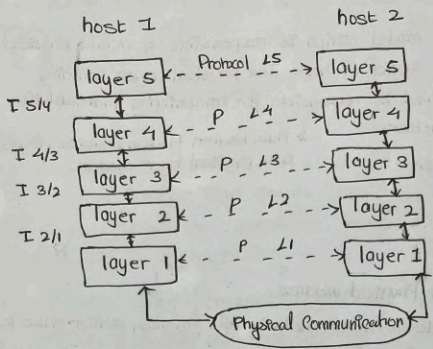
Unit One

① Draw and Explain Software network Protocol Hierarchies.?



This diagram explains how communication between 2 host takes place. The data items are processed through different layers of host 1 to host 2. The virtual communication is represented by dotted line between peer layers and physical communication is represented by solid line. Actual communication takes place through physical solid line and interface represent between two layer explains about service provided. Thus, layer, protocol and interface makes up Network Architecture.

② Explain OSI Model in detail.

① Physical layer

-> lowest layer of osi model which is responsible of actual physical connection between device or host. The physical layer contains information in bits and is responsible for transmitting individual bits from one node to another.

* Hub, Router, Modem, Cables, Repeater are physical layer models.

-> i) Bit Synchronization
ii) Bit rate Control
iii) Physical topologies.
iv) Transmission mode.

② Data link layer. * Physical Address

-> Responsible for node-to-node delivery of frames, which make sure data transfer is error free from one node to another, over the physical layer.

Sublayer: logical link Control (LLC) & Media Access Control (MAC)

-> i) Framing, Physical Addressing (MAC)
ii) Error Control, Flow Control, Access Control.

* Switch and Bridge are Data link layer.

③ Network layer. * logical Address

-> Responsible for the transmission of Packets from one host to another such that it selects shortest path to transmit packets to number of router available.

* Routers are network layer.

-> i) Routing
ii) logical Addressing

iii) Transport layer * Port Address

-> Responsible for end-to-end delivery of complete segments and provides acknowledgement for successfull transmission or retransmit for error found.

-> i) Segmentation & Reassembly
ii) Service point Addressing.

v) Session layer.

-> Responsible for establishment of connection, maintenance of session, authentication and ensure security.

i) Session establishment, maintance, termination.
ii) Encryption & authentication.

vi) Presentation layer. { translation layer }

-> Responsible to extract data from application layer and manipulate as per the required formate.

i) Translation
ii) Encryption / Decryption.
iii) Compression.

vii) Application layer. { Desktop layer } * Application Specific Address.

-> Responsible to produce the data, which has to be transfered over the network and serves as a window to access the network and display information

i) FTP
ii) Mail Services.
iii) Network Virtual Terminal.

Example: Browser.

③ Explain TCP/IP Protocol test Suite and how they Compare with OSI model.

→ TCP/IP protocol was developed and designed by department of defence during early 1960s, which have standard protocols. It is based on ~~consite~~ concise version of OSI model. It consist of four layer.

① host to host
② Internet
③ Application layer
④ Network Access layer (host to Nehoork)

TCP/IP	OSI
-> Transport Control Protocol	-> Open System Interconnectfon
-> 4 layers	-> Consist 7 layers.
-> More reliable	-> less reliable
-> Session layer is combined to application layer with presentation layer	-> OSI have separate application layer with different presentation and session layer.
-> develop protocol than Models	-> develop models than Protocol.

Unit 2: Physical layer.

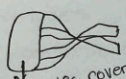
① Classify transmission media in detail with diagram.

① Twisted - Pair Cable. (Coax)

-> Uses metallic (copper) wires wound about each other such that it accepts and transport the signals in the form of electric current.

Unshielded Twisted Pair (UTP)

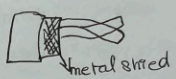
- Copper wire twisted around one another that has ability to block interference and does not depend on physical shield.



Eg: telephone

Shielded twisted Pair (STP)

-> Wire has metal casing that prevents and improve quality of cabals by preventing the penetration of noise or crosstalk.



Eg: Cold climate

② Coaxial Cable.

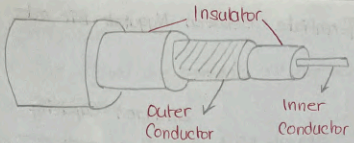
-> This is 2 parallel conductors containing/having a separate insulated protection cover and as a whole has a plastic covering.

