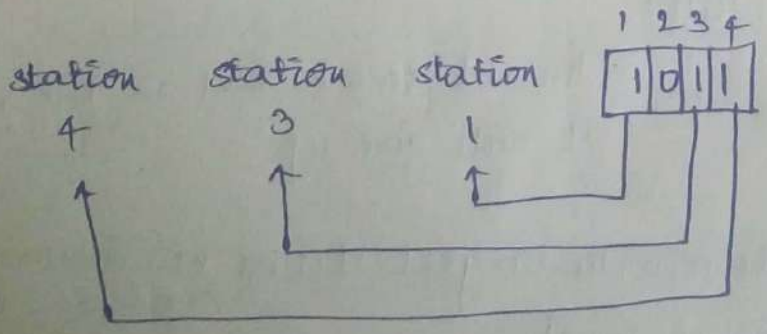
* Token pass:

- There is only one token in the network.
- The token is passed through every node in the network.
- Only the node that has the token can transfer data.

* Types of Controlled Access Protocol: (actual ones)

- Reservation access protocol:

→ Stations take turns transmitting a single frame at a full rate (R) bps
→ Transmissions are organized into variable length cycles
→ Each cycle begins with a reservation interval that consists of (N) minislots. One minislot for each of N stations.
→ When a station needs to send a data frame, it makes reservation in its own minislot.
→ By listening to the reservation interval, every station knows which stations will transfer frames, and in which order.
→ The stations that made reservations can send their data frames after the reservation frame.



- Polling:

→ Stations take turns accessing the medium.

→ Centralized: (data exchange done by this)

- One device is assigned as primary station and the others as secondary stations
- When the primary has a frame to send, it sends select frame that has address of secondary
- When primary ready to receive, it sends poll frame for each device to ask if it has data to send or not. If yes, data transmitted otherwise NAK is sent.
- Polling can be done in order (round-robin) or based on predetermined order.

→ Distributed:

- No primary secondary
- Stations have known polling order based on some protocol.
- Station with highest priority has access first & then right next to station
- Token passing network: (distributed polling)

Listen state

listen
If the arriving bits & check the dest. address to see if it is its own address or send it to next station

Transmit state

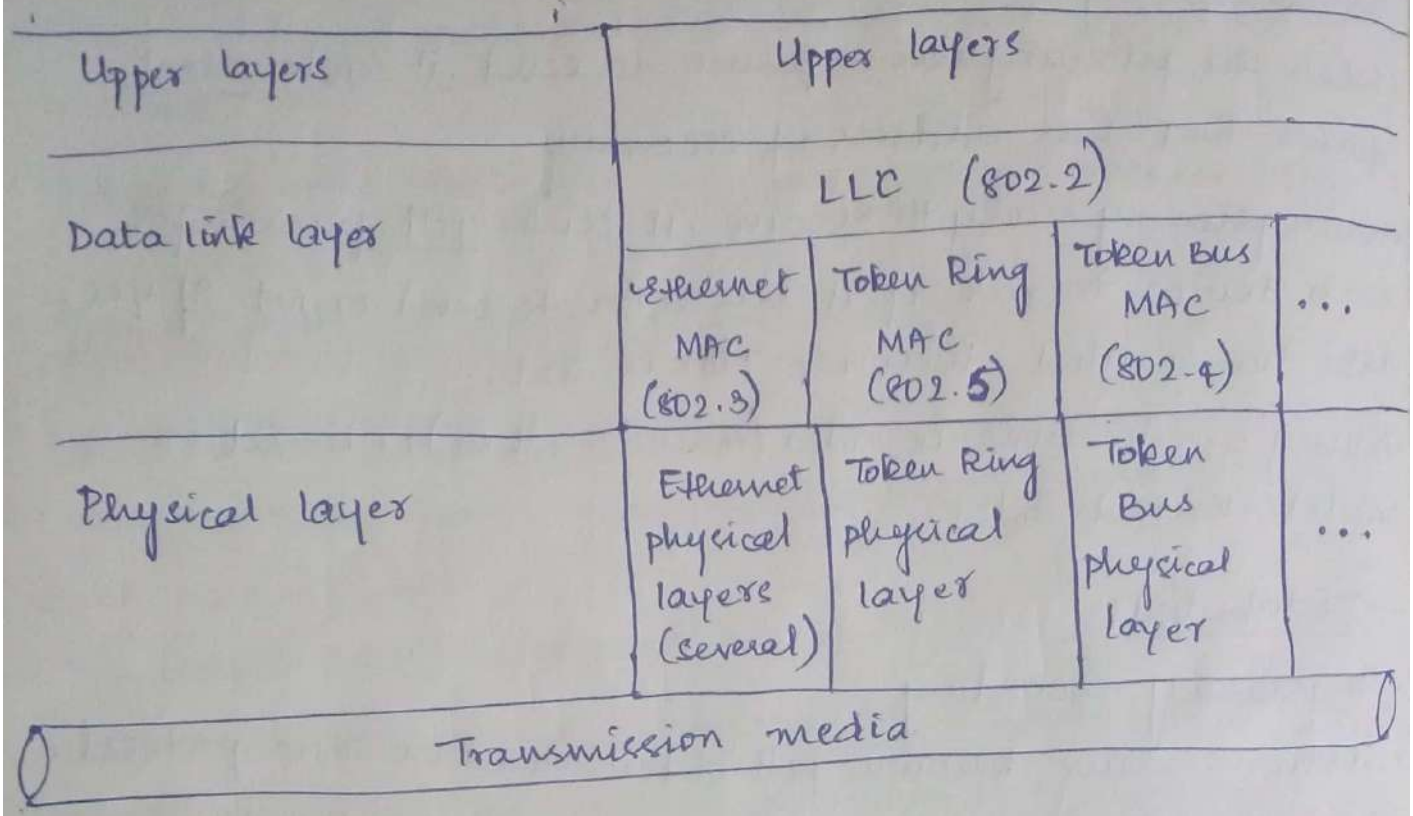
station captures a special frame called free token & transmits its frames. Sending station is responsible for reinserting or removing free token from the medium.

*Channelization protocols:

Available bandwidth of a link is shared in time, freq, or through code b/w diff stations.

* IEEE Standard for LANs: (Ethernet) (wired LAN)

LLC : Logical link control MAC : Media Access Control



* Standard Ethernet

Ethernet evolution

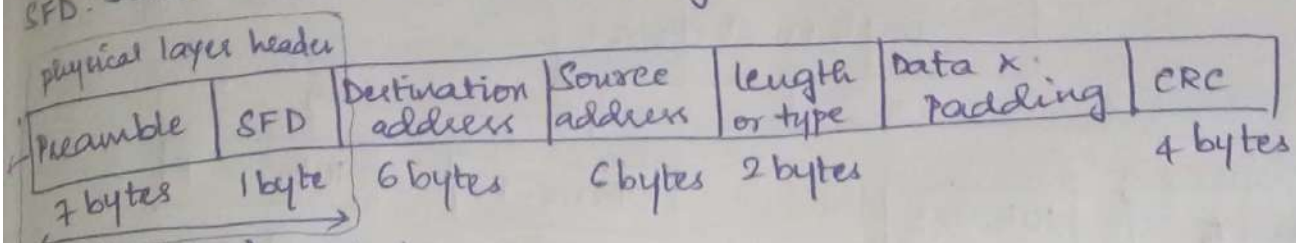
- Standard Ethernet — 10 Mbps
- Fast Ethernet — 100 Mbps
- Gigabit Ethernet — 1 Gbps
- Ten-Gigabit Ethernet — 10 Gbps

* MAC Sublayer:

In Standard Ethernet, the MAC sublayer governs the operation of the access method. It also frames data received from the upper layer and passes them to the

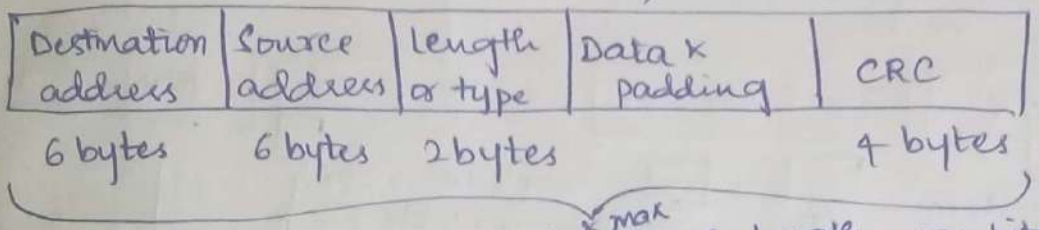
Preamble: 56 bits of alternating 1s and 0s

SFD: Start Frame Delimiter, flag (10101011)



* Minimum & max. lengths:

Min. payload length = 46 bytes
Max. " " = 1500 "



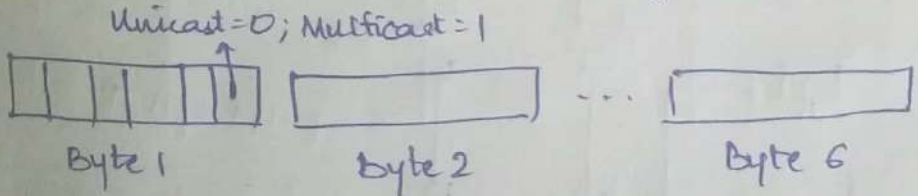
* Min. & max. frame length: 512 bits or 64 bytes &
12,144 bits or 1518 bytes

* Addressing: ipconfig command

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6-byte physical address

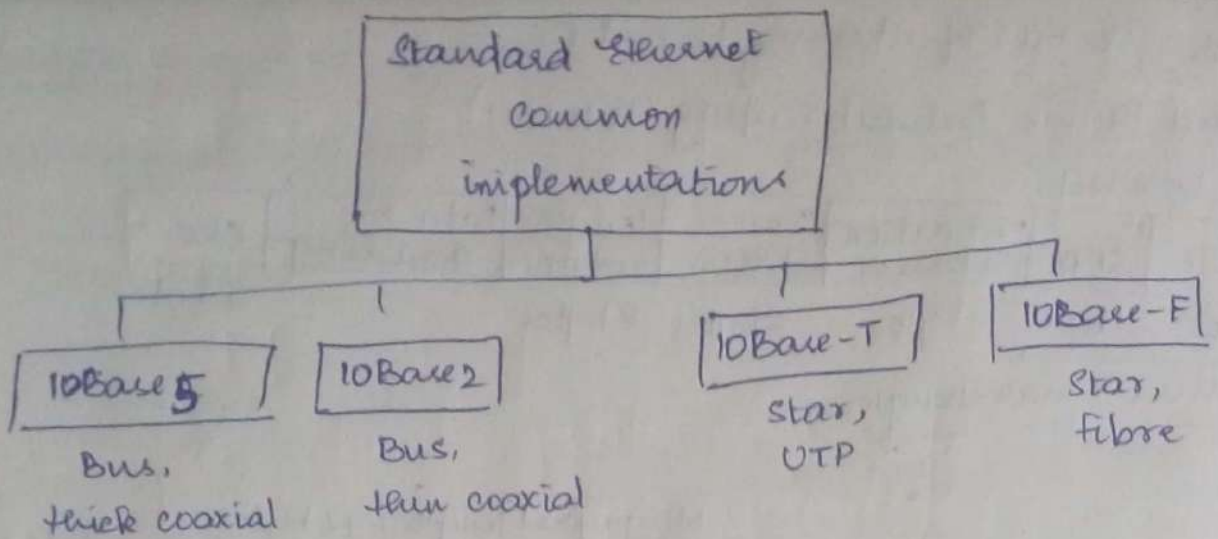
06 : 01 : 02 : 01 : 2C : 4B

6 bytes = 12 hex digits = 48 bits

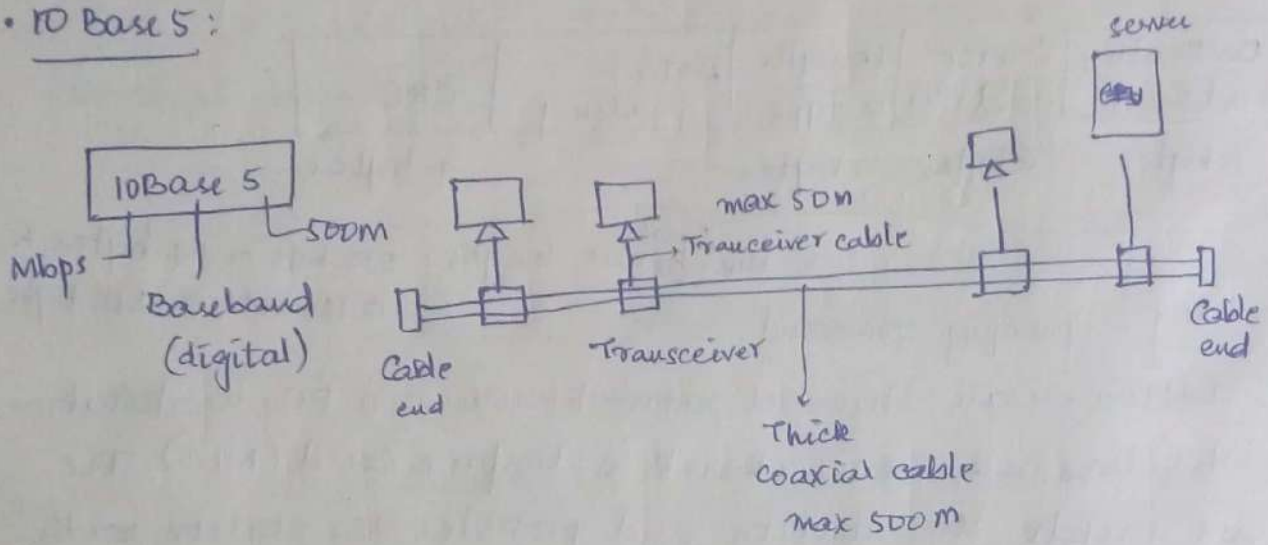


* Physical Layer:

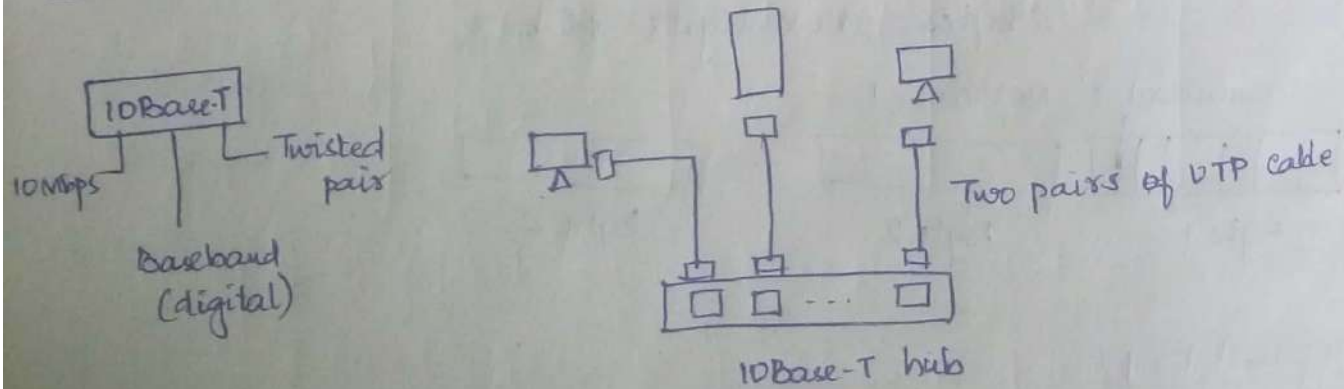
The Standard Ethernet defines several physical layer implementations; four of the most common are shown →



- 10 Base 5:



- 10Base-T:



- Summary of Standard Ethernet implementations:

Characteristics	10Base 5	10Base 2	10Base-T	10Base-F
Media	Thick coaxial cable	Thin coaxial cable	2 UTP	2 Fiber
Max. length	500m	185 m	100m	2000 m

* Fast Ethernet:

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel. IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Standard Ethernet but it can transmit data 10 times faster at a rate of 100 Mbps

topology:

pt to pt

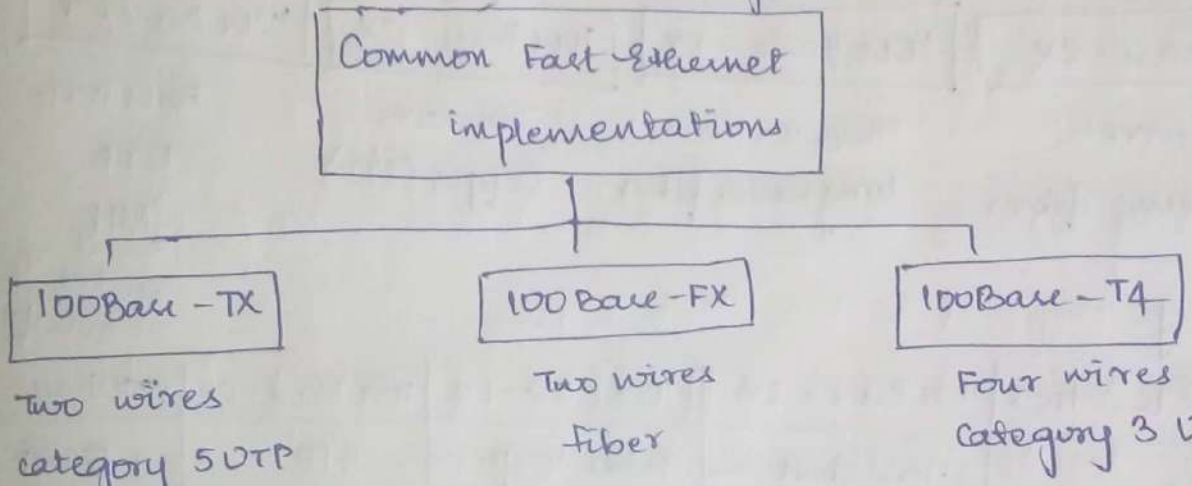
Star

Supports unlike physical media segments (one per collision domain) ← Class I Repeater

