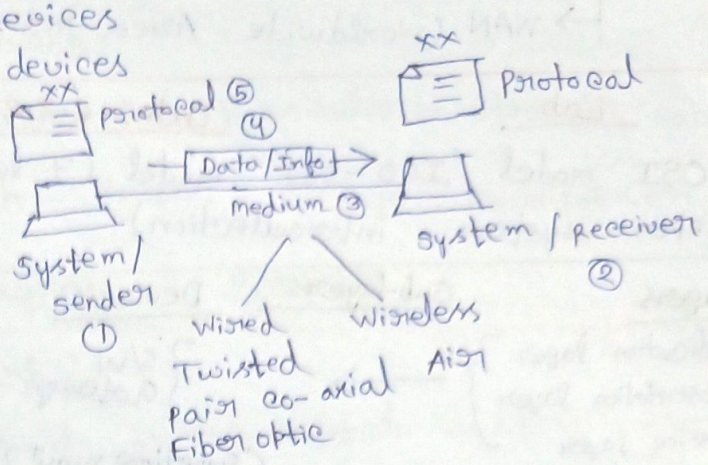
Computer Networks

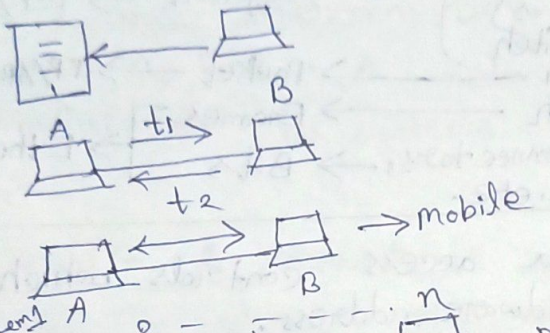
Date:- 5.8.24

* Connectivity between devices
* Communication between devices
* Resource shearing
* Security



Data Flow

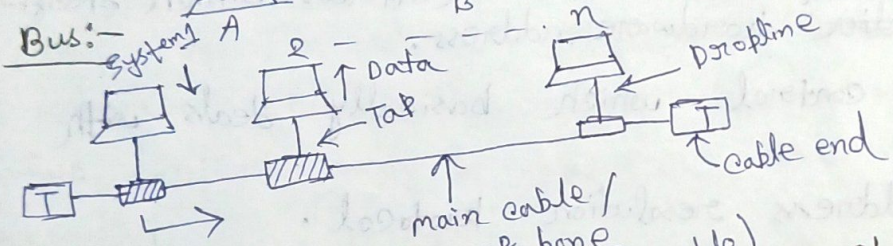
→ Simple
→ Half Duplex
→ Duplex / Full Duplex



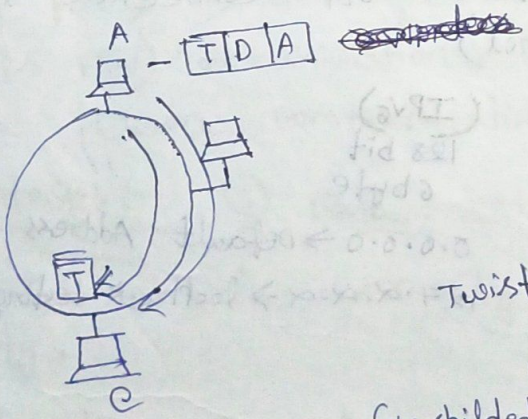
Physical Topologies

→ Bus
→ Ring
→ Star
→ mesh
→ Hybrid / Tree
→ wireless

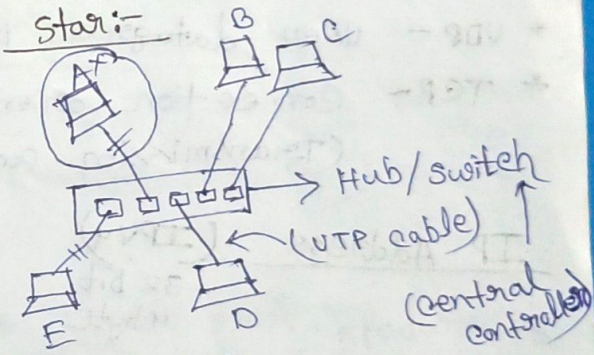
Bus:-



Ring:-



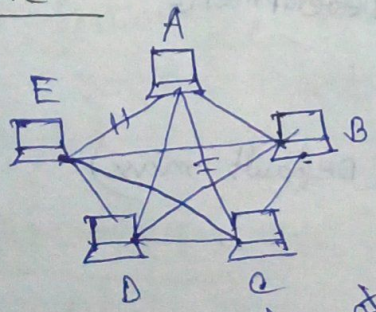
Star:-



Twisted Pair cable

UTP (unshilded) STP (shilded)

mesh:-

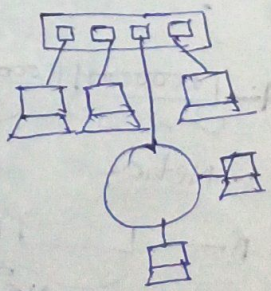


$\frac{n(n-1)}{2}$

n = no. of systems

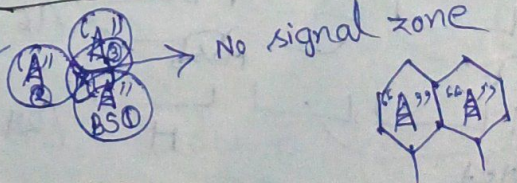
Hybrid / Tree:-

Star +



wireless

Handoff management



Catagories of N/w –

- LAN (Local Area Network) (few Km / 10 Km)
- MAN (metropolitan Area Network) (100 Km)
- WAN (worldwide Area Network) (world wide)

Lab **Date:- 6.8.24**

OSI model / ISO-OSI model (7 layer) (open system intercallection)

TCP/IP (5 layer) 4 layer

Layers	Sub-layers	Devices	Data format	Protocol
⑦ Application layer, ⑥ Presentation layer	→	S/W Gateways	S/W Gateways / Application	FTP, HTTP, SMTP, Pop3 etc
⑤ Session layer				
④ Transport layer	→	(sometime may be uses) L4 switch	→ segment	→ TCP / UDP
③ Network layer	→	Router	→ Packet	→ IP/ARP / RARP
② Data link layer	MAC LLC →	Switch	→ Frames	→ Ethernet
① Physical layer	→	Ports, Connectors, Mux. etc.	→ Bits	→ Ethernet

* Full form of MAC – deals with media access controls which specifically ~~build~~ ~~medior~~ hardware address.
* LLC – Logical link control which basically deals with logical address.
* RARP – Reverse address resolution protocol.
* UDP – User datagram protocol.
* TCP – Connection oriented, UDP – Connection less (Transmission control)

IP Address

(IPV4) 32 bit 4 byte

(IPV6) 128 bit 6 byte

- class A → 0 – 127
- class B → 128 – 191
- class C → 192 – 223
- class D → 224 – 239 → multicasting
- class E → 240 – 255 → Research & Development

0.0.0.0 → Default Address

127.x.x.x → loopback testing Address

class A – Netid | Hostid /8 (Default mass)

class B – Net | Host /16

class C – Net | H /24

Private IP Add (Any organization IP Add)

A: 10.0.0.0 → 10.255.255.255

B: 172.16.0.0 → 172.32.255.255

C: 192.168.0.0 → 192.168.255.255

* Similar types – Cross cable & Dissimilar – Straight cable

Assignment – Hub, Switch, Router, Bridge, multiplexer

Defination, working diagram & principle

---

① What is computer network?