* One kind is 50-ohm cable, is commonly used when it is intended for digital transmission from the start.
* Other kind is, 75-ohm cable commonly used for analog transmission and cable television.

Advantage:
- High Bandwith
- Better noise Immunity
- Easy install and expand
- Inexpensive.

Dis': Single failure in Cable can distrub whole network.

-> Radio Frequency Signal
-> TV cables.
-> Ethernet.



③ Optical

-> Is a glass or plastic cable that accept and transport the ~~Single~~ signals in the form of light.

Advantage

Higher Bandwith.
Noise Resistance
less Single Attenuation

Disadvantage.

- Expensive
- Difficultin maintenance and installation
- Fragility.

Q/2) What is Fourier Series?

-> Is tool that changes a time domain signal to frequency domain signal and vice versa.

Q3) Explain Transmission Impairment?

-> i) Attenuation – lose of energy.

$$dB = 10 \log_{10} P_1/P_2$$

ii) Distortion - Singal change its form or shape. In composite Single

iii) Noise - Thermal / Induced / crosstalk / Impulse.

$$SNR = \frac{\text{Power of signal}}{\text{Power of noise}} \qquad SNR_{dB} = 10 \log_{10} SNR$$

Q/4) What is bit rate and differentiate Between Nyquist Bit rate and Shannon Capacity.

Nyquist Bit rate	Shannon Capacity
-> Noiseless Channel	-> System presence of noise
-> theorm stated that :	-> States the theorm :
Bitrate = $2B \log_{10} L / \log_{10} 2$	Capacity = $B \log_2 (1+SNR)$
-> tells us how many singnal levels we need.	-> gives us the upper limit. -> bit per second.

Q/5) Explain line coding and what are the various scheme of line coding?

-> line coding process to convert digital bits in digital signal.

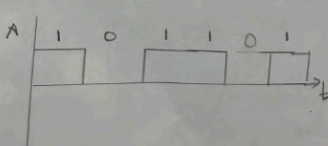
At the sender side digital data are encoded to digital signal and at the receiver side digital data are recreated by decoding digital signal.

-> Scheme of line coding is divided into 5 parts.

9) Unipolar (NRZ)

-> It shows all signal level either all above or below axis.

The positive signal defines 1 and negative signal defines 0. Since signal does not return in the middle of bit thus it is called NRZ.

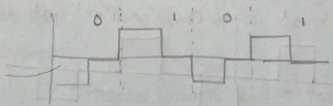


ii) Unipolar

-> The signal are present at the both axis and uses two level of amplitude.

Eg: NRZ-level and NRZ-Invert

Return to Zero. (RZ) - Signal goes to zero in Middle of each bit.



iii) Biphase (Manchester and Differential Manchester)

Manchester = Combination of RZ and NRZ-L

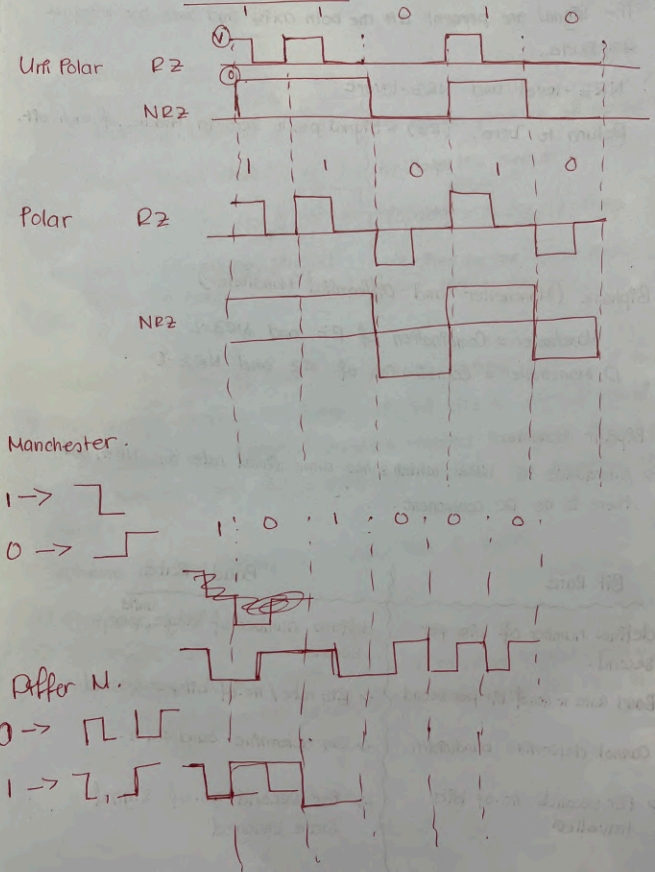
D. Manchester = Combination of RZ and NRZ-I

iii) Bipolar Schemes

-> Alternative to NRZ, which has same signal rate as NRZ, but there is no DC component.