Single physical media (2 per collision domain) ← II

full duplex ← Switches

autonegotiation



Summary of fast ethernet implementations:

Characteristics	100Base-TX	100Base-FX	100 Base-T4
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
No. of wires	2	2	4
Max. length	100m	100m	100m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

* Gigabit Ethernet:

The need for an even higher data rate resulted in the design of gigabit ethernet protocol (1000 Mbps). The IEEE

Topology:

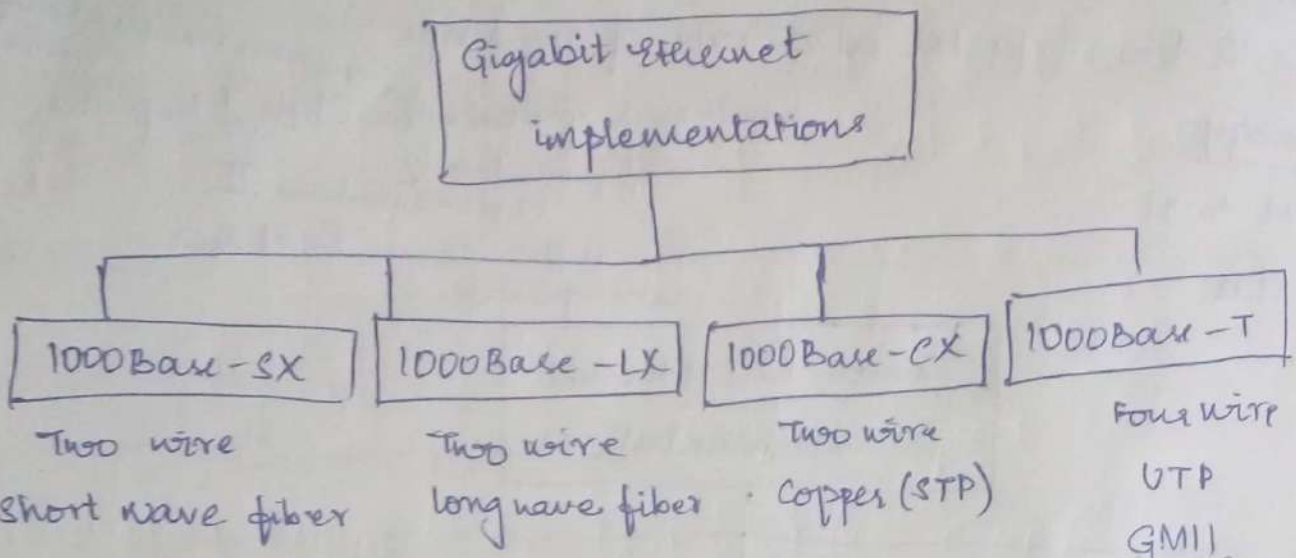
Point to pt

Star

Two Stars

Hierarchy of stars

Carrier Extension
Frame Bursting



Summary:

Characteristics	1000Base-SX	1000Base-LX	1000Base-CX	1000Base-T
Media	Fibre short wave	Fiber long wave	STP	cat 5 UTP
No. of wires	2	2	2	4
Max. length	550 m	5000 m	25 m	100m
Block encoding	8B/10B	8B/10B	8B/10B	
Line	NRZ	NRZ	NRZ	4D-PAM5

*Summary of 10 gigabit ethernet implementations:

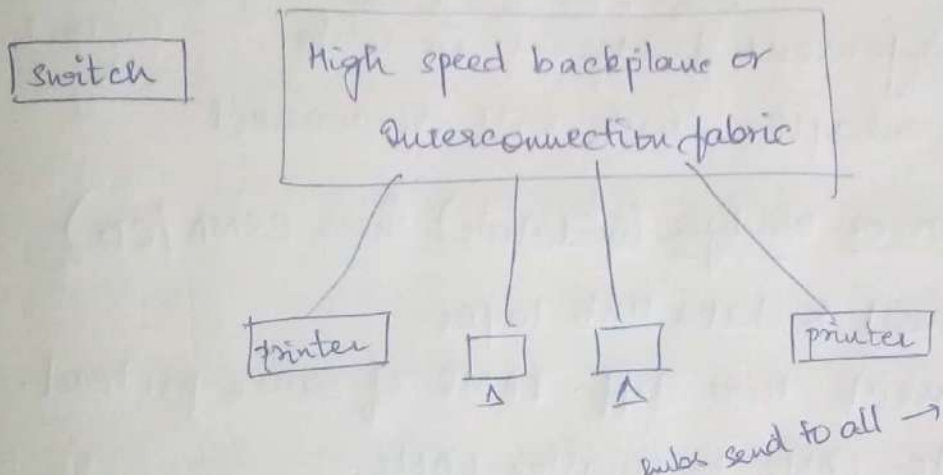
Characteristics	10GBase-S	10GBase-L	10GBase-E
Media	Short wave 850-nm multimode	Long wave 1310 nm single mode	Extended 1550 nm single mode
Max. length	300m	10 km	40 km

Ethernet in MAC: (connecting devices)

Hub: (physically star, logically bus) no privacy

- Separate transmit & receive pair of wires.
- The repeater in the hub retransmits the signal received on any input pair onto ALL output pairs
- Essentially the hub emulates a broadcast channel with collisions detected by receiving nodes.

Switched ethernet: (improve on Hub concept)



hubs send to all → so collisions

- The switch learns destination locations by remembering the ports of the associated source address in a table.
- The switch may not have to broadcast to all o/p ports. It may be able to send the frame only to the destination port.
- a big performance advantage over a hub, if more than one frame transfer can go through the switch concurrently.
- The advantage comes when the switched Ethernet backplane is able to repeat more than one frame in parallel. (a separate backplane bus line for each node).
- The frame is relayed onto the required output port via the port's own backplane bus line.
- Collisions are still possible when two concurrently

• Note - each parallel transmission can take place at 10 Mbps.

* Switched Ethernet Hub:

• Since servers are often shared by multiple nodes, one can employ a switching hub with a port which operates at a higher rate than the other ports.
• Extra buffering inside hub to handle speed mismatches.
• Can be further enhanced by higher rated port full duplex

* Hubs vs repeaters: → only sends/receives data
→ can't be used in higher layers
Network management features in hub
Issues with adapter, hub will disconnect
corrupted signal → regen signal

* ~~Connecting devices~~: Bridges: (Switches) (uses CSMA/CD)

• works in physical & data link layer
• used to connect two diff. LANS of same protocol.
• used to divide LANs to smaller LANs
• performs filtering whether a frame should be forwarded/dropped to another interface.
• This is done by bridge/forwarding table with address & port no. (or interface, time) Addr. / Port no.
• Initially table is empty, later filled with frames ~~sending~~ sent to other LANs.
• If no entry is there matching the frame, it is added otherwise the interface no.s are updated.
• If the frame received is matching with interface no. then the frame is forwarded else discarded.
• Switch doesn't allow multi

• When using switches, the network should not contain any loop

• Loops can cause no. of frames in the LAN to increase indefinitely.

• Problem:

Two bridges forward the same frame & redundancy occurs & that's why shortest path is taken using spanning tree algorithm.

So bridges block few ports so that loops are not formed.
(based on shortest path)

BPDU
Bridge Protocol Data Unit

1. built in ID (48 bits)
Smallest ID = root
2. Shortest path
3. Shortest tree

*Switches:

• Used to connect individual computers

• Allows more than one device connected to the switch directly to transmit simultaneously.

• Can operate in full duplex

• Two types:

Store & forward Cut through

*Routers: (3rd layer)

• Operates at network layer - packets

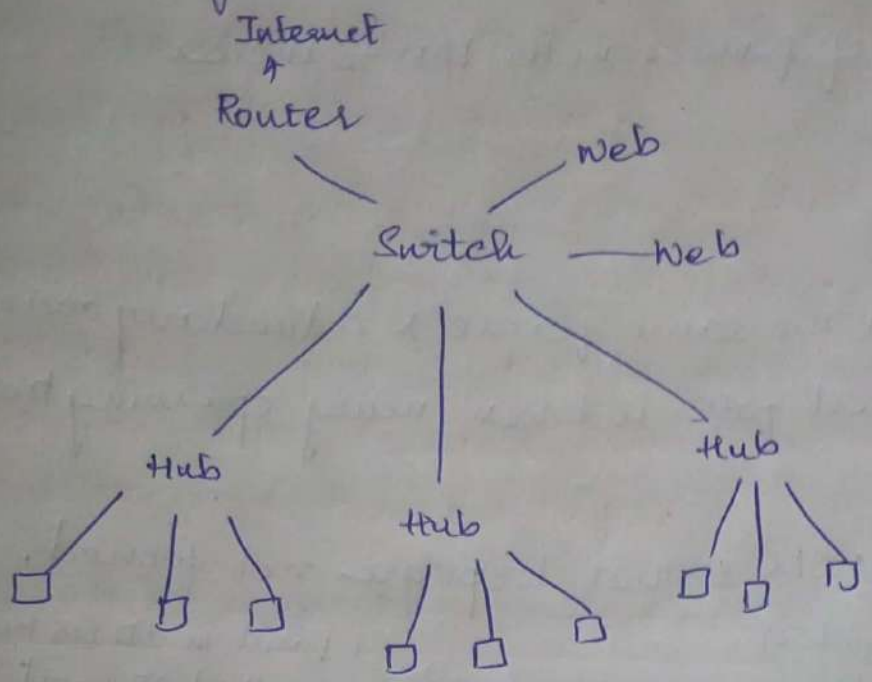
• Connect LANs and WANs with similar or diff protocols

• Routers isolate both collision & broadcast domains.
Switches & bridges isolate →

• Deals with global address (logical/IP addressing) not MAC addr.

• routers communicate with each other & exchange routing

- Determine best route using routing algorithm.
- Forwarding / discarded



* Comparison:

	hubs	bridges	routers	switches
Traffic isolation	No	Y	Y	Y
plug & play	Yes	Y	N	Y
optimal routing	No	N	Y	N
cut through	Yes	N	N	Y

* Gateway: (Application, Transport layer) (All 7 layers)
- Passage to connect two networks together that may work upon diff - networking models.
- work as messenger agents (take data, interpret, transfer)
- also called protocol converters & can operate at any network layer
- complex than switch or router.

3 Network Layer:

SA-1
Network layer design issues:

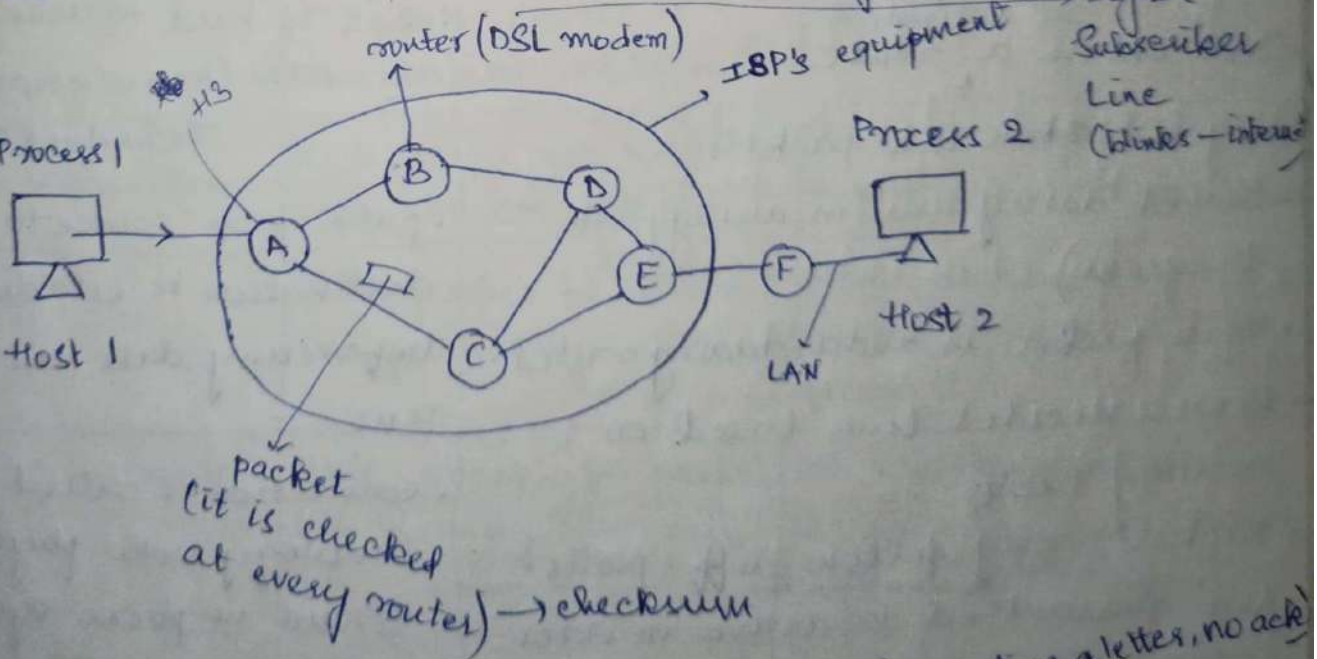
- Responsible for delivering packets b/w endpoints over multiple links
- Network layer is the lowest layer in the OSI reference model that deals with end to end transmission.

The design issues are:

→ Store & forward packet switching (restating the content of network layer protocols)
→ Services provided to transport layer
→ Implementation of connectionless & connection-oriented service
→ Comparison of virtual-circuit & datagram subnets]

SA-16
Store & forward packet switching:

Customer equipment - outside oral
Carriers # - routers connected by transmission lines



Packet switching (connection types)
- connectionless: datagram (Ex: posting a letter, no ack)
- connection oriented: virtual circuit

Data divided into small parts (packets), transmitted node to node, processed & forwarded

* Services provided to transport layer:

- The services should be independent of router technology.
- The transport layer should be shielded from the no., type & topology of routers present.
- The network addresses made available to transport layer should use a uniform numbering plan, even across LANs & WANs
- Topology of network should be hidden
- Network layer designers have freedom in writing specification of services to transport layer.

* Connection-oriented (TCP) or connectionless (UDP, datagram):

Internet community - connectionless; routers job is moving packets & nothing else subnet is inherently unreliable. hosts should provide error & flow control	Telephone companies - connection-oriented subnet should provide reliable service successful experience with telephone system without connections, QoS is hard to achieve
Ex: Internet	Ex: ATM (Asynchronous Transfer Mode)
• Can't choose a single route	• path from source to destination is established before any data can be sent
• Msg is broken into packets	• connection is called VC (analogy with physical circuit in phone system)
• called datagram (in analogy with telegram)	• Avoid choosing new route for each packet
• Each packet is individually routed.	• Each packet has ID for which VC it belongs.
• Routers decides line based on routing table	
• Packets may follow diff. paths	
• Not guaranteed to arrive in order	

x: A can easily know connection 1 packets of H1 from connection 1 packets of H3

cannot do this

Thus A assigns diff. connection ID to outgng traffic for second conn.

To avoid conflicts, routers need ability to replace conn. IDs in outgng packets

This is called label switching

Ex: H1 has established connection 1 with H2

first entry in each routing table

H3 later establishes connection with H2

A's table

In		Out	
H1	1	C	1
H3	1	C	2

unit 3 diagram but H3 is connected to 'A'.

LA-1

Comparison of VC x datagram:

Issue	Datagram subnet	Virtual circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source x destination address	Each packet contains a short VC no.
State information	Routers do not hold state info abt connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allotted in advance for each VC
Congestion control	Difficult	

11

* [SA 6] Routing Algorithm:

Network layer software responsible for deciding which O/P line an incoming packet should be transmitted on.

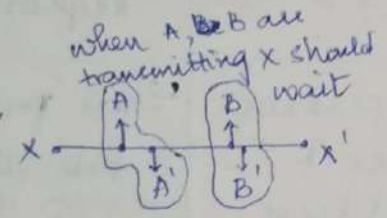
Datagrams: require computation of decision making tables for each packet.

VC: routing decision are made only when new VC is being set up.

Session routing: data packets follow the same routing for the entire session.

Prop. in a routing alg.:

→ correctness
→ simplicity
→ robustness
→ stability
→ fairness
→ efficiency



routing table

static (manual entries)

dynamic (updated automatically when there is change in Intent)

A routing protocol is a combination of rules & procedures that lets routers in the Internet inform each other of changes.