⇒ A network is a group of interconnected systems sharing services, and interconnecting by means of a shared communication, link. A network therefore requires two or more individual systems with something (data/information) to share.

② Protocal:- A protocol is a set of rules that governs data communications. It represents and agreement between the communicating devices. Without a protocol two devices may be connected but not communicating.

③ Need or advantages of networking:-

(i) Sharing files, (ii) Sharing resources, (iii) sharing programs & Backups, (iv) communication; (v) connectivity, (vi) Improve person to person communication.

Disadvantages:- (i) Data crashes (cable fault., failure of server etc), (ii) Data security, (iii) privacy, (iv) cost or complexity.

④ Characteristics of Data communication system:-

(i) Delivery, - The data should be delivered to the correct destination. It should reach only the intended user and not to any other.

(ii) Accuracy- The system must deliver the data accurately.

(iii) Timelines:- For the audio & video data the system

should deliver the data in a timely manner.

⑤ Direction of Data flow:-

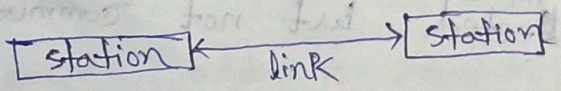
(i) Simplex - In simplex mode the communication is unidirectional, as on a one way street. only one of the two devices on a link can transmit the other can only received.
Ex:- Keyboard

(ii) Half Duplex - In Each station can transmit & received capabilites, but not at the same time. when one device is sending the other can only receive.

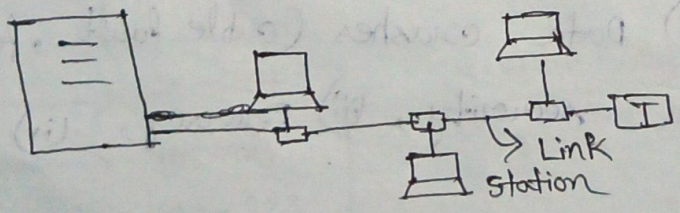
(iii) Full Duplex / Duplex:- In full duplex mode, both station can transmit and received simultaneously.

⑥ Type of Connection:-

(i) Point to point connection:- It provides a dedicated linked between two devices. The entire capacity of the link is reserved for transmission between those two devices.



(ii) multipoint connection:- A multipoint connection is one in which more than two specific devices share a single link. In a multipoint environment the capacity of the channel is shared.



⑦ Server:- A server is a computer program or device that provides a service to another computer program and it's user. (server is a service provider)

⑧ Client:- Client is any computer hardware or software device that request access to a service provided by a server.

* After installing the client software this will called network / work station.

(9) **Workgroup** – In a logical group of computer work with a peer to peer then it's called workgroup.

(10) **Domain:–** In a logical group of computer work with a client server then it's call Domain.

* MAC Add: AB : 8·A : – – – – – –
XX : XX : XX : XX : XX : XX
OUT (organizationally Unique Identifier) → other values (this should be unique)

Date:- 12.8.24

Analog Signal

FDM (Frequency Division multiplexer)

WDM (web)

nxm

Data Signal

TDM

Time Division

A B C D

MUX

De-mux

(Time slot Interchange)

TSI

A – 3
B – 1
C – 2
D – 4

A B C D

B C A D

FT

This field for error checking purpose

H | Preamble | DA | SA | Type | Data | FCS / CRC

Minimum size of ethernet Frame is = 64 byte
Maxm is = 1518 byte

8by | 6by | 6by | 2by | Upto 1500 by | 4by

18 byte
Data – 46 byte
1500 + 18 = 1518 byte

General Ethernet Frame

* FCS – Frame check sequence, CRC – cylic redundancy check.

A P S T N D P

D
H D
H P
H D
H D
H D T

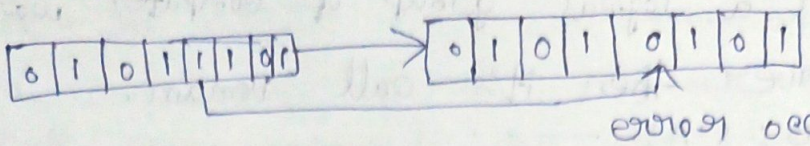
Data
H Data
H Data

H T

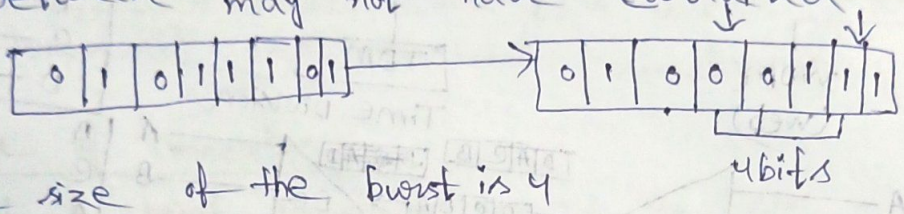
(11) **Types of errors:–** Depending on the number of bits in error we can classify into two types –

(i) **Single bit error** – This term suggest that only one bit

in the given data unit such as byte is in error. This means that only one bit will change from one to zero & zero to one.



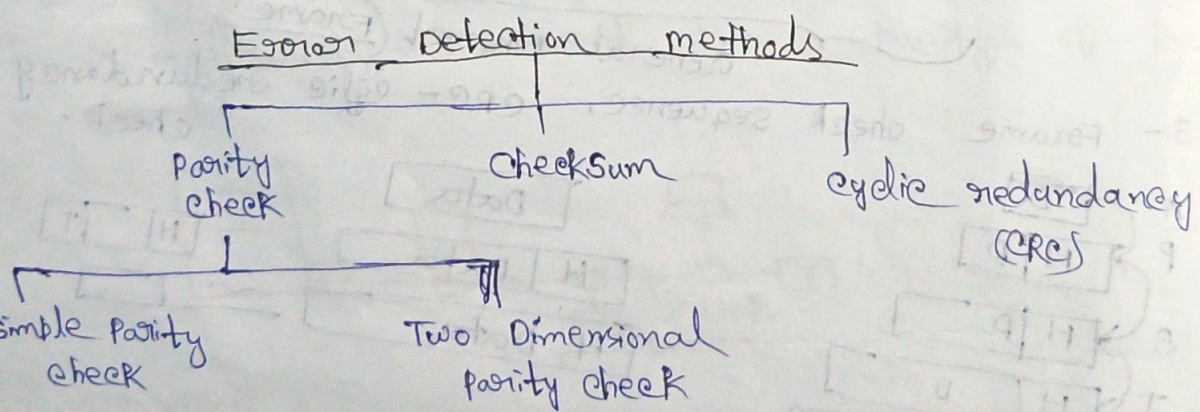
(ii) **Burst Error:-** If two or more bits from a data unit such as a byte change from one to zero or from zero to one then burst error are occurd. The length of the burst is measured from the first ~~product~~ corrupted bit to the last corrupted bits. Some of the bits in between may not have corrupted.