Bit Rate	Baud Rate
defines number of bits per second.	defines number of single units per second.
-> Baud Rate * no. of bit per second	-> Bit rate / no. of bit per second.
-> Cannot determine bandwidth	-> Can determine bandwidth.
-> Per seconds no. of bits travelled	-> Per second no. of signal state changed.

line Coding (11010)



Unit 3

Pure Aloha (wait ACK)	Slotted Aloha
time is continous and not globally synchronised	time is discrete and globally synchronised.
Max Effe = 18.4%	Max Eff = 36.8%
doesn't reduce no. of collision	reduce no. of collision to half

CSMA/CD (sense medium)	CSMA/CA
✓ effective after the collision	Effective before collision.
✓ wired connection network	v wireless network.
✓ Efficient than simple CSMA	v similar to simple CSMA.

Q/ Elementary data layer protocol.

i) ~~Wait~~ Stop and wait ARQ.
-> keeps copy of frame and waits for ACK. If negative it retransmits copied frame.

ii) Go-Back-N ARQ.
-> Retransmits all the frame although some have received or was delivered safely.

iii) Selective Repeat ARQ.
-> Retransmit only those frame which are lost, damaged or currupted.

Hamming Code.

$P_1 P_2 P_4$ - Parity bits.

7bit

D_7	D_6	D_5	P_4	D_3	P_2	P_1

For P_1 = Check 1bit, skip 1bit (1,3,5,7,9...)

For P_2 = Check 2bit, skip 2bit ~~(2,3,6,7,...)~~ (2,3,6,7,10,11)

For P_4 = Check 4bit, skip 4bits. (4,5,6,7,12,13,14,15)

$\therefore P_1 = P_1 D_3 D_5 D_7$ $\quad P_2 = P_2 D_3 D_6 D_7$ $\quad P_4 = P_4 D_5 D_6 D_7$

Eg: Sender send 1101 check Even parity.

D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	1	0		1		

$P_1 = P_1 D_3 D_5 D_7$

$= P_1\ 1\ 0\ 1$

Even $\therefore P_1 = 0$

$P_2 = P_2 D_3 D_6 D_7$

$P_2 = P_2\ 1\ 1\ 1$

$P_2 = 1$

$P_3 = P_3 D_5 D_6 D_7$

$P_3 = P_3\ 0\ 1\ 1$

$P_3 = 0$.

Q/ 7 bit Hamming Code is received as 1011011. Assume Even Parity State whether the code is correct or wrong, if wrong locate bit in error?

Given: 1011011

D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	1	1	0	1	1

$P_1 = 1$
$P_2 = 1$
$P_4 = 1$

$P_1 D_3 D_5 D_7$
1 0 1 1
Odd ∴ P_1 (Error)

$P_2 D_3 D_6 D_7$
1 0 0 1
Even (No Error)

$P_4 D_5 D_6 D_7$
1 1 0 1
P_4 (Error) odd.

Correcting Error: $E =$

P_4	P_2	P_1
1	0	1
D	E	0

decimal value = 5
which shows that 5th bit is In Error.
∴ Correct word/bit = Invert 5th bit
its 1 = 0

∴ Correct word = 1001011

Random Access Protocol.

Pure Aloha - Station sends the data, wait for Ack. If the station does not receive Ack, it waits for random amount of time (T_b) and re-send data.

Slotted Aloha - Similar to pure Aloha, but time is divided into slots. They can only resend during beginning of of slots. If they missed out slots they have to wait. Thus collision controlled.

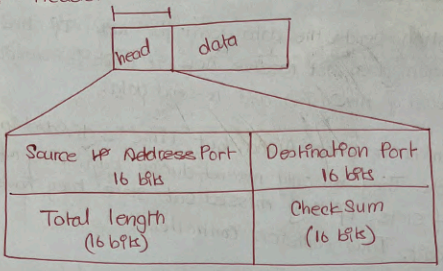
Control Access Protocol

Reservation - make reservation before sending data.