* Routing vs Forwarding:

Routing: filling & updating routing tables

Forwarding: making the decision which routers to use based on routing tables

* Adaptive (or Dynamic: DVR, HR) vs Non-Adaptive (or Static: shortest path, flooding) Algorithms

Adaptive: change their routing decisions to reflect changes in the topology

Non adaptive:

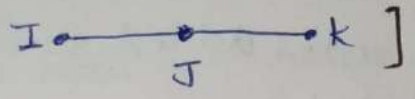
Routing decision is based on pre-computed measurements or estimates & do not update the table based on current traffic & topology.]

SA-4

[Optimality Principle:

If router J is on the optimal path from router I to router K then the optimal path from J to K also falls along the same (optimal path) route.

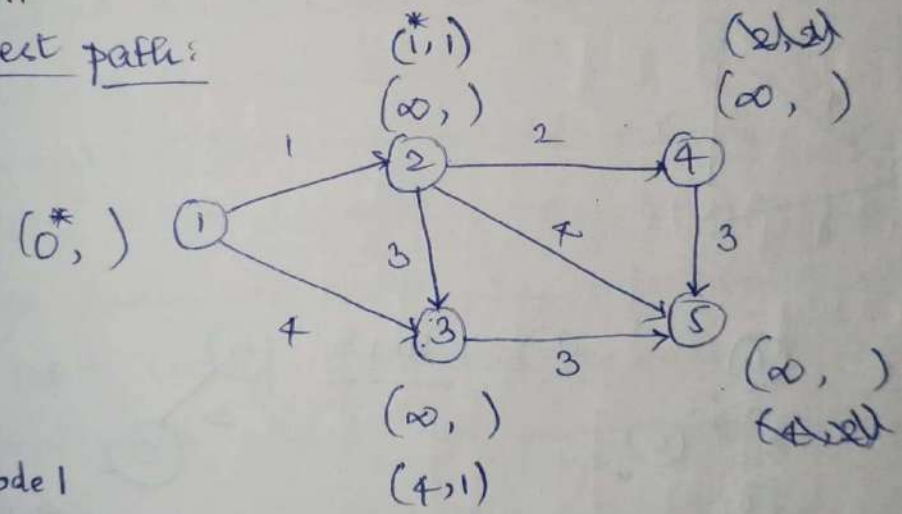
Each portion of a best path is also a best path; the union of them to a router is a tree called the sink tree



]

SA - 11

[Shortest path:



(∞,) = temp. nodes

(0*, 0) = permanent node

from Node 1

i=1: Node 2 : min(∞, 0+1) = 1 ✓

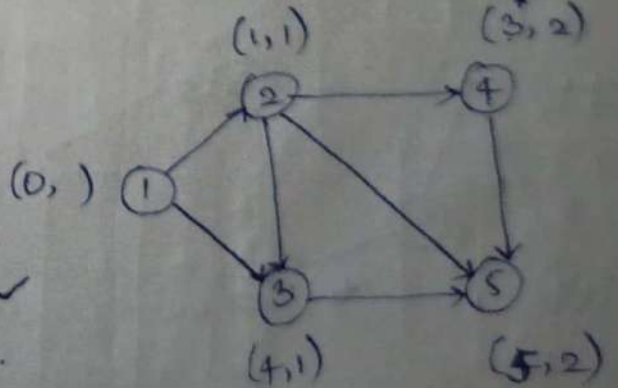
Node 3 : min(∞, 0+4) = 4

then take node 2

i=2: Node 3 = min(4, 1+3) = 4.

Node 4 : min(∞, 1+2) = 3 ✓

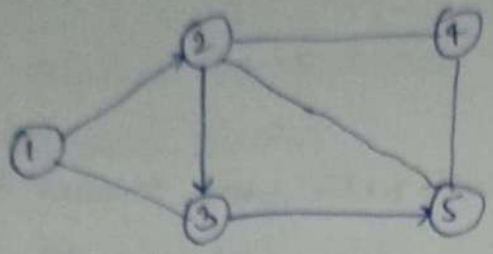
Node 5 : min(∞, 1+4) = 5.



i = 4:

Node 5 : min (5, 3+3) = 5 (backtrack)

Node 3 becomes permanent x
5 can be reached from it

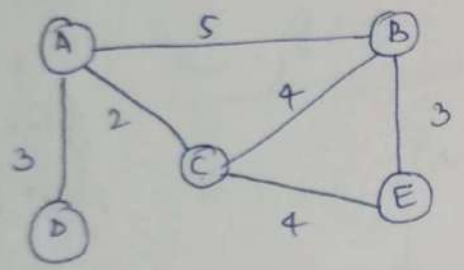


]

* Dijkstra's alg.:

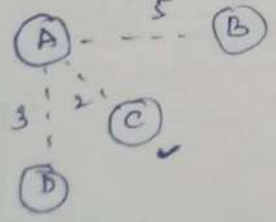
- Start with sink, set dist. to other nodes ∞
- Relax dist. to adj nodes
- Pick the lowest adj node, add to sink
- Keep continuing this until all nodes added to sink.

(pic)

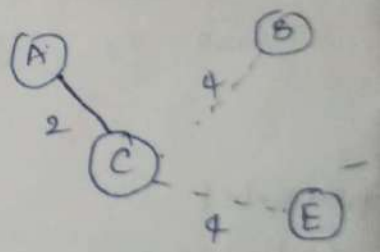


Step1:

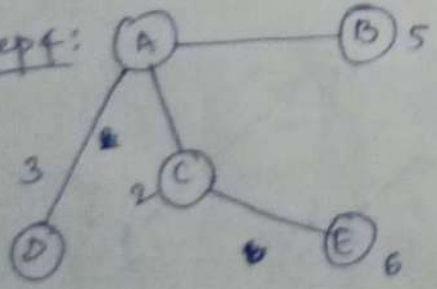
Step2:



Step3:



Step4:



routing table A

Node	Cost	Next router	cost	Next
A	0	–	5	–
B	5	–	–	–
C	2	–	4	–
D	3	–	8	A
E	6	C	3	–

SA-3

* Flooding: (packets arrive more than capacity)
every incoming packet is sent out on every outgoing line except the one it arrived on.
Generates vast no. of duplicate packets, in fact, an infinite no. unless some measures are taken to damp the process.
One such measure is to have a hop counter contained in the header of each packet that is decremented at each hop (router), with the packet being discarded when the counter reaches zero.
The hop should be initialized to the length of the path from source to destination.
If the sender does not know how long the path is, it can initialize the counter to the worst case namely the full diameter of the network.
A variant of flooding called selective flooding partially addresses these issues by only sending packets to routers in the same direction. In selective flooding the routers don't send every incoming packet on every line but only on those lines which are going approximately in the right direction.
Flooding broadcasts packets, but creates loops in the system]

"sequence no."
"keep track of pkts"

* Distance Vector Routing:
- DVR uses Bellman Ford routing alg.
- DV is a distributed routing alg.
- Shortest path computation is split across nodes (each router maintains its own routing table giving the best known distance * link to use to every router in the network)

Alg:

- Each node knows dist. of links to its neighbours
- Each node advertises vector of lowest known distances to all neighbours
- When node uses received vectors to update its own
- Repeat periodically

Bellman ford alg: (dynamic programming)

Initialize d x p:

For each node j — These are initial estimates of the dist.

$d_j = \square$

$d_j = 0$

Set source dist. $d_s = 0$

Repeat the following process |N|−1 times:

For each link (i, j) in G, perform relax process, where

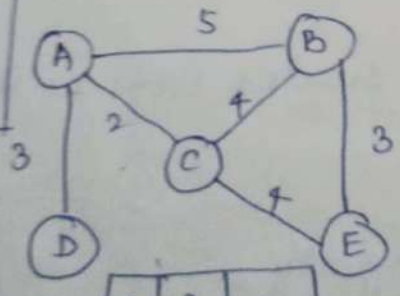
relax:

- if $(d_j > d_i + w_{ij})$ then
  - $d_j = d_i + w_{ij}$ → dist. b/w i x j
  - $p_j = i$

$d_x(y) = \min_v \{c(x,v) + d_v(y)\}$

cost of least cost path from x to y; source; neighbours dist.

To	cost	next
A	0	-
B	5	-
C	2	-
D	9	C
E	6	C



A	5	-
B	0	-
C	4	-
D	8	A
E	3	-

A	3	-
B	8	A
C	5	A
D	0	-
E	9	A

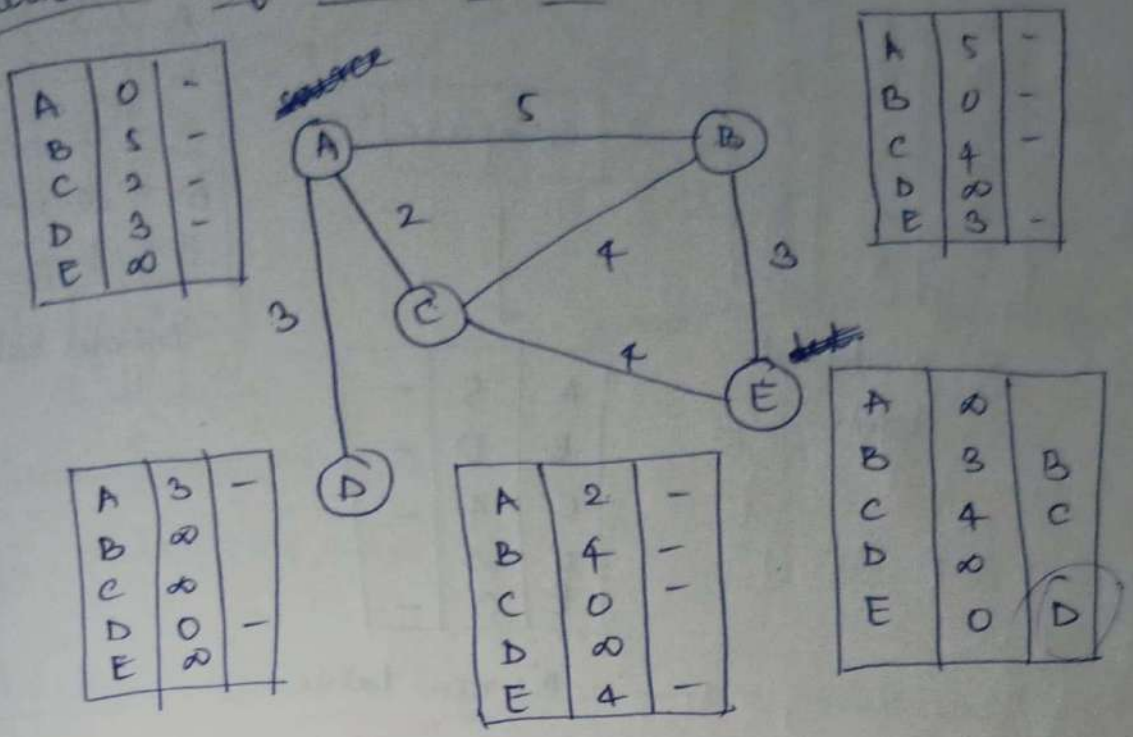
A	2	-
B	4	-
C	0	-
D	5	A
E	4	-

A	6	C
B	3	-
C	4	-
D	9	C
E	0	-

$d_A(E) = \min\{c(A,C) + d_C(E), c(A,B) + d_B(E)\}$

$= \min\{2+4, 5+3\} = 6$

Initialization of tables in DVR:



In DVR, each node shares its table with its immediate neighbor periodically (eg: every 30s) & when there is a change

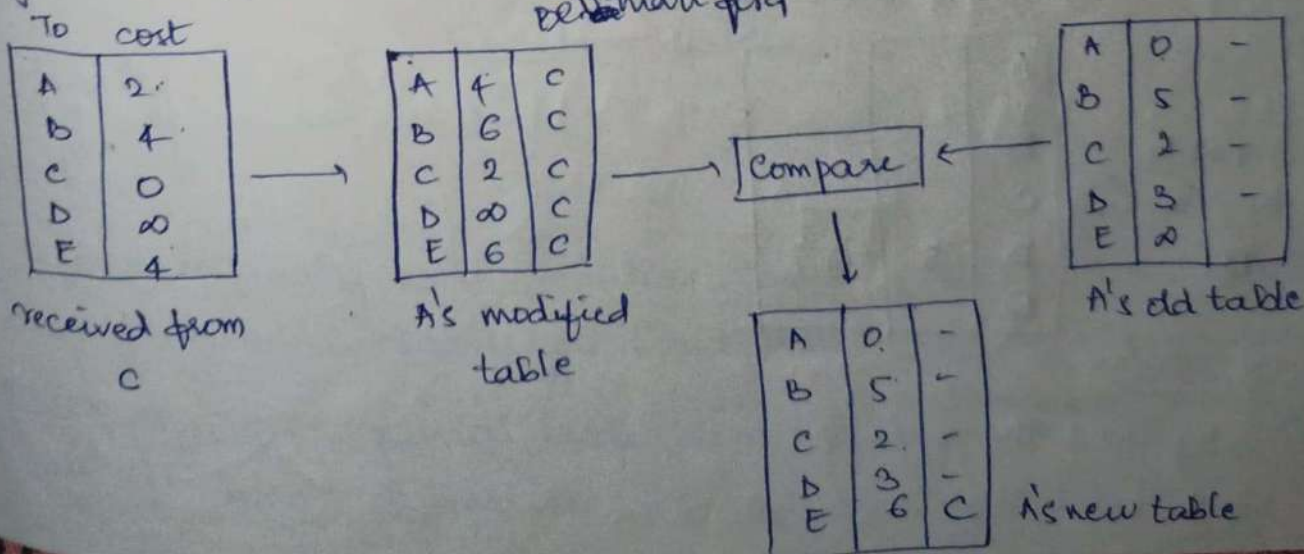
Updating in DVR:

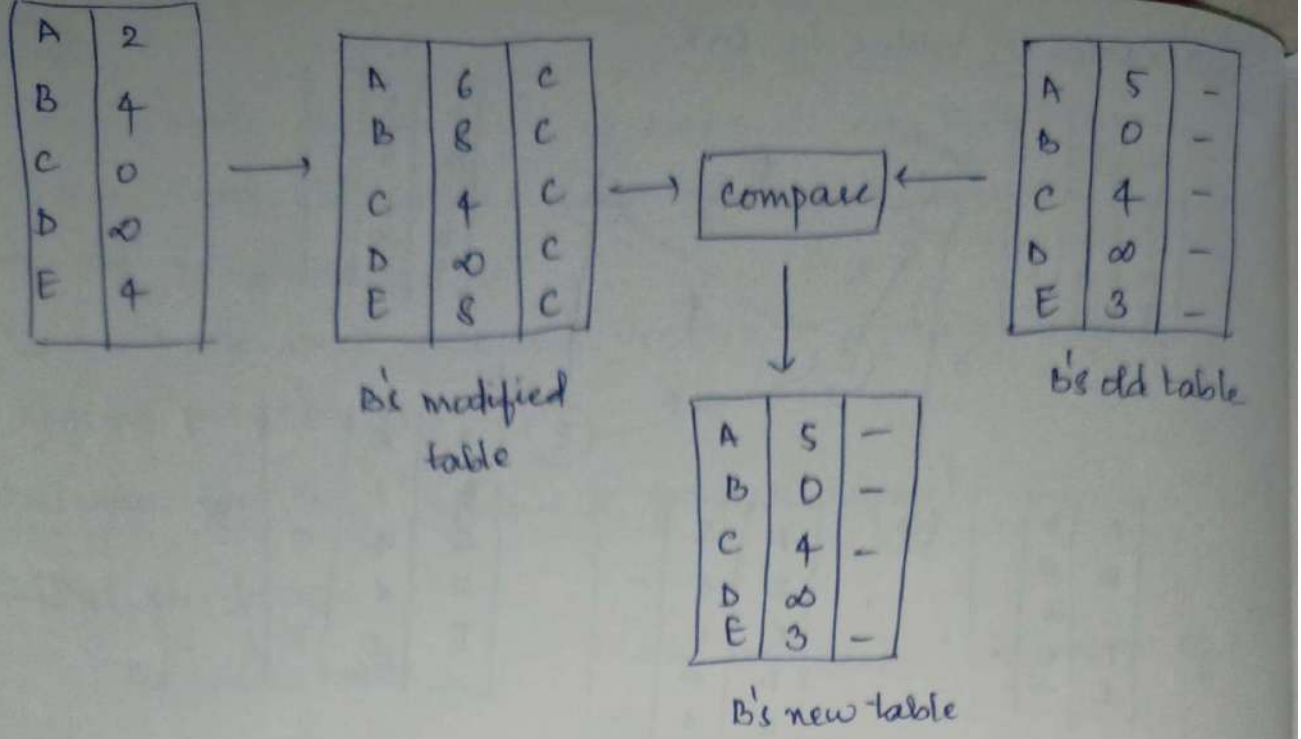
Step 1: Add cost (2) to table received from neighbor C