The size of the burst is 4

(12) **Code word:-** The code word is the small n bit encoded block of bits. It contain messages or data bits and parity bits or redundant bits.

(13) **Redundancy:-** Error detection uses the concept of redundancy which means adding extra bits for detecting errors at the destination.



LAB

Date:- 13.8.24

Straight cable (for connect dissimilar type of parts)

Left		Right
① white/green	⟷	① white/green
② Green	⟷	② Green
③ white/orange	⟷	③ white/orange
④ Blue	⟷	④ Blue
⑤ white/Blue	⟷	⑤ white/Blue

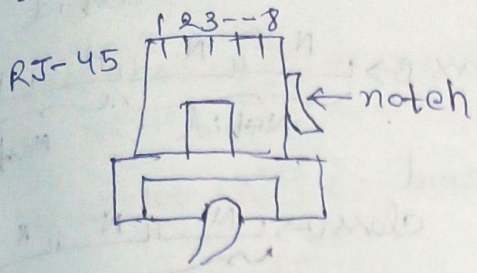
(UTP cable)
cat 5, cat 5e, cat 6, cat 6e etc
Connector used
RJ-45 (for 4 pairs) [Register jack]
RJ-11 (for 2 pairs)

⑥ orange ⟷ ⑥ orange

⑦ white/Brown ⟷ ⑦ white/Brown

⑧ Brown ⟷ ⑧ Brown

Defination, Diagram, How to construct



Cross cable

Left	Right
① white/green TX+	① white/orange (TX+)
② Green TX−	② orange (TX−)
③ white/orange RX+	③ white/Green (RX+)
④ Blue	④ Blue
⑤ white/blue	⑤ white/Blue
⑥ orange RX−	⑥ Green (RX−)
⑦ white/Brown	⑦ white/Brown
⑧ Brown	⑧ Brown

(UTP cable)

cat5, cat 5e, cat6, cat6e etc

Connector used

RJ-45 (for 4 pairs)

RJ-11 (for 2 pairs)

Router Startup

Power on

↓

POST

↓

Boot strap loader (os)

↓

Loads Ios file from flash to RAM

↓

Looks for startup config in NVRAM

No → Configure the Router through auto setup → Router> (user executive mode)

Yes → Loads it to RAM → Configure the Router → Router> (user-Exec. mode)

Router Components

① Post (Power on self test)

② Bootstrap loader (os loading)

③ ROM

④ EEPROM (Flash) → contain IOS file ↑ Internetwork OS

⑤ NVRAM → contain startup config file

⑥ DRAM

⑦ ROMMONITOR (ROMMON)

⑧ configaration Register → value stored in the configaration Register, control the booting sequence.

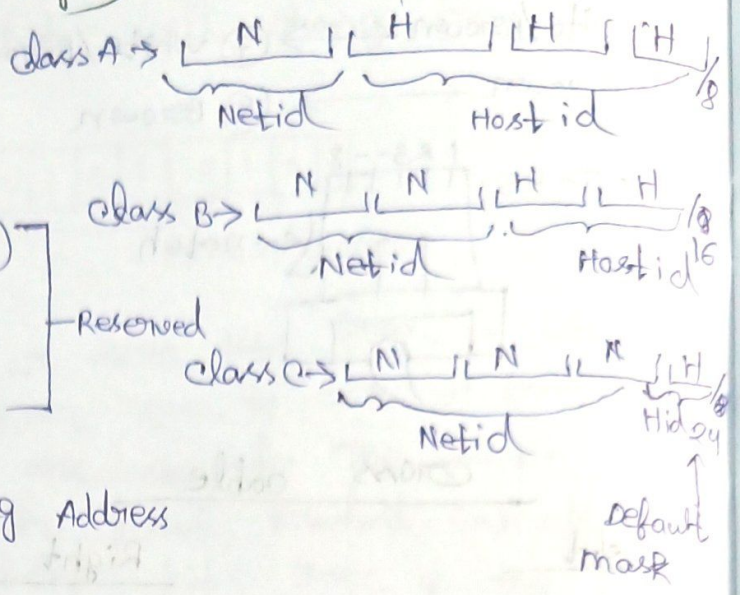
* If all host id are enable then it's called broad cast.

IPv4 Addressing (32bit / 4byte)

Class A → 0-127
Class B → 128-191
Class C → 192-223
Class D → 224-239 (multicasting)
Class E → 240-255 (Research & Development)

Reserved

0.0.0.0 → Default Address
127.x.x.x → Loop back testing Address



Private Address:

Class A: 10.0.0.0 – 10.255.255.255
Class B: 172.16.0.0 – 172.31.255.255
Class C: 192.168.0.0 – 192.162.255.255

* If default then it's called classfulled IP address.
If not " " " classless " "

* Q 192.168.100.0/24 required 4 subnets.
Find out, ① Net id of subnets.
② Subnet mask of the subnets.
③ Host range of the subnets.
④ Broad cast Add of the subnets.