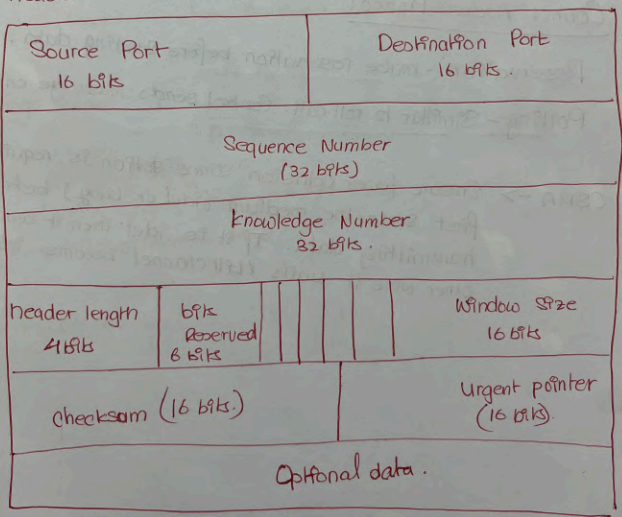
Polling - Similar to roll call. Control sends massage on turn.

CSMA -> Ensure fewer collision since station is required to first sense the medium (idel or busy) before transmitting data. If it is idel then it sends data, other wise it waits till channel becomes idele.

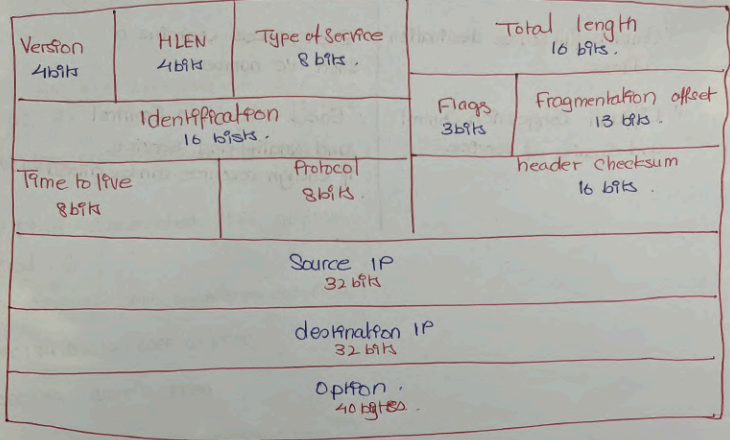
UDP header



TCP header

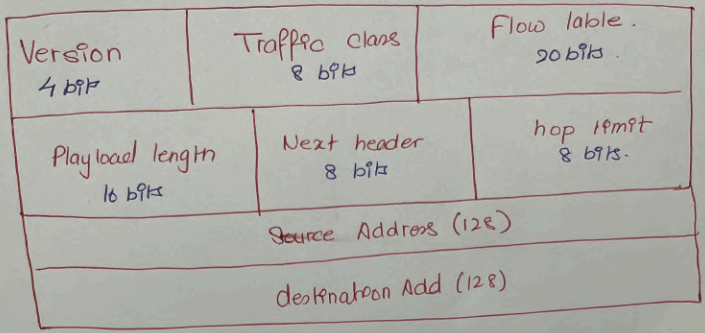


IPV4 header



The header is 20 to 60 bytes in length and contain information essential to routing and delivery. It is customary to show header in 4 byte section

IPV6 header


Version
4 bit
Traffic class
8 bit
Flow lable.
20 bits.
Playload length
16 bits
Next header
8 bit
hop limit
8 bits.
Source Address (128)
destination Add (128)

Unit 4 – (Network Layer: IP Addressing)

1. Subnetting

- A subnetwork or subnet is logical sub division of IP networks.
- Practice of dividing a network into two or more network is called subnetting.

1.1 Subnetting – 5 Steps.

i) Identify the class of IP address and note Default subnet Mask.

ii) Convert Default subnet mask into Binary.

iii) Note the number of hosts required per student and find subnet generator (SG) and octect position.

iv) Generate New Subnet

v) Use SG and generate the network ranges (subnets) in appropriate octect position.

