Computer Network

Date - 05/08/19

* 5 Credit cource (3 Theory, 2 Lab)
* Beij's Guide of Socket Programming (Online PDF)
* Larry Peterson → Bruce Davie
* A. S. Tannabuam

Scanned by CamScanner

* What is Computer Network ?

Ans → It is an interconnection of autonomous devices.

interconnection → able to exchange data in a meaningful manner.

meaningful → Understandable to indented user.

Understandable → for this protocol is used.

protocol → set of rules
protocol → is the basis of information exchange.

autonomous → Do not control each-other

devices → any computing devices (e.g printer, computer, mobile etc)

* Network Facilitates →
  (1) Data Sharing
  (2) Hardware sharing
  (3) Resource Sharing (Software or Hardware resources)

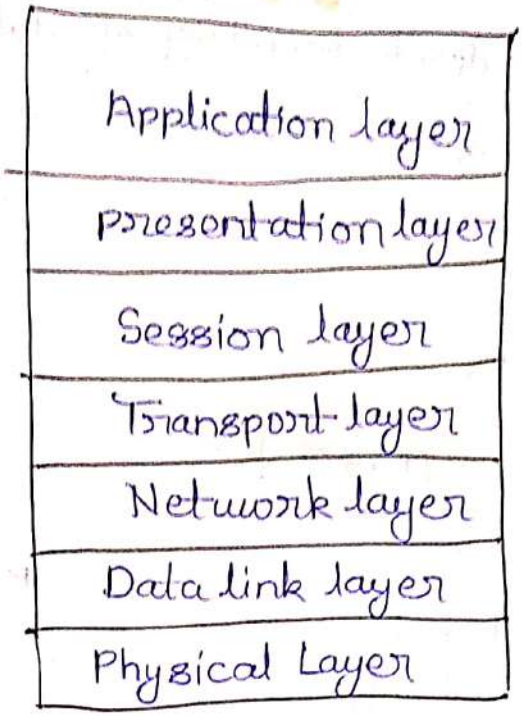
* Network reduces the cost of deployment also.

* How to visualize a network ?

for this, OSI (Open System Interconnection) model is used which contains seven layers namely Application, presentation, session, transport, Network, Datalink, physical. given by ISO in 1984.

Scanned by CamScanner

OSI model



✡ Responsibilites / Services of physical layer ? (802X mod

(1) To convert bits into signals. (Digital Encoder/Analog Modulator)

(2) Define the medium of communication.

telephone ⟶ twisted pair

Computer ⟶ Cat-6 cable

WLAN ⟶ 2.4 GHz / 5 GHz band

(3) Interface for connection.

* To fulfill these responsibilities, protocols is used.

Cat-6 → 100 Gbps

Cat-5 ⟶ 500 Mbps

802.3 Lan ⟶ Manchaster encoding is used.

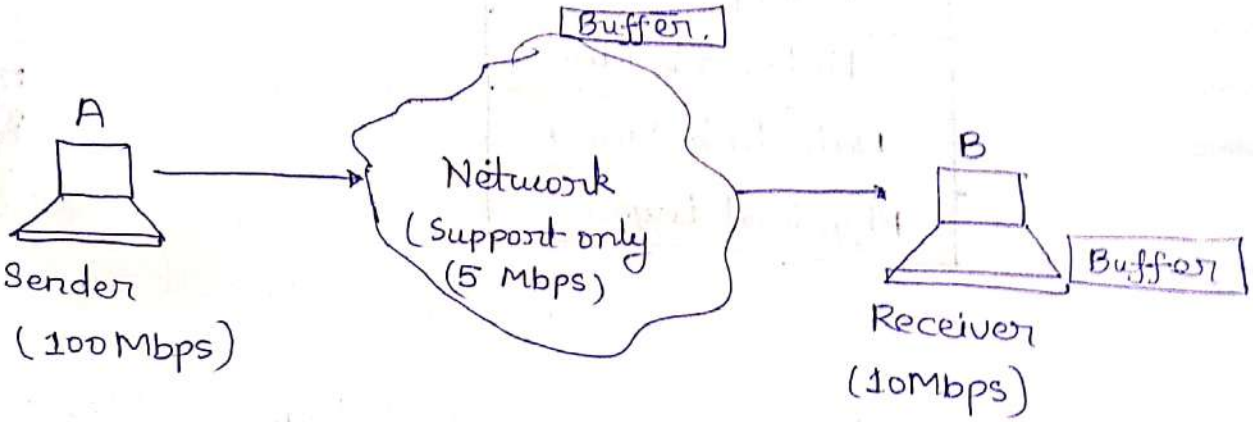
Scanned by CamScanner

✡ Services / Responsibilities of Data Link Layer (DLL)

(1) Framing → To decide boundary of data packets.

(2) Flow control

(3) Error control



* Network has only 5 Mbps data speed, so it will accumulate 95 Mbps data in its buffer and after some point of time, the network buffer become full and no futher packets will be accepted.

* And same thing also happens at receiver end as it also has the capacity of only 10Mbps.

* That's why, flow control protocols are necessary to limit the data rate.

$$\min [\text{Max (Network), Receiver}]$$

$$= \min (5\text{Mbps}, 10\text{Mbps})$$

$$= 5\text{ Mbps}$$

Scanned by CamScanner

* Error control

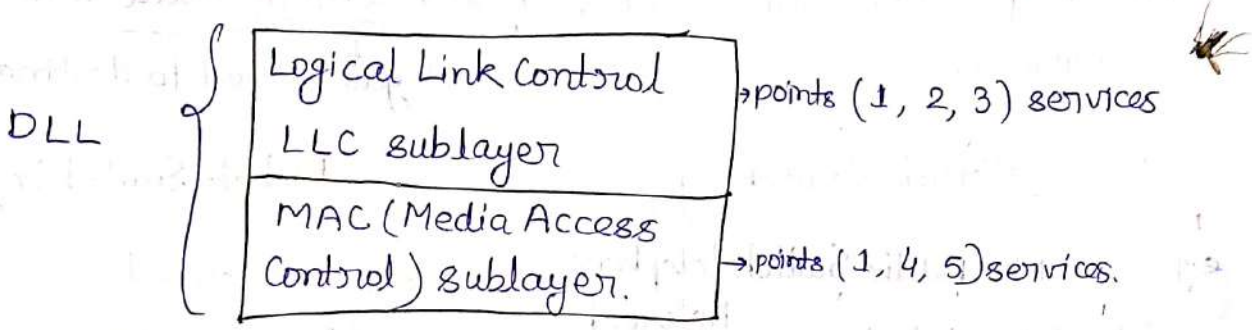
↓

Error detection and congestion protocols are used at Data Link Layer.

(4) Addressing (48 bits Ethernet address

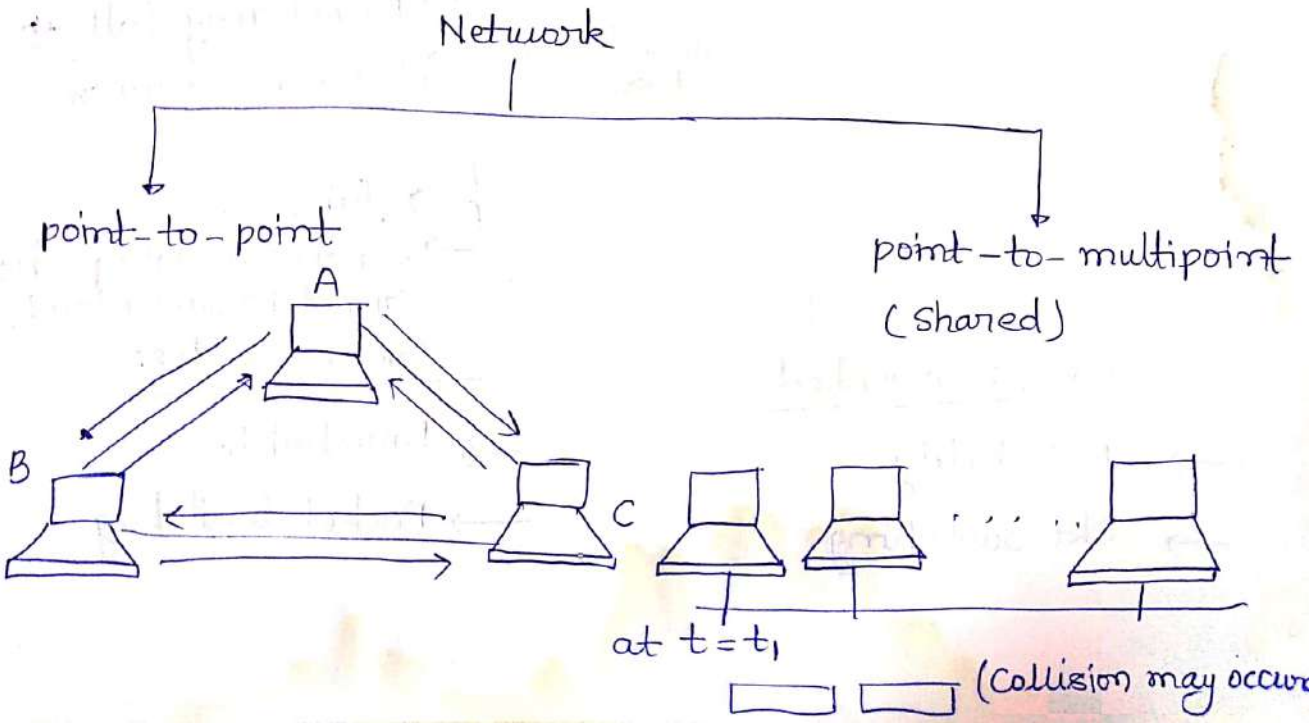
↓

also known as MAC address/Global address)



(5) Medium Access Protocols.

✡ Types of Network



Scanned by CamScanner

Date- 08/08/19

* Bluetooth, WiMax etc are wireless sharing medium.
* MAC layer is required only in case of local area network (Sharing Medium)

  802.2 ⟶ for LLC.

* For error control, CRC (Cyclic Redundency Check) and checksum is used.

✡ Responsibility/Services of Network layer ⟶

(1) To provide connectionless based effort data delivary services.
(not gaurenteed to destination)

Circuit Switching

e.g. PSTN → Public Switch Telephone Network
(Land line telephone)

Packet Switching

e.g. Internet
(Postal System)

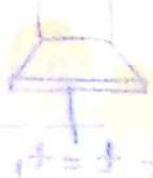
- → delay
- → lost of packets.
- → Packet may follow different routes. (connection less.)
- → fairness.
- → Sequence of data packets can not be gaurenteed.

Connection oriented

- → Reliability
- → Ckt Switching

Connection less

- → Unreliable
- → Packet Switching



Scanned by CamScanner

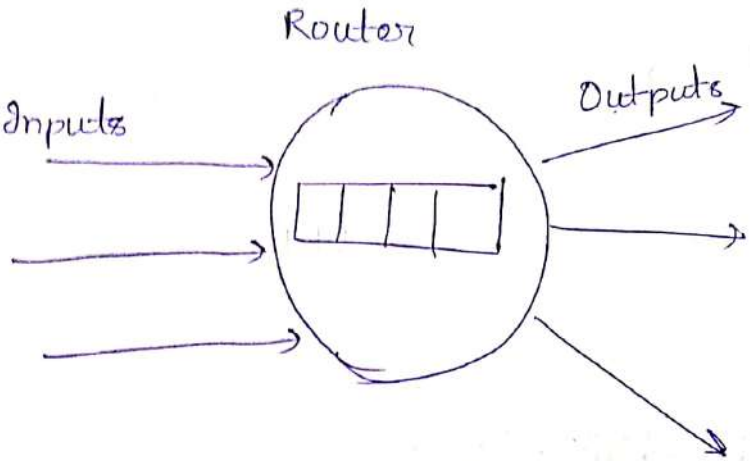
* ckt switching

* Connection orientation can be acheived over packet switched networks as well as circuit switched networks.

* Connectionless means always Packet Switching.

(2) Routing

→ RIP
→ OSPF
} Protocols



(3) Logical address →

IPv4 and IPv6

32-bits address

128-bits address.

(4) It is also responsible for congestion feedback.

Scanned by CamScanner

✡ Transport Layer ⟶

→ It provides connection oriented (Reliable) as well as connectionless (Unreliable) services.

→ logical Addressing (Port Number – 16 bits) 0 to 2^{16}

→ Congestion control

TCP ⟶ Connection Oriented

UDP ⟶ Connectionless.

✡ Responsibilities/Services of Session Layer ⟶

(1) Dialog Control

(2) Session Management → Initialization, Maintainance, termination.

(3) Synchronization of the communication.

* Responsibilities of presentation layer ⟶

(1) Syntax of data

(2) Semantics of data

(3) Encoding

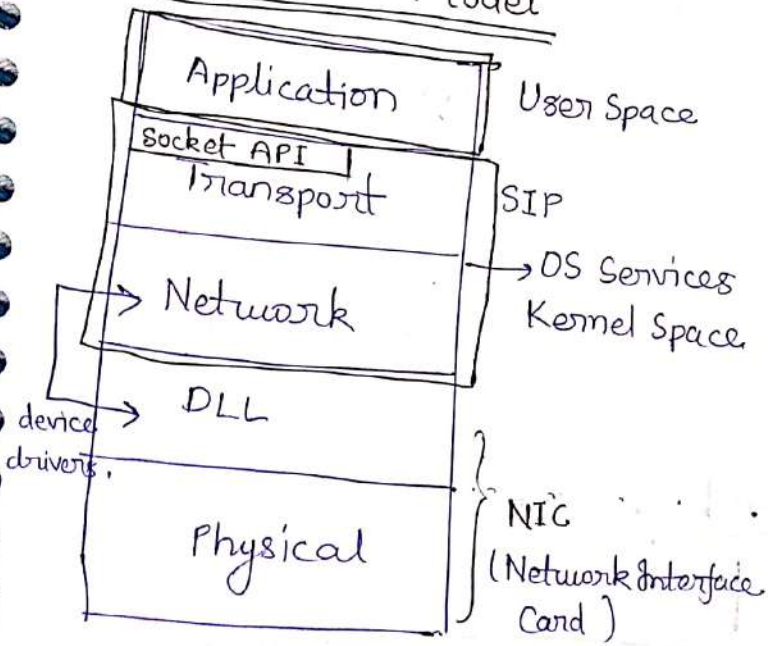
Scanned by CamScanner

✡ Services of application layer →

→ DNS, HTTP, Telnet, FTP all protocols runs on application layer.

Working Model →

TCP/IP Model



OSI model

- Application Layer.
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Data Link Layer
- Physical Layer

htons → Host to Network short (16 byte)
htonl → Host to Network long (32 byte)
ntohs → Network to Host short
ntohl → Network to Host long

→ System calls.

API → Application Program Interface

Scanned by CamScanner

Socket API

↓

logical entity

↳ IP + Port no.

STREAM Socket → TCP

DGRAM Socket → UDP

Raw Socket → any protocol of any layer.

char* tcp1(char *s) ↓

char* tcp2(char *s) ↑

* Classification of Networks →

- point-to-point
- point-to-multipoint

→ PAN
→ LAN
→ MAN
→ WAN

Network Design
- Client
- Server

Area Network
- PAN
- CAN
- LAN
- MAN
- WAN

Network Topology
- Bus
- Ring
- Star
- Tree

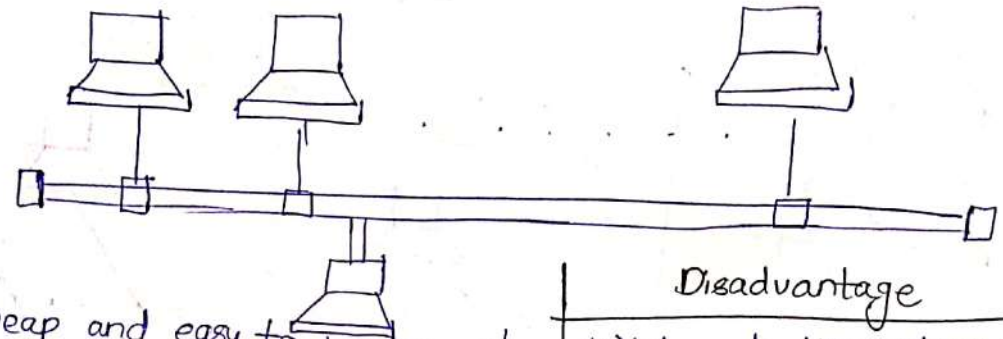
Network Protocol
- Proprietary
- Open (TCP/IP)

Wired or Wireless

Scanned by CamScanner

✡ Topologies for Network deployment

(1) BUS topologies



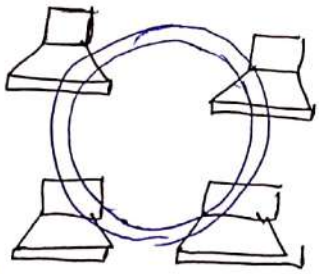
* Cheap and easy to implement.
* Requires less cable.
* Does not use any specialized network equipment.

Disadvantage

* Network disruption when computers are added or removed
* A break in the cable will prevent all systems from accessing the network difficult to troublshoot

(2) RING topologies

* Cable faults are easily located, making troubleshooting easier.



Disadvantage

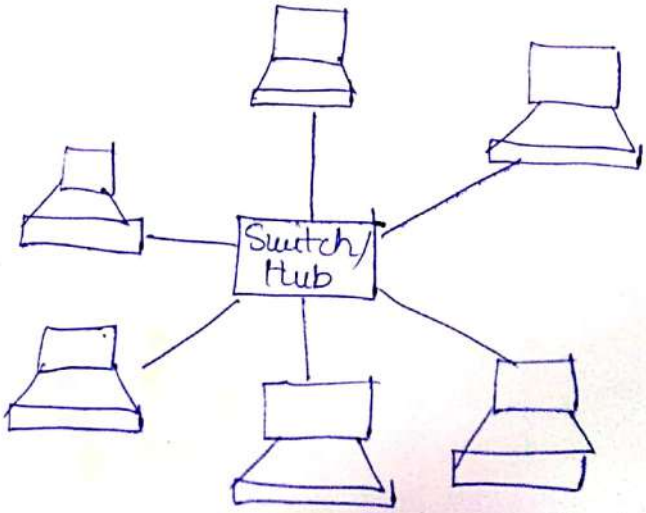
* A single break in the cable can disrupt the entire network.
* Expansion to the network can cause network disruption.

(3) STAR Topologies

* Most widely implemented.

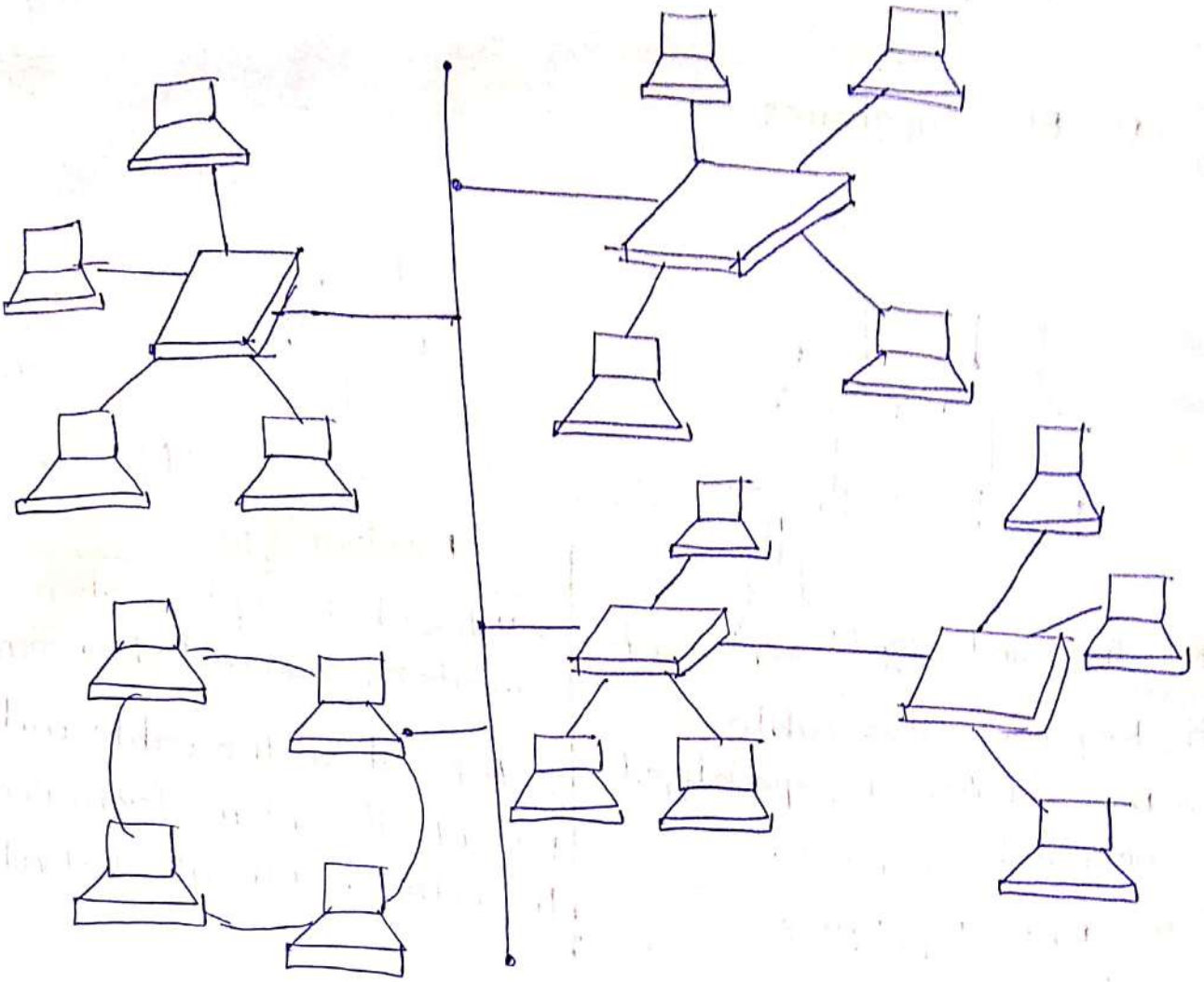
Disadvantages →

* Requires more cable.
* More difficult to implement.