⇒ $2^n - 2 \geq 5$ where, S = no. of subnets Req.
$2^n - 2 \geq 4$ n = no. of network bits is to the added
$2^n \geq 6$
$n = 3$

192.168.100.[000]00000 /24
N

192.168.100.[001]00000
N H

192.168.100.32 – 1st Net
192.168.100.33 – 1st host
192.168.100.62 – last host
192.168.100.63 → Broad cast

192.168.100.32/24 + 3 = 27

Q 192.168.100.0/24 Subnet required 2
Find out ① Subnet id of 1st subnet
② Subnet mask of the subnet
③ Host Range ④ B'cast Add

⇒ 192.168.100.00000000/24 → Given IP Add

$2^n - 2 \geq 5$

$2^n - 2 \geq 2$

$2^n \geq 4$

$n = 2$ →

192.168.100.[00]000000/24

192.168.100.[01]000000/24+2 = 26 – 1st subnet id

↑ Subnet mask

192.168.100.[01]000001/26 → 1st host id

192.168.100.[01]111110/26 → last host id

Q 172.16.0.0/16 Subnet Req = 70,

⇒ 172.16.0.00000000/16 → Given IP Add

$2^n - 2 \geq 5$

$2^n - 2 \geq 70$

$2^n \geq 72$

$n = 7$

172.16.00000000.00000000/16

172.16.[00000010].00000000/16+7 = 23 → 1st host id

N N N

172.16.00000010.00000001/23 → 1st host id

172.16.00000010.11111110/23 → last host id

172.16.00000011.11111111/23 → B'cast id

172.16.2.0/23 – 1st subnetid

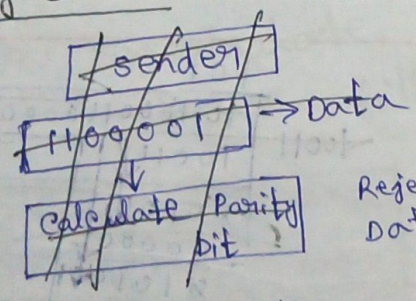
172.16.2.1/23 – 1st hostid

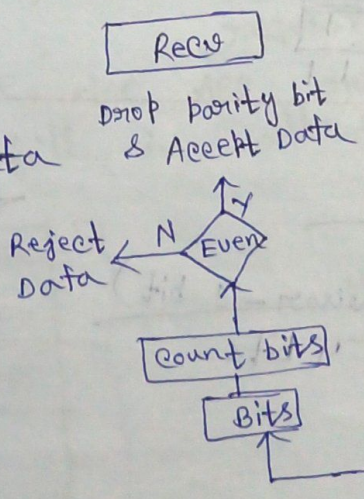
172.16.3.254/23 – last host id

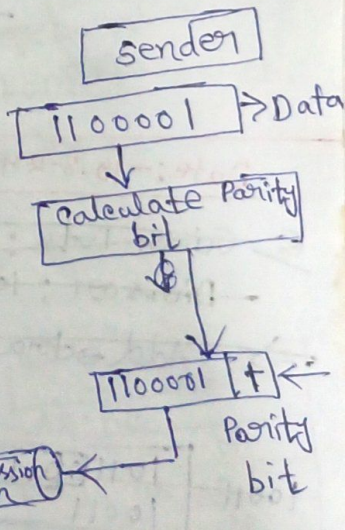
172.16.3.255/23 – B'cast id

Date:-18.8.24

Parity check







1110100 – Even (1's)

1010100 – odd (1's)

1101100

1000100

Two dimensional parity check

Data: 1100111 (A) 1011101 (B) 0111001 (C) 0101001 (D)

A ⟹

```
A → 1100111 | 1
B → 1011101 | 1
C → 0111001 | 0
D → 0101001 | 1
    ---------------
    0101010 | 1
```

Data Processing: 11001111   10111011   01110010   01010011
/ (codeword)

[01010101] Redundant Bits

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

CRC
(Generator)

Given Data: 100100
Divisor: 1101

Add extra bits: (Divisor − 1 bit)
= 4 − 1 = 3

```
          111101
1101 | 100100 [000]
       1101
       -----
       01000
        1101
       -----
        01010
         1101
        -----
         01110
          1101
         -----
      →   00110
           0000
          -----
           01100
            1101
           -----
      →     00[001] → Remainder
              [001]
               011
```

Polynomial Exp

Given Data: $x^7 + x^5 + x^2 + x + 1$

Divisor:
1 0 1 0 0 1 1 1
x^6 x^4 x^3

* $x^3 + x + 1$
1 0 1 1

Date:- 19.8-24

~~Q Given Data: 10110011~~
~~Divisor: 10011~~
~~Add extra bits: (Divisor − 1 bit)~~
~~= 4 bits~~

```
10011 | 10110011
        10011
        -----
        00101
```

```
             101
10011 | 10110011[0000]
        10011
        -----
        00101 0
         00000
        -----
         010100 1
          10011
         -----
          001110 1
            10011
           -----
            11110
```

Checksum

Given Data: 10101001   00111001

```
      10101001
      00111001
      --------
Sum:  11100010
CheckSum: 00011101
```

0 0 → 0
0 1 → 1
1 0 → 1
1 1 → 0 carry 1

So, ultimate data process: 10101001 00111001 00011101 (checksum)

* [H | Data | T] — H: Next layer Point out; T: Error checking purpose.

Date:- 20.8.24 LAB

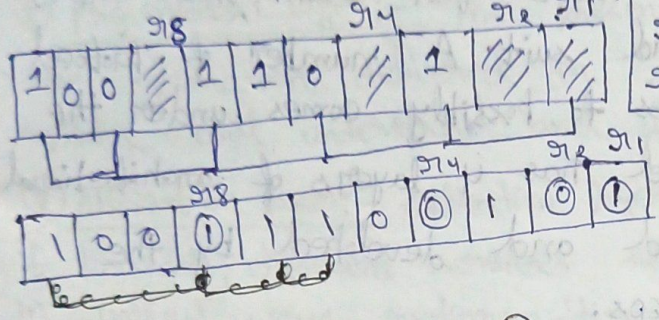
① Given IP address 10.0.0.0/8, create 12 subnets.