Q/ Subnet IP addres 216.21.5.0 into 30 host in each student?

Sol: Given: No. of host = 30

216.21.5.0

Class C: 255.255.255.0

Binary: 11111111.11111111.11111111.00000000

No. of host = 30 (11110) 5bits

-> Reserve 5 bits of last byte.

11111111.11111111.11111111.111 00000
SG

SG = 32 Octect P = 4

-> New Subnet mask:

255.255.255.224 or /27

We have 27 1s in New subnet mask

-> Network Ranges (subnet)

Start: 216.21.5.0 – 216.21.5.31

1st	216.21.5.	32	– 216.21.5.63
2nd	11	64	11 95
3rd	11	96	11 127
4th	11	128	11 159
5th	11		

and so on

1st subnet

Network Address : 216.21.5.0

Boradcast 11 : 216.21.5.31

Q/2) Subnet IP address 196.10.20.0 into 50 hosts in each subnet.

Sol: 196.10.20.0

→ Class C : Default S.M = 255.255.255.0

→

Binary : 11111111.11111111.11111111.00000000

→

No. host = $5\emptyset^{2}$ (110100) 6bits

Reserve 6 bits of last byte

11111111.11111111.11111111.11000000

SG = 64 Octect P = 4

New subnet mask : 196.10.20.192 or /26

→ Network Range

196.10.20. 1920 – 196.10.20.63

196.10.20. 64 – 196.10.20.127

196.10.20. 128 – 196.10.20.191

196.10.20. 192 – 196. 10. 20.

Network ID = 196.10.20.0

Boradcast ID = 196.10.20.63

1st Usable IP = 196.10.20.1

last Usable IP = 196.10.20.62

Q/3) What is Network ID, Brodcast Address, First Usable IP, or last Usable IP on the subnetwork that the node 192.168.1.15/26 belongs to.?

Sol: /26 means.

255.255.255. + Two bits.

i.e 11111111.11111111.11111111.11000000

decimal subnet is

255.255.255.192

SG = 64 Octect.P = 4

Network ID : 192.168.1.0

Boradcast ID : 192.168.1.63

First Usuable IP : 192.168.1.1

last Usuable IP : 192.10.20.62

Q4/ Subnet the IP address 150.15.0.0 into 500 hosts in each subnet.

Sol: Class B - Default Subnet mask is : 255.255.0.0

-> 11111111.11111111.0.0

No. of 500 host = 500(111110100) 9bits

SG = 2 Octect Position: 3

-> 11111111.11111111.11111[10].00000000

-> New Subnet: 255.255.254.0 or /23

-> Network Ranges (subnets)

150.15.0.0 - 150.15.1.255
150.15.2.0 - 150.15.3.255
150.15.4.0 - 150.15.5.255

$2^9 = 512$ Hosts per Network (subnet)

$2^7 = 128$ Subnet (Network)

Q5) What is subnetwork address if destination is 200.45.34.56 and subnet mask is 255.255.240.0?

Sol:

200.45.34.56 in binary

11001000.00101101.00100010.00111000

255.255240.0 in Binary.

11111111.11111111.11110000.00000000

Subnetwork address = And operation of destination and subnet mask

11111111.11111111
11001000.00101101.0010 0000.0000.
=> 200.45.32.0 } Subnetwork Address.

Q6) What is subnetwork Address if destination is 19.30.80.5 and the subnet mask is 255.255.192.0?

Sol: 19.30.80.5 in binary

00010011.00011110.01010000.00000101

255.255192.0 in binary.

11111111.11111111.11000000.00000000

00010011.00011110.01000000.00000000

19.30.64.0 } subnetwork Address.

Q7/ A Company has granted site address 201.70.64.0 (class C). The company need six Subnet. Design Subnet?

Sol: Given: 201.70.64.0

Class C: 255.255.255.0

Six Subnet given by (2^3) 3 bits.

11111111.11111111.11~~000000~~.11100000

New subnet => 255.255.255.224

Subnet Generator = 31 5bits are zero

Quardent = 4th.

Subnet Range are:

201.70.64.0 - 201.70.64.031

201.70.64.32 - 201.70.64.63

201.70.64.64 - 201.70.64.95

201.70.64.96 - 201.70.64.127

201.70.64.128 - 201.70.64.159

201.70.64.160 - 201.70.64.191

1st Usable = 201.70.64.1

last Usable = 201.70.64.62

Nehoork ID = 201.70.64.0

Boradcast ID = 201.70.64.63

Q8/ A company has granted site address 181.56.0.0 Class (B). The company needs 1000 subnets. Design Subnets.