Scanned by CamScanner

(4) Hybrid Topology

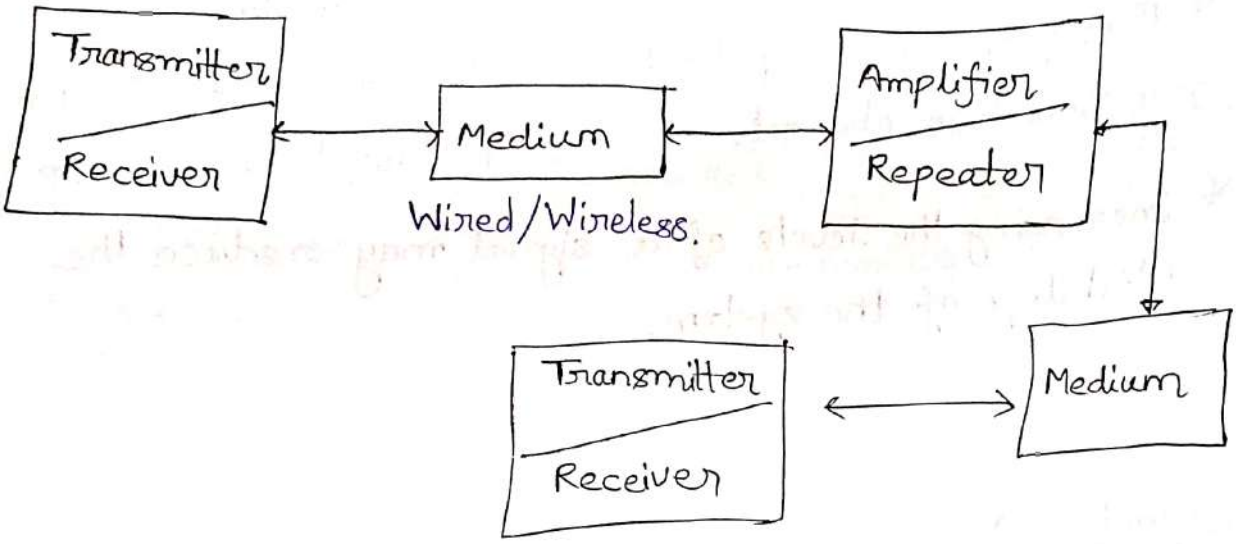


Scanned by CamScanner

19/08/19

Physical Layer

Abstract Communication Model



Amplifier ⟶ Used for Analog signal

Repeater ⟶ Used for Repeat. Digital signal.

Channel ⟶

It is a logical point to point connection between the sender and receiver.

Capacity of the channel ⟶

It is defind in terms of bandwidth / spectrum.

Bandwidth ⟶

$$BW = f_{max} - f_{min} \text{ Hz}$$

f_{max} ——————

f_{min} ——————

Scanned by CamScanner

Nyquist Theorem ⟶

$$C = 2H \log_2 V \text{ bits/sec}$$

H = Bandwidth of medium.

V = no. of discrete level used in the signal

* This formula is applicable for noiseless channel.

* Increasing the levels of a signal may reduce the reliability of the system.

Signal ⟶

It is electrical or electromagnetic encoding of data.

Que Channel BW = 4000 Hz

Signal level used = 4

How much data rate is acheivable through this channel.

Soln H = 4000Hz

V = 4

$$C = 2 \times 4000 \log_2 4$$

$$= 8000 \times 2$$

$$C = 16000 \text{ bits/s}$$

Scanned by CamScanner

Shannon Capacity theorem →

$$C = H \log_2 \left(1 + \frac{S}{N}\right) \text{ bit/sec}$$

$\frac{S}{N}$ = signal to Noise Ratio (SNR)

H = BW (Hz)

* Unit of SNR is dB.

$$\left(\frac{S}{N}\right) 1\,dB = 10 \log_{10} \left(\frac{S}{N}\right)$$

* Shannon capacity is used to determine the theoretical highest data rate for a noisy channel.

Que Signal is sent over a channel of 3kHz, post signal to noise ratio is 20dB. What is max acheivable data rate over the channel.

Sol^n

$$\frac{S}{N} = 20\,dB$$

$$\Rightarrow 20 = 10 \log_{10} \left(\frac{S}{N}\right)$$

$$\Rightarrow \frac{S}{N} = 100$$

$$C = 3 \times 10^3 \log_2 (1 + 100)$$

$$= 3 \times 10^3 \log_2 101$$

$$C = 3000 \log_2 101 \text{ bit/sec}$$

Scanned by CamScanner

✡ Analog Vs Digital

Analog Data ⟵ PSTN Network / QAM-16 ⟶ Analog Signal

Analog Data ⟵ Mobile Communication ⟶ Digital Signal

Digital Data ⟵ Modem / dial up internet connection ⟶ Analog Signal

Digital Data ⟵ 802.3 / Manchester Encoding ⟶ Digital Signal

Advantages of Digital Signal ⟶

Repeater, dsp (Digital Signal Processing)

* The effect of distortion, noise and interference is much less in digital signals as they are less affected.
* The signal is un-altered as the pulse needs a high disturbance to alter its properties, which is very difficult.
* Combining digital signal using TDM is easier than combining analog signal using FDM.
* The configuring process of digital signals is easier than analog signals.
* Digital signals can be saved and retrieved more conveniently than analog signals.
* The capacity of the channel is effectively utilized by digital signals.

Scanned by CamScanner

Disadvantage of digital Signal

* Generally, more bandwidth is required than that for analog systems.
* Synchronization is required.
* High power consumption (Due to various stages of conversion)
* Introduce sampling error.
* As square wave is more affected by noise, That's why while communicating through channel we send sine waves but while operating on device we use square pulse.

Advantage and disadvantage of Analog Signal

Advantages →

* Major advantages of the analog signal is infinite amount of data.
* Density is much higher.
* Easy processing.

Disadvantages →

* Unwanted noise in recording.
* If we transmit data at long distance then unwanted disturbance is there.
* Generation loss is also a big ~~com~~ cons of analog signal.

Scanned by CamScanner

✡ Medium

* Properties of Medium ⟶

Guided Media ⟶

Features →

* High speed
* Secure
* Used for comparatively shorter distances.

(a) Twisted Pair Cable ⟶

(i) UTP ⟶

* Least expensive
* Easy to install
* High speed capacity

Disadvantages ⟶

* Susceptible to external interference
* Lower capacity and performance in comparision to STP.
* Short distance transmission due to attenuation.

(ii) STP

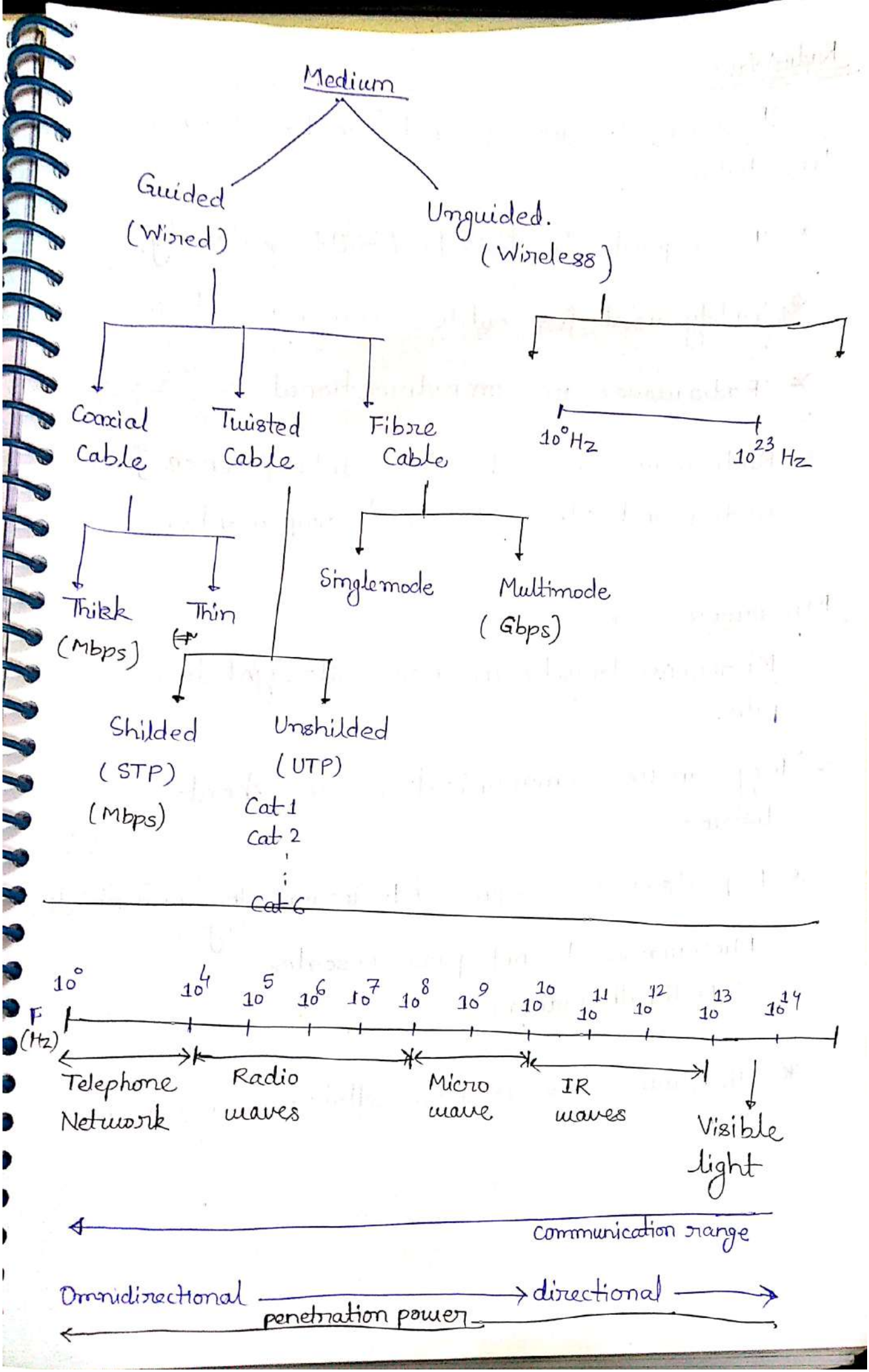
Advantage ⟶

* Better performance at a higher data rate in comparision to UTP.
* Eliminates crosstalk.
* Comparitively faster.

Disadvantages ⟶

* Comparitively difficult to install and manufacture
* More expensive
* Bulky

Scanned by CamScanner



Scanned by CamScanner

Radio Wave

It is easy to generate and can travel over long distances.

* It can penetrate obstacles (buildings) easily.
* Widely used for outdoor communication.
* Radio waves are omnidirectional.
* Radio waves are subject to interference from motor and other electrical equipements.

Microwave ⟶

Microwave travels in near straight line path.

* They can use communication over short distances.
* Repeaters are required to increase the communication range.
* Microwaves do not pass obscales. (Multipath fading)
* Microwaves are used for cellular communication.

Scanned by CamScanner

Infrared (IR) waves →

* It ranges from 700nm to 1mm.
* IR waves are longer than those of visible light but shorter than those of radio waves.
* IR light is invisible to the human eye, although longer IR waves can be sensed as heat.

Light waves →

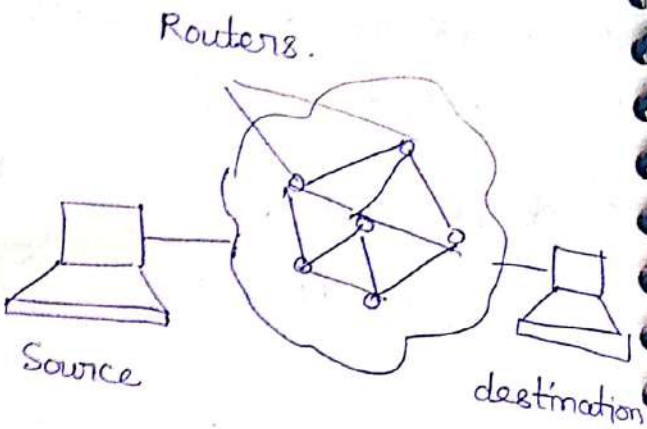
* LEDs are used to generate light waves.
* Visible light is just one particular type of electromagnetic radiation.

Scanned by CamScanner

Date - 22/08/19

✱ Network Performance →

(1) End to End delay

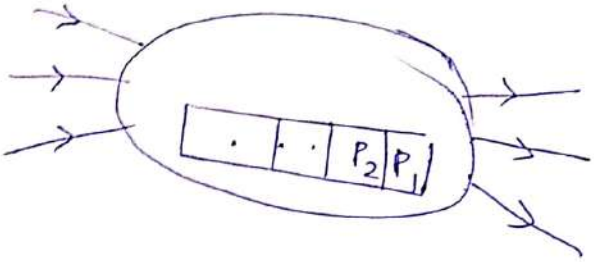


Channel Utilization

It is defind as fraction of time channel occupied.

Throughput →

It is defind as bits per second (successfully received data by receiver)



(1) Transmission delay →

Time elapse between first and last bit of a packet.

(2) Propagation delay →

Time travel to length of link/wire.

(3) Processing delay at each end →

(4) Queuing delay →

Scanned by CamScanner

① end to end delay (minimum)

$= \sum_{\text{no. of intermediate nodes}}$ (Transmission delay + propagation delay + Processing delay + Queuing delay)

② Throughput (Maximum)

Scanned by CamScanner

Physical layer continues.....

* Converting bits into signal →

(1) digital data → digital signal

[Encoding Techniques]

There are four parameters regarding encoding techniques

→ Net DC component present in the signal
→ Clock information
→ Error detection
→ cost [bits/signal]
→ Complexity

-ve
-ve
+ve
+ve

(1) NRZ (Non return to Zero) series of encoding
(2) Multilevel Binary
(3) Biphase Encoding
(4) Encoding for long distance transmission.
(5) Block Encoding

NRZ

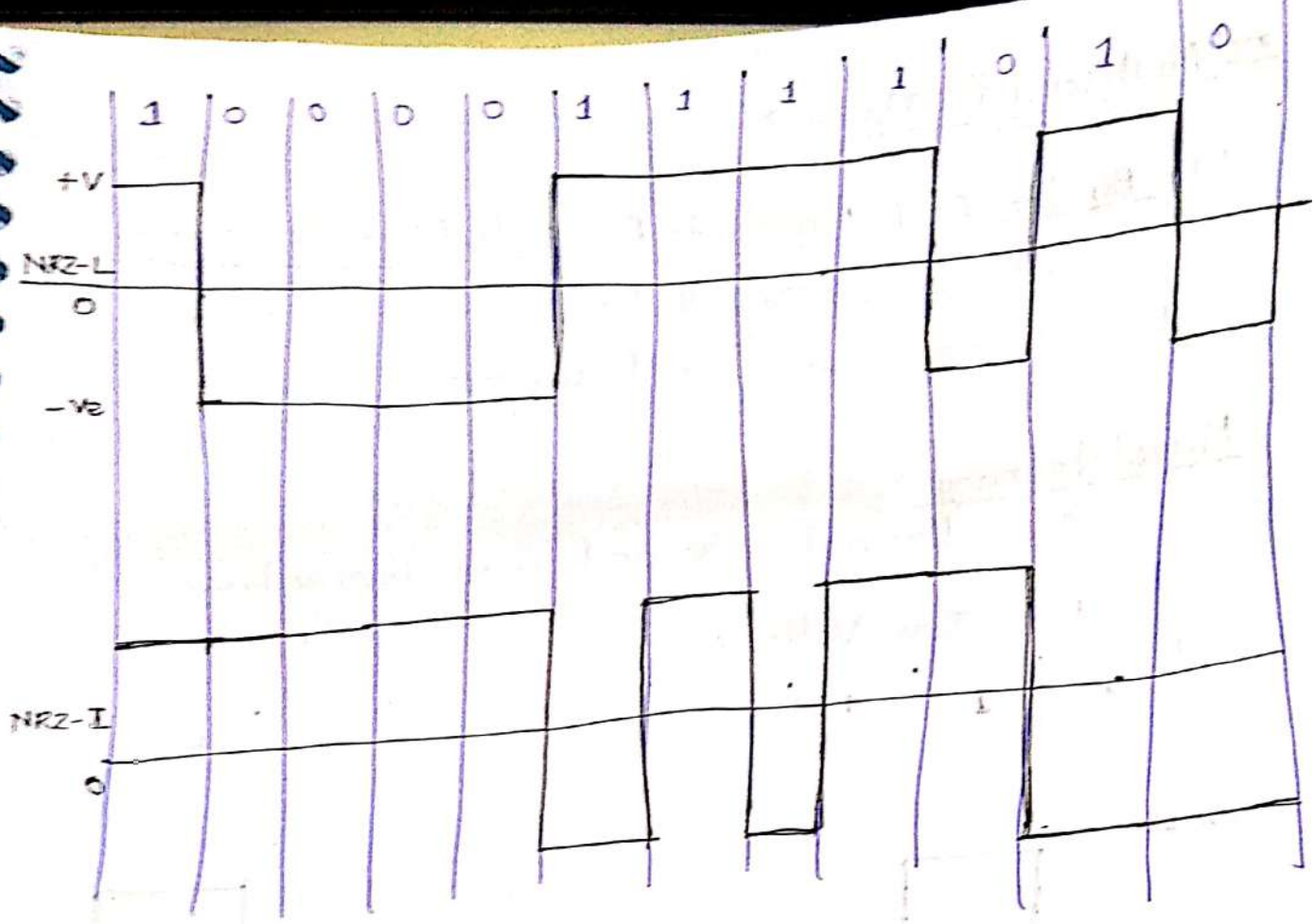
NRZ-I (differential Encoding)

0 : No transition at the beginning of bit interval
1 : transition.

NRZ-L

0 : high voltage level
1 : low voltage level

Scanned by CamScanner

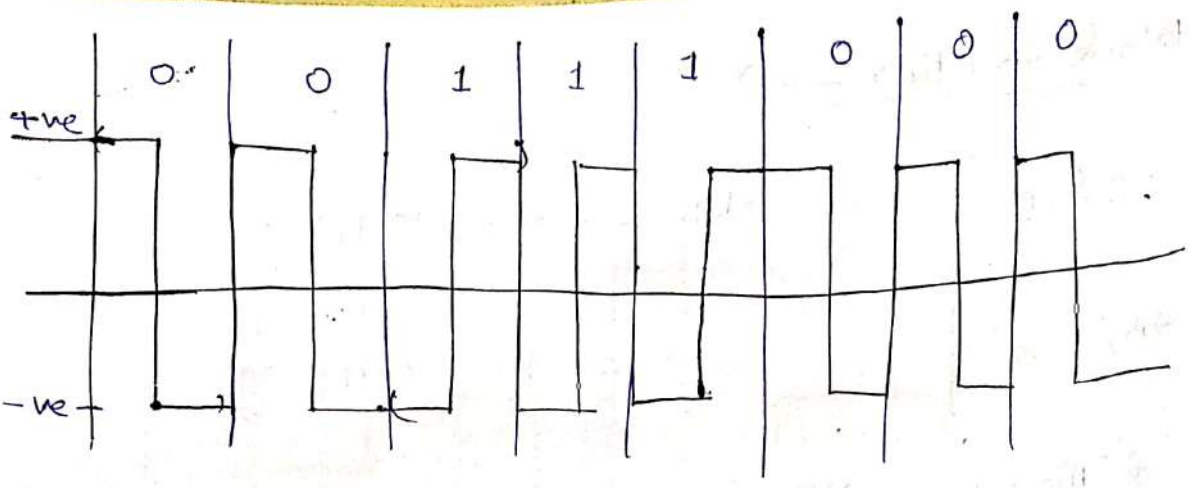


* Net DC component undesirable in the signal.

* DC component is not desirable in signal because it cannot pass through some comm. system like transformer and also lead to distortion.

* DC component also results loss of compon unwanted signal.