Theory

Hamming Code

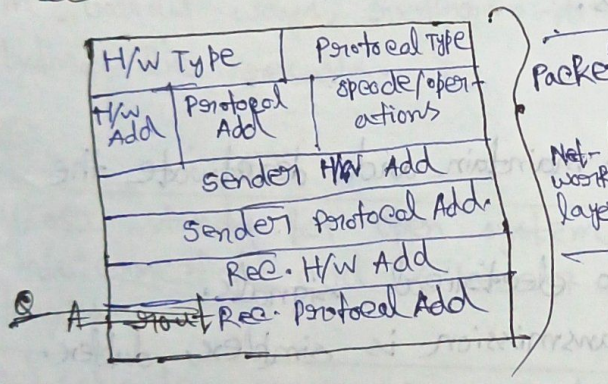
Data Bits: 10111 01

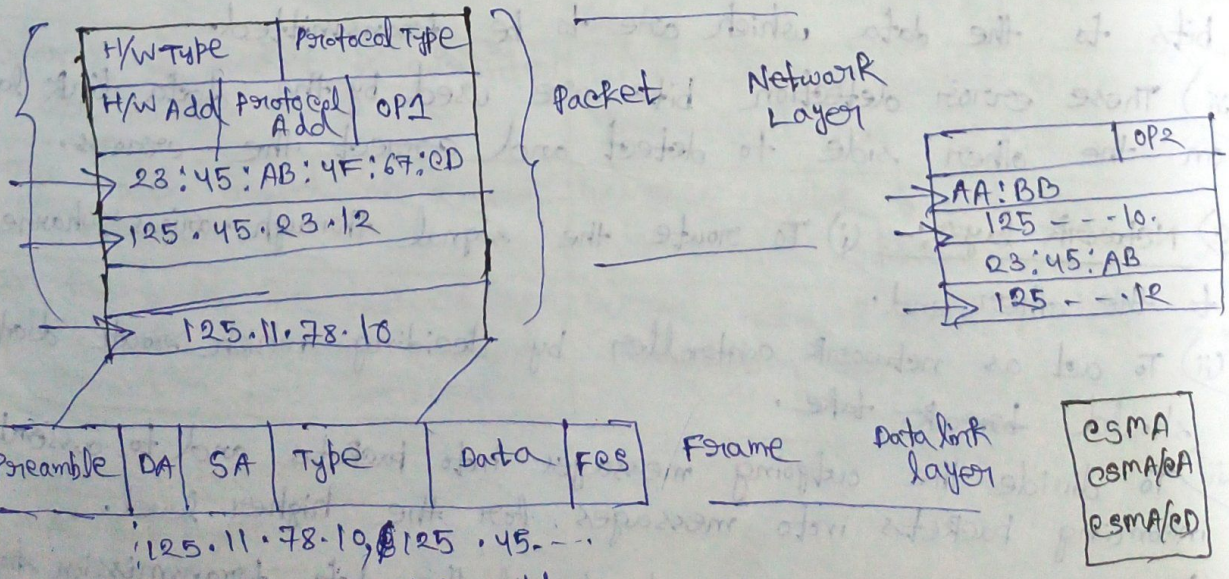
Position of redundant bits: r1: 1,3,5,7,9,11; r2: 2,3,6,7,10,11; r4: 4,5,6,7; r8: 8,9,10,11



codeword — 10011100101

② A router with IP address 125.45.23.12 & physical address 23:45:AB:4F:67:CD has received a packet for a destination with IP address 125.11.78.10 & physical address AA:BB:A2:4F:67:CD. Show the entries in the ARP request packet sent by router. Encapsulate the ARP request packet in a data link frame. Fill in all the fields.





Date:- 23.8.24

(14) OSI model:- OSI stands for open system interconnections which was developed in 1980s and developed by international standard organizations. This is a conceptual model use for network communication. This OSI model consists of 7 layers and each layer is connected to each other. The data moves down the OSI model and each layer adds additional information. When the data is ~~reached~~ received at the last layer of the OSI model then the data is transmitted over the network. Once the data is reached on the other side then the process will get reversed.

(15) TCP/IP model:- TCP model stands for Transmission control protocol and Internet control suit. A number of protocol that make the internet ~~comes~~ to possibly comes under the TCP/IP model. A TCP/IP model has 4 layers of architectural model. TCP/IP was designed and developed by the department of defence in 1960s.

(16) Functions of OSI model:-

(a) Physical layer:- (i) To activate, maintain and deactivate the physical connections.

(ii) To convert the digital bias into electrical signals.

(iii) To decide whether the transmission is simplex, dublex.

(b) Data link layer:- (i) Syncorization and error control for the information which is to be transmitted over the physical link.

(ii) To enables the error detection and it acts error detection bits to the data which are to be transmitted.

(iii) These error detection bits are used by the data link layer on the other side to detect and correct the errors.

(c) Network layer:- (i) To route the signal through various channel to the other end.

(ii) To act as network controller by deciding which route data should ~~break~~ take.

(iii) To divide the outgoing messages into packets and to assemble incoming packets into messages for the higher level.

(d) Transport layer:- (i) It decides if the data transmission should

take place on parallel paths or single paths.

(ii) It does the function such as multiplexing, splitting or segmenting on the data.

(iii) Transport layer guarantees transmission of data from one end to another (end to end point connection or communication).

(e) Session layer:- (i) This layer syncorize and manages the conversation between two different application. This is the level at which the user will established system to system connection.

(ii) It controls logging on or off, user identification, billing and session management.

(f) Presentation layer:- The presentation layer makes it sure that the information delivered in such a form that the reciding system will understand and use it.

(g) Application layer:- Application layer is at the top of all the layers, it provides different services such as manipulation of information in various ways, retransmitting the files of information, distributing the results.

(17)

OSI	TCP/IP
(i) OSI stands for open system interconnection and it has 7 layers.	(i) TCP/IP stands for Transmission control protocal or internet protocal and it has 4 layers.
(ii) Separate session layer and presentation layers are there.	(ii) Session layer charecteristics are provided by transport layer and presentation layer charecteristics are provided by application layer.
(iii) Delivery of packet is guranteed to OSI model.	(iii) Delivery of packet is not guraunteed in TCP/IP model.
(iv) This model based on a vertical approach.	(iv) This model based on a horizontal approach.
(v) In this model the network layer provides both connection oriented and connection less services.	(v) The network layer provides only connection less services.

Date:- 2.9.24

MAC Sub layer

Multible Access

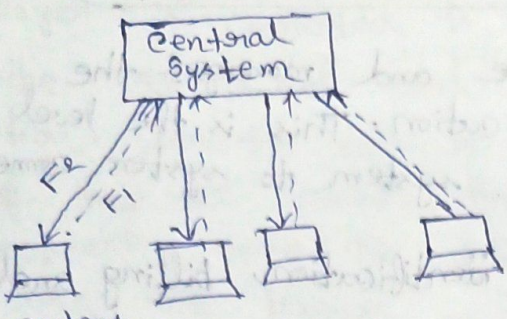
ALOHA

Pure ALOHA — Slotted ALOHA

CSMA

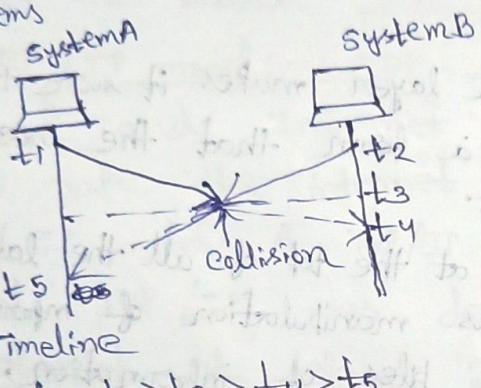
CSMA/CD (carrier sense multible Access with collision Detection)

CSMA/CA (with collision avoidence)



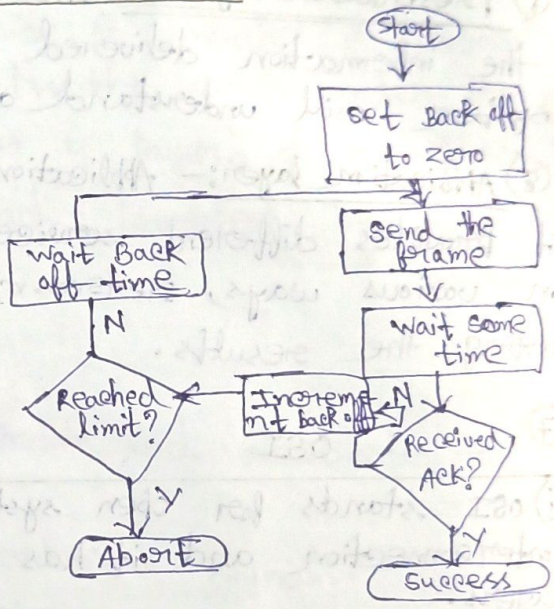
F1 = B'cast Frequency from systems

F2 = B' cast Frequency from central system.