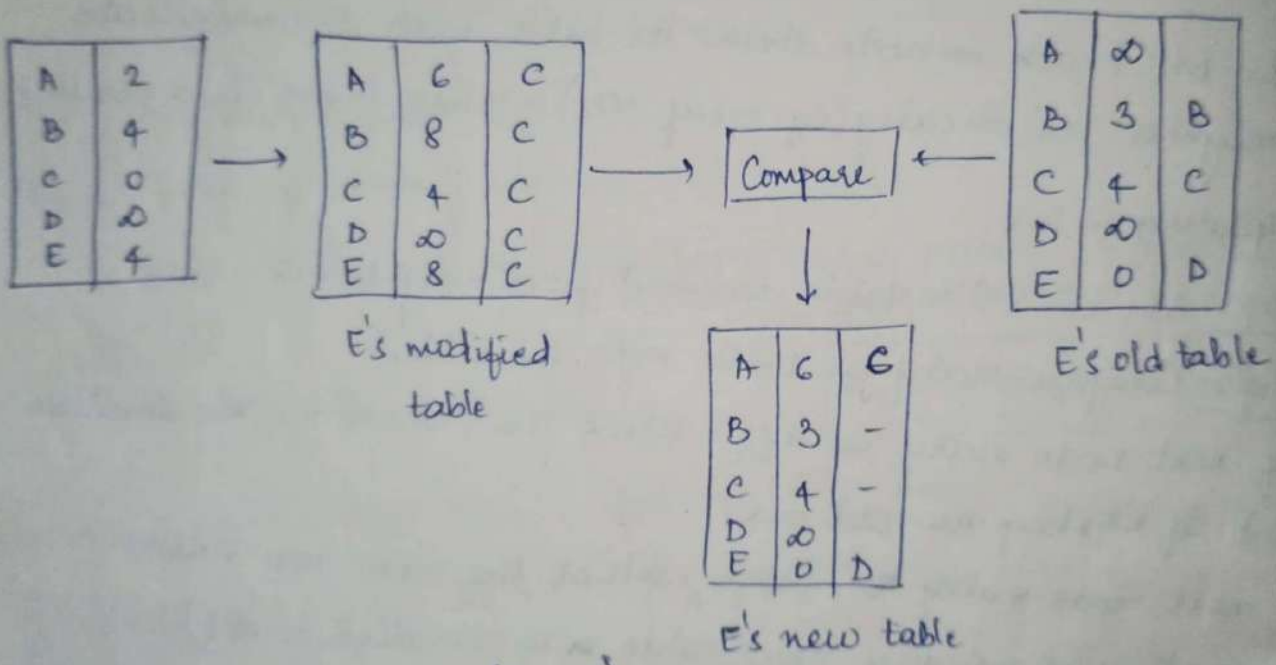
Step 2: Compare modified table with old table

If next node entry is diff, select the row with the smaller cost. If tie, keep the old one

If next node entry is same, select the new row value (regardless of whether new value is smaller or not)



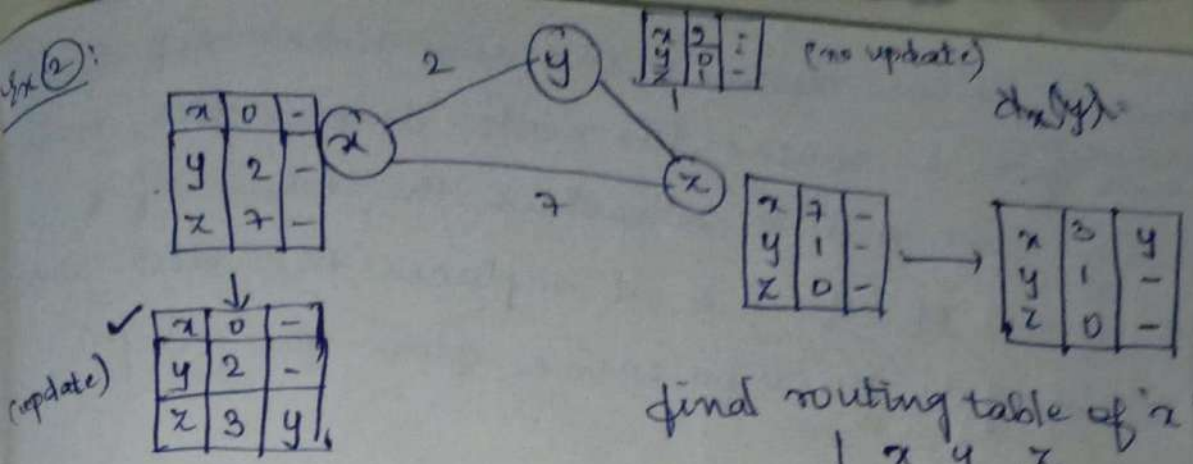




C-A-D (least)

C table to reach D

A		
B		
C		
D	5	A
E		



find routing table of 'x'

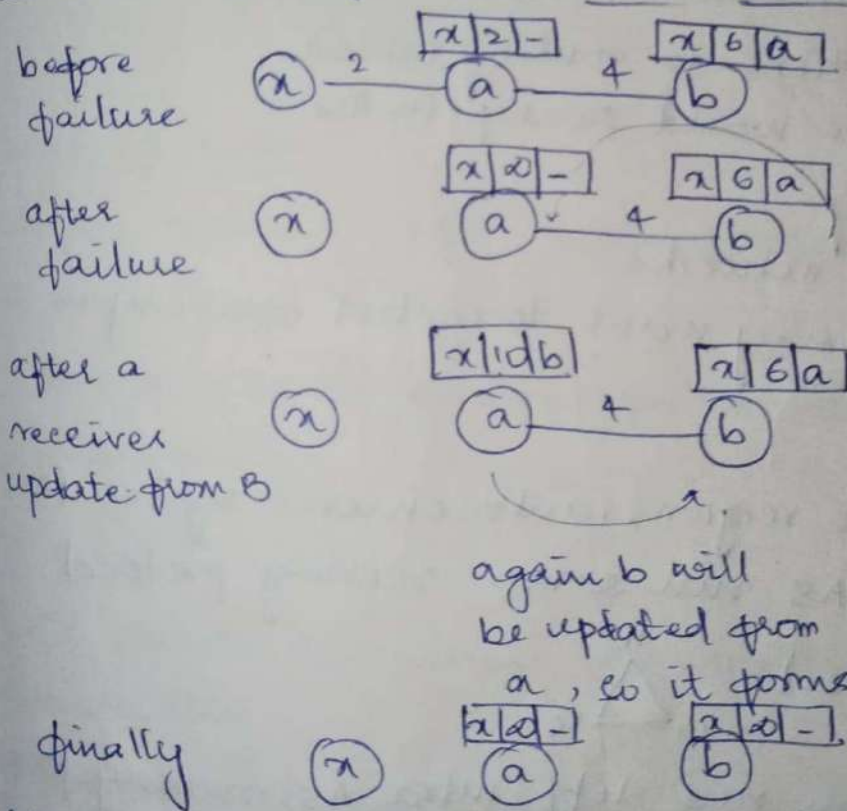
$d_x(y) = \min\{2+0, 7+1\} = 2$

$d_x(z) = \min\{2+1, 7+0\} = 3$

	x	y	z
x	0	2	3
y	2	0	1
z	3	1	0

Drawbacks:

- Count to infinity (or) two node instability: (SA-13) (three → no solutions)



multicast (1) (last bit of IP addr)
one to many
unicast (0)
one to one
broadcast (F)
one to all

Solutions:

- define infinity to be smaller value = 100. At 100, it will stop due to instability. Can't use DVR in large networks
- Split Horizon – partial table sent. If B ~~can't reach~~ thinks is A via X, then it won't advertise the info coming from A as it already came from A

• Split Horizon & Poison reverse → DVR uses timer, if there is no news from a router, the node deletes the route from its table. But still B advertises the value of X but if the source of info is A, it replaces the dist. with infinity - saying hi the info came from you only.

LA-3b ex

★[Hierarchial routing:

So far we assumed

• All routers are identical
• Network is "flat"
• These are not true in practice

Scale: with 200 million destination:

• can't store all destinations in routing tables
• routing table exchange would swamp links

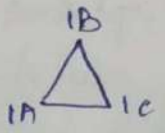
administrative autonomy

• internet - network of networks
• each network admin may want to control routing in its own network.

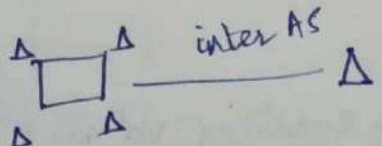
(pic)

• aggregate routers into regions, autonomous system (AS)
• routers in same ~~AS~~ AS run same routing protocol

→ intra-AS routing protocol



→ routers in diff AS can run diff intra AS routing protocol



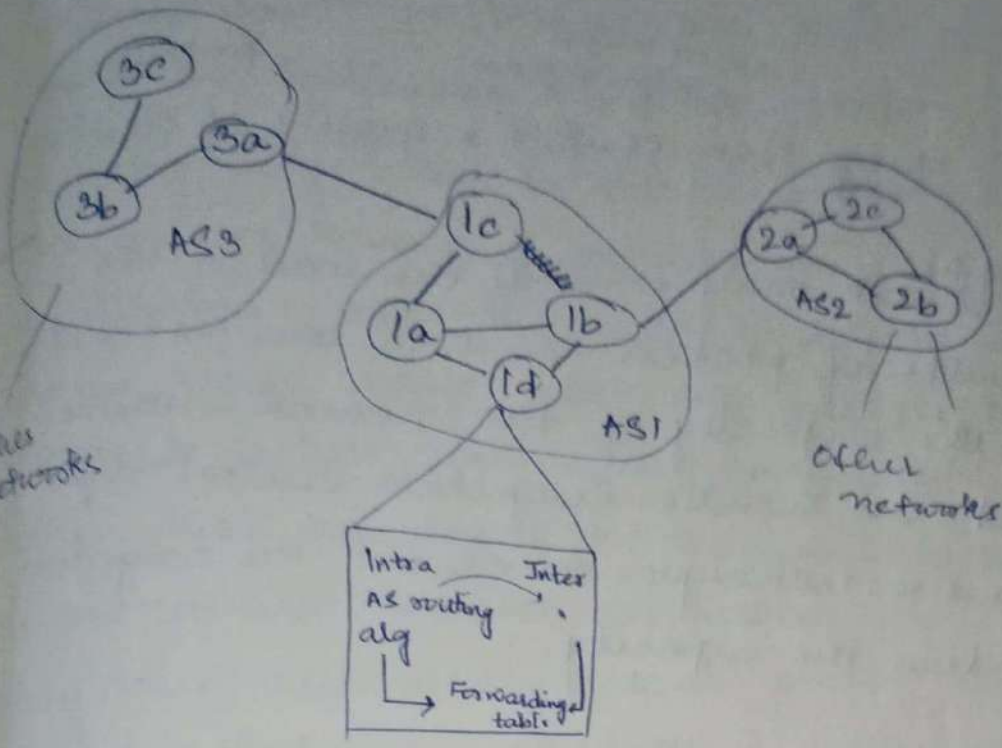
gateway router:

→ at "edge" of its own AS
→ has link to router in another AS

border gateway protocol

exterior interior

* Interconnected ASes:



- forwarding table configured by both intra- and inter-AS routing algorithm.
  → intra-AS sets entries for internal destinations
  → inter-AC & intra-AS sets entries for external destinations.

* Inter AS tasks:

- suppose routes in AS1 receives datagram destined outside of AS1:

  router should forward packet to gateway router but which one?

AS1 must:

learn which destinations are reachable through AS2, which through AS3

- propogate this reachability info to all routers in AS1

* Intra-AS routing:

- Also known as Interior Gateway Protocols (IGP).
- Most common intra-AS routing protocols:
  → RIP (Routing Information Protocol) (open - Internet)
  → OSPF (Open Shortest Path First) (open - Internet)

→ IGRP (Interior Gateway Routing Protocol) (Cisco proprietary)

* Congestion:

we try to avoid ↗ traffic congestion

create appr. env ↗ for traffic

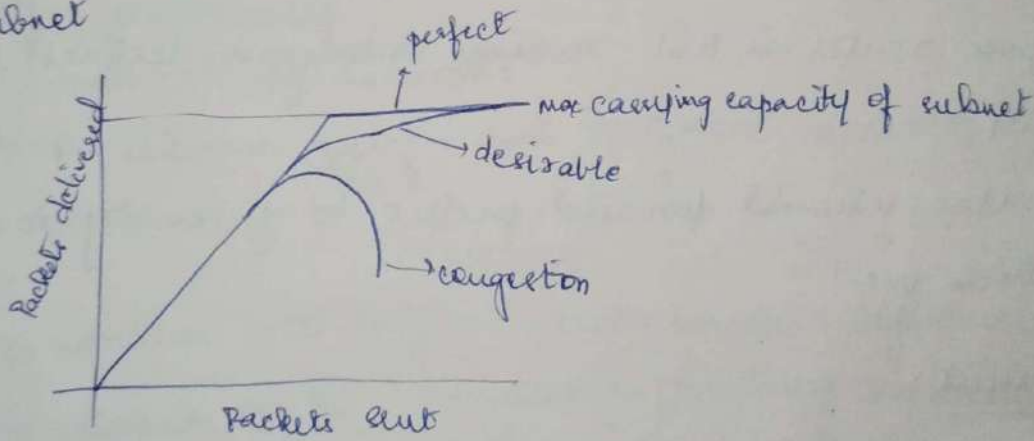
. The main focus of congestion control & quality of service is data traffic.

= traffic descriptor & profiles.

. Congestion in a network may occur if the load on the network - the number of packets sent to the network - is greater than the capacity of the network - the no. of packets a network can handle. Congestion control refers to the mechanisms & techniques to control the congestion & keep the load below the capacity.

* Congestion control algorithms:

Congestion - the situation in which too many packets are present in the subnet



* Causes of congestion:

. Congestion occurs when a router receives data faster than it can send it

- Insufficient bandwidth
- Slow hosts
- Data simultaneously arriving from multiple lines destined for the same outgng line

. The system is not balanced
- correcting the problem at one router will probably just move the bottleneck to another router

- Incoming msgs must be placed in queue O/P
. The queues have a finite size
- Overflowing queues will cause packets to be dropped
- Long queues delays will cause packets to be resent.
- Dropped packets will cause packets to be resend.
. Senders that are trying to transmit to a congested destination also become congested.
- They must continually resent packets that have been dropped or that have timed-out.
- They must continue to hold outgoing/unacknowledged msgs in memory.

*Congestion control(vs) flow control:

. Flow control
- controls point-to-point traffic b/w sender & receiver
eg: a fast host sending to a slow host
. Congestion control
- controls the traffic throughout the network.

*Congestion control:

Congestion control refers to techniques & mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. In general, we can divide congestion control mechanisms into two broad categories:

Open loop congestion control
Closed loop " "

* Congestion Control.

- When one part of the subnet (one or more routers in an area) becomes overloaded, congestion results.
- Because routers are receiving packets faster than they can forward them, one of two things must happen:
  - The subnet must prevent additional packets from entering the congested region until those already present can be processed.
  - The congested routers can discard queued packets to make room for those that are arriving.

Two categories

- Open loop sol^{n}s
  - Attempt to prevent problems rather than correct them
  - Does not utilize runtime feedback from the system.
- Closed loop sol^{n}s
  - Uses feedback (measurements of system performance) to make corrections at runtime.

General principles

- Analogy with control theory < open loop approach / closed " "

- Open loop approach
  - Problem is solved at the design cycle
  - Once the system is running midcourse ~~corr~~ corrections are NOT made
  - Tools for dng open loop control:
- Deciding when to accept new traffic
- " " " disregard packets & which ones

- Making scheduling decision at various points in the network.
- Note that all those decisions are made without regard to the current state of the network.

- closed loop approach

- It is based on the principle of feedback loop. The approach has three parts when applied to congestion control:
  - → Monitor the system to detect when & where congestion occurs
  - → Pass this info to places where action can be taken
  - → Adjust system operation to correct the problem.

Congestion control

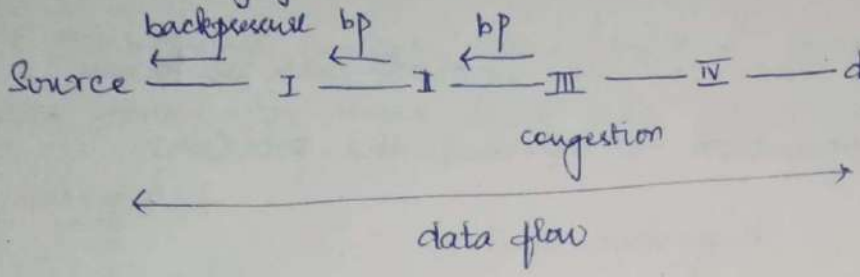
- open loop
  - retransmission policy
  - window " (out of order)
  - ack " (picky banking)
  - discarding " (flow control)
  - admission "
- closed loop
  - back pressure
  - choke packet
  - implicit signaling
  - explicit "

*Choke packets:

- A more direct way of telling the source to slow down.
- A choke packet is a control packet generated at a congested node & transmitted to restrict traffic flow.
- The source, on receiving the choke packet must reduce its transmission rate by a certain percentage
- Ex: ICMP source quench packet

* Warning bit / backpressure:

- A special bit in the packet header is set by the router to warn the source when congestion is detected.
- The bit is copied & piggy-backed on the ack and sent to the sender.
- The sender monitors the no. of ack packets it receives with the warning bit set and adjusts its transmission rate accordingly



* Congestion: prevention: (minimize congestion)

Layer	policies
transport	• retransmission policy • out of order caching " • ack " • flow control " • time out determination (long response time, packets waste)
network	• virtual circuits <> datagrams in subnet • packet queing & service policy (priority based queuing of pckts) • " discard " • routing alg • packet lifetime management (time before discard)
data link	transport layer as

congestion → most alg work with this

which packet to discard

* Admission control:

Once congestion has been detected no more virtual circuits are set up until the problem has gone away.