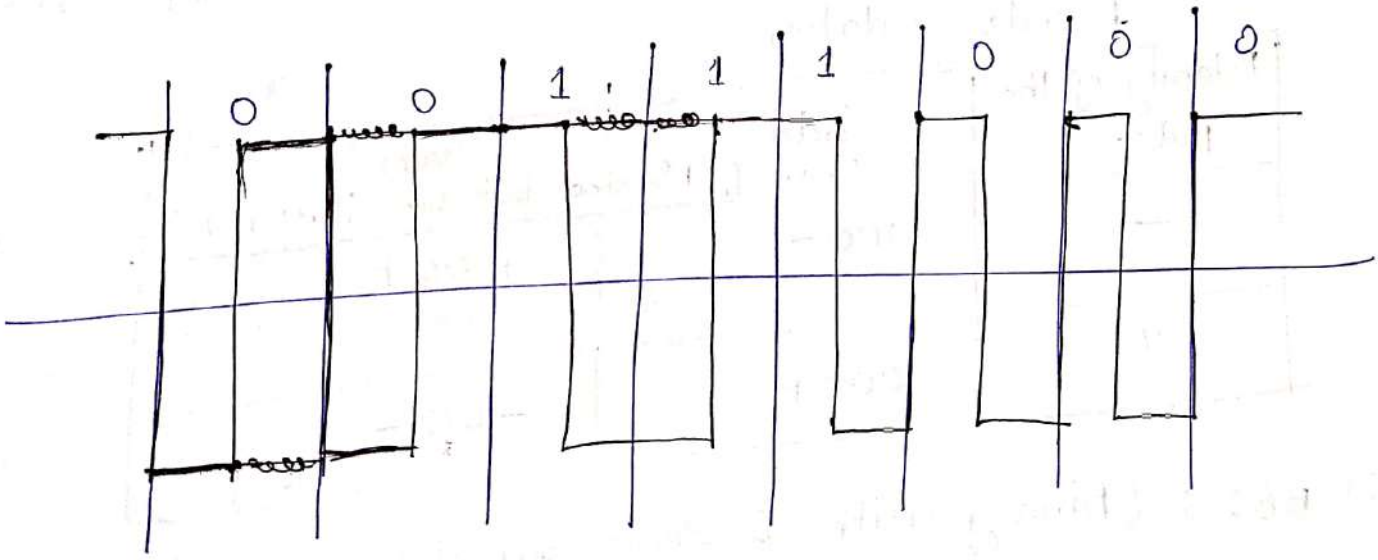
Scanned by CamScanner



(b) Differential Manachester Encoding

0 : Transition at the begining of bit interval

1 : Absense of transition at the begining of bit interval.



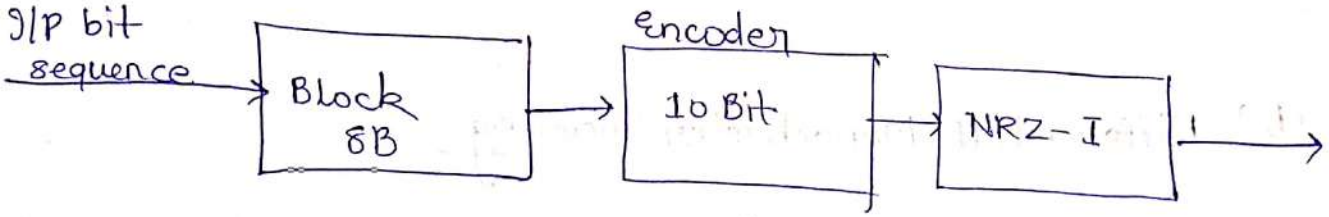
* Manchester technique is used in Ethernet IEEE 802.3
* Differential Manchester technique is used in token ring.

Scanned by CamScanner

* Block Encoding →

5B/8B	5 bit → 8 bit mapping
8B/10B	8 bit → 10 bit mapping

* They use NRZ-I to transmit the data.



✡ Encoding for long distance → (Based on Bipolar AMI)

(1) HDB3 (High Density Binary with 4 Zero Substitution)

· 1 code voilation

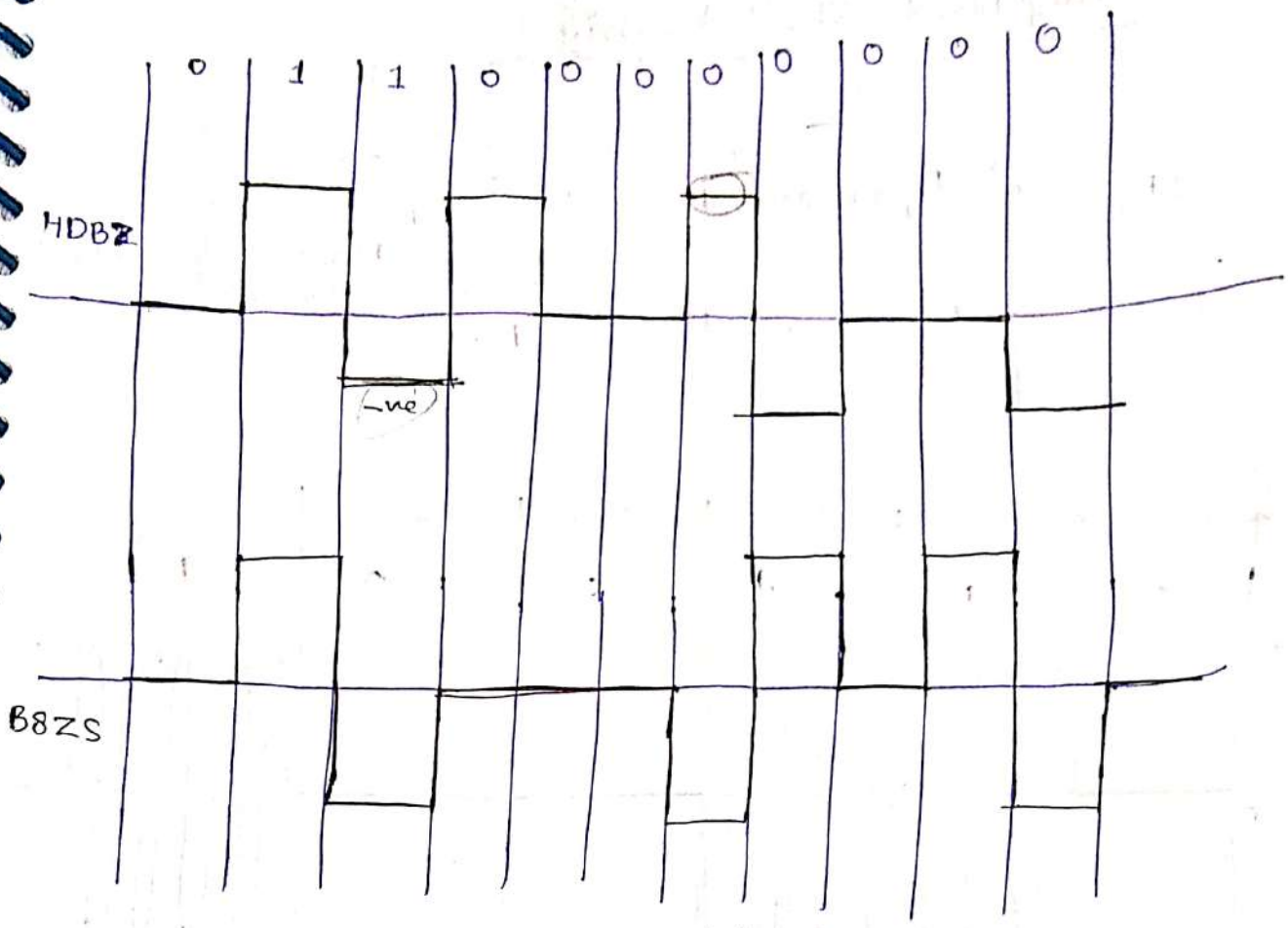
Polarity of the pulse	odd (no. of 1's since last substitution)	even (no. of 1's since last substitution)
−	000−	+00+
+	000+	−00−

(2) B8ZS (Binary with 8 Zero Substitution)

by substituting 2 code voilation.

Polarity of the pulse	odd	even
+	000+	−0+−
−	000−	+0+−

Scanned by CamScanner



(2) Digital Data —— Analog ~~Encoding~~ Signal

$$S(t) = A \sin(\omega t + \phi)$$

- A → Amplitude
- ω → frequency
- ϕ → Phase

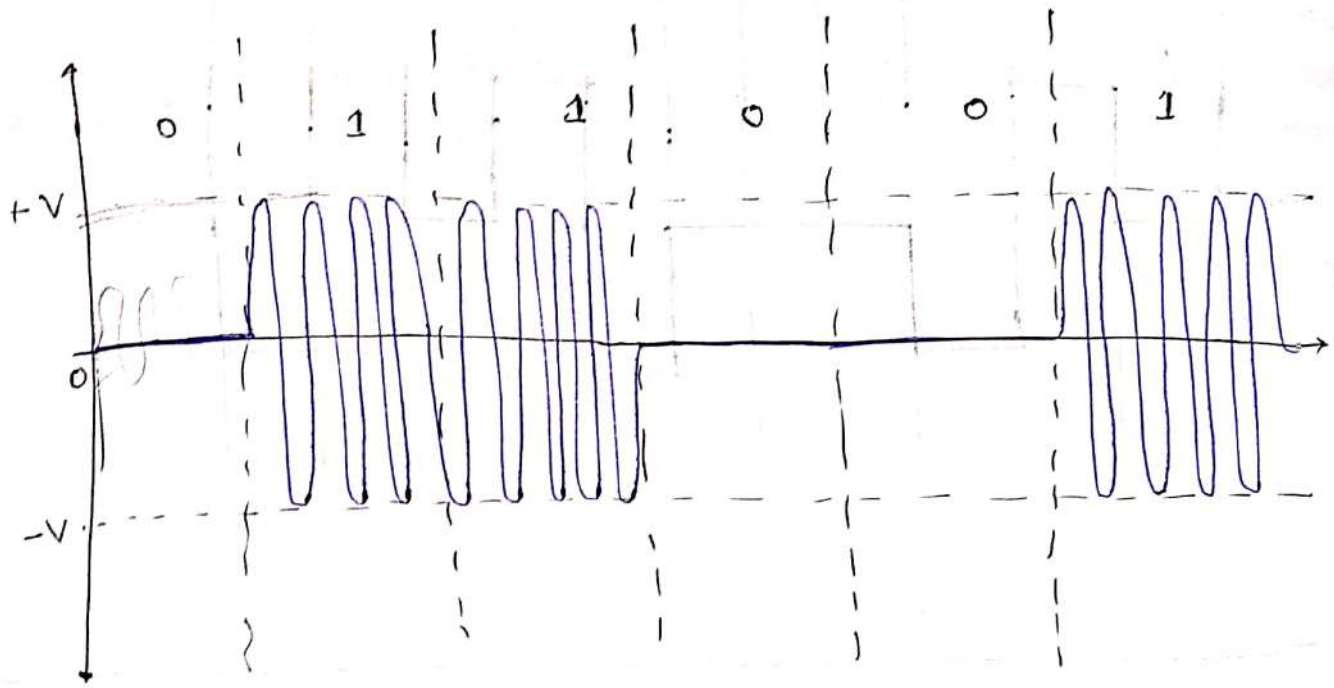
* Analog signal generation is known as Modulation techniques.

Scanned by CamScanner

(1) ASK (Amplitude Shift Keying)

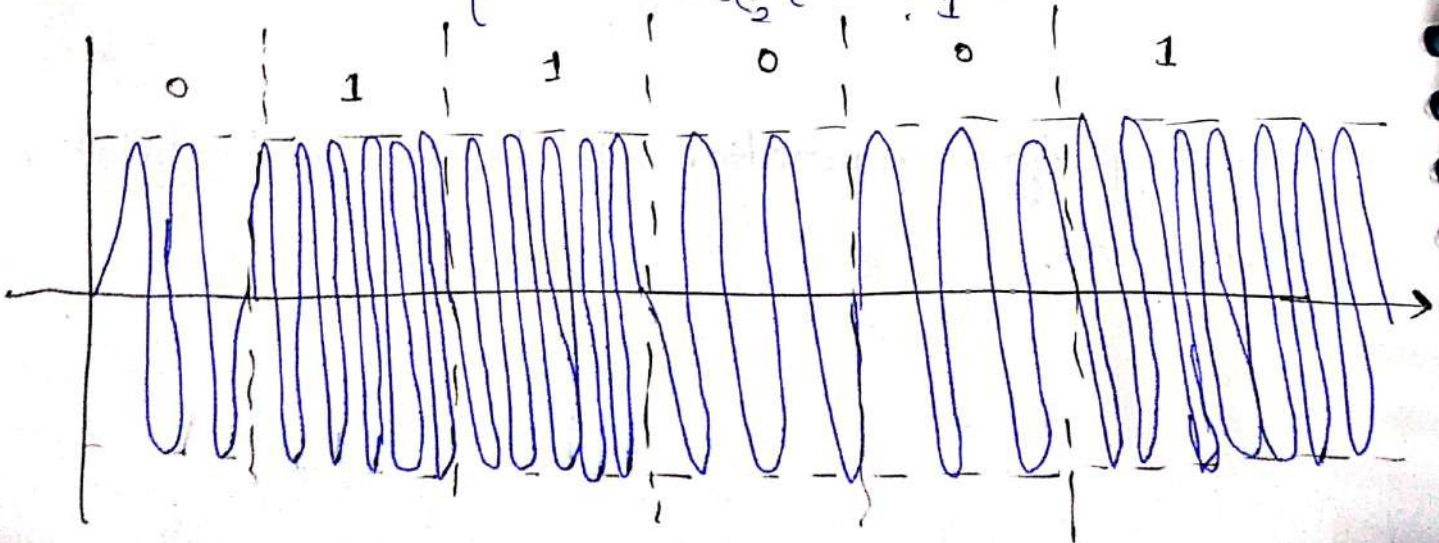
$$s(t) = \begin{cases} A_1 \sin 2\pi f_c t & : 0 \\ A_2 \sin 2\pi f_c t & : 1 \end{cases}$$

Phase, frequency } constant



(2) FSK (Frequency Shift Keying)

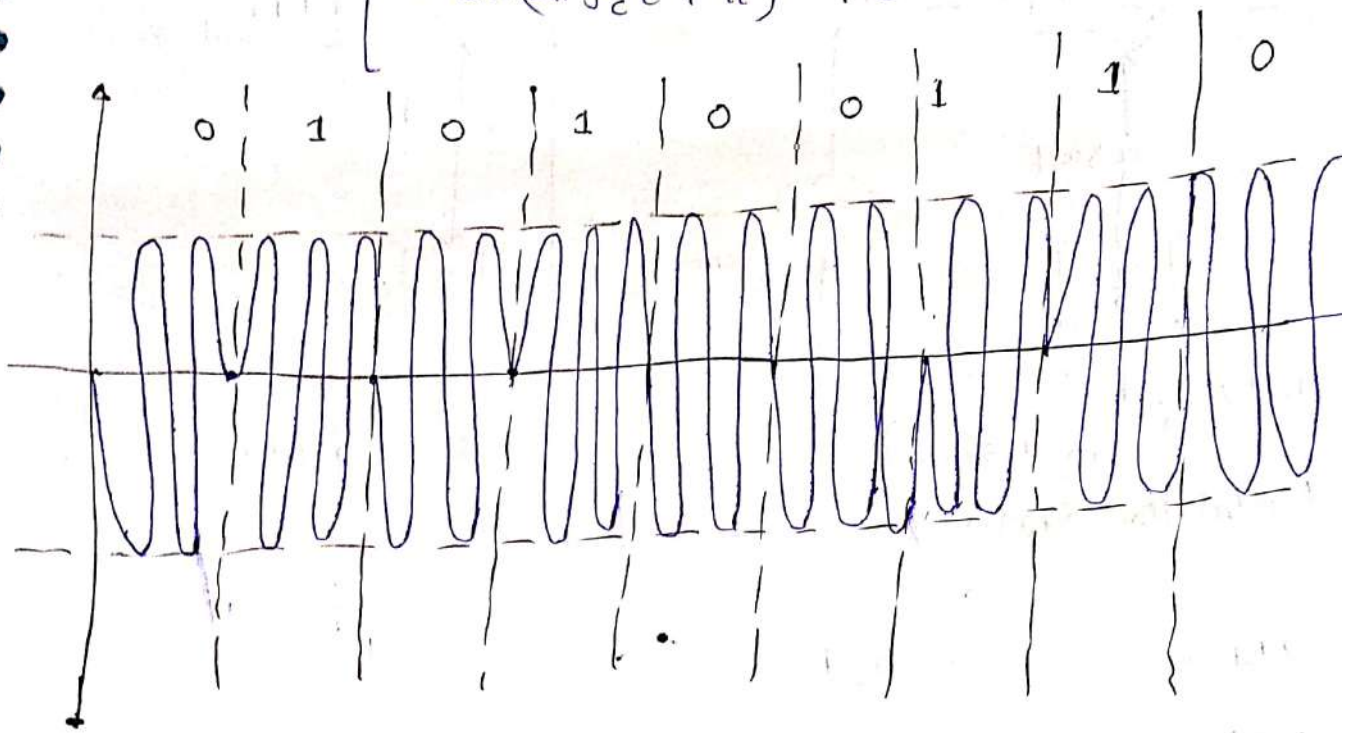
$$s(t) = \begin{cases} A \sin 2\pi f_{c_1} t & : 0 \\ A \sin 2\pi f_{c_2} t & : 1 \end{cases}$$



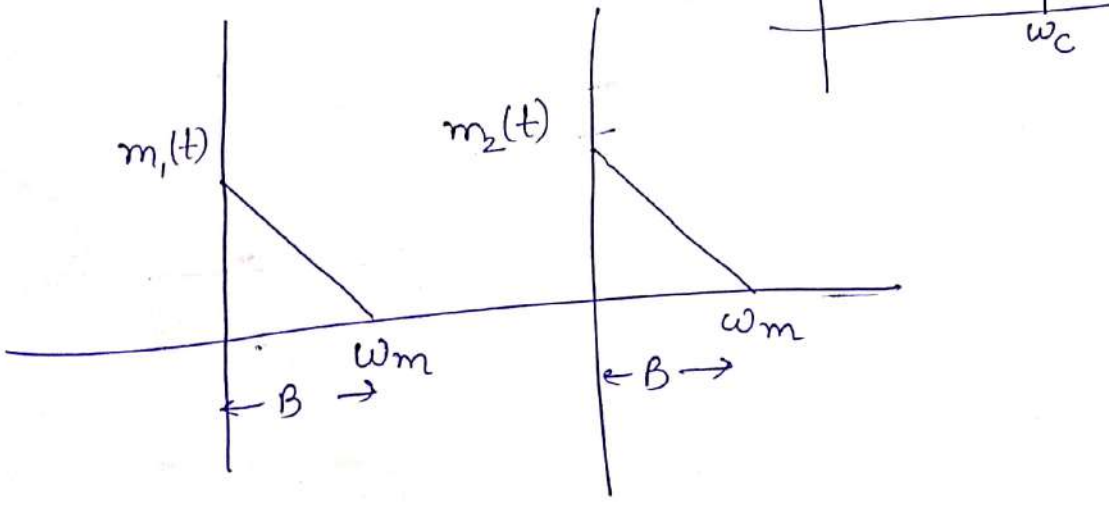
Scanned by CamScanner

(3) PSK (Phase Shift Keying)

$$s(t) = \begin{cases} A \sin 2\pi f_c t & : 0 \\ A \sin(2\pi f_c t + \pi) & : 1 \end{cases}$$



QAM techniques

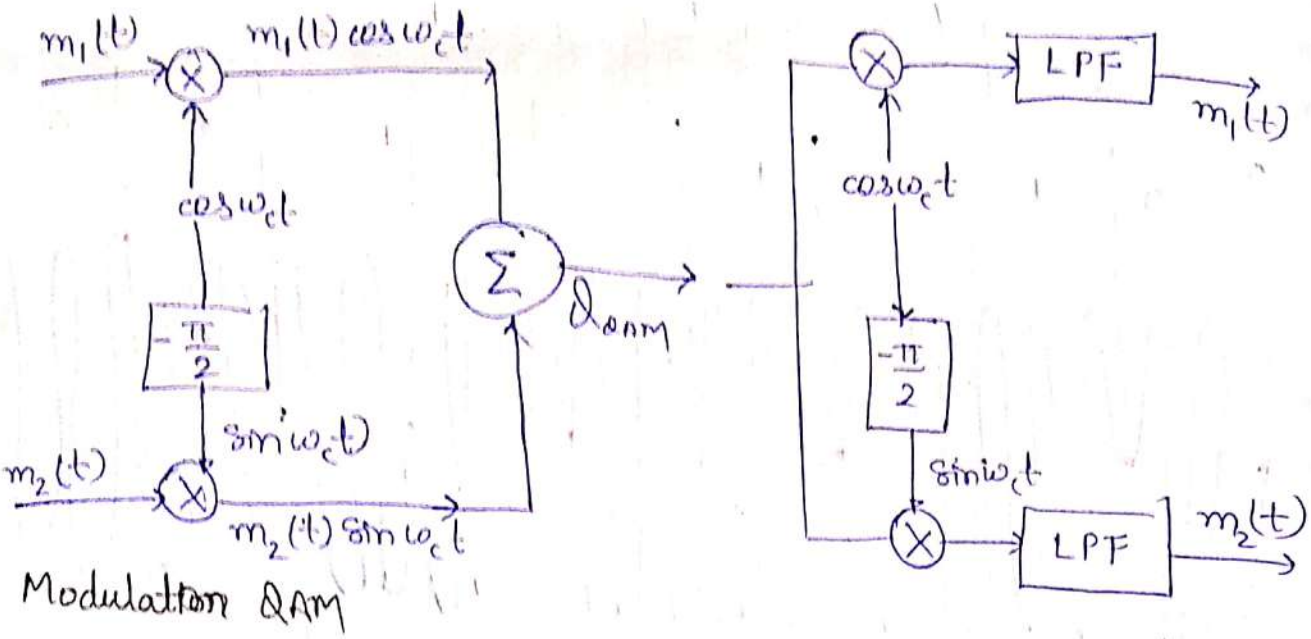


$$Q_{QAM} = m_1 \cos \omega_c t + m_2(t) \sin \omega_c t$$

Scanned by CamScanner

Block diagram of QAM ⟶

$Q_{QAM} = m_1(t) \cos \omega_c t + m_2(t) \sin \omega_c t$



Modulation QAM

⟶ BPSK 0, 1

⟶ QPSK (00, 01, 10, 11)

⟶ 16 QAM (0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111)

Scanned by CamScanner

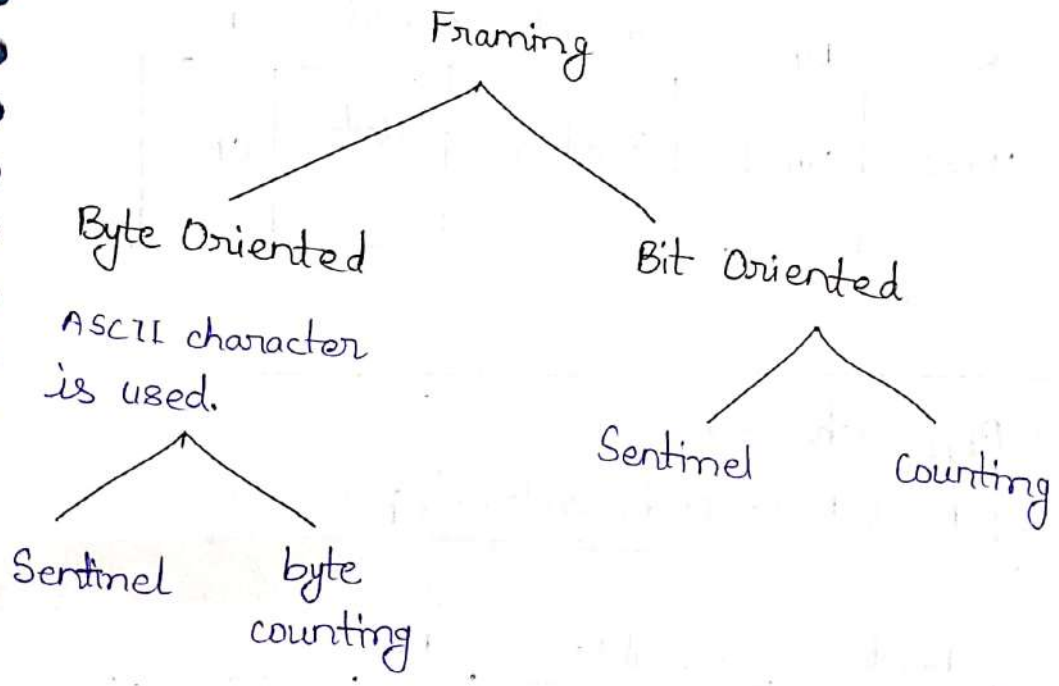
Date- 26/08/19

Data Link Layer

* Framing →

Computer network operates as a packet switched network which means block of data is exchaned between the nodes.