Given: 181.56.0.0

Class B: 255.255.0.0

11111111.11111111.00000000.00000000

1000 Subnet given by (2^{10}) 10 bits.

New Subnet mask.

11111111.11111111.11111111.11000000

255.255.255.192

Subnetgenerator = 64

Quardent = 4th.

1st subnet:

181.56.0.0 — 181.56.0.63

1022th subnet

181.56.255.64 - 181.56.255.127

Q/ Organisation granted 130.56.0.0/16
The administrator wants to create 1024 subnet. Find 1st/last Address.

Sol: 130.56.0.0 /16

Subnet => 11111111.11111111.00000000.00000000

To get 1024 subnets ($2^{10}=1024$) = 10 bits.

New subnet => 11111111.11111111.11111111.11000000

Subnet generater = 64

Quadernt = 4th.

Subnet = 255.255.255.192 OR (26)

1st Subnet: 130.56.0.0 - 130.56.0.63

Usable Subnet => 130.56.0.62

32-26 = 6

1st 00111110
last 00000000
00111111

1st Address = 130.56.0.0

last Address = 130.56.0.63

Num of Address = last - 1st Address
=> 63 - 0 = 63

Super Netting.

The multiple networks are combined into bigger network termed as Supernetwork.

Rules

① Number of Blocks must be power of 2 {1,2,4,8,...}

② The Block must be contiguous in the address space (no gaps between the blocks)

③ The third byte of first address in Super block must be evenly divisible by number of Blocks.

Q/ We need to make a supernet out of 16 class c blocks. What is supernet mask?

→ 16 Means we need 4 bits
{ $2^4 = 16$ }

Class C: 255.255.255.00

11111111.11111111.11111111.00000000

→ 11111111.11111111.11110000.00000000

255.255.240.0

Q/ Given: 205.16.32.0

Supernet mask = 255.255.255.248

→ 11111111.11111111.11111000.00000000

since, 1st Supernet mask have 21 1's ∴ Default would have 25 1's since difference is 3.

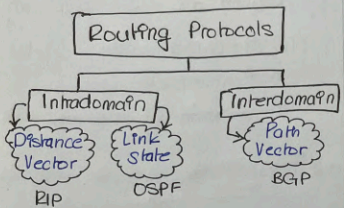
$2^3 = 8$ blocks.

205.16.32.0 – 205.16.39.255.

Unit V – Network Layer : Routing

Unicast Routing Protocols.

Process of forwarding unicasted traffic from a source to destination on an internetwork



RIP - Routing Information P

Is a dynamic routing protocol which uses hop count metric & Distance Vector Routing to find shortest or best path. btw source and destination.

1. Path Vector Routing

Maintains the path information that gets updated dynamically.

There is atleast one node called Speaker node, in each AS that creates a routing table and advertises it to speaker nodes in neighbouring node.

1.1 Steps in path vector Routing.

→ Initialization
→ Sharing
→ Updating - loop prevention

1.2 BGP

Border Gateway Protocol (BGP) is an interdomain routing using path vector routering.

- Using TCP connection - reliable
- last for long time so it is called as Semi permanent connection.

2. Distance Vector Routing.

Also known as Bellman floyd Algorithum and its dynamic algorithum

2.1 Bellman Floyd Algorithum.

let $d_x(y)$ be cost of least-cost path from node x to node y. The least costs are related by

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

x = source y = distination

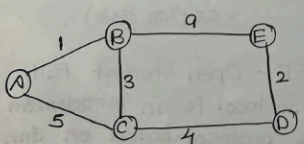
v = intermediate node.

-> It is iterative, distributed & asynchronous

-> Each router maintains a table known as vector.

Remark: Cost and No. of Intermediate node should be minimum

Eg: Create Routing table for hop 'B' of following Topology.



RIP -> Routing Information Protocol.