Alternative:

VCs are set up but they don't pass through the areas which are facing congestion

If congestion is met, vc is redrawn

Datagram

Whenever packet arrives at a router, the router decides of line on which the packet will be forwarded on.

$$u_{new} = a \cdot u_{old} + (1-a) \cdot f$$

If 'u' is not above certain threshold value → no congestion
else congestion (enters warning state)

→ warning bit
→ choke packets
→ hop by hop " "

* Traffic shaping: (unregulated traffic → bursty)

Another method of congestion control is to shape the traffic before it enters the network

Traffic shaping controls the rate at which packets are sent (not just how many)

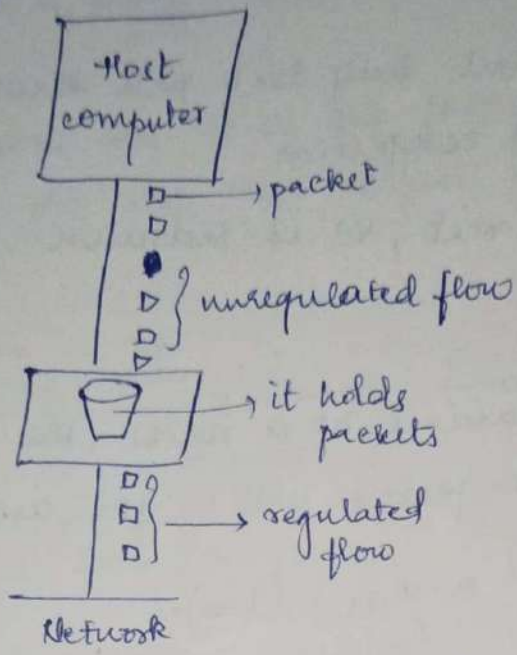
At connection set up time, the sender & carrier negotiate a traffic pattern (shape)

Two traffic shaping algo:

→ leaky bucket
→ Token "

* Leaky bucket alg:

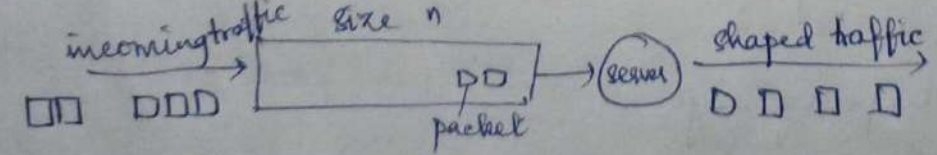
Used to control rate in a network. It is implemented as a single-server queue with constant service time. If the bucket (buffer) overflows then packet is discarded



- leaky bucket enforces a const. o/p rate (avg rate) regardless of the burstiness of the I/p. Does nothing when I/p is idle.
- The host injects one packet per clock tick onto the network. This results in a uniform flow of packets, smoothing out bursts & reducing congestion.
- When packets are the same size (as in ATM cells), the one packet per tick is okay. For variable length packets though, it is better to allow a fixed no. of bytes per tick.

Eg: 1024 bytes per tick will allow one 1024 byte packet
or
two 512 " "
or
four 256 " " on 1 tick

traffic shaper:

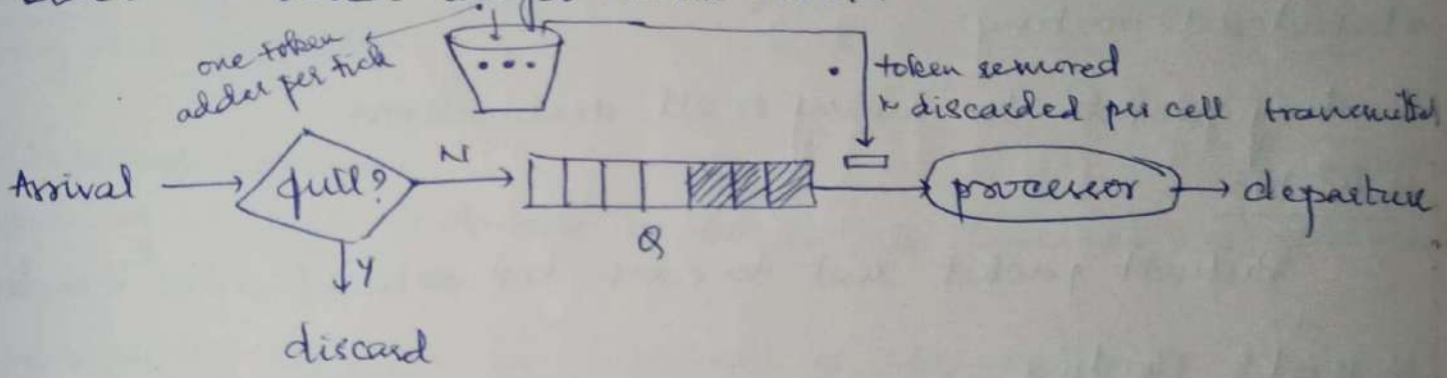


- possible packet loss due to buffer overflow

- Too restrictive, since conforming traffic does not need to be completely smooth.

* Token bucket alg:

- In contrast to LB, TB allows O/P rate to vary, depending on the size of burst
- The bucket holds tokens. To transmit a packet, the host must capture & destroy one token
- Tokens are generated by a clock at the rate of one token every Δt sec
- Idle hosts can capture & save tokens (upto the size of bucket) in order to send larger bursts later.



If sufficient tokens available, packets enter network without delay.

* Leaky vs Token:

- LB discards packets, TB discards tokens
- TB, a packet can be transmitted if there are enough tokens to cover its length in bytes
- LB sends packets at an avg rate, TB allows for large bursts to be sent faster by speeding up the O/P.
- TB allows saving up tokens to send large bursts. LB doesn't.

* Load shedding:

- When buffers become full, routers simply discard packets
- Which packet is chosen to be victim depends on the application & on the error strategy used in the data link layer.
- For a file transfer, for eg: cannot discard older packets since this will cause a gap in the received data
- For real time voice/video it is probably better to throw away old data & keep new packets.
- Get the application to mark packets with discard priority.

* Broadcast routing:

Sending packets to many or all destinations

Method 1:

distinct packet sent to each destination (wastes bandwidth)

Method 2: Flooding

every incoming packet sent on every outgoing line except the one it arrived on (too much bandwidth req.)

Method 3: Multidestination routing

one to many destinations, not all

packets contain list of destinations & all routers can see it

Method 4: Spanning tree

all routers but not all links (no cycles)

Method 5: Reverse Path Forwarding

It uses a preferred line (S to D route) & all other packets

arriving from other routes are discarded.

*Multicast routing

Processes are grouped and communicate with other grps
For very large grps, multicast routing is used
All routers must be aware of which processes are part of which grp

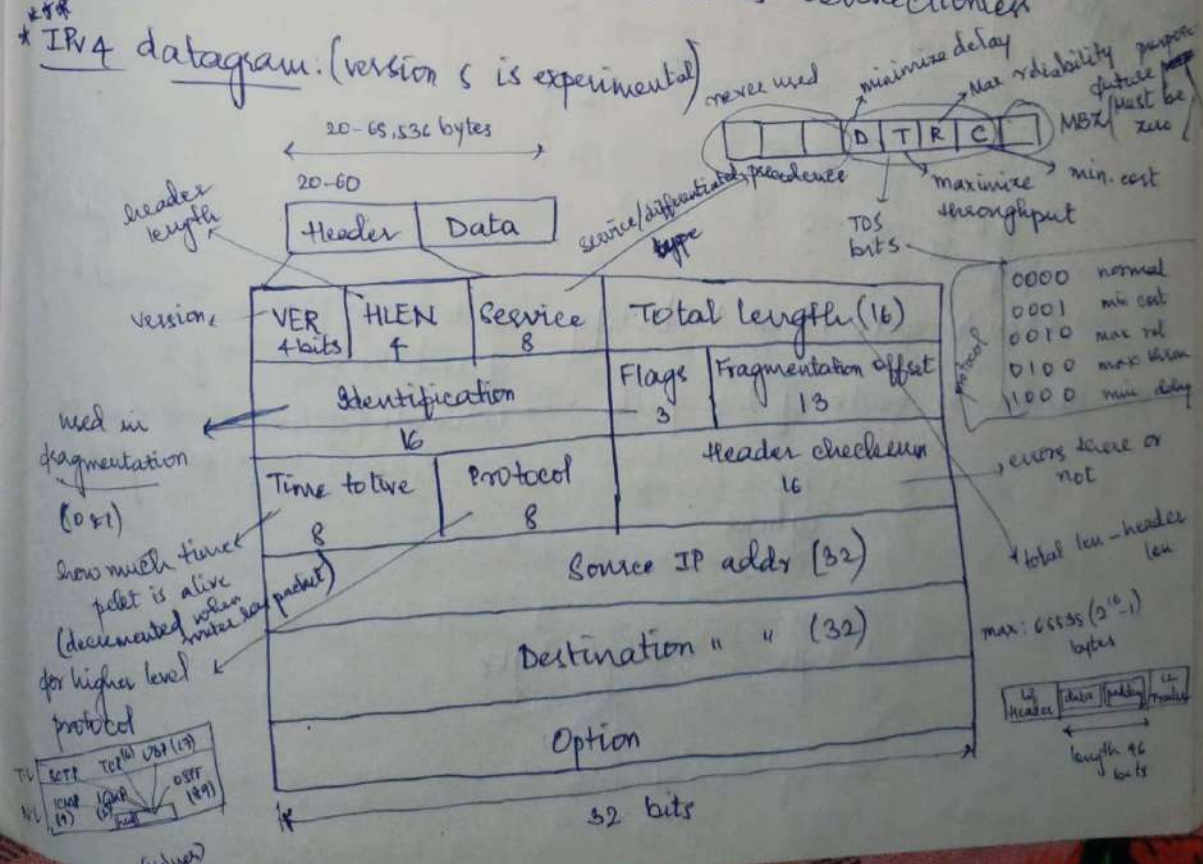
*Internetworking:

Connecting from one source to destination through LANs and WANs by using routing info stored in routers.
Network layer is responsible for host to host delivery & for routing the packets.

*IP: (Internet Protocol)

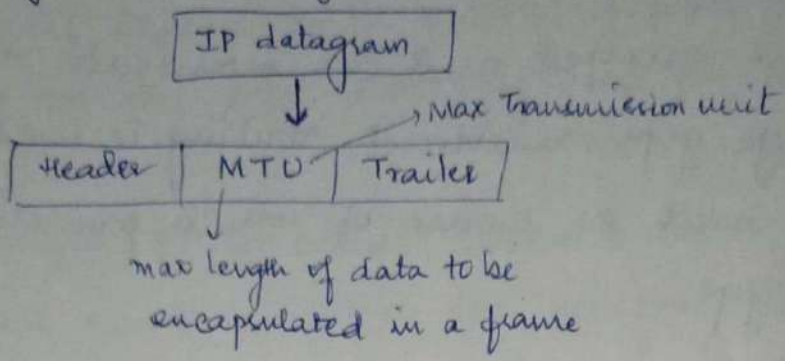
- Switching at the network layer (N.L) in the internet uses datagram approach
- Communication at N.L in internet is connectionless

*** IPv4 datagram: (version 5 is experimental)



Fragmentation (division of packet into smaller packets)

max length of IPv4 datagram 65,535 bytes

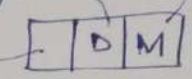


Ethernet ⟶ 1,500

Identification: identifies a datagram originating from source host

Flags: the first bit, second bit, third bit (more fragment bit)

(reserved) (do not fragment bit) (1 / 0 → last or only fragmented packet)

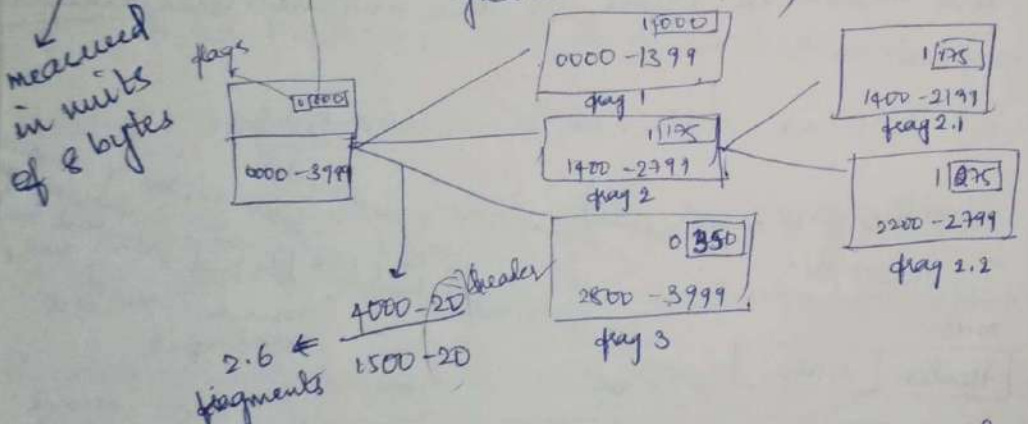


1 → more packets are to

Fragmentation offset: (13 bits cannot represent a sequence of bytes greater than 8191)

measured in units of 8 bytes

1500 → MTU

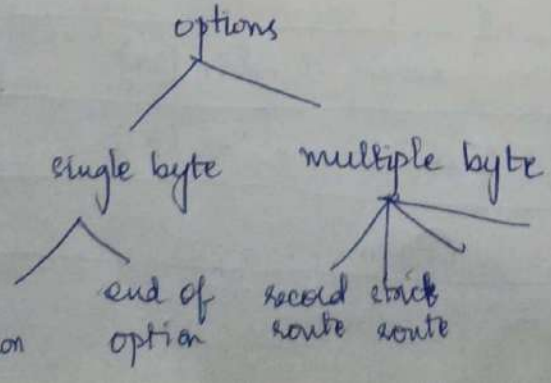


packet)

Options (how to route, how to identify, how to trace places traversed by

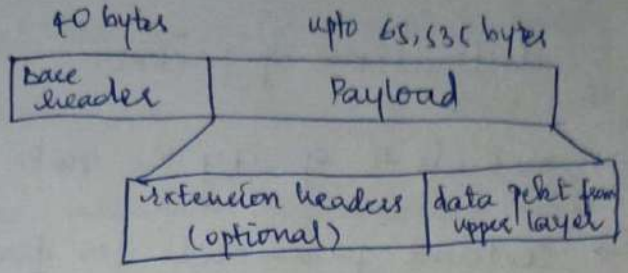
IPv4 header is made of two parts ← fixed (20 byte long)

variable (options that can be max 40 bytes)



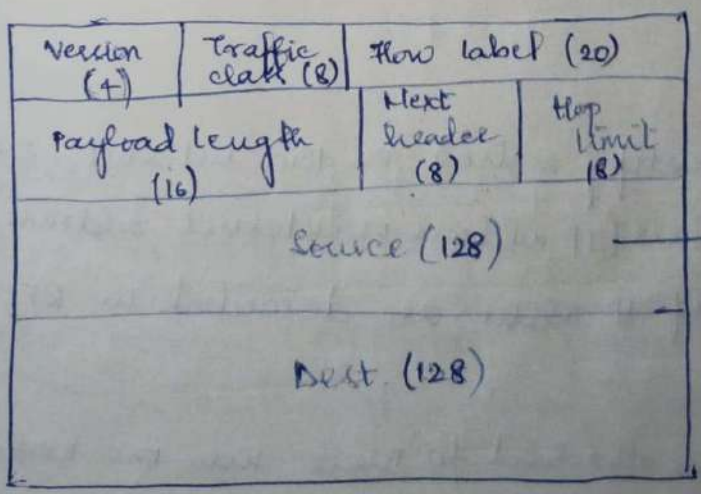
IPv6 datagram:

- It defines three types of addresses ← unicast, anycast (grp of computers with same prefix addr), multicast



- The use of address space is inefficient in IPv4.
- Min delay strategies & reservation of resources are req. to accommodate real-time audio & video transmission.
- No security mechanism (encryption & authentication) is provided.
- IPv6 (IPng: Internetworking protocol, next generation)
  - Larger address space (128 bits) ⟶ 2^{128}
  - Better header format
  - New options
  - Allowance for extension
  - Support for resource allocation: flow label to enable the source to request special handling of the packet.
  - Support for more security.