Interfaces are transmitting and receiving stream of bits. Therefore it is required to mark the boundary of frame on the bitstreams, for this framing protocol is used.



✡ Byte Oriented Protocal →

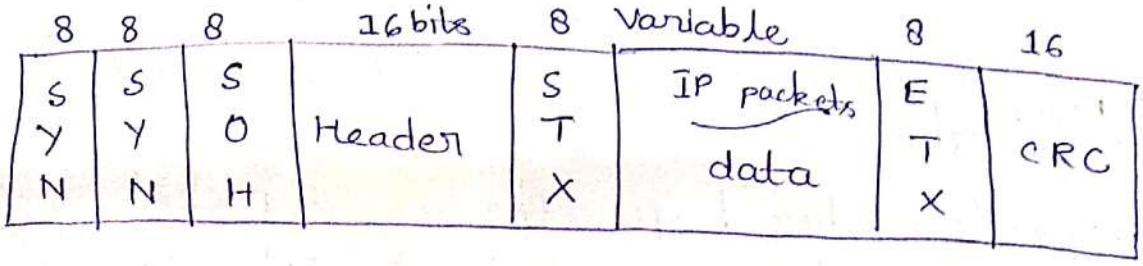
(BISNYC, DDCMP)

↓ based on

Sentinel approach

Scanned by CamScanner

BISYNC

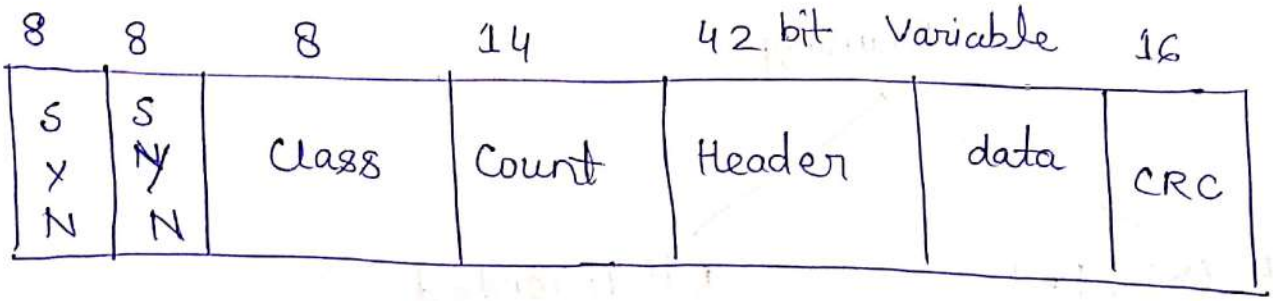


→ Byte Stuffing

SOH = Start Of Header
STX = Start of Transmission
ETX = End of Transmission.

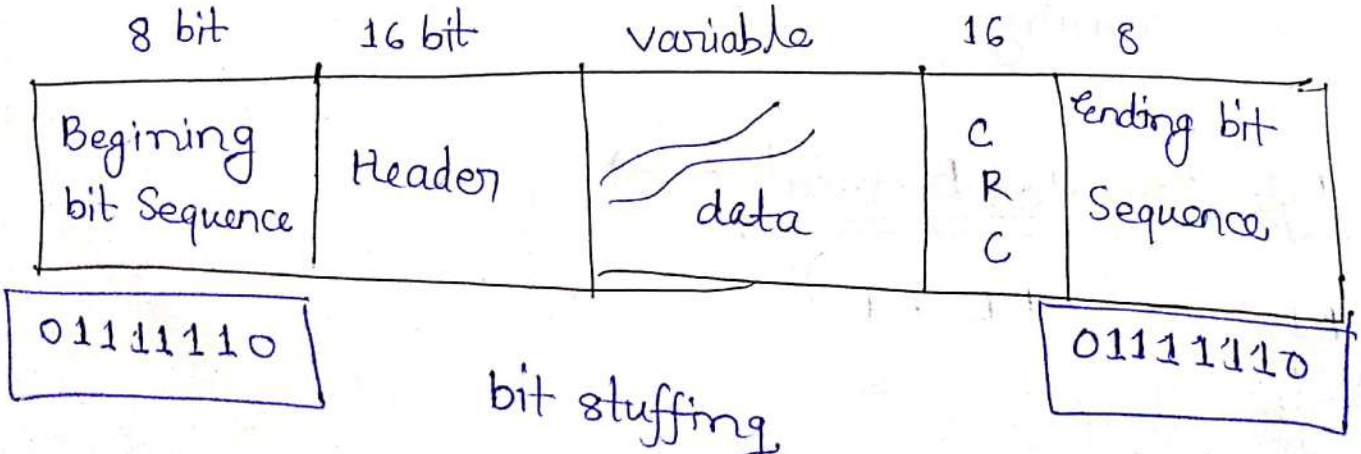
DLE = Data Link Escape character.

DDCMP (Byte Counting Approach)



Bit Oriented Approach →

HDLC (High Level Data Link Control) protocol

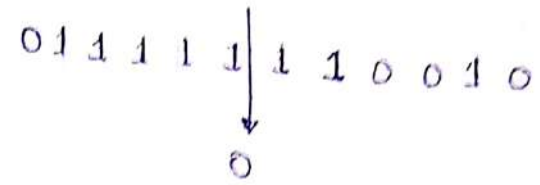


bit stuffing

Scanned by CamScanner

* Whenever, except starting and ending bit sequence five 1's are encountered, then a zero will be stuffed.

e.g.



* Receiver process will be, whenever five 1's are receiver, it will check next bit, if it is zero, then take out that bit and marks subsequence bit as part of bit.

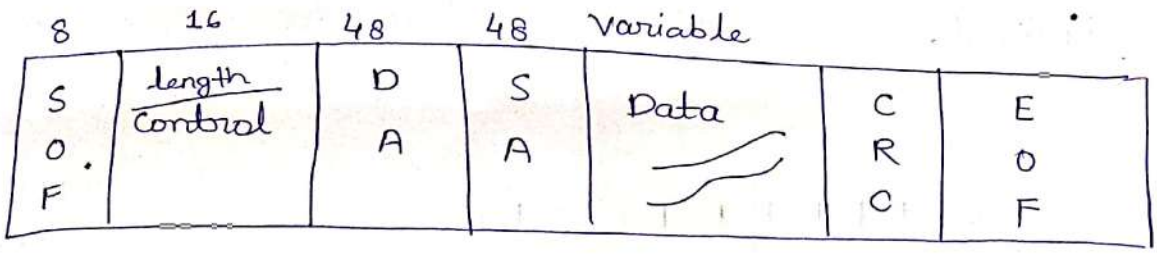
If the next bit is 1 then there are two possibilities —

* If next bit is zero, then that is boundary of frame.
* If next bit is 1, then frame data received is an error.

* The above protocol discussed works of ISP.

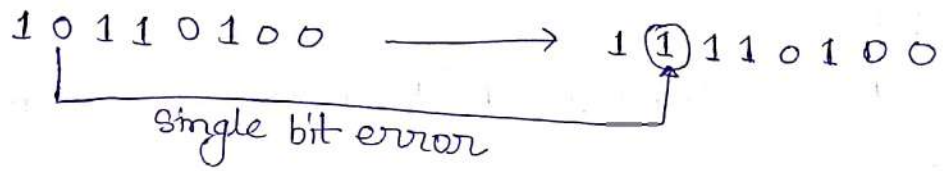
Scanned by CamScanner

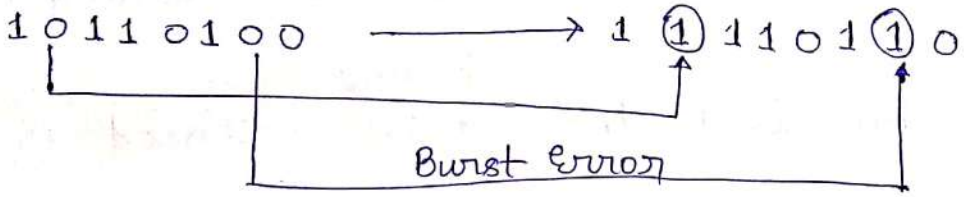
For Ethernet (802.3)



This has also Byte Oriented and Sentinel

✡ Error Control →





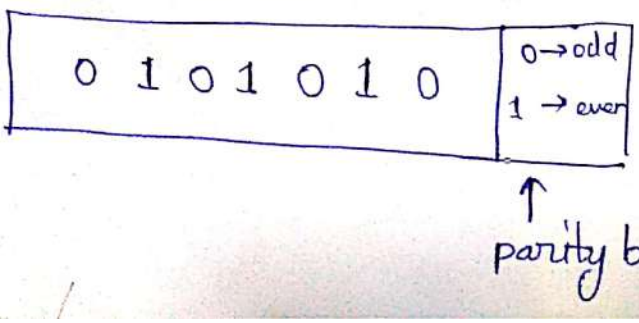
✡ Error Detection Techniques →

(1) Parity Check

→ Scalability

→ No. of extra bits required

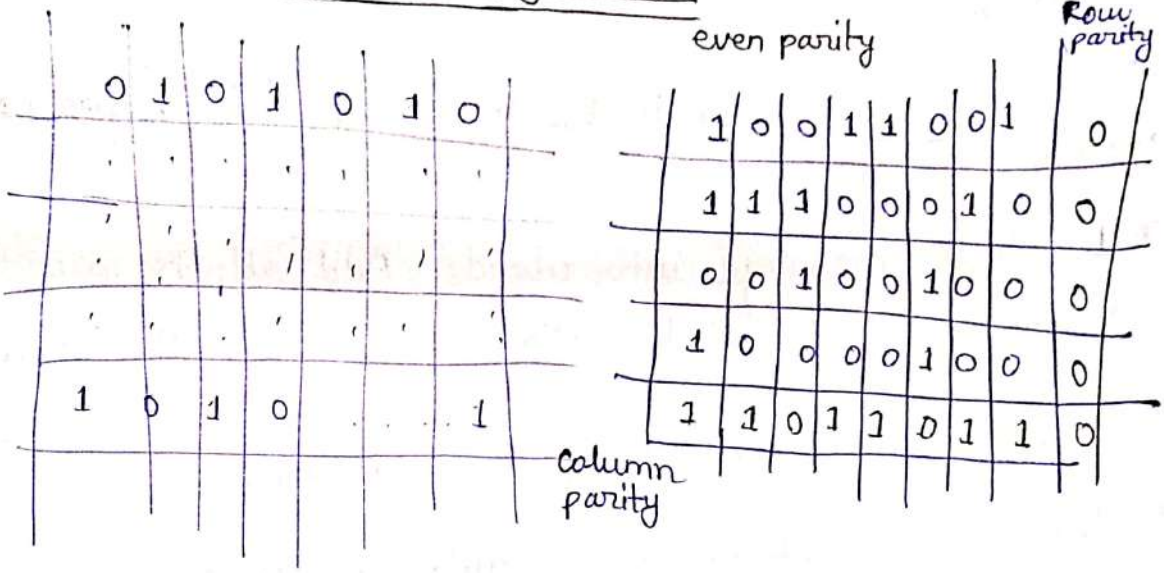
→ power of Error detection.



Scanned by CamScanner

* Enforcement of odd parity means no. of 1's is odd, and for even, 1's should be even.

✡ Two dimensional parity check



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

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

Scanned by CamScanner

✡ Checksum

* Checksum use 1's compliment arithmatic for its implementation.

Algorithm

* Consider a message to be made up of bytes or words.
* Divide the message into words. Add all the words using 1's complement arithmatic to get the sum.
* Complement the sum to get checksum.
* Transmit checksum along with the message.

Receiver

* Divide the received message into words. Add all the words including checksum.
* Complement the sum.
* All zeros employees no error, else error.

* power of error detection.

It can detects all error where odd no. of bits are envolved in error. (most of 2 bit or 4 bits error)

Scanned by CamScanner

Date - 29/08/19

Example

$M = \underbrace{10101001}_{W_1}\ \underbrace{00111001}_{W_2}$

```
  10101001
+ 00111001
-----------
  11100010
```

Sum

Take complement

W_3 | 00011101 |

Checksum

Transmit massege

$= W_1 + W_2 + W_3$

```
  11100010
  00011101
-----------
  11111111
```

compliment = 00000000

Let the received word is

```
  10101111
+ 11111001
-----------
 (1)10101000
  |_______|
-----------
```

Sum 10101001

$W_1 + W_2 + W_3$ =

```
  10101001
  00011101
-----------
  11000110
```

compliment 00111001 [There is an Error]

Scanned by CamScanner

✡ CRC (Cyclic Redundancy Check) ⟶

* CRC is implemented using special class of polynomial arithmatic known as Polynomial Arithmatic modulo tool.

* For implementation of CRC following properties are important —

(a) Any polynomial B(x) can divide a polynomial C(x) if B(x) is of same or higher degree than C(x).

(b) The remainder obtained when C(x) is divided by B(x) by substracting B(x) from C(x).

(c) To substract B(x) from C(x), we simply perform Ex-OR operation on the pair of matching coefficients of the polynomials and degree of polynomial is defind as —

Let $C(x) = x^3 + 1$

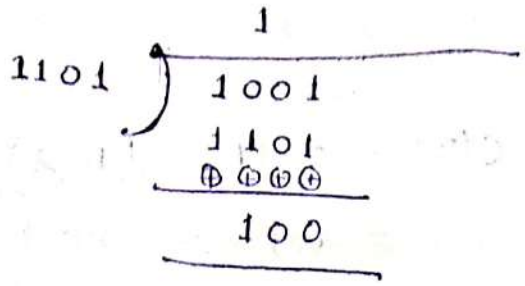
$B(x) = x^3 + x^2 + 1$ degree = 3

Binary Equivalance

$B(x) = 1101$

$C(x) = 1001$

Scanned by CamScanner



CRC at Sender side →

* Let R be the degree of polynomial C(x). [Both Sender and Receiver known that . . . polynomial].
* Append R 0 bits at the end of message bit string and call it S(x).
* Divide S(x) by C(x) to get the remainder R(x).
* Substract R(x) from S(x) and call it T(x)
* Transmit T(x).

At Receiver Side

* Let Receiver receive massege and call it M(x).
* Divide M(x) by C(x).
* If remainder is Zero, that accept or otherwise discard.

Scanned by CamScanner

Example

message = 1011

$C(x) = x^2 + 1$ (D: 2)

$= 101$

$M(x) = 101100$

```
        1001
101 ) 101100
      101↓
      x001
       000
      x010
       000
      x100
       101
       001
```

```
  101100
⊕    001
--------
  101101
```

Standard Part CRC

* $CRC-16 = x^{16} + x^{15} + x^2 + 1$

* $CRC-CCITT = x^{16} + x^{12} + x^5 + 1$ (telecom)

* $CRC-12 = x^{12} + x^{11} + x^2 + x + 1$

At receiver

```
        1001
101 ) 101101
      101↓
      x001
       000
      x010
       000
      x101
       101
       000
```

No error

Let the received bit is 101001

```
        1000
101 ) 101001
      101↓
      x000
       000
      x000
       000
      x001
       000
       x01
```

Since remainder is not zero hence there is an error in received message.

Scanned by CamScanner

Power of Error detection

It can detect all errors where odd no. of bits are involved in error, 2 bit, and most of the 4 bit errors and most of burst errors.

---

*Error Correction Techniques

Hamming Code

$m + r + 1 \leq 2^r$

To impliment the algorithm we need to find the no. of r bits required for the implemention which can be obtained by

$$(m + r + 1) \leq 2^r$$

where m = no. of message bits

r = no. of redundant bits (parity bits).

Step 1

* bits are numbered from left to right as 1; 2, 3 .... starting from 1 to $(m+r)$.
* Power of 2 bits positions are reserved for redundant bits.
* Remaining positions are filled with message bits from left to right.

Scanned by CamScanner

* Each p redundant bit shall enforce parity (even or odd) on the subset of redundant bit.

* Subset of parity bits can be determined as follows —

Example

$M = 1011 = 4$

$4 + r + 1 \leq 2^r$

$R = 3$

odd parity

001 1	010 2	011 3	100 4	101 5	110 6	111 7
R_1	R_2	M_3	R_4	M_5	M_6	M_7
		1		0	1	1

$(R_1, 3, 5, 7)$ → 1 0 1 → $R_1 = 1$

$(R_2, 3, 6, 7)$ → 1 1 1 → $R_2 = 0$

$(R_4, 5, 6, 7)$ → 0 1 1 → $R_4 = 1$

Codeword = 1 0 1 1 0 1 1

Scanned by CamScanner

At receiver

odd parity

Received Message is 1011010

(1, 3, 5, 7) (2, 3, 6, 7) (4, 5, 6, 7)

1100 0110 0010

P_1	1	1	0	0	1
P_2	0	1	1	0	0
P_4	1	0	1	0	1

111 = 7

It means there is an error in 7th position.

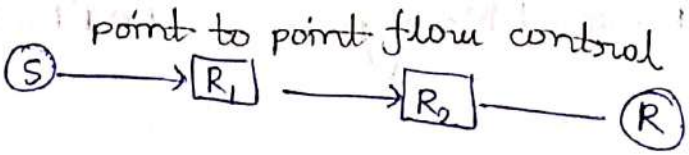
Hence the correct output will be

= 1011011

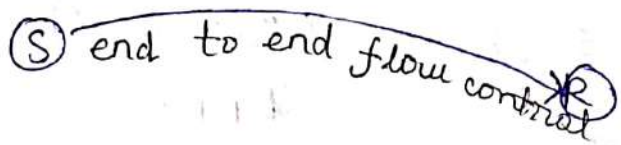
Scanned by CamScanner

✡ Flow Control ⟶

* Data link layer



* Transport Layer



* flow control techniques are required to deal with the problem of fast transmitter and slow receivers
* Flow control techniques are also responsible for order of data packets (Sequence of data packects)
* These techniques also cares of lost data packets.

ARQ

* Automatic Repeate request is implement on all the nodes on network.

(1) LLC protocols are required to deliver frames relibly and ~~leaves~~ need some feedback mechanism.

(2) This can be implemented by the use of ACK and timers.

Sender's process

* Sender transmit a frame and keeps a copy of it.
* Associates a timer with copy of frame and wait for ACK.

Scanned by CamScanner

* If ACK is not received before time out then retransmitt the frame.