① B to A

B-A = 1 -> Minimum Cost *

B-C-A = 8

B-E-D-C-A = 20

② B to C

B-C = 3 *

B-E-D-C = 15

B-A-C = 6

③ B to E

B-E = 9 *

B-AC-D-E = 12

B-C-D-E = 9

④ B to D

B-E-D = 11

B-C-D = 7 *

B-A-C-D = 10

Table (Routing) for hop 'B'

Destination	Cost	Next hoop
A	1	A
C	3	C
E	9	E
D	7	D

Remark:

① It compares the delay in its local table with delay in neighbour's table and cost of reaching destinati

② If the path via the neighour has a lower cost, then the router updates its local table to forward packets to the neighbours.

3. link State Routing

also known as Dijkstra's Algorithm

-> Technique in which each router shares knowledge of its neighborhood with every other router in the network.

3.1 Three keys to Understand LSR

- knowledge about neighbourhood : Instead of sending its routing table a router sends the information about its neighborhood only.
- Flooding

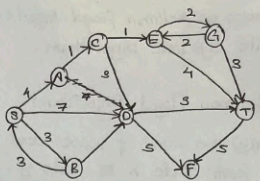
Each router sends the info to every other router on internetwork except its neighbours. Then every router that receives the packet send the copies to all its neighbours. This is called Flooding.

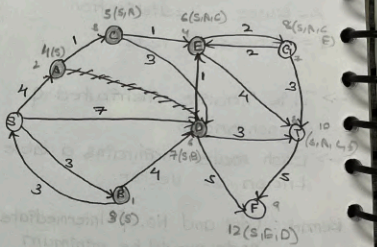
Reliable Flooding.

Initial State ; Each nodes knowons the cost of its neigbour

final State ; Each node knowons entire graph.

Q/ Shortest Path from S to F





Shortest Path : 12 (S,E,D)

Sequence : S-B-A-C-E-D-G-T-F
For optimum Path
0+3+4+5+6+8+7+8+10+12
= 55 (Min. cost)

OSPF - Open Shortest Path first protocol is an intradomain routing protocol based on link State routing.

Distance Vector Routing

-> Bellman-Ford Algorithum

-> Bandwidth required is low due to local sharing.

-> Based on local knowledge info. from neighbours

-> Traffic is less

-> Implementation is RIP

link state Routing

-> Dijkastra's Algorithum

-> Bandwidth required is more due to flooding.

-> Based on global knowledge. Info about entire network.

-> Traffic is more.

-> Implementation on OSPF.

Method to calculate direction and distance of vector of next hope from obtained information of router. from neigbour router.

Used by every router to share information or knowledge about rest of the routers on network.

B. Congestion Control Algorithum

Congestion occurs if the load on network, the number of packets sent to the network, is greater than the capacity of the network to handle number packets.

Congestion Control refers to techniques that can either prevent congestions, before it happens, or remove congestions.

-> Open loop
-> closed loop.

1. Open loop.

Protocol that should be used in order to prevent congestion and congestion should not occur in first place.

1.1 Retransmission Policy

-> It retransmits when frame is lost, Ack is lost and frame is damaged.

timer value small - more transmission
timer value large - delay in response.

1.2 Window Policy.

In Go-Back-N window, when the timer for a packets times out, a number of packets may be resent, although some may have arrived safe and sound at reciver.

∴ Selective with repeat window is better than Go-Back-N.

1.3 Acknowledgement Policy

If a receiver does not acknowledge every packets it receives, it may slow down the sender and congestion is prevented. Therefore Selective Ack and Cumlative Ack is needed.

1.4 Discarding Policy.

In case of Congestion we should discard packet which is

- low priority
- Newer Packet
- Discard packet which is not nearest to destination.

packets which are just about to enter the destination's network should not be discarded.

1.5 Admission policy.

If there is insuffficent resource to handle transmission, then do not accept the packets.

∴ Solution to Open Conjection.

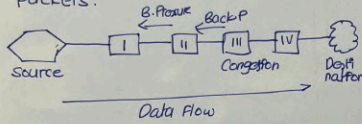
-> Selective repeat window is better
-> Should sent cumalative Ack
-> Higher priority packets should not be discard.

2. Closed loop

→ Allows system to Enter Congestion State if it occurs, detects it and then proceeds to remove congestion.

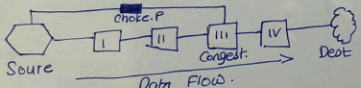
2.1 Back Pressure

When a router is congested, it informs the previous upstream router to reduce rate of outgoing packets.



2.2 Choke packet of Choke point

It is sent by router to Source, Similar to ICMP's Source quench.