IPv6 header



Extension headers:

Hop-by-hop options ⟶ options that need to be examined by all devices on the path

Destination " ⟶ " " " " " " "

destination of packet

routing ⟶ methods to specify the route for datagram

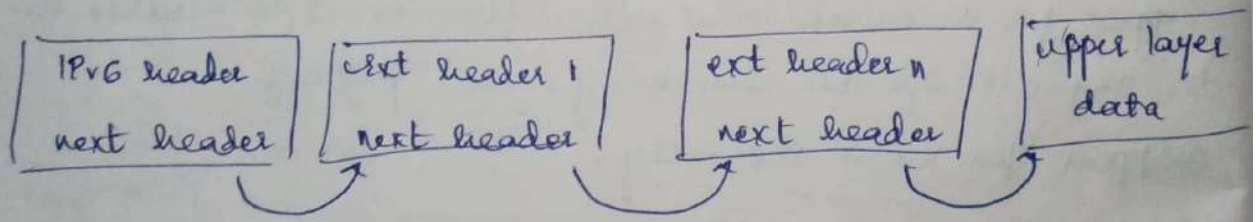
fragment ⟶ contains parameters for fragmentation of datagram.

authentication header ⟶ info used to verify the authenticity of most parts of the pckt

encapsulating security payload ⟶ carries encrypted data for secure communication

destination options ⟶ options that need to be examined only by the destination of pckt

mobility ⟶ parameters need with mobile_IPv6

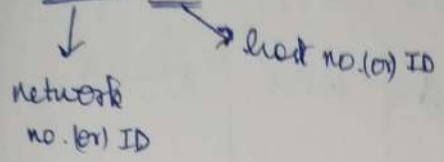


* IP addresses:

- To be able to identify a host on the internet, each host is assigned an address (IP address or Internet address)
- The standards of IP addr are described in RFC 1166 - Internet no.s → R_ for Count
- When the host is attached to more than one network it is multi homed & it has one IP addr for each network interface

- An IP addr is a 32 bit binary no.
- IP addresses are used by the IP protocol to uniquely identify a host on the internet.
- IP datagrams (the basic data pckts exchanged b/w hosts) are transmitted by some physical network attached to the host; each IP datagram contains a source IP addr & a dest. IP addr.
- IP adds are usually represented in a dotted decimal form (as the decimal representation of four 8 bit values concatenated with dots).

Ex: 128.2.7.9



binary format of 128.2.7.9 = 10000000 00000010 00000111 00001001

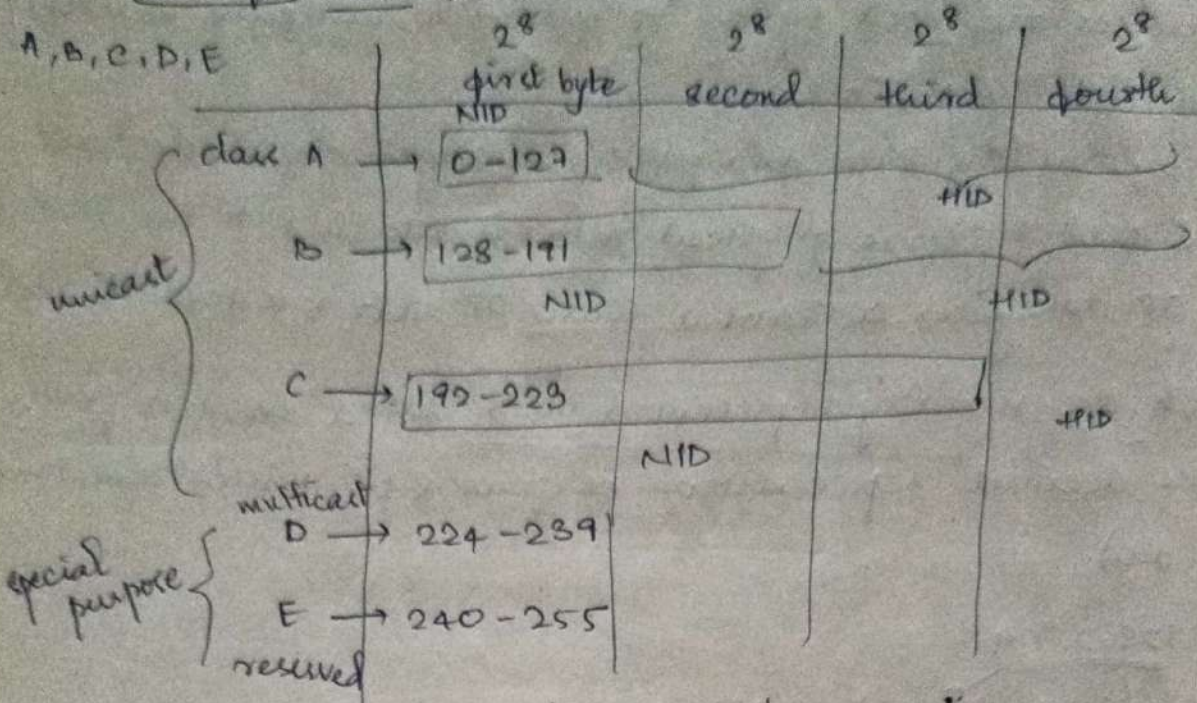
- IP address is made of 4 grps of decimal no.s b/w 0-255 separated by dots
- Some no.s are special (0.0.0.0 or 255.255.255.255) & are used to designate the default gateway, a broadcast or multicast addr or some reserved no.s for developers to play with.

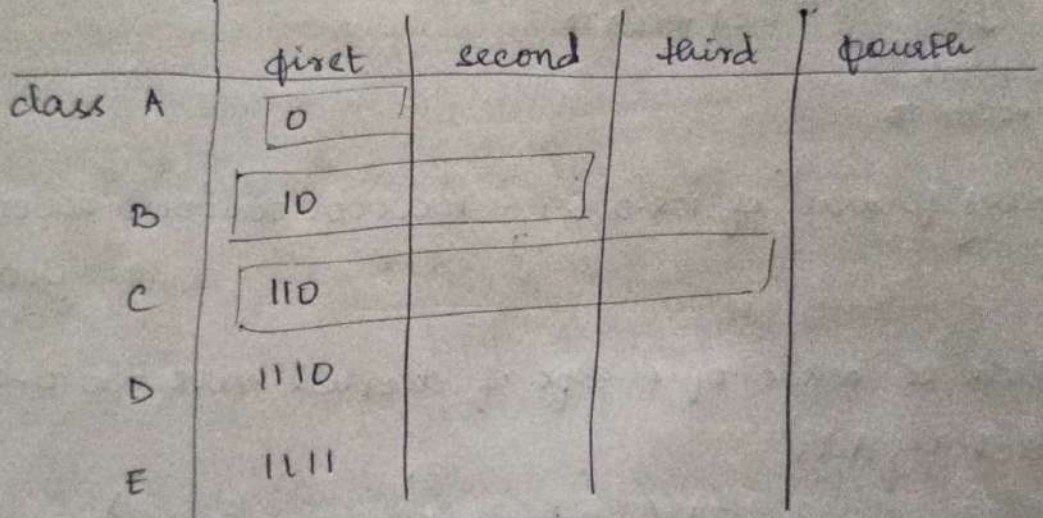
* IPv4 addresses:

32 bit long
unique & universal
address space = 2^{32} or 4,294,967,296

10000000 00001011 00000011 00011111 — dotted decimal notation
128.11.3.31 — binary notation

* In classful (CIDR) addr, the addr is divided into 5 classes





Ex: 14.23.120.8 ⟶ class A

00000001 00001011 ___ ___ ⟶ class A

252.5.15.111 ⟶ class E

11000001 10000011 ___ ___ ⟶ class C

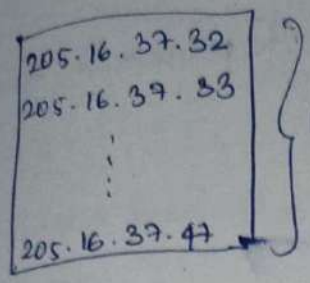
* Inefficient NID or HID (by company) leads to wastage of addr. So we have classless addr. (Interdomain routing):

* In IPv4 addr, a block of addr can be defined as

x.y.z.t/n mask

addr

* The first addr in block can be found by setting the rightmost 32−n bits to 0's



No can.

205.16.37.39/28

32−28 rightmost bits to 0's

205.16.37.32/28 first addr.

supernetting (combining multiple N/w into single N/w)
(converting NID to HID)

* last addr in block can be found by setting the rightmost 32−n bits to 1's.

205.16.37.39/28

32−28 rightmost bits to 1's

205.16.37.47/28 last addr

~~subnetting~~

* The no.s of addr in a block = 2^{32-n}

another method

First addr can be found by ANDing given addr with mask (bit by bit)

/28 → 3(11111111) . 11110000

32−28 = 4

subnetting

↓

single network used to ~~find~~ divide multiple ~~addr.~~ N/w

subnet mask for class A → 255.0.0.0

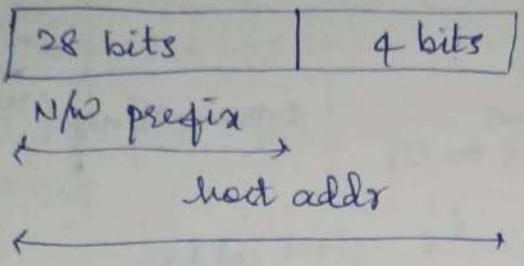
B → 255.255.0.0

C → 255.255.255.0

* Last addr can be found by ORing the given addr with complement of mask.

* first addr ⟶ given as N/w addr that represents the organisation

* Hierarchy in ~~telep~~ IP addr:

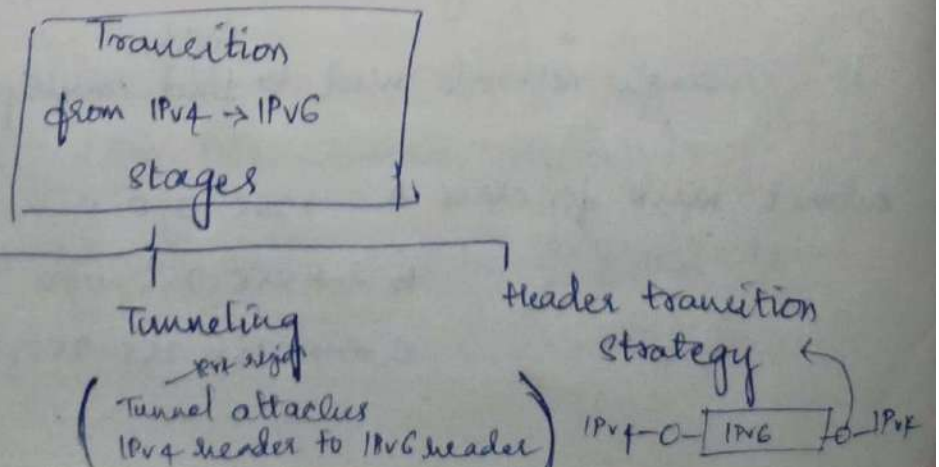


* NAT (Network Address Translation):

Converting private addr ⟶ NAT ⟶ local addr Internet

Converts LAN side addr to WAN side addr & vice versa when datagram travels from S to D.

* Internetworking: (direct link b/w S to D) (Network layer)
Connecting two or more networks together to make internetwork or internet.



* Network layer protocols:

- ICMP
- IGMP (Internet Group Message Management Protocol)
  → manages membership of host (multicast)
- IP
- DHCP
- SMTP
- ARP (Address Resolution Protocol)
- RARP (Reverse " " ")

Bootstrap protocol
* BOOTP: automatically assigns IP addr

Logical addr (N/W layer) (IP)
↓
ARP
↓
Phys. Addr (data link) (MAC)

↑
RARP
↑

* MAC & IP are necessary for mapping

Static (table having IP & MAC)
if machine knows IP, it can look for MAC in this table
Limitations: keep changing
So updates must be done periodically

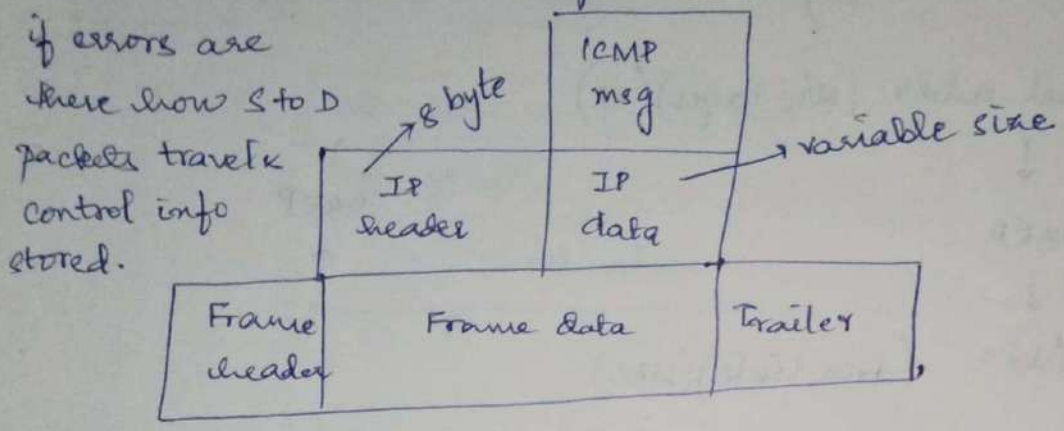
dynamic use (ARP, RARP)
ARP request → broadcast
" reply → unicast
proxy ARP sends all ARP requests to routers
(same with RARP)

ARP packet: (same with RARP)
Hardware type (1 for ethernet)
protocol " (S/W)
hardware length (len in bytes of hardware addr)
protocol " (" " " protocol ")
operation request 1, reply 2 (3, 4 RARP)

source { Sender hardware addr (ethernet)
" protocol " (IP)

dest. { target hardware " (ethernet)
" protocol " (IP)

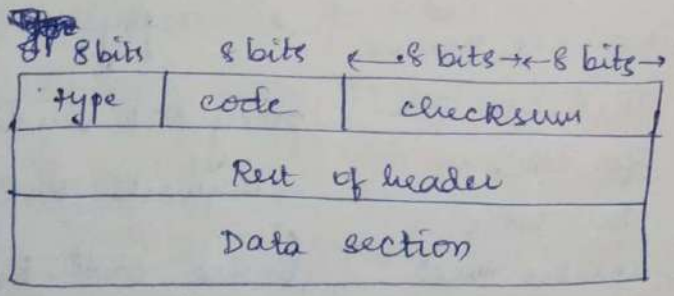
* ICMP (Internet Control Msg protocol):

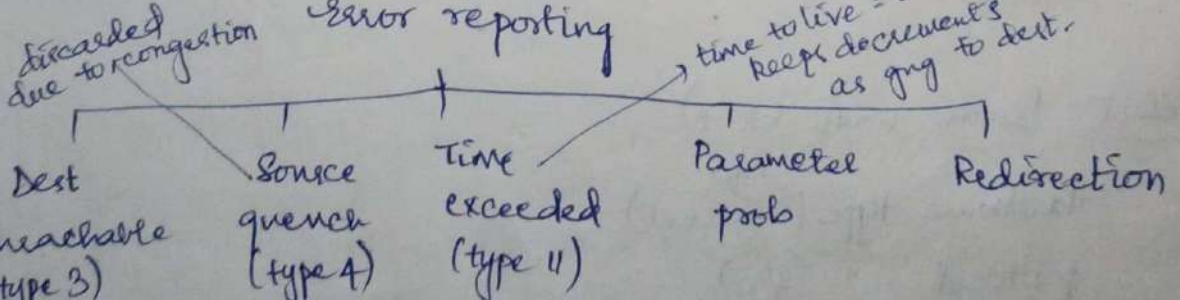


Types of msgs:

. Error reporting → it reports errors (router or host may encounter)

. query (get specific info from router or host) → ICMP diagnoses N/w problems by 4 diff pairs of msg.