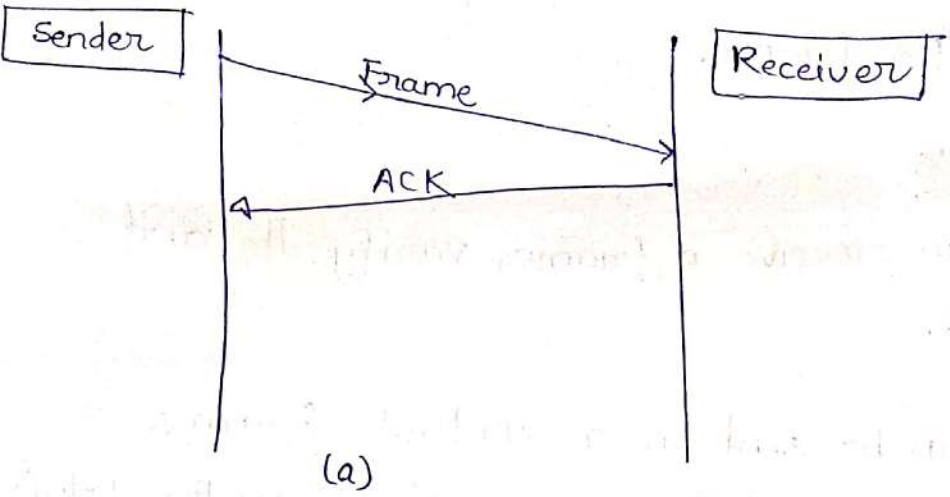
Receiver's process

* Receiver can receive a frame, varify it and send the ACK.

* This ACK can be sent on a control frame (Header without any data or piggyback on the datafram it is about to sent). This is known as ARQ.

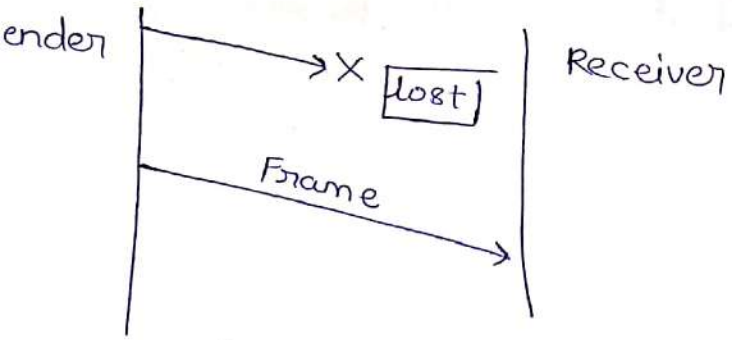
Scanned by CamScanner

Date 05/09/19



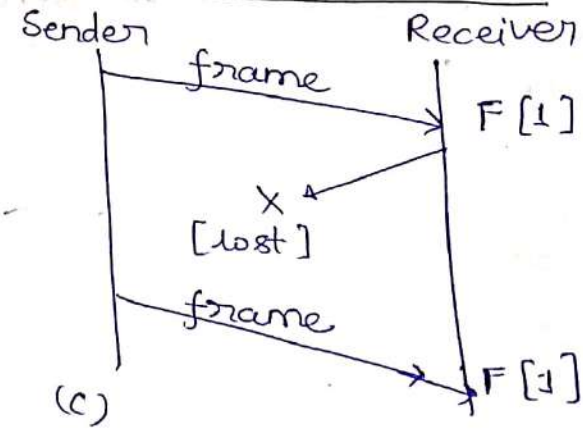
(a)

When frame has lost



(b)

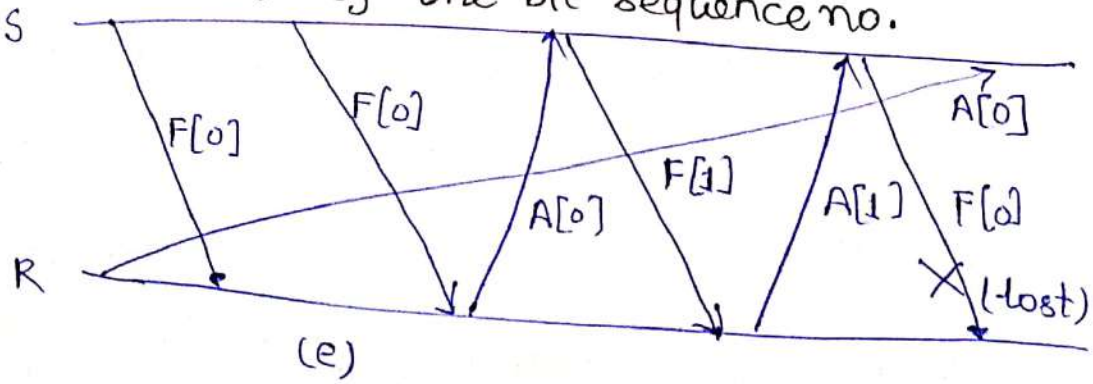
When the ACK is lost



(c)

* Sequence no. is used to avoid the duplicate copies of frame

In case of one bit sequence no.



(e)

Scanned by CamScanner

* Stop and Wait protocol can be considered as 1 bit ARQ

Problems

* One bit sequence number is not sufficient for stop and wait protocol as shown in figure (e)

* Only one frame can be transmitted at any point of time, which means link capacity cannot be utilized sufficiently

Que Available link capacity is 1.5 Mbps, timer value = 45 ms and frame size = 1 kB. How many frames can be transmitted to fully utilize link capacity?

Soln

$$\text{no. of frames} = \frac{1.5 \times 10^6 \times 45 \times 10^{-3}}{1 \times 10^3}$$

$= 18.$

Scanned by CamScanner

* To solve the above problems of

(1) N bits sequence no. should be used.

(2) TTL (Time to leave) constrains should be added for frame and ack.

(3) To utilize link capacity, more than one frame should be sent within the timeout value.

(4) These solution have been encorpted in sliding window protocal.

$$SWS = \frac{\text{link capacity} \times \text{timeout value}}{\text{frame Size.}}$$

(Sender Window size)

$$\text{total no. of bits in sequence} = \frac{(\text{Max. Sequence No.} + 1)}{2} \geq SWS$$

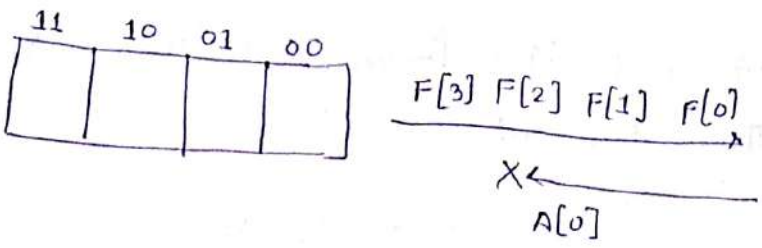
for $SWS = 8$

$$\Rightarrow \frac{\text{Max. Sequence No.} + 1}{2} \geq 8$$

$$\Rightarrow \text{Max. Sequence No.} \geq 15$$

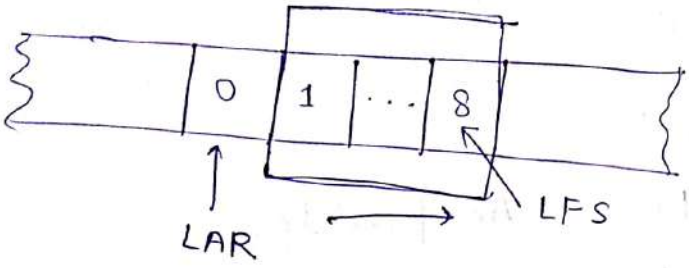
$$\text{no. of bits} = \log_2(15) = \log_2(\text{Max. Sequence No.})$$

Scanned by CamScanner



✡ Sliding Window Protocols →

At Sender



Algorithm

For SWS, sender will maintain following variables -

(a) Sequence No.

(b) SWS → Size of Sender's window (buffer)

(c) LFS (Sequence No. of Last frame Sent)

(d) LAR (Sequence No. of Last ACK received)

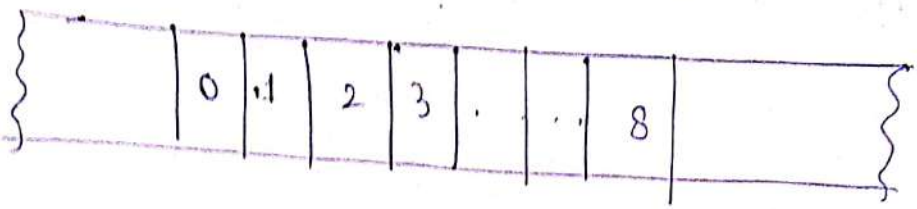
(1) Transmit frames untill (LFS − LAR) ≤ SWS.
~~so sender~~

(2) After each transmission, increament LFS, on receipt of ACK, ~~implement~~ increament LAR.

Scanned by CamScanner

* Sender will retransmit the frame if ACK is not received within timeout.

At receivers



RWS = Receivers Window Size
LFS = Seq. no. of Last Frame Acceptable
NFE = Seq. no. of Next Frame Expected.

Sequence no. represented

SeqNoToAck → This variable represents seq. no. of out of order received.

* Receiver can receive

$$LFA - NFE + 1 \leq RWS$$

Algorithm

* Frame arrives with sequence no., if seq. no. is within receiver's window, then accept else discard. (Which means sequence no. is $\leq$ LFA and $\geq$ NFE)

if (SeqNo. $\leq$ LFA && Seq.No. $\geq$ NFE)
then accept else discard.

Scanned by CamScanner

* If SeqNo. = NFE, then send ACK and set NFE = NFE + 1;

* If SeqNo != NFE
  Stop sending ACK.
  then set SeqNo.To Ack = Seq.No.

for e.g. Let NFE = 2 SeqNoTo Ack = 5

then Seq.No = 5

* Once all frame with sequence no.
  SeqNo < SeqNoTo Ack received
then Send ACK with value
  SeqNoTo Ack (Cummulative ACK)

Set NFE = SeqNoTo Ack + 1

and LFA = SeqNoTo Ack + RWS

Advantages

* Order of data is ensured.
* Loss of data is cared.
* Sliding Window is reliable of communication.
* It will ensure the flow control.

Scanned by CamScanner

RWS = 1 Stop and Wait Protocol

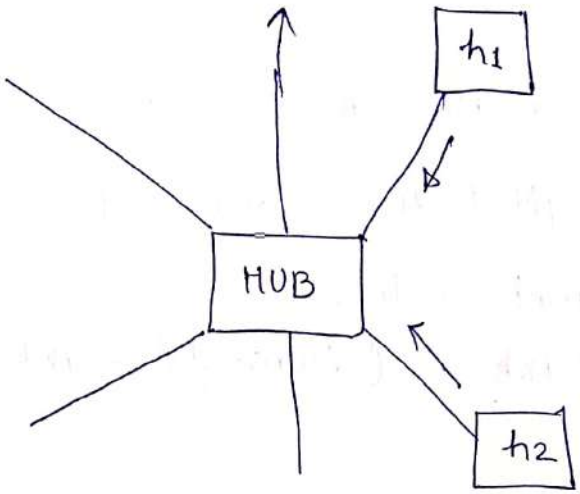
SWS = RWS In general

SWS < RWS No meaning

✡ Medium Access ~~Protocols~~ Control

* Requires in multipoint network. (Shared Network)

broadcast type

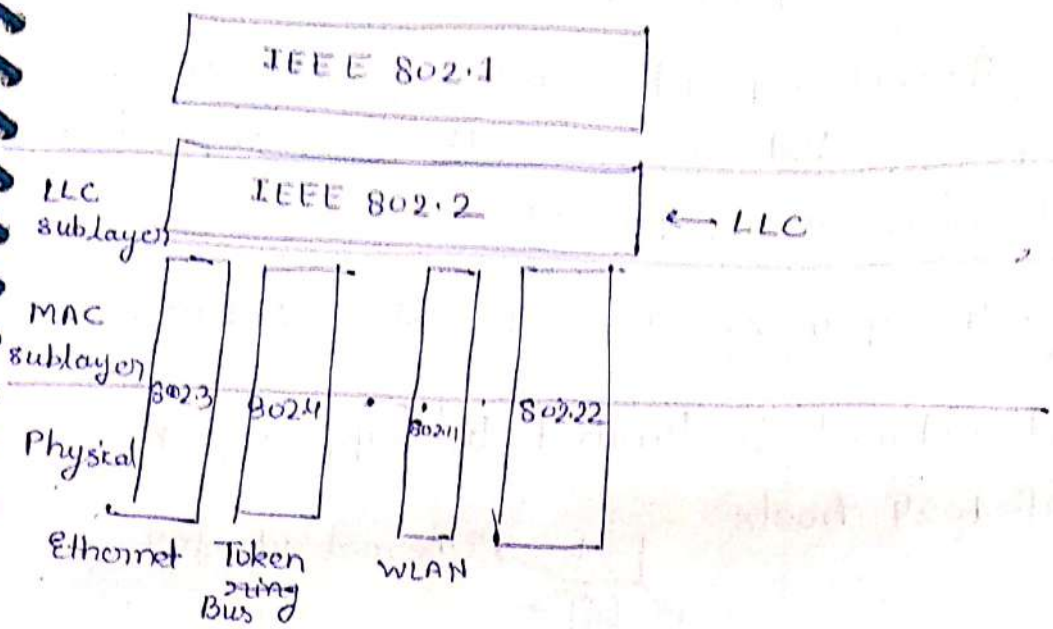


* MAC is nothing but Regulatory Mechanism to use the medium by host.

(1) MAC sublayer is only used in shared network for eg. Ethernet, WLAN, Cellular System etc.

(2) 802.1X Standard has covered the whole idea of different MAC options.

Scanned by CamScanner



802.15 → PAN
802.16 → WiMAX

SIG = Special Interest Group.

Ethernet

(1) Physical

* Each ethernet segment can be upto 500 m long of 50Ω coaxial cable.
* Post tab into cable of connection and should be 2.5 m apart from each other.
* Bus topology ~~is~~ should be used for deployment of network.
* Transceiver should be capable of detecting weather the ~~like~~ link is idle or busy.
* Transceivers are implemented in ethernet.
* Signal placed on the link are broadcast in network.

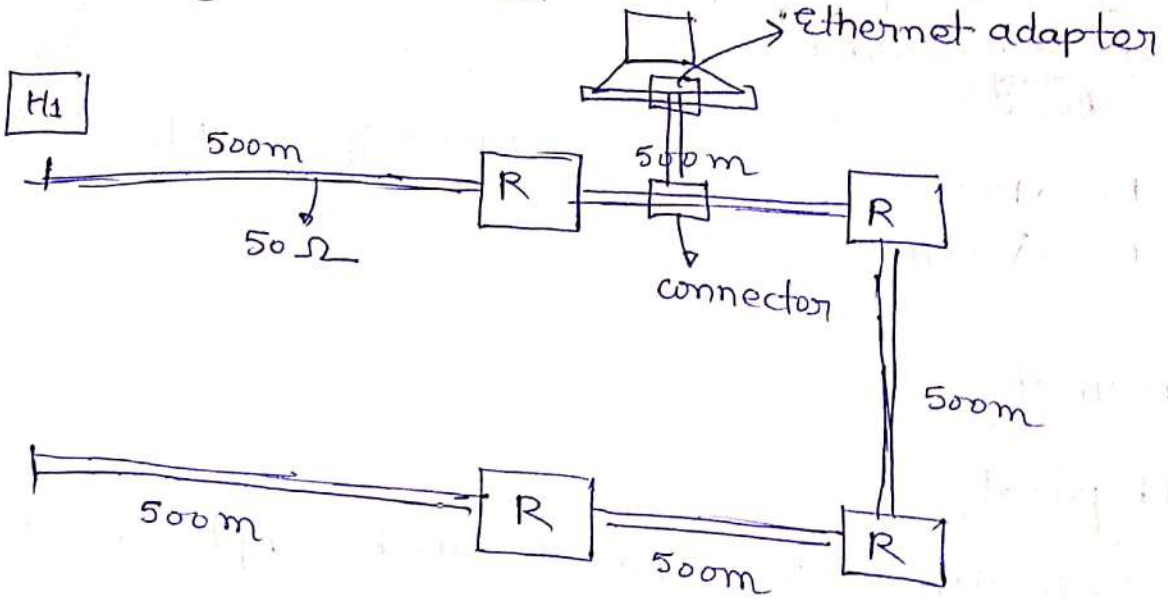
Scanned by CamScanner

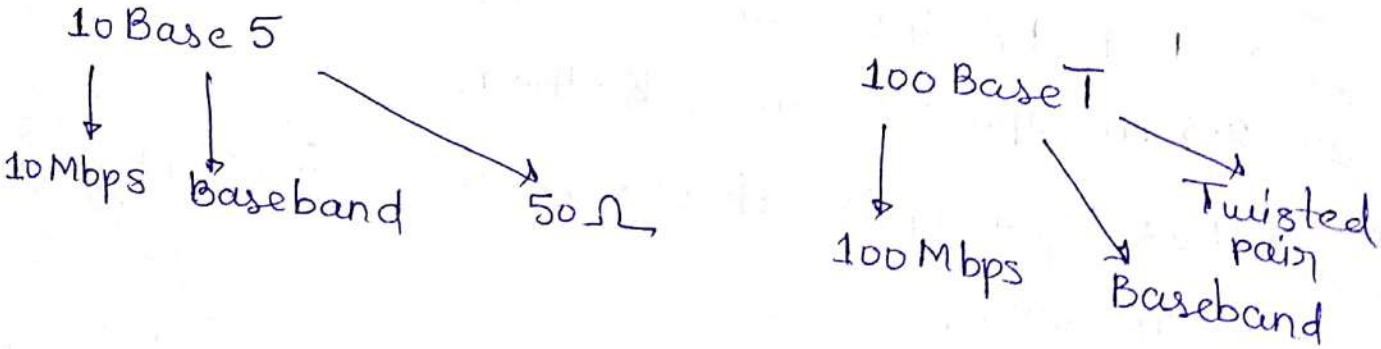
* Manchester encoding is used.

* Multiple ethernet segments can be joined by the use of repeaters but not more than 4 repeaters can exist between any pair of host.

* Limiting the span of ethernet upto 2.5 km.

* Ethernet network is limited to support a max of 1024 hosts.

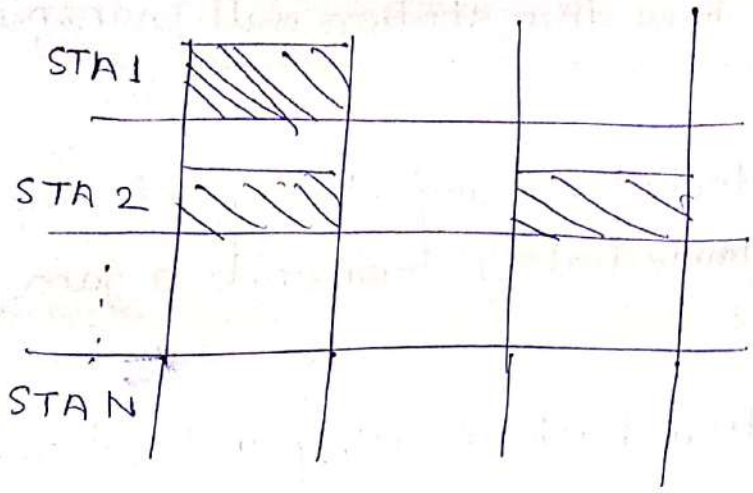




Scanned by CamScanner

✡ Slotted ALOHA →

≅ 33% bandwidth utilized bandwidth is acheived by using Slotted ALOHA.



(1) MAC protocol is known as 1-persitence CSMA/CD with binary exponential backoff where 1-persistance means

CSMA/CD

CS → All nodes are able to determine when the link is idle or busy.

MA → Multiple access means multiple nodes can transmit their data at any point of time on shared link.