$t_1 > t_2 > t_3 > t_4 > t_5$

ALOHA



CSMA

→ Presistence

⇒ ↳ Non-Persistent

↳ Persistent

↳ 1-persis

(18)

Persistence:-

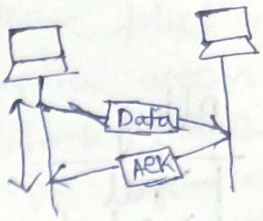
The CSMA protocol operates on a principal of carrier sensing. In this protocol a station ~~listens~~ lisence to see the presence of transmission within bracket carrier on the cable and decides to act accordingly.

Non-persistent- In this scheme if a station wants to transmit a frame and if finds that the channel is busy then it has to wait for fix interval of time. After this time it again checks the status all the channel and if the channel is free then transmit the data.

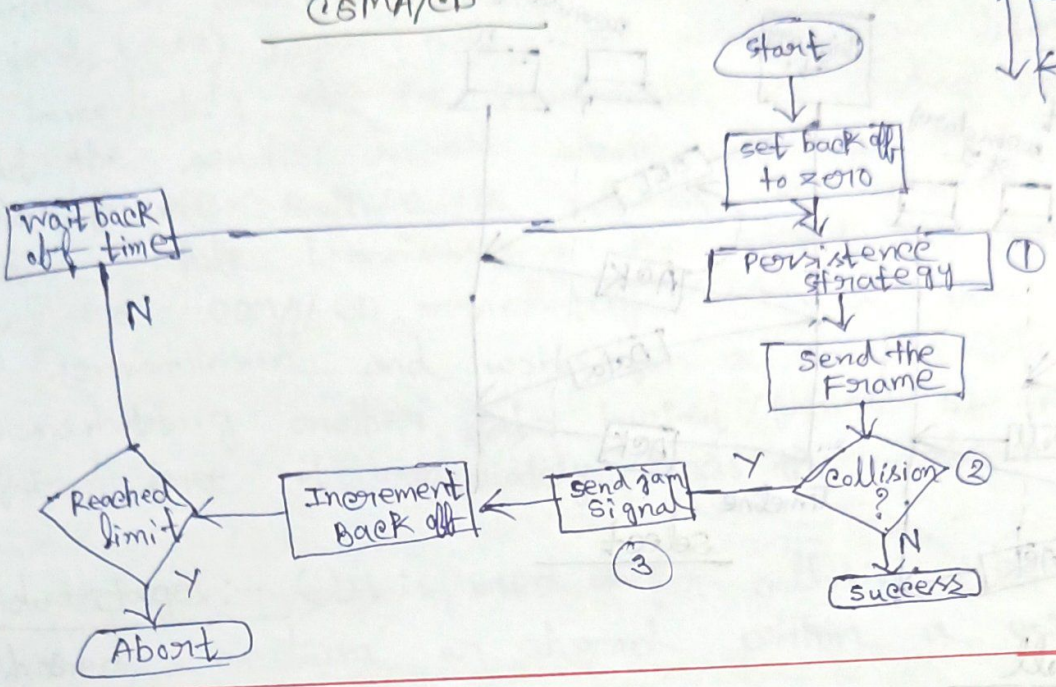
(i) 1-Persistent:- The station which wants to transmit continuously monitors the channel until it's idle and then transmit immediately.

(ii) P- Persistent:- The possibility of such collision and re-transmissions is reduced in the P-Persistent. All the waiting

station are not allowed to transmit simultenously as soon as the channel became idle. A station is assumed to be transmitting with a probablity of p.