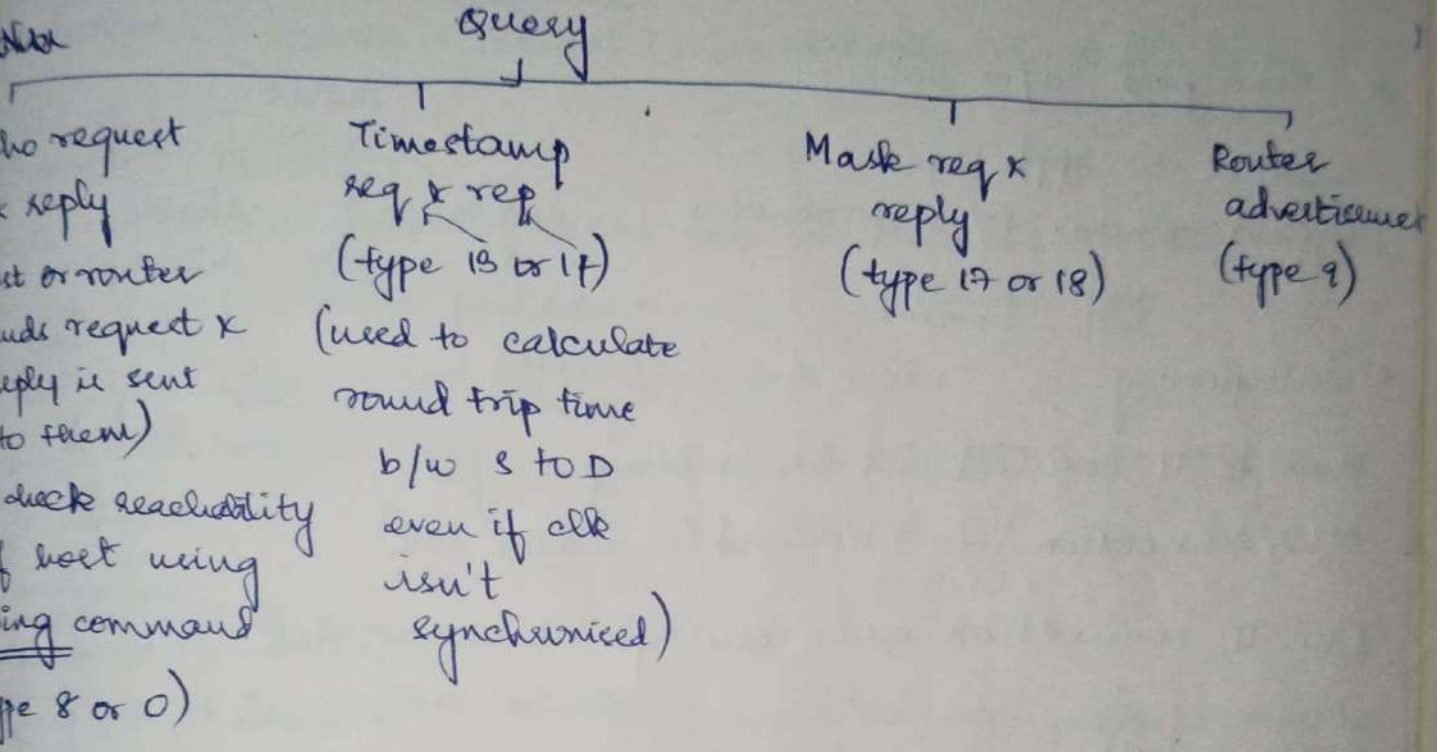
- No ICMP error msg will be generated in response to a datagram carrying an ICMP error msg.

" " for a fragmented datagram that is not the first fragment.

" for a datagram having a multicast addr.

" for a datagram having a special addr such as 127.0.0.0 or 0.0.0.0

* A router cannot detect errors in packet.



* Debugging tools: (Linux)

ping

traceroute

* DHCP (Dynamic Host Configuration Protocol):

Client & server may be on same or diff N/Ws:

same → port nos need

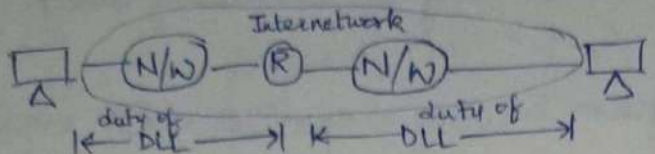
diff N/Ws → connect through relay agent & internet

DHCP server dynamically assigns IP addr & other config para. to each device on network for comm.

4. Transport Layer

(node to node) DL → MAC or physical
(NL → logical → IP
(host to host) TL → port no.s (well known) → HTTP → 80

* Process to process comm. / peer to peer comm.



duty of DLL → | ← | ← duty of DLL →
duty of Transport layer →
→ control over all N/Ws

* Transport layer services duties:

- services to appl. layer
- logical comm. b/w processes

duties → multiplexing
duties → flow (sliding control window)
duties → reliable delivery → duplicate control
loss control → lost packet
seq. control → no.s are given
error control
addr. → end to end delivery (access point)

segment payload

* Multiplexing

Multiple TL connections are using single N/W connection → upward (to reduce cost)

One TL connection uses multiple NL connection → downward (increases throughput)

* Transport service primitives: (Berkeley's (or))

primitives that appl. might call to transport data for simple connection oriented service

- Client calls connect, send, receive, disconnect
- Server calls listen, receive, send, disconnect

listen	(none)	block until some process tries to connect
connect	conn. req	actively attempt to establish a conn.
send	data	send info
receive	(none)	block until a data packet arrives
disconnect	discon. req	this side wants to release conn.

*Port no.: → appl. batti communication pt utaru

registered

. Port no. for a client host prog. defines itself randomly by the transport layer at this is called ephemeral or dynamic or private port no. ranging from 49,152 to 65,535.

. Port no. for servers are universally assigned by (internet assigned no. authority) called well known port no. ranging from 0 to 1023

ICANN → Internet Cooperation for Assigned Names & Nos.

*Socket addr: (48 bit)

. Process to process delivery needs two identifiers, IP addr & port no, at each end to make a connec.

IP addr + port no. → socket addr

client socket addr → defines client process uniquely

Server " " → " Server " "

*Connection Establishment:

Key problem is to ensure reliability even though packets may be lost, corrupted, delayed & duplicated

. Don't treat an old or duplicate pckt as new

. (Use ARQ & checksum for loss/corruption)

Approach:

. Don't reuse sequence no.s within twice the MSL (Max. Segment Lifetime) of 2T = 240 secs

. Three-way handshake for establishing connection

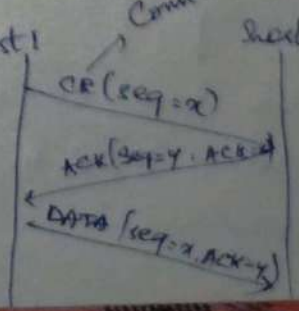
Use sequence no. approach

(or)

Three way handshake need for initial packet

. Since no state from previous connection

. Both hosts contribute fresh seq. no.s



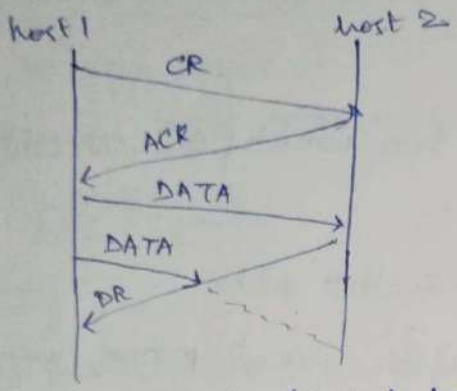
It protects against odd cases:
- Duplicate CR. Spurious ACK does not connect (old conn. can't be used again)
- Duplicate CR & DATA - Same plus DATA will be rejected

* Connection release:

DR → Disconnect request

Key problem is to ensure reliability while releasing

Asymmetric release (when one side breaks connection) is abrupt & may lose data



Normal release seq. initiated by transport user on host 1
- Both DRs are ACKed by the other side.

errors
- final ACK lost, host 2 times out & releases conn.
- lost DR causes retransmissions
- extreme: many lost DRs cause both hosts to timeout.

* Crash recovery:
- hosts & routers are subject to crash.
- router crash is easier to handle since transport entities are alive at the host, routers are only intermediate nodes which forward packet. they do not have transport layer entity.
- One host is sending a file to server. TL at server simply passes TPDU (Transfer protocol Data unit) to TL. While transmission was on going, server crashes.

. Server crashes & comes up → table initiated, ??
. Server sends a broadcast TPDU to all host, announcing that it has just crashed & requesting that its clients inform it about status of all open connection.
. Each client can be in one of two states:
  S_0 → no outstanding TPDU
  S_1 → 1 TPDU outstanding
. Now it seems that if TPDU is outstanding, client should transmit it, but there can be many situations
→ If server has first sent ACK & before it can send TPDU to next layer, server crashes. Now, client will get ACK so it will not retransmit & TPDU is lost by server
→ If server first sends packet to next layer, then it crashes before it can send ACK - In this case though server has already received TPDU, client thinks TPDU is lost & it will retransmit.
. Server can be programmed in 2 ways:
1. ACK first
2. write "
. Three events are possible at server, sending ACK (A), sending pkt to next layer (w), crashing (c)
. Three events can occur in six ways:
AC(W) → Ack sent, crash, write isn't done
AWC
C(AW)
C(WA)
WAC
WCA
. Client can be programmed in 4 ways
→ always transmit last TPDU
→ never " " "

→ transmit only in S_0
→ " " " S_1

Server strategy

Host strategy	← first ACK, then write → Ac(w)	AWC	C(AW)	← first write, then ACK → C(WA)	WAC	ack(A)
always retransmit	OK	DUP	OK	OK	DUP	DUP
never "	LOST	OK	LOST	LOST	OK	OK
retransmit in S_0	OK	DUP	"	"	DUP	"
" " S_1	LOST	OK	OK	OK	OK	DUP

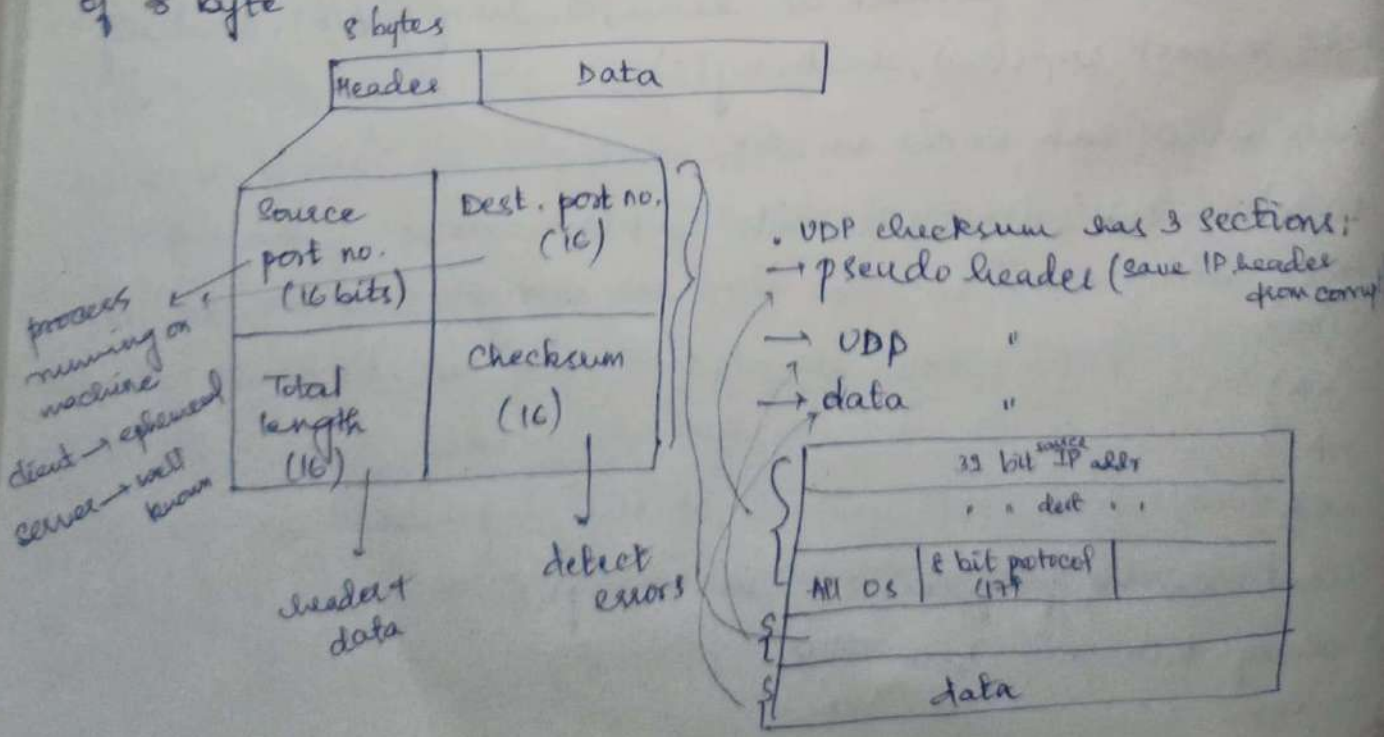
protocol functions correctly

protocol generates duplicate msg

protocol loses a msg

* UDP: (User Datagram Protocol)

- It is a connectionless, unreliable transport protocol
- It is so powerless, it perform process to process comm. with very limited error checking.
- If a process wants to send a small msg & does not care much about reliability, it can use UDP.
- UDP packets called user datagrams, have a fixed size header of 8 byte



. UDP is used where little concern is given for flow & error control
. UDP is suitable for multicasting
. UDP is used for SNMP → management process
. " . " RIP → route updating protocol

drawbacks:
. provides basic functionality
. " no sequencing & reordering
. damaged / lost packets are difficult to recover / find out.

* TCP: (Transmission Control Protocol)
. reliable, connection oriented process to process protocol
. TCP also uses port no. unlike UDP
. It creates virtual conn. b/w two TCP's to send data
. uses flow & error control mechanism at TL.

20 → FTP, Data
21 → " , control
23 → TELNET (Terminal N/W)
25 → SMTP
53 → DNS
67 → BOOTP
80 → HTTP
111 → RPC

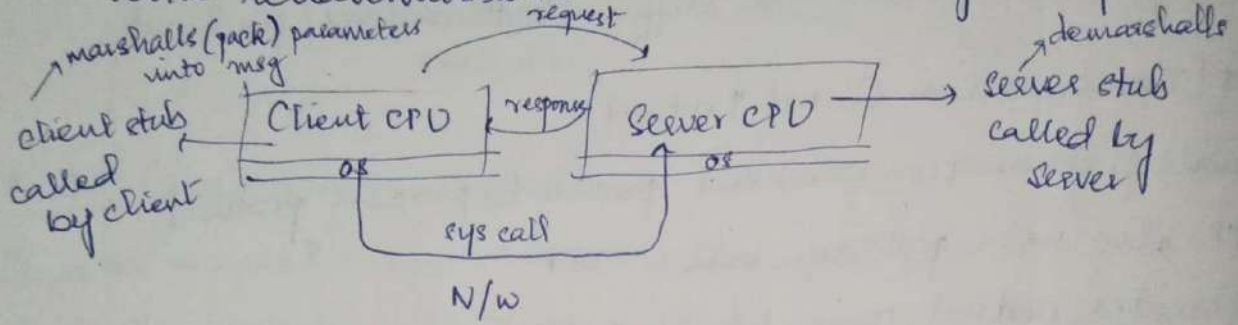
* Stream delivery service:
. TCP allows sending process to send data as a stream of bytes & receiving process receives it.
. But they can't be of same speed (processes)
. & TCP needs buffer for storage, a circular array of 1-byte location to implement a buffer.

- The IP layer in b/w TCP needs to send data in pckts not as a stream of bytes.
- So at TL, TCP groups a no. of bytes together into segments.