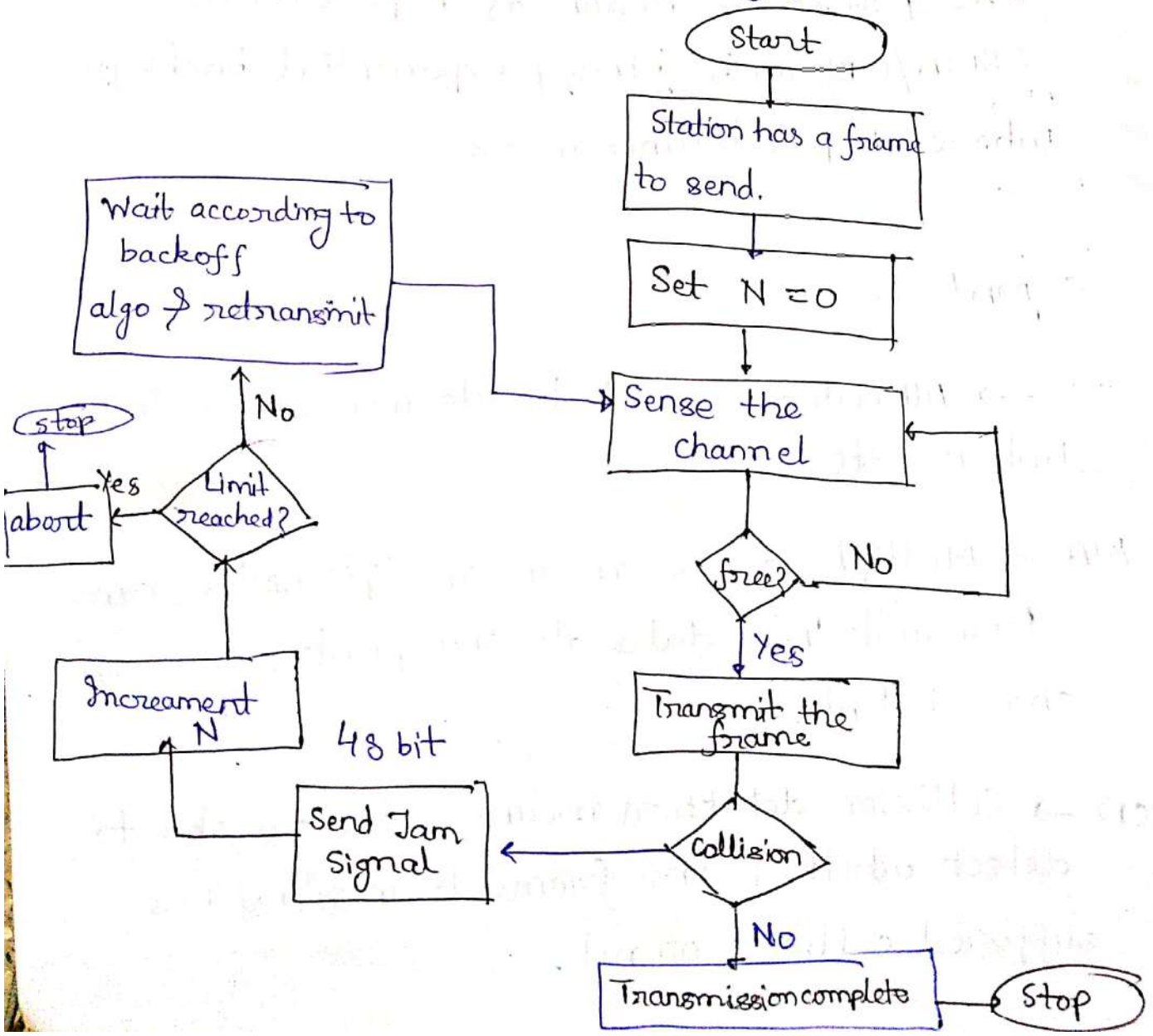
CD → Collision detection means nodes are able to detect whether the frame transmitted has suffered collision or not.

Scanned by CamScanner

Date - 12/09/19

MAC protocol

* Whenever a station has frame to send, it senses the channel.
* If the channel is free, then station will transmits otherwise wait.
* If collision is detected by any station of the network, then it immediately transmit a jam signal.
* On collision station backoff using a local counter and try retransmission accordingly.



Scanned by CamScanner

N = maximum no. of retransmission.

$N_{max} = 16$

✡ Backoff algorithm

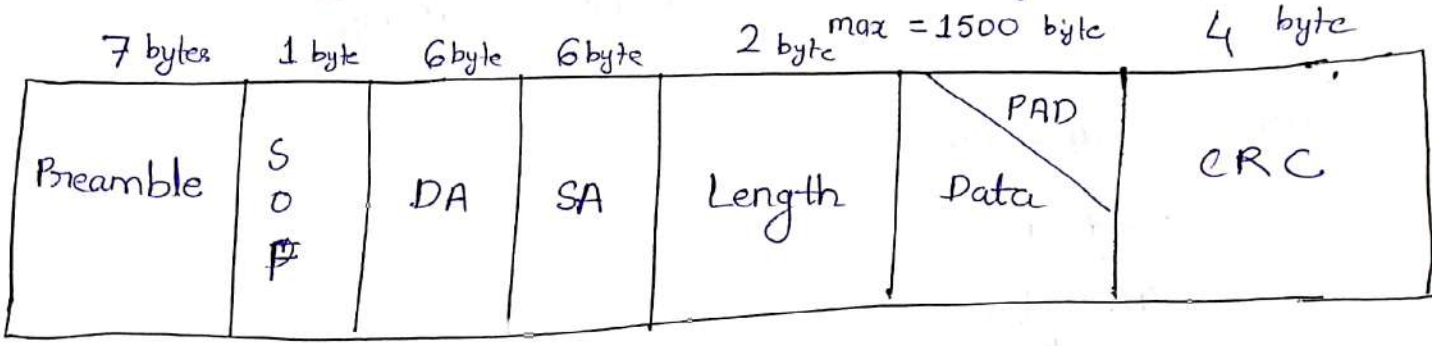
Binary Exponential Back off algorithm

* Upon collision, the sending station increaments local counter Q. The backoff interval is randomly selected using uniform distribution over L where $L = 2^K$ Slots.

* K is initially set to 0.

✡ Frame Format of Ethernet →

min = 46 byte
max = 1500 byte



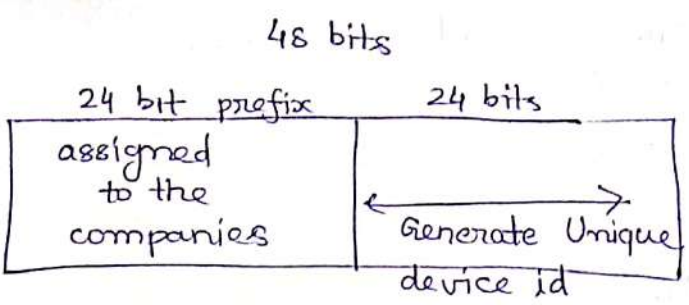
SOF = Start of frame.

MTU = Maximum Transfer Unit ⩽ 1500 byte

48 bit address (6 bytes) → (Globally Unique Address)

→ Mac MAC address
→ Physical address
→ NIC → Network Interface Card
→ Global address

Scanned by CamScanner



IEEE 802.3

min = 46
max = 1500

7 bytes	1 byte	6 byte	6 byte	2 byte		4 byte
Preamble	SOF	DA	SA	Type	data / Pad	CRC

RTT = Round Trip Time

for 10 Mbps Ethernet

RTT = 51.2 μsec

∴ Data = 51.2 × 10 = 512 bits = 64 bytes.

min = 64 − (6+6+2+4)

= 64 − 18

= 46 bytes

MAC address

ipconfig → Windows
Ifconfig → Linux

2A : 46 : 3C : 49 : 5E : 6F

Presentation notation.

0100110 . . . . 01 → Network representation

48 bit

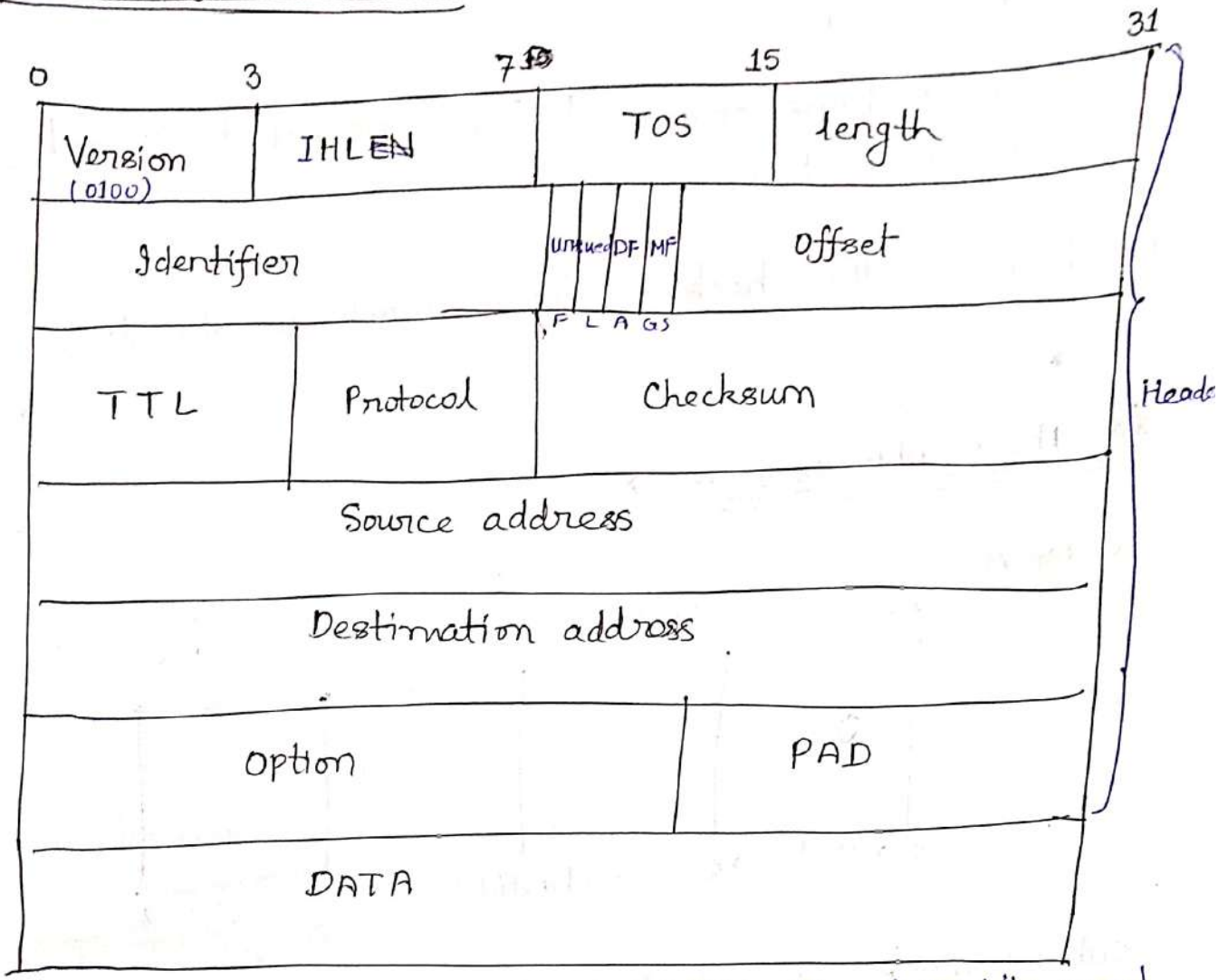
Scanned by CamScanner

Network Layer

→ IPv4 → 32 bit address
→ IPv6 → 128 bit address
} logical address

* IPv4 is used to define the network and to distinguish network.

Header of IP packets →



IHL = No. of 32 bits word in the header.

Length = No. of bytes in IP packets.

Types of services (TOS)
→ min delay
→ max throughput
→ reliability
→ low cost.

Scanned by CamScanner

Date- 23/09/19

Example 4450 bytes IP packet

F1	Id = X	MF = 1	offset = 0
F2	Id = X	MF = 1	offset = 1500
F3	Id = X	MF = 0	offset = 3000

If DF = 1, further fragmentation is not done.

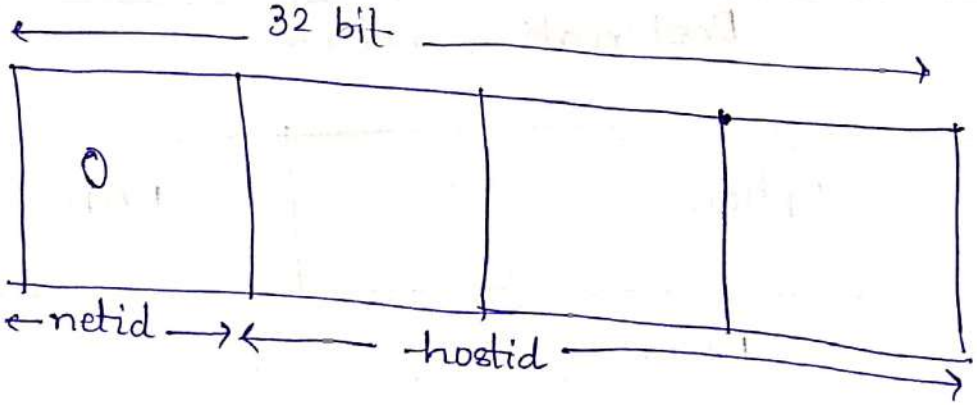
TTL = Time to Leave

= No. of hops required for a packet to reach its destination.

Checksum → This checksum is used only for header.

IPv4 addresses →

Class A



subnet mask = 255.0.0.0

netid = IP && subnetmask

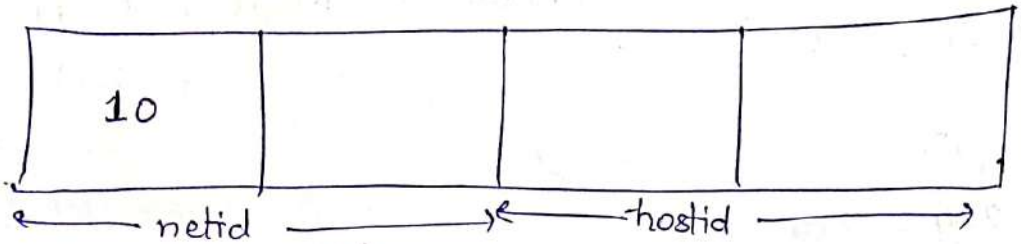
Scanned by CamScanner

Range 0 — 126

00000..0
01111...

127 is defind as a special address (loopback)

Class B

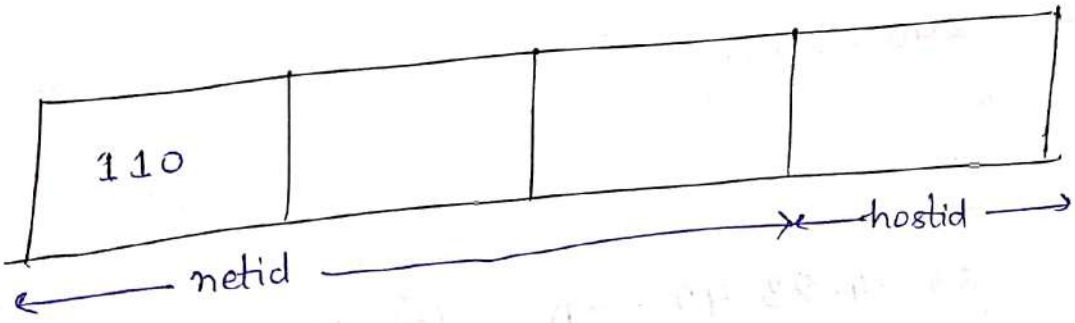


Subnet Mask = 255.255.0.0

Range = 128 — 191

100....0
1011...1

Class C



Subnet mask = 255.255.255.0

Range = 192 - 223

1100...0
1101...1

Scanned by CamScanner

Class D

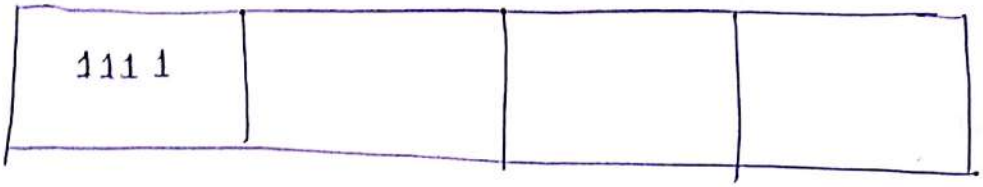
* Class D addresses are known as Multicast IP addresses.

Range 224 – 239

1110 0
11101 1

Class E

Reserved IP addresses



Range- 240 – 255

---

① 63.24.23.49 → A

(2) 64.25.28.36 → A

(3) 63.29.28.47 → A How many networks are there?

(4) 129.69.68.29 → B

⑤ 129.68.69.27 → B

⑥ 129.69.39.28 → B

(1)

net

(2)

(3)

(4)

(5)

6

Scanned by CamScanner

(1) 63.24.23.49

netid = 255.0.0.0 & 63.24.23.49 = 63.0.0.0

(2) netid = 64.0.0.0

(3) netid = 63.0.0.0

(4) 129.69.0.0

(5) netid = 129.68.0.0

(6) netid = 129.69.0.0

① & ③ belongs to same network as network 1.

Similarly ④ & ⑥ belongs to same network as network 3.

There there are four different networks.

* 63.255.255.255 (destination IP) → Broadcast packet

↳ Every host has to accept this packet and processed in network.

Scanned by CamScanner

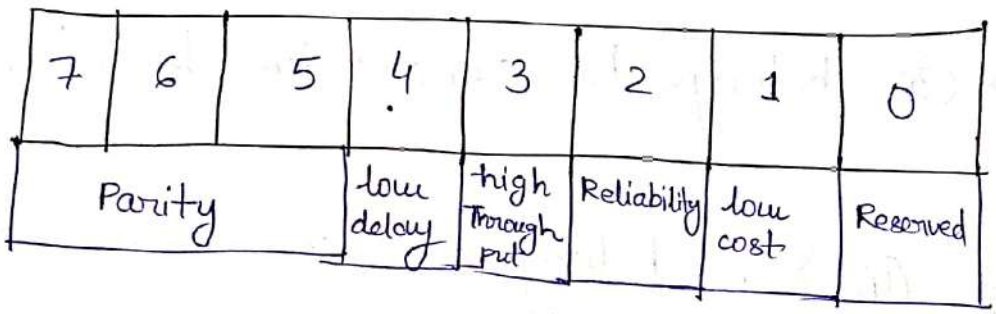
63.0.0.0 also reserved and used for management purpose.

✡ Loopback address →

The IP specifies a loopback network with the IPv4 address ~~172~~. 127.0.0.0/8.

The most commonly used IP address on the loopback network is 127.0.0.1 for IPv4 and ::1 for IPv6

✡ TOS (Types of Services)



✡ Subnetting

(RFC 917)

(RFC 950) Variable Length Subnetting Mask

Scanned by CamScanner

Date - 26/09/19

Public IP ⇒ Private IP

↓ ↓

on the internet With in the organisation

↓

Subnet

e.g. 172.16.0.0 B - class.

Default Subnet Mask = 255.255.0.0

DSM

netid = IP && DSM

Subnetid = IP && UDSM

Rest of the bits = hostid

000 00000 . 00

000 11111 . 11

Subnetid	Start IP	End IP
172.16.0.0	172.16.0.0	172.16.63.255
172.16.64.0	172.16.64.0	172.16.127.255

* Router support is required for subnetting.

Scanned by CamScanner

Example

netid = 192.27.26.0

A = 70 host 1

B = 64 host 00 → 255.255.255.128

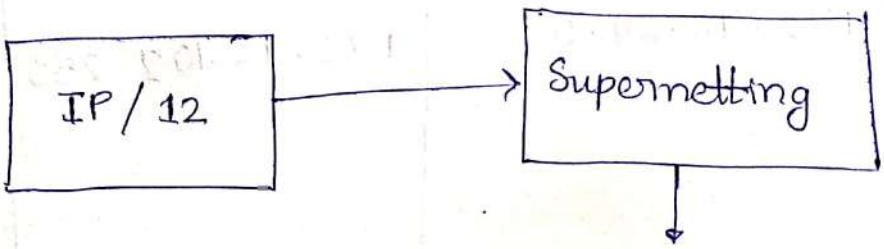
C = 32 host 010 → 255.255.255.0

D = 28 host 011 → 255

Here VLSM is used.

Classless IP address →

These IP addresses are used in backbone network



To represent set of networks as one element

↓

To reduce the no. of entries in the routing table.

Scanned by CamScanner

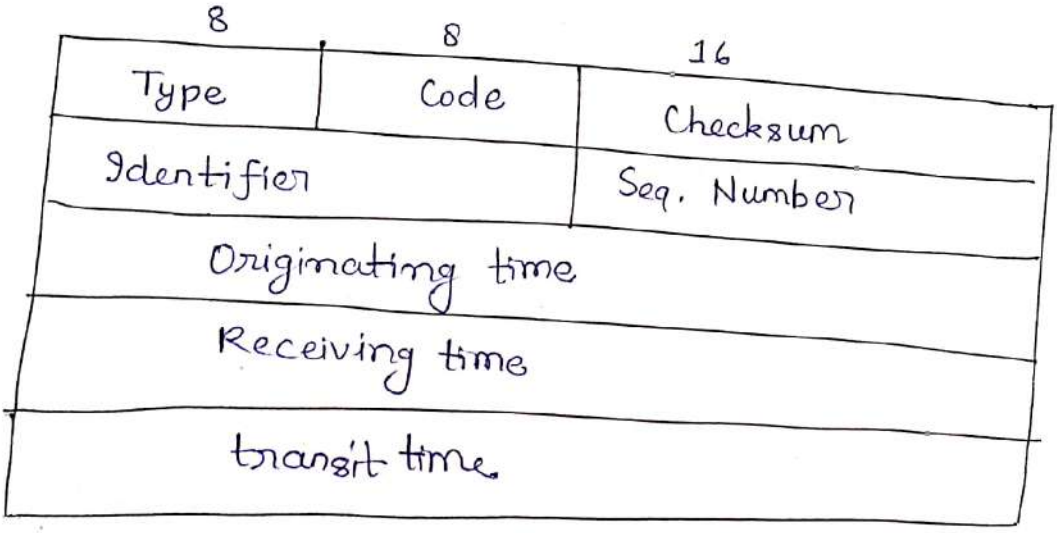
Routing table

Destination net id	next hop
172.0.0.0/16	X

ICMP (Internet Control Messaging Protocol)

→ Also known as error reporting protocol.

Packet format



Code	meaning
0	Network unreachable
3	Port unreachable
4	Fragmentation needed if DF = 1

Type	meaning
0	echo reply
3	destination unreachable
4	source quench
11	time exceeded.
:	:

Scanned by CamScanner

✡ Router ⇒ Interface Id

(1) IP is assigned to the interface and not the device.