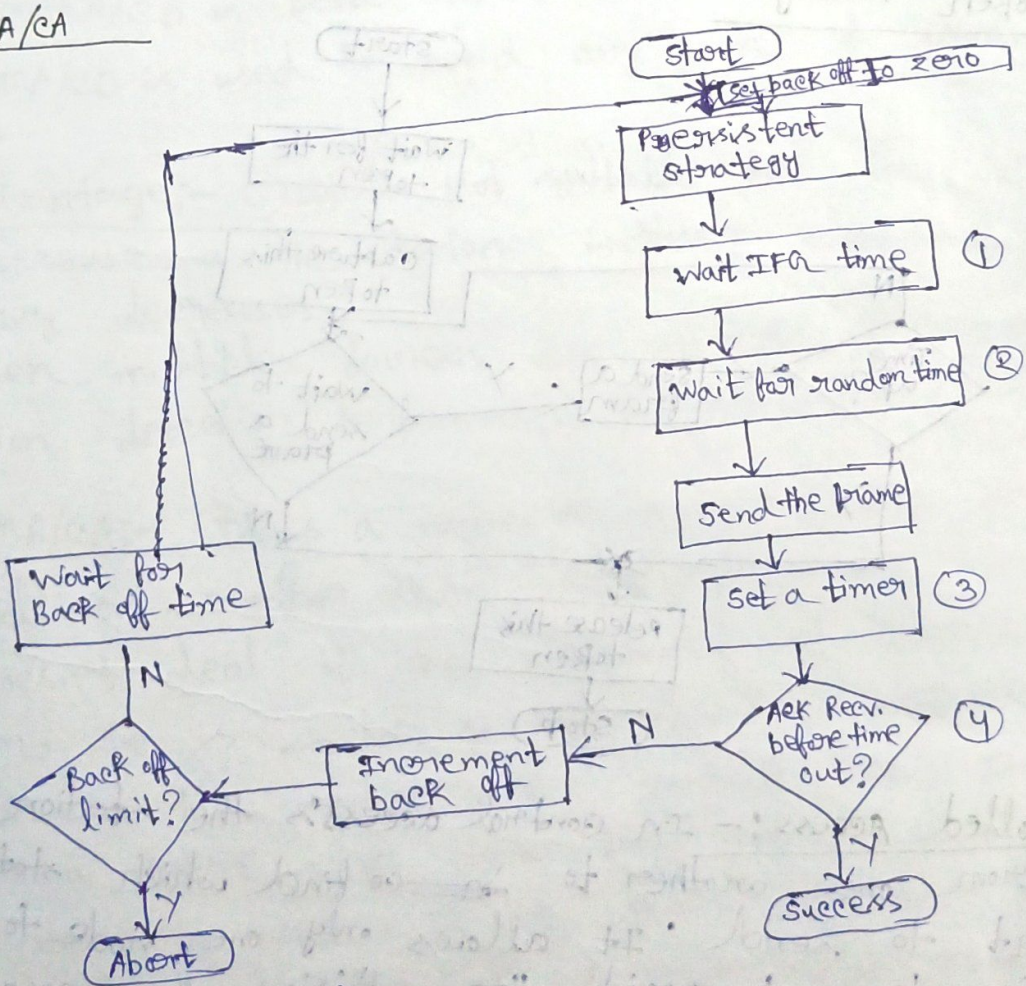


CSMA/CD

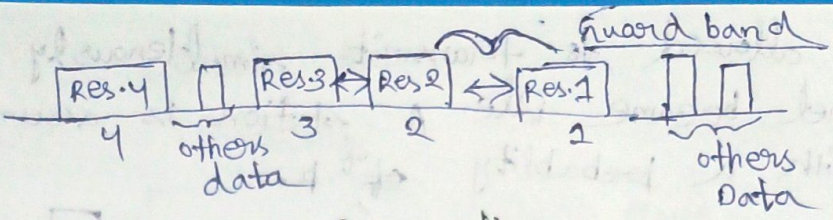


Date:- 3.9.24

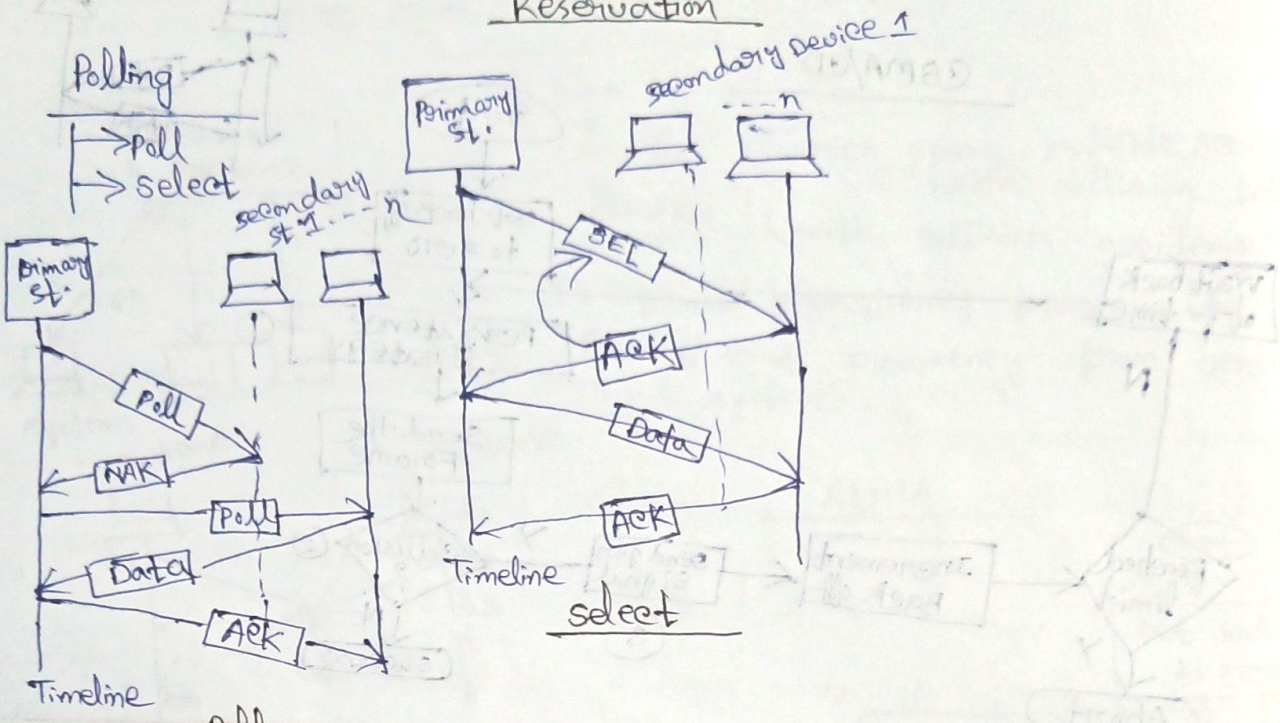
CSMA/CA



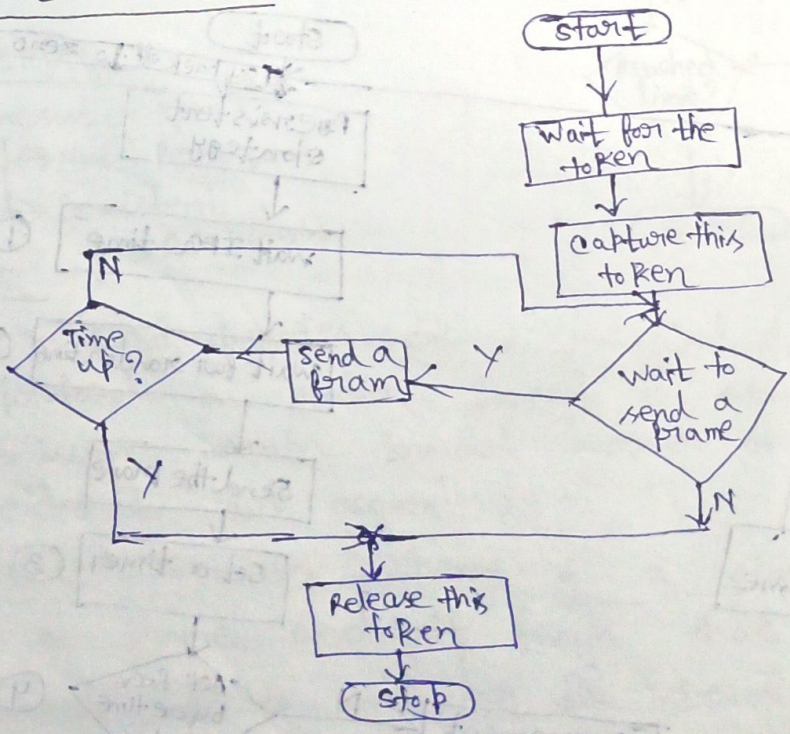
* IFG - Inter frame gap time
* Control Access - (i) Reservation, (ii) Polling, (iii) Token Passing



Reservation



Token Passing



(b) **Controlled Access:-** In control access's the station seek data from one another to ~~in co~~ find which station has the right to send. It allows only one node to send data at a time, to avoid the collision of messages on a shared medium. The three control access methods are - Reservation, Polling and Token Passing.