UDP Protocols:

* Remote Procedure Call: (RPC)

- RPC connects applications over the N/w with the familiar abstraction of procedure calls
- Stubs package parameters/results into a msg
- UDP with retransmissions is a low-latency transport



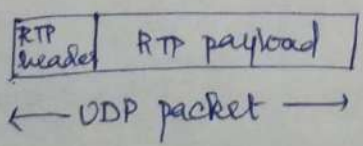
drawbacks:

flexibility

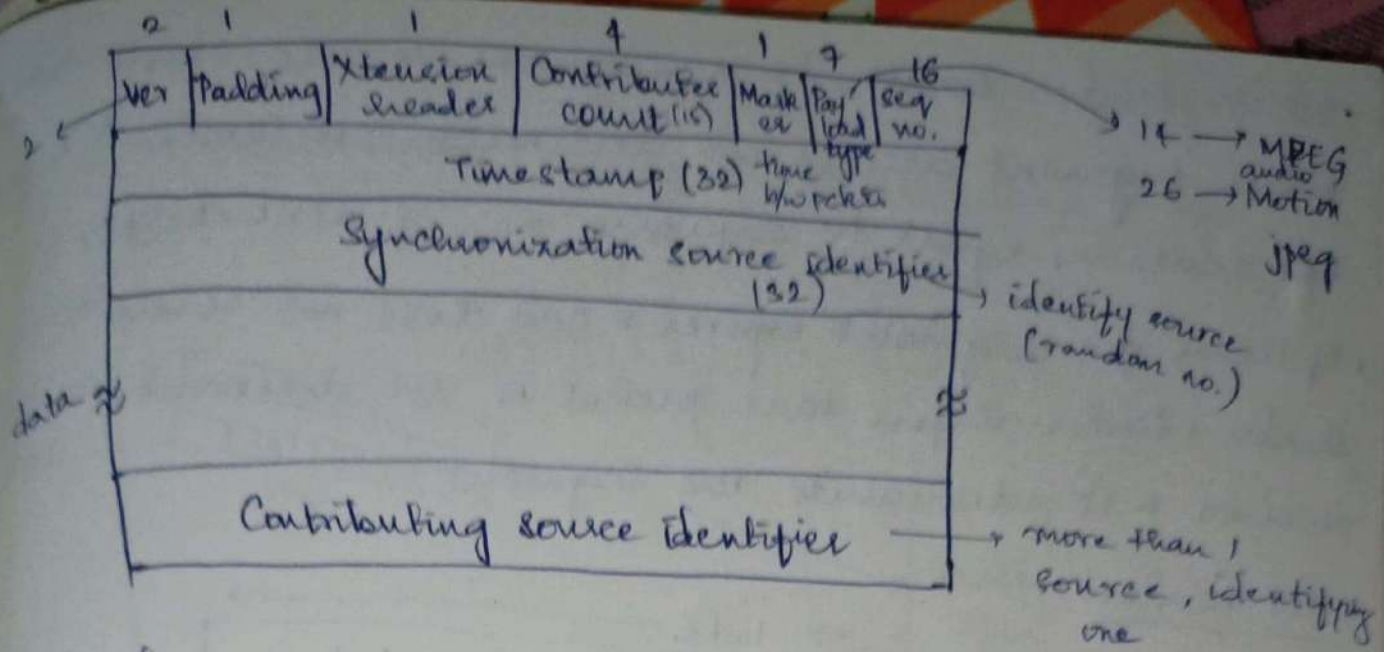
* RTP (Real time transport protocol):

- RTP provides support for sending real time media over UDP
- Often implemented as part of the application

Applications: multimedia application, media mixing, seq., timestamps, voice over internet protocol



- RTP header (32 bit) contains fields to describe the type of media & synchronize it across multiple streams
- RTCP writer protocol helps with management tasks



TCP Protocols

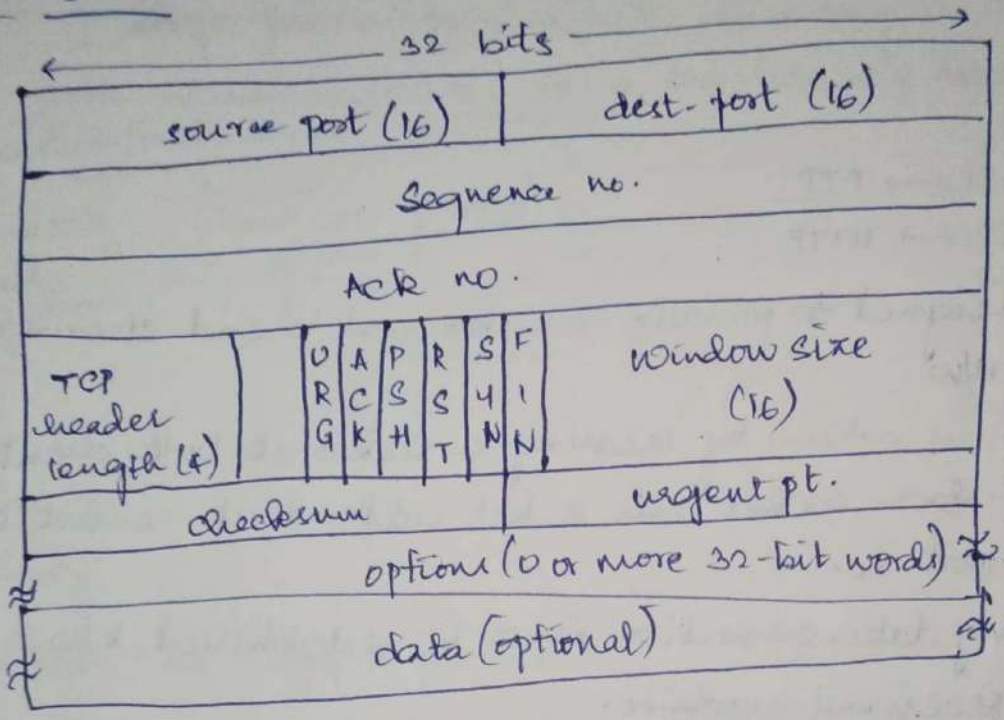
20, 21 ⟶ FTP

80 ⟶ HTTP

- TCP was designed to provide reliable end to end stream over unreliable N/W
- TCP service is obtain by creating a socket at both client & server side. Each socket has socket addr. that consist of IP addr. & port no.
- Before sending data, connection must be established b/w sending & receiving machine.
- One socket can be used to establish many connection, many sender can connect with same receiver socket. TCP connections are identified by pair of sockets at both the end.
- TCP connections are full duplex & point to point. TCP does not support multicast & broadcast.
- TCP connection is byte stream, not a message stream.
- Sending & receiving TCP entities exchange data in form of segment.
- TCP segment consist of 20 byte header plus optional part followed by data.

- When sender transmits a segment, it also starts timer. When segment arrives at destination, it sends ACK. ACK contains equal to sequence no. of next data.
- If timer for segment expires & ack does not reach to sender, sender infers that packet is not delivered to receiver & it retransmits the segment.

* TCP header:

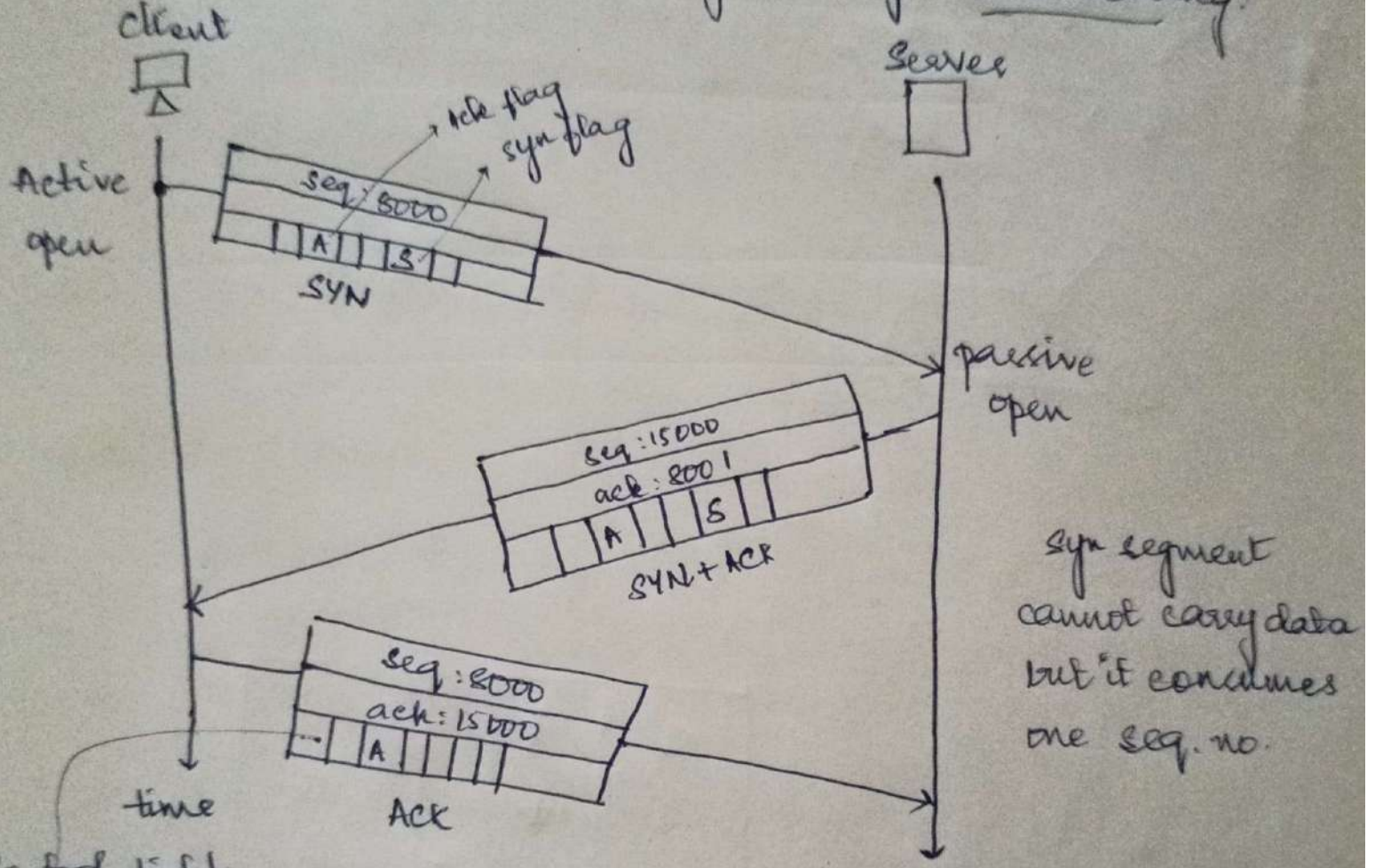


* TCP Connection:

TCP is connection oriented. All of the segments belonging to a msg are then sent over this logical path. Using a single logical pathway for the entire message facilitates the ACK process as well as retransmission of damaged or lost frames. You may wonder how TCP, which uses services of IP, a connectionless protocol, can be connection-oriented. The pt is that a TCP connection is logical, not physical, TCP operates at a higher level. TCP uses the services of IP to deliver individual segments

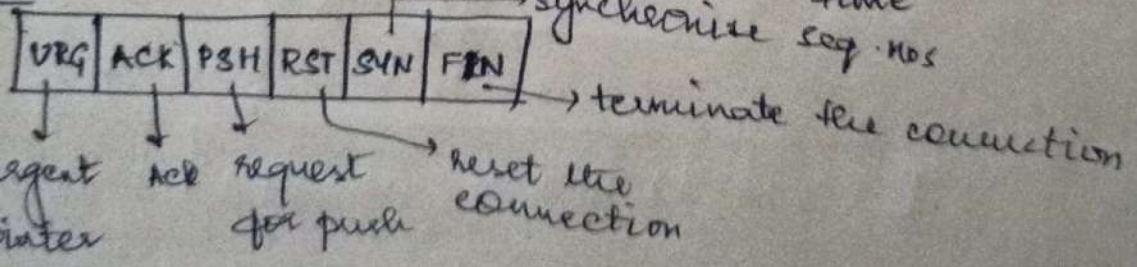
to the receiver, but it controls the connection itself.

* Connection establishment using 3-way handshaking:



syn segment cannot carry data but it consumes one seq. no.

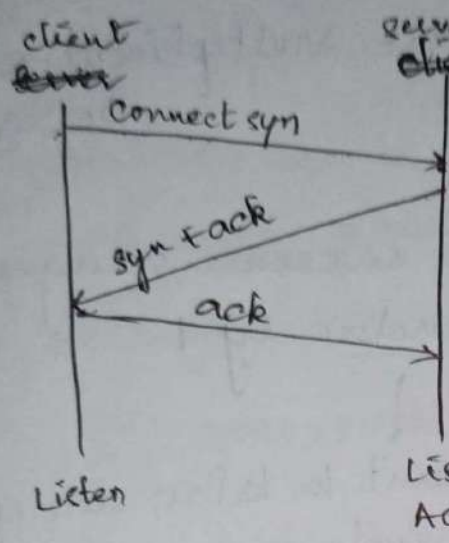
* Control field:



CN

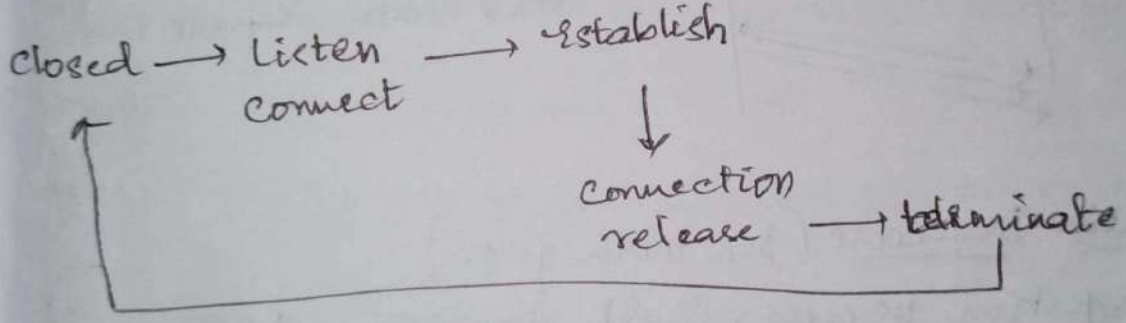
TCP connection management: (3 way handshake)

→ TCP connection establishment + TCP connection release



Sending 'FIN' + ack bit by client or server saying i don't have anymore data

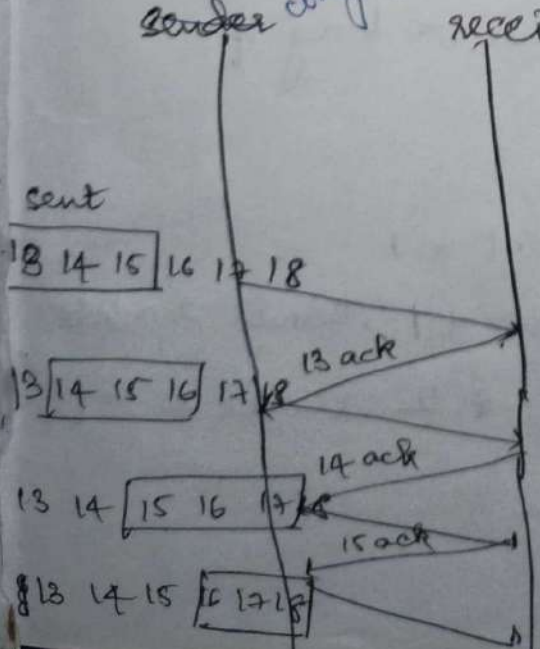
timers

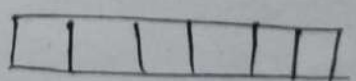


TCP sliding window:

sender congestion → flow control

receiver → decides window acceptance





Suppose receiver can accept 6 segs.

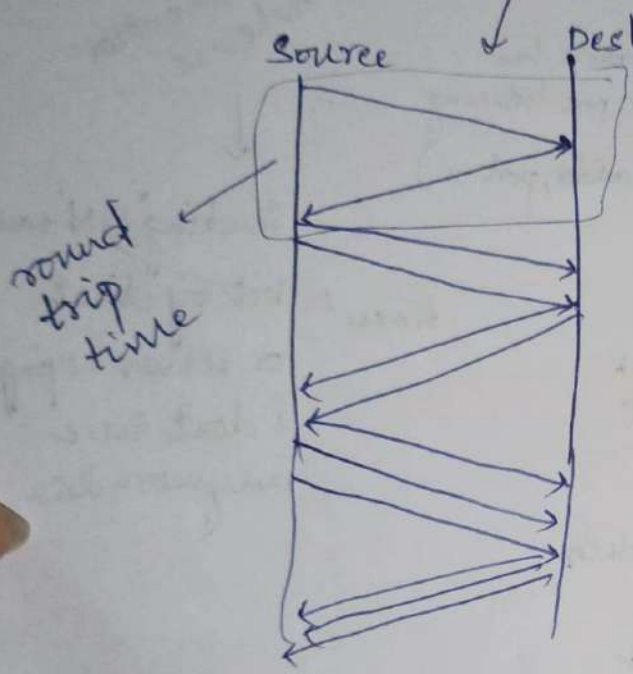
window size = min(receiver, congestion)

if ack lost, in-order window will leave a spot empty

* Congestion Control:

If overload of segments occurs, receiver experien
congestion.

We use AIMD (Additive Increase Multiplicative
Decrease)



We increase congestion window by 1

↓

can't be below size of single packet i.e MSS (Max. Segment Size)

Multiplicative Decrease (Saw tooth graph)

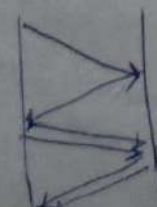
If congestion occurs, half the segments.

Ex: 4 are sent, congestion, 2 are sent

We use Slow Start as AIMD takes too long if capacity of receiver is more.

↓

① We'll use congestion window set to 1
② after ack, congestion window +1, sends 2 packets
③ after 2 acks, " " +2, sends 4 " (2^3



5. Application layer

- **Services provided:**
  - provides services to the user, takes services from transport layer.
  - The protocols can be removed from this layer easily as it doesn't provide services to transport layer
  - The protocols need to be standardized & documented

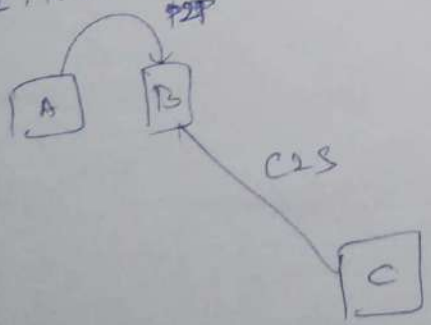
    eg: DHCP, SMTP, HTTP, FTP etc

* **Application architecture:**

We use 2 predominent architectural paradigms

- client-server (requests) eg: web, FTP etc.
- peer to peer (direct communication b/w pairs of hosts (intercommunicating) peers

eg: Skype, BitTorrent P2P



connected, stateful FTP server

Control connection b/w client & Server. & sometimes data connection if data is there

opens & closes for every file transfer

end of token → Controlled Line feed

Control transfer port no. → 21
Data " " " → 20

* Security for FTP:
The FTP protocol was designed when security was not a big issue. Although FTP requires a passwd, the passwd is sent in plaintext (unencrypted), which means it can be intercepted & used by an attacker. The data transfer connection also transfers data in plaintext which is insecure. To be secure, one can add a security socket layer b/w the FTP application layer and TCP layer. In this case FTP is called SSL-FTP.

* TELNET
Same as putty but no need of server