(2) Router is a device which is having multiple interfaces and each interface is connected to a different network.

Scanned by CamScanner

✡ Routing protocol and forwarding algorithm

To create, update and maintain the routing / forwarding table

Take a packet out from the queue and forward it on appropriate interface.

forwarding Algorithm

If [netid of destination equal to netid of one of the interface, then deliver the packet to the destination over that interface) ~~as if~~ else if netid of the destination is in the routing table then deliver the packet to the next hop else, deliver the packet to the default ~~hop~~ router.

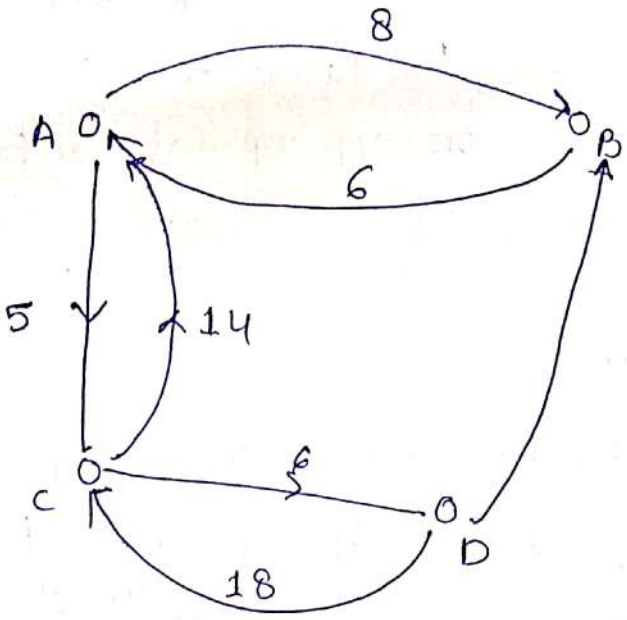
✡ Routing Protocols ⟶

* The routing protocol are representing network as graph G(V, E) where routers represent set of vertices and link between routers are represented as set of edges.

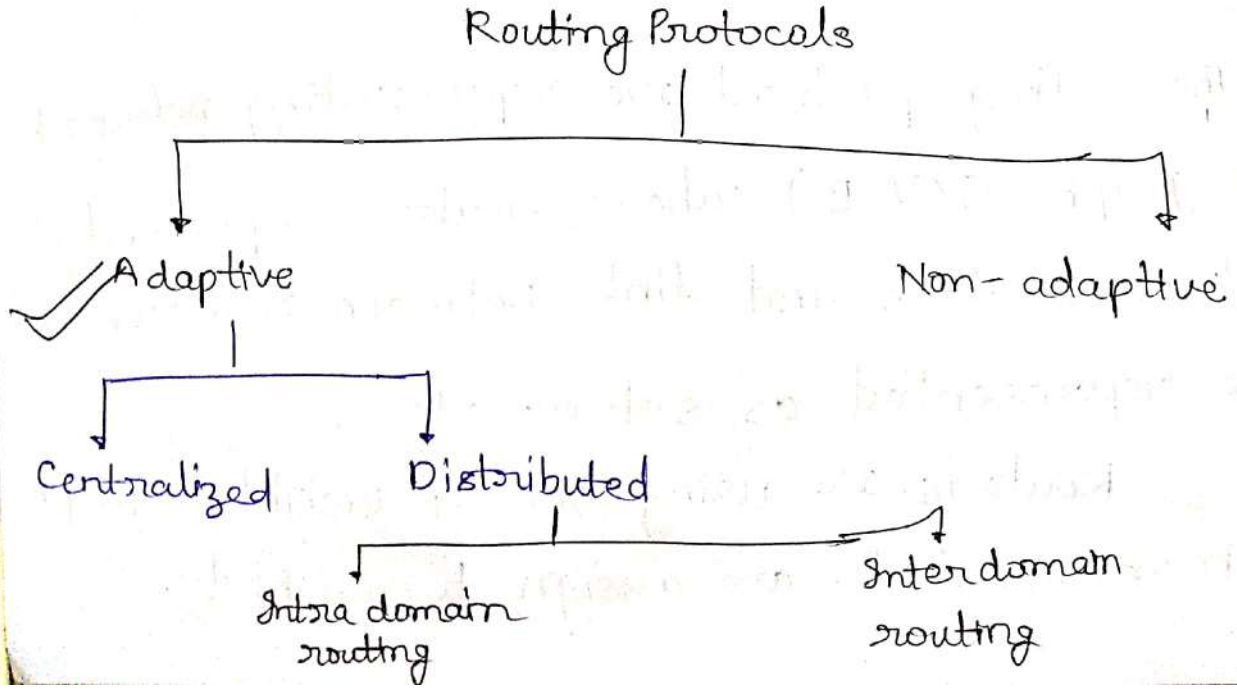
Routers are using set of weighted graph which means links are assign to weightet.

Scanned by CamScanner

They are also using directional graph wherein weights can be different on two direction of same link.



A domain is a set of networks managed by one administrative entity. Domains can also represented by domain id (32 bits)



Scanned by CamScanner

30/09/19

Intra-domain routing

- Distance Vector (RIP)
  - Routing Information Protocol V_1 & V_2
  - → Use distance vector routing algorithm.
  - → periodic update interval = 30 sec
- Link State [OSPF]

Inter domain routing

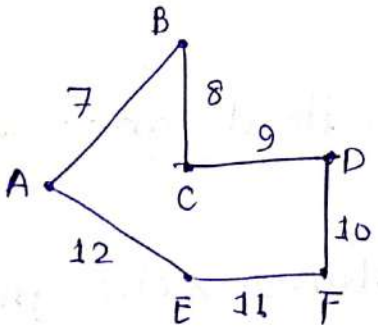
- Link State [OSPF]
- Path vector (BGP)

✡ Distance Vector Algorithm

(1) Historically known as old ARPANET routing algorithm, as ~~the~~ well as Bellman-Ford algorithm.

→ Each router maintains it's ID (IP address).

→ It also maintains list of neighbours and its cost.



for D

C	F
9	10

Scanned by CamScanner

Distance Vector

Destination	cost
A	0
B	x
C	y
D	z
:	:

Reachability to itself = 0

Unreachable nodes = ∞

Routing Table

Present	cost	Next hop	timer

Algo

→ Each router transmit its distance vector to its neighbours.

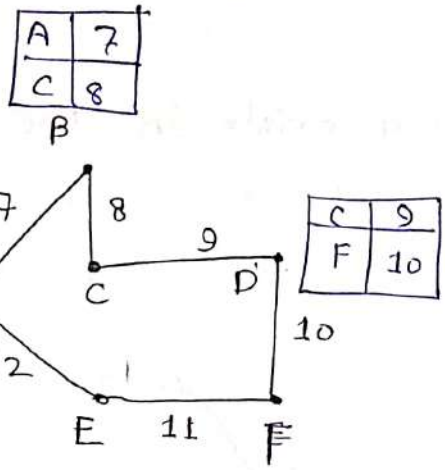
→ Each router recalculate its distance vector when —

(a) It receives distance vector from its neighbour containing different information.

Scanned by CamScanner

(b) If discover the topology change.

→ On receipt of distance vector, each router determine the min cost path for a destination and add that entry in the routing table.



A	
B	
E	
D	
F	

Advantages of DV →

(1) [redacted].

(2) Overload is ~~load~~. low.

(3) Good information propagate very fast.

* 20 bytes are allocated to create distance vector.

Scanned by CamScanner

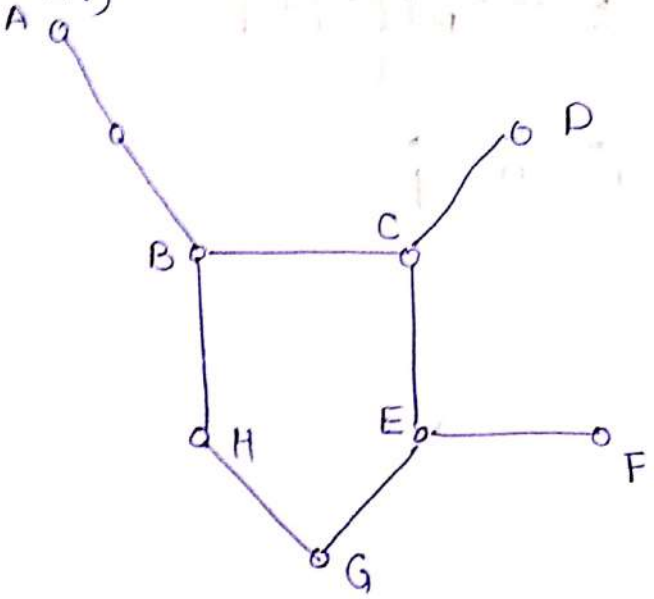
Disadvantages ⟶

(1) bad information may never converge (or take too long time to converge)

(ex. count to infinity

(2) Routing loops may exists in the network.

(Because every node take decision based on the local information)



Solutions (Used with RIP protocol)

(1) Max hop count = 16

(2) Split Horizon with poisson reverse.
(also eliminate two level loop)

(3) triggered entry. update.

Scanned by CamScanner

Date - 14/10/19

✡ Link State Routing Protocol →

* In link state routing, each router do the following —

(1) Discover it neighbours and learn their network address.

(2) Measure the cost to all its neighbours.

(3) Create Register the packet containing all information and call it LSP (link State Packet)

(4) Send this packet to all other routers to network using reliable fading.

(5) Every router will construct a local topology of the network using information of LSPs.

(6) Compute shortest path to all the other destinations using local topology and apply ~~extra~~ Dijikstra algorithm for finding shortest path for each destination.

(7) Create the routing table using next hop router in the shortest path.

Scanned by CamScanner

Dijkstra Algorithm

→ Initially mark all nodes except source with infinite distance and a blank.

→ Set working node = source node and sink node = destination node.

→ While

Working node ≠ sink node

(1) Mark working node as permanent node

(2) Examine all adjacent nodes

If the sum of label of working node + cost to the adjacent node ≱ the current label distance

then re-label the distance on adjacent node with the cost +

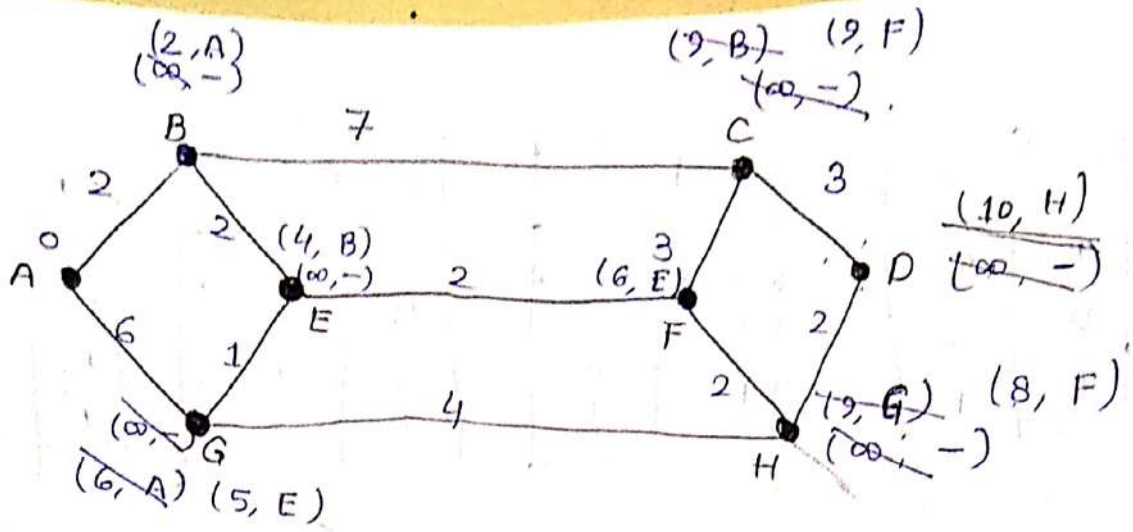
(3) Examine all the nodes, except permanent nodes and mark the smallest labelled node as permanent node.

(4) Set working node = permanent node.

While

reconstruct the path back from sink to source

Scanned by CamScanner



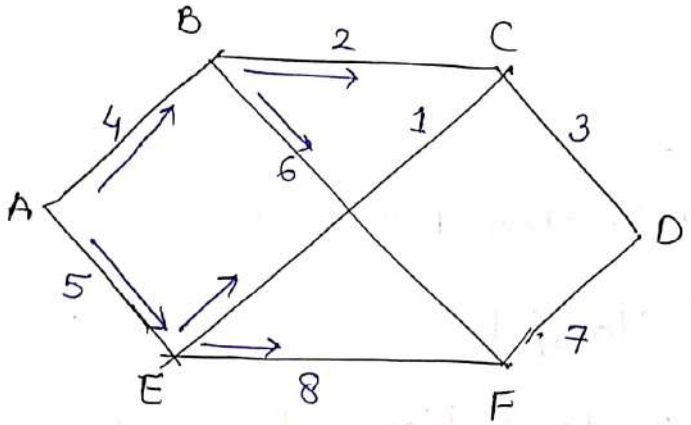
for A to D

Working Node = ~~A~~ ~~B~~ ~~E~~, ~~G~~, ~~F~~ ~~H~~ D

Sink Node = D

D → H → F → E → B → A

Link State Algorithm



LSP

A	
Age	
Seq No.	
B	4
E	5

← (How long this information is valid)

← to track recent info. and avoid duplicate

B	
Age	
Seq No	
A	4
C	2
F	6

Scanned by CamScanner

C	
B	2
D	3
E	1

D	
C	3
F	7

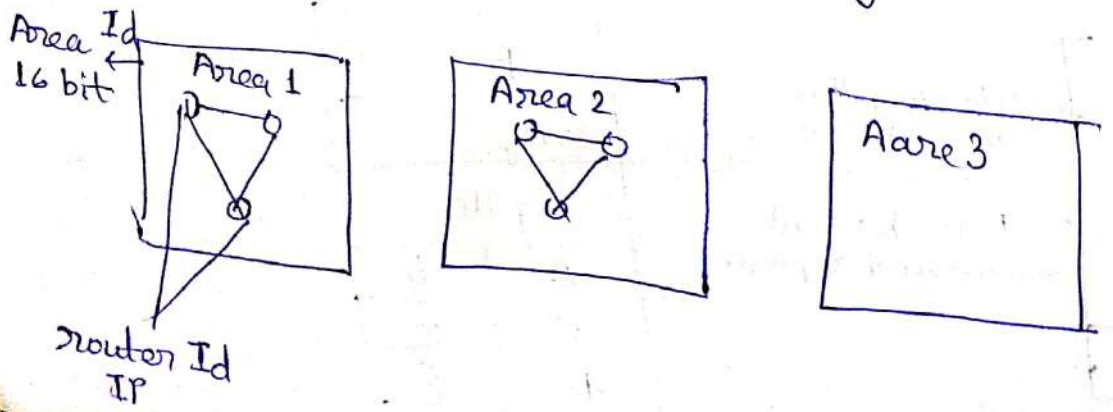
E	
A	5
C	1
F	8

F	
B	6
E	8
D	7

✡ OSPF (Open Shortest Path First)

(1) Classless / Classful

(2) Maintain 2 level hierarchy in the network.



Scanned by CamScanner

(3) Send broadcast on any change or after 30 min.

(4) LSP are reffered as LSA (Link State Advertisement)

OSPF maintain 3 -tables

(1) Neighbour table
(2) topology table
(3) Routing table.

Note → 5 different types of LSA are used by OSPF

(1) Router LSA
(2) Network LSA
(3) Network summary LSA
(4) ASBR summary LSA
(Autonomous System Boundary Router)
(5) External LSA

Scanned by CamScanner

Date- 21/10/19

BGPv4 (Border Gateway Protocol)

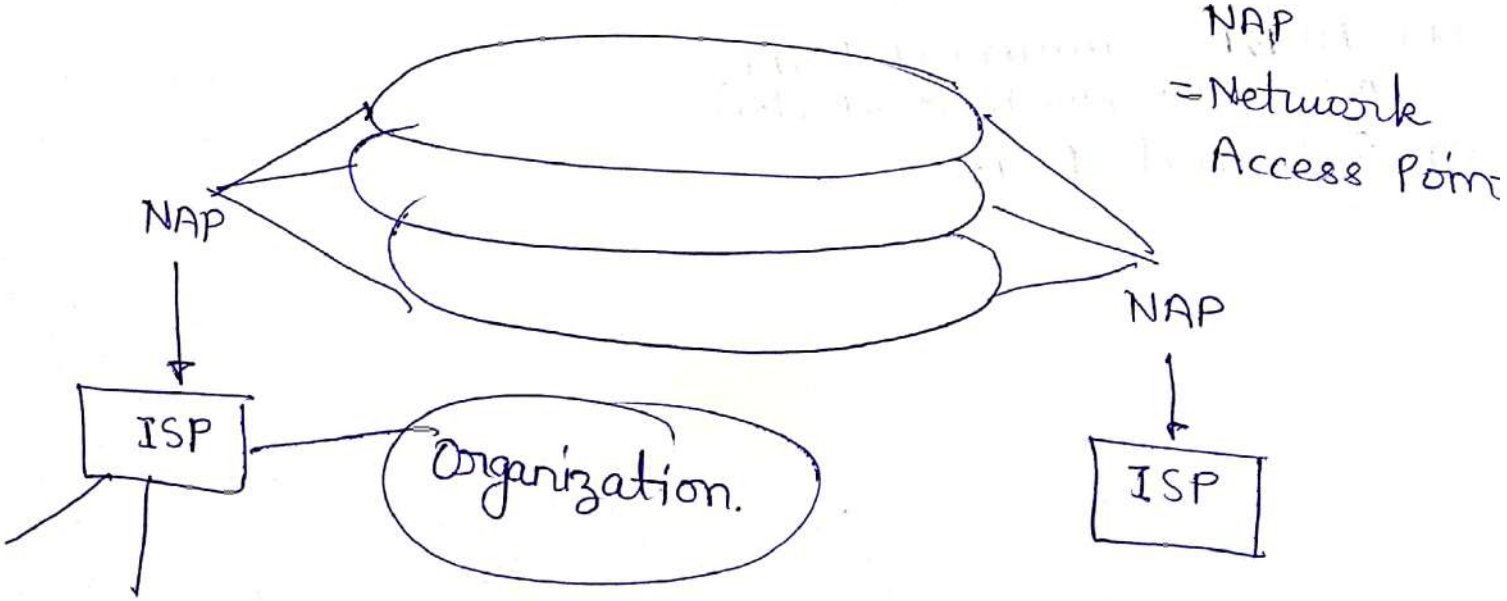
→ It operates as path vector routing.

→ Also similar to distance vector routing.

Path vector

destination	Path	Next hop	Cost

CIDR → Class less Inter Domain Routing



NAP
= Network
Access Point

Scanned by CamScanner

Transport Layer

* It provides connection oriented services which is relible service by TCP protocol.

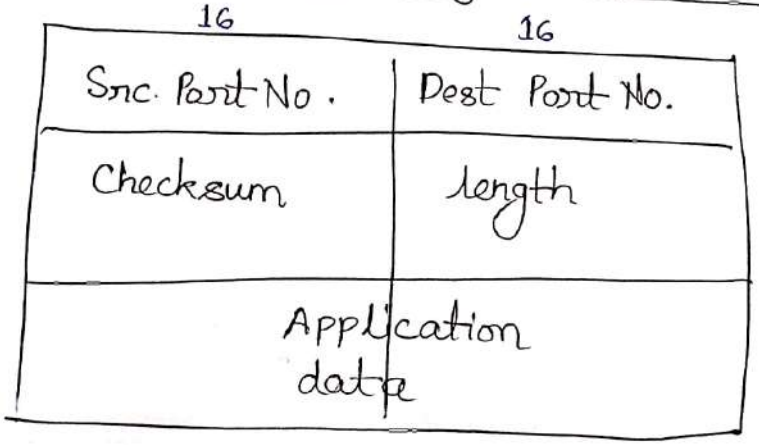
* Extends the unreliable service of the n/w layer (UDP).

* Providing port number (16 bit)
  (multiplexing and demultiplexing of data stream)

* Every socket should provide unique port no.)

* Congestion Control

UDP (User Datagram Protocol) →



* It is the simplest transport layer protocol,

* It is simply extends the underlying best effort data delivery services of network layer to application layer.

Scanned by CamScanner

* It adds source port no. and dest. port no. in the header to recognize a socket in a host.

* Checksum is used for error checking.

* Length is used to determine no. of bytes in application layer.