Date:- 6.9.24

* Automatic Repeat equation
* Flow control

(20) CSMA/CD - The carrier sense multiple access / collision detection protocol is used to detect a collision in the media access control (MAC) layer. once the collision was detected, the CSMA/CD immediately stop the transmission by sending the signal so that the sender doesn't waste all the time to send the data frame. suppose a collision is detected from each station while broadcasting the packets or frames. In that case the CSMA/CD immediately sends a jam signal to stop transmission and waits for a random time before transmitting another data packet / frame. If the channel is found free it immediately sends the data and return it.

Advantages:- (i) It is used for collision detection on a shared medium or channel within a very short time.

(ii) CSMA/CD is better than CSMA/CA for collision detection.

(iii) CSMA/CD is used to avoid any form of waste transmission.

Dis advantage:- (i) It is not suitable for long distance networks because as the distance increases CSMA/CD efficiency decreases.

(ii) when multiple devices are added to a CSMA/CD, collision detection performance is reduced.

(21) CSMA/CA:- It is a network protocol that uses to avoid a collision rather than allowing it to occur, and it doesn't deal it the recovery of packets after a collision. It is similar to the CSMA/CD protocol that operates in the media access control layer. In CSMA/CA whenever a station sends data frame to a channel, it checks whether it is in used. If the share channel is busy, the station waits until the channel enters ideal mode.

Advantages:- (i) when the size of data packets is large the chances of collision in CSMA/CA is less.

(ii) It controls the data packets and sends the data when the receiver wants to send them.

(iii) It is used to prevent collision rather than collision detection on the shared channel.

Disadvantages :- (i) sometime CSMA/CA takes much waiting time as usual to transmit the data packet.

(ii) It consumes more band-width by each station.

(22) CSMA/CD	CSMA/CA
(i) It is type of CSMA to detect the collision on a shared channel.	(i) It is the type of CSMA to avoid collision on a shared channel.
(ii) It is used 802.3 Ethernet network protocol.	(ii) It is used 802.11 Ethernet network protocol.
(iii) It is work is wired network.	(iii) It works in wireless network.
(iv) It is effective after collision detection on a network.	(iv) It is effective before collision detection on a network.
(v) whenever a data packet conflicts in a shared channel it resends the dataframe.	(v) whereas the CSMA/CA waits until the channel is busy and doesn't recover after a collision.
(vi) It minimizes the recovery time.	(vi) It minimizes the risk of collision.

Date:- 10.9.24

(23) IP v4:- IP stands for internet protocol version 4 is the most widely used system for identifying devices on a network. IP v4 was primary version brought into action for production within the ARPANET in 1983. IP version 4 addresses a R32 bit integer which will be expressed in dotted decimal notation.

IP v4 addresses consist of 3 parts-

(i) Network- The network part indicates the distinctive varities that appointed to the network. The network part identifies the category of the network that is assign.

(ii) Host:- The host part uniquely identifies the machine on

your network. This part of IPV4 before address is assign to every host. For each host on the network, the network part is the same, however the host hall must vary.

(iii) Subnet Number:- Local networks that have massive number of host are divided into subnets and subnet numbers are avoided appointed to that. Default subnet mask are in case of class A - 8, for class B - 16 and class C - 24

(24) Characteristics of IPV4 :- i) IPV4 is a 32 bit IP address.
(ii) It has unicast, broadcast and multicast addresses.
(iii) IPV4 supports VLSM (variable net subnet masking / virtual length subnet masking)
(iv) IP V4 security permits encryption to keep up privacy & security.

(25) class Full IP addressing :- It means is a way of organising and managing IP addresses, which are used to identify devices on a network. The class of an IP address determines the network portions and host portions based on it's class specific subnet mask or default subnet mask.

(26) class less IP addressing :- The network address identifies a network on the internet. Using this we can find a range of addresses in the network and total possible number of host in the network. In that particular case we have added extra network bits along with default classes of IP addresses.

Routing
- Static Routing (manually put IP address)
- Dynamic Routing
  - Distance vector Routing Protocal
    - RIP, IGRP (classful)
    - (Balanced) :→ EIGRP, (classless)
  - Link State Routing Protocal
    - OSPF (classless)
  - → Interior Routing Protocal (RIP, IGRP, EIGRP, OSPF)
  - → Exterior " " (BGP)

EIGRP - [Some features of DVRP & Some LSRP]

* OSPF= open shortest path fast
* IGRP= Interior gateway Routing Protocol
* EIGRP= Enhanced " " "
* Interior routing protocol is used to exchange routing information within Autonomous System.
* RIP- Routing Information protocol.
* BGP- Border Gateway Protocol

(27) Converge- When all routers have routes to all network or when all routers are synchorized means having routes to all remote networks then they're said to be converge

RA# Show ip route ←1

Router	IP	Hop	Interface
C	10.0.0.0	0	f0
C	10.0.0.0	0	s0

Date :- 13.9.24

(28) Static Routing- It's also known as non-adaptive routing which doesn't change the routing table unless the network administator changes or modifieds them manually. static Routing doesn't use complex routing algorithms and it provides higher or more security than dynamic routing.

Advantages- (i) It can easily implement in small network.
(ii) It doesn't need band-width use between routers.
(iii) It is a more secure routing.

(29) Dynamic Routing- It's also known as adaptive routing which changes the routing table according to the change in topology. It uses complex routing algorithms and it doesn't provide high security like static routing. when the network change occurs, it sends the message to the router to ensure that changes then the ~~bounds~~ routes are recalculated for sending updated routing information.

Advantages :- (i) Easy to configure.

(ii) more effective and selecting the best route to a destination remote network and also for discovery remote networks.

(30) Static Routing	Dynamic Routing
(i) In static routing rotes are user defined.	(i) In dynamic routing routes are updated according to the topology.
(ii) In static routing doesn't use complex routing algorithms.	(ii) It use complex routing algorithm.
(iii) It provides higher security	(iii) Less security.
(iv) It's manual.	(iv) It's automated.
(v) It's implemented in small network.	(v) It's implemented in larger network.
(vi) Less bandwidth is required.	(vi) more bandwidth.
(vii) Static routing is difficult to configure.	(vii) Easy to configure.

Date:- 20.9.24

1. which of these is a standard interface for serial data transmission?
⇒ (ii) RS232C.

2. which type of topology is best suited for large business which must carefully control and coordinate the operation of distributed branch outlets?
⇒ (iv) Star / (iii) Hierarchical

3. which of the following transmission directions listed is not a legitimate channel?
⇒ (iv) Double Duplex

4. "Parity bits" are used for which of the following purposes?
⇒ (iii) To detect errors.

5. what kind of transmission medium is most appropriate to carry data in a computer network that is exposed to electrical interferences?
⇒ (ii) optical fiber

6. The term HTTP stands for?
⇒ (iii) Hypertext transfer protocol

7. A proxy server is used as the computer?

⇒

8. which software prevents the external access to a system?

⇒ (i) Fire wall

9. which one of the following.