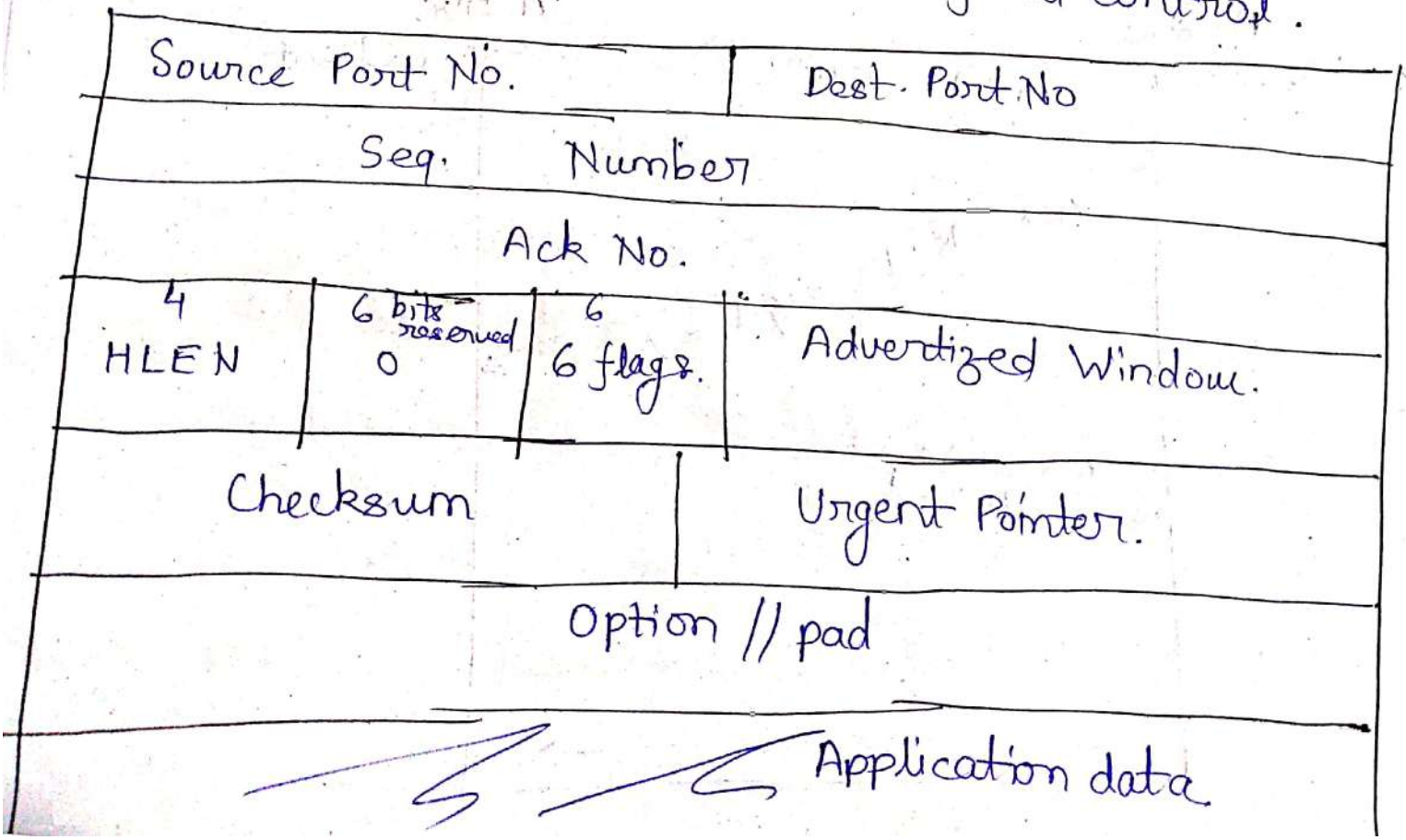
Scanned by CamScanner

Date - 31/10/19

Transport Layer

TCP Header

* TCP provides connection orientation which means it requires an explicit connection establishment and closing phase.
* TCP is connection oriented and byte oriented protocol.
* TCP provide full duplex communication.
* TCP uses adaptive timeout mechanism.
* TCP also provide congestion control.
* TCP provides end to end flow control.



Scanned by CamScanner

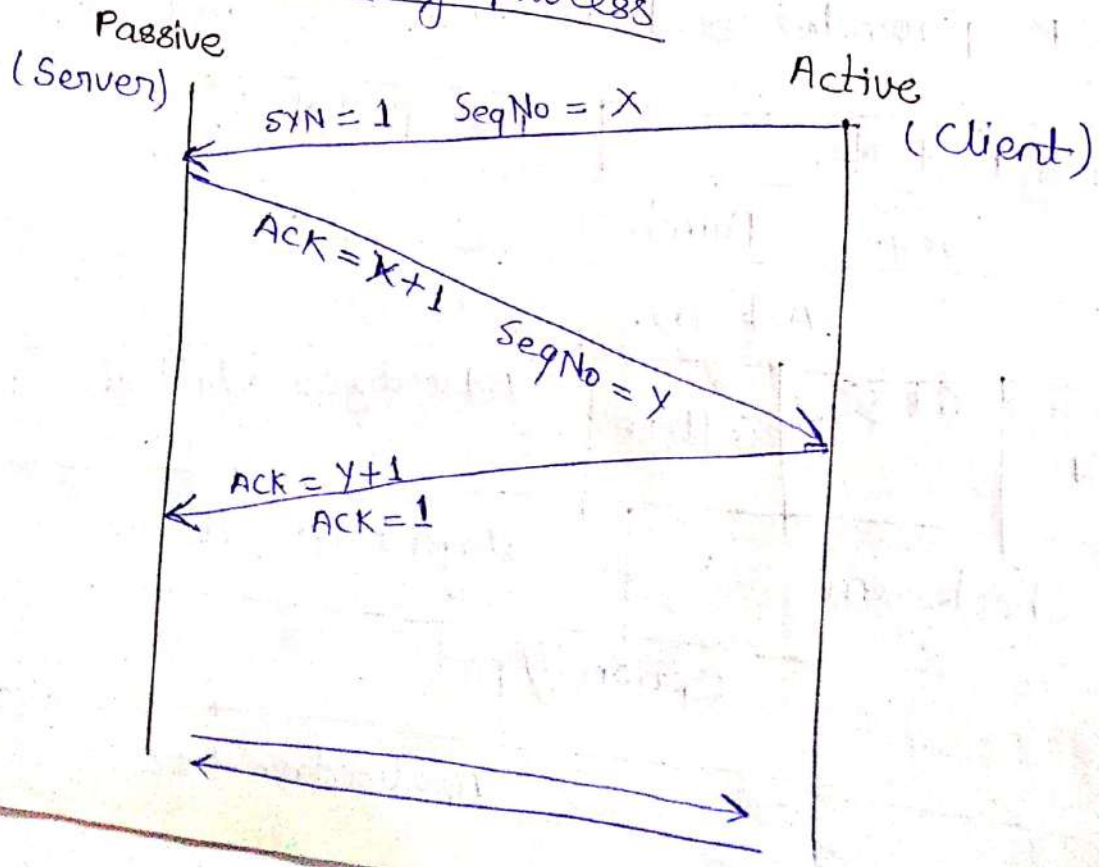
* Seq No., Ack No., Adevertize window is used to implement flow control. (Sliding Window Protocol (SWP

Flags

(1) URG → Urgent Pointer
(2) ACK → Acknowledgement.
(3) PSH → Push
(4) RESET
(5) ~~SINK~~ SYN → Synchronization
(6) FIN → final.
(Used for terminating the connection)

* Connection establishment in TCP

3-Way handshaking process

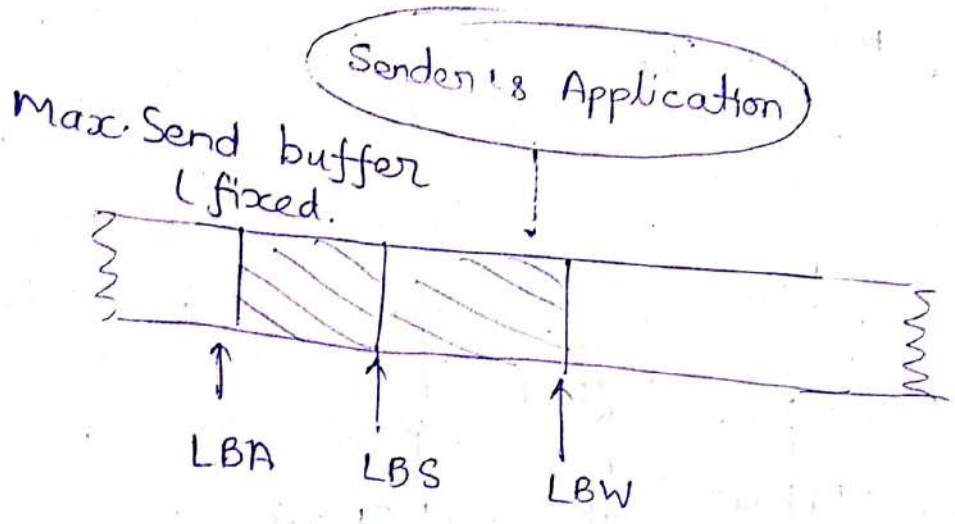


Scanned by CamScanner

(Source port No., Source IP
Dest. Port No., Dest. IP) → provides unique TCP connection.

✡ Flow control by TCP using SWP →

(1) The same SWP protocol as discussed in data link layer will be used by TCP with following changes —



* Rather than using a fixed window size, receiver uses variable window size.
* Two buffers are maintained —
  (a) Max send buffer
  (b) Max receive buffer

Scanned by CamScanner

* It add' source port no. and dest. port no. in it header

* Checks

* Length applica

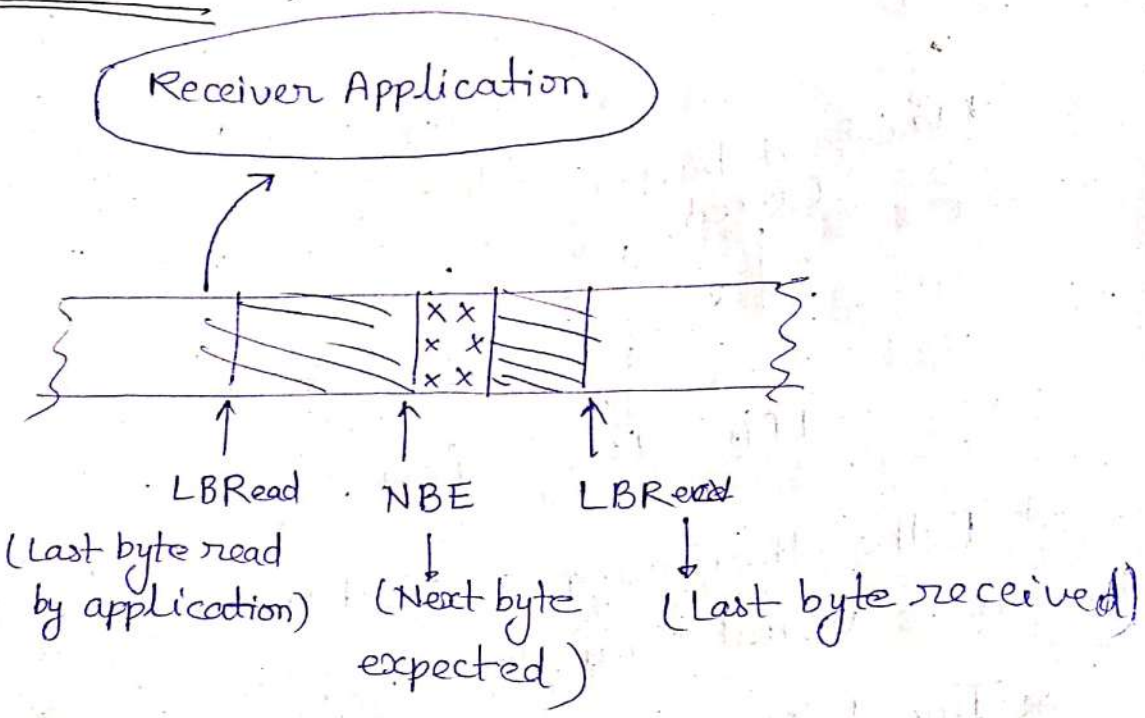
* Sender maintains three variables

(a) LBA → Last byte Ack.

(b) LBS → Last byte Send

(c) LBW → Last byte written by

Receiver's Process →



* Receiver receive data if too [LBRecvd (last byte received) − LBRead] ≤ Max. receive buffer.

* Then it compute advertize window.

Advertize window = Max. receive buffer − (LBRecv − LBRead)

Scanned by CamScanner

Effective Window = AdvertizeWindow − (LBS − LBA)

* Sender can subsequently send effective window amount of data.

MSS = Max. Segment Size.

* TCP uses adaptive timeout for the segment it sent.

* The idea is take a running average of RTT and then compute the timeout value as the fraction of RTT.

Estimated RTT_n

$= \alpha$ * Estimatted RTT_{n-1} + $(1-\alpha)$ Sampled RTT_{n-1}

$\alpha = 0.8$ or 0.9

Timeout for n^{th} segment

$= 2.$ Estimated RTT_n

Case 1

estimated = 10 s Sampled = 8 s, $\alpha = 0.8$

⇒ Estimatted $RTT_n = 9.6$ s

Scanned by CamScanner

port no. and dest. port no. Date 03/11/19

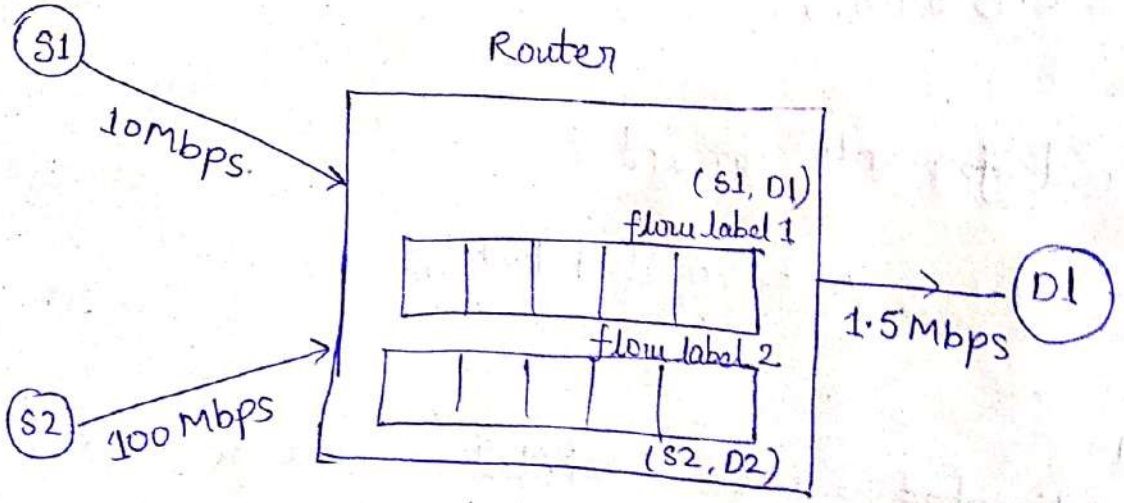
case-2

Advantages of SWP

* SWP provides reliable and gaurenteed delivery of data.
* Seq. No. ensures order of data.
* Advertize window enforce flow control.
* One more window is used with TCP protocol known as congestion window which will be used for congestion control.

✡ Resource Allocation and Congestion Control

Network Layer



Scanned by CamScanner

Weighted Fair Queuing →

* To provide equal share of resources to every user at every router, it is required to transmit bit-by-bit data from every flow in round-robin fashion.
* This scheme can be emulated using weighted fair queuing algorithm.

Algorithm Step →

(1) Suppose clock fix each time a bit is transmitted.

(2) Let P_i denotes the length of packet i

→ S_i denotes the time at which packet P_i start getting transmitted.

→ F_i denotes the time ~~with~~ when packet i finish its transmission. A_i = Arrival time

$$F_i = S_i + P_i * t$$

(unit time)

i denotes any packet from any flow.

$i = 1, 2, 3 \ldots\ldots$ for every incoming packet.

Scanned by CamScanner

... and dest. ...

When router will start transmitting packet?

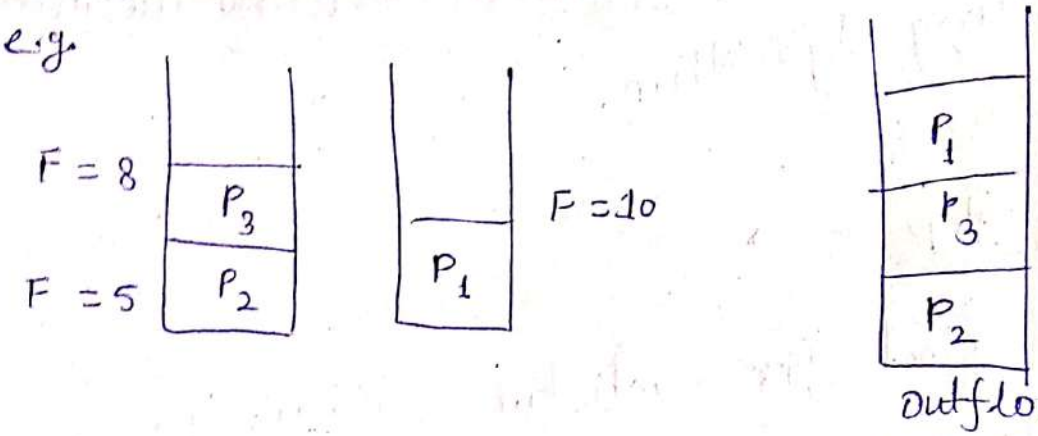
A_i ← when no packet in queue

f_{i-1} ← when packets are waiting in queue

then

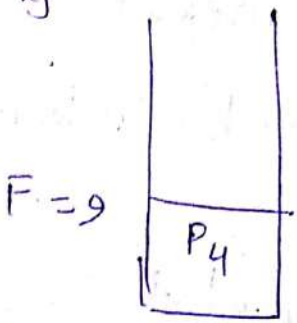
$$F_i = Max(F_{i-1}, A_i) + P_i * t$$

e.g.



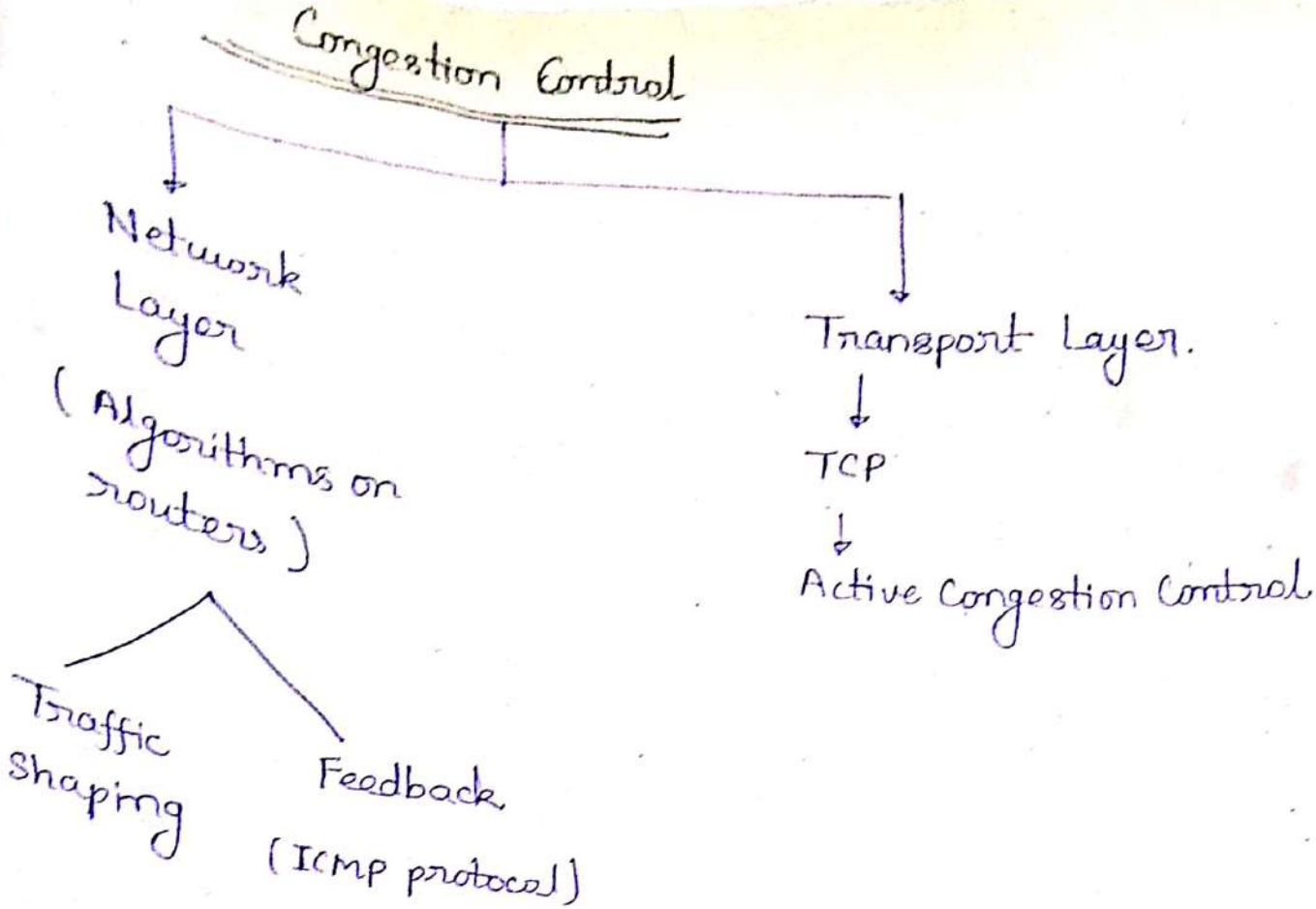
non-primitive

But if



It has to wait, and will be transmitted only after P_1.

Scanned by CamScanner



Congestion avoidence (Proactive)
Congestion Control (Reactive)

Scanned by CamScanner