2.3 Implicit Signaling.

Packets may be discarded and source can detect these as implicit indication of congestion. (Connectionless Network)

2.4 Explicit Signaling.

→ network alerts source and destination about congestion and to slow down rate of transmission (Connection Oriented)

Backwards - Packet sent in opposite direction of packet travel.

Forwards - Packet sents in same direction of packet travel.

C. Quality of Services (QoS)

✓ To provide good quality of services is to build a network with enough capacity for whatever traffic will be thrown at it.

Name of solution is called over-provisioning.

1. Flow Characteristics.

i) Reliability
ii) Delay
iii) Jitter - Variation in delay
iv) Band with.

2. Techeniques to Improve QoS

Scheduling
- FIFO Queuing
- Priority Queue
- Weighted Fair Queue.

Traffic Shaping
- leaky Bucket
- Tocken Bucket.

Traffic Shapping

Traffic Shaping - is a technique for regulating / controlling the average rate and brust rate of flow of data in network

SLA - Service level Agreement

Monitoring of Traffic Flow is called traffic policing.

-> leaky Bucket
-> Token Bucket.

Unit 6 - Transport layer

1. Transport layer

-> The transport layers is responsible for process to process delivery i.e the end delivery of a packet, part of a massage, from one process to another.

1.1 Client/Server Paradigm.

-> Most common way to achive process to process delivery.

* local host called client
* Remote host called Server

>Both have same name.

-> For communication we must define following:

① local host
② local Process
③ Remote host
④ Remote Process.

Remarks.

IP address: defines the host among different host in the world

Port Number: defines one of the processes on this particular host.

1.2 IANA Ranges.

International Assigned Number Authority (IANA) has divided port numbers into 3 stages:

ⓐ Well known Ports.

Ports ranging from 0 to 1023 are assigned and controlled by IANA. These are well known Ports.

ⓑ Registered Ports.

Ports ranging from 1024 to 49,151 are not assigned or controlled by IANA. They are only registered with IANA to prevent duplication.

③ Dynamic Ports.

Ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used by any process and are emphemeral ports.

1.3 Stock Address.

The combination of an IP address and port number is called stocket address.

Eg: Client Stock Address
Server Stock Address.

1.4 Multiplexing

At Sender site, there may be several process that needs to send packets. However, there is only one Transport layer Protocol at any time. This is many to One relationship and requires multiplexing.

Demultiplexing.

And at the receiver site, the relationship is one to many and requires demultiplexing.

∴ At last transport layer delivers each massage to apporpriate process based on port number.

1.5 Connectionless Vs Connection-Oriented Services.

Connectionless

- No Connection needed
- Packets are not numbered
- May get delayed or lost
- No Ack either.

Connection-Oriented Services.

- Connection is established.
- reliable Connection
- less Congestion
- Suitable

2. User Datagram Protocol (UDP)

UDP is a connectionless, unreliable transport protocol. It does not add anything to the services of IP except to provide process-to-process communication.

2.1 User Datagram

Source Port Number: Used for running source host. 16 bits long which range from 0 to 65,535.

Destination Port Number: Used for running destination host. 16 bits long which range from 0 to 65,535.

length: defines the total length of user datagram, header plus data.

UDP length = IP length - IP header's length.

Checksum: Used to detect errors over the entire user datagram.

∴ This four component together makes user datagrame, which have fixed size header of 8 bytes.

2.2 UDP Operation

- Connectionless Service – no relation between datagram. not numbered
- No FIDO control and Error Control
- No error control except checksum.
- Encapsulation and decapsulation.

2.3 Queuing.

3. Transmission Control Protocol (TCP)

TCP is connection Oriented Protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at transport layer.

Three Way handshake.

Since it is connection oriented, computers first establish connection. And its done using Three way handshaking.

First, Sender sends SYN message to the receiver then they receiver sends back SYN ACK message to confirm that message has been received. After receiving SYN ACK message, again sender sends ACK message to receiver. In this way, the connection is established.

Difference between TCP and UDP

	TCP	UDP
Full Form	Transmission Control Protocol	User Datagram Protocol.
Connection	It is connection oriented protocol, which means the connection needs to establish before transmission of data.	It is connectionless connection which means system sends the data without checking whether system is ready or not.
Reliable	TCP is reliable protocol as it is provides assurance for the delivery of data packets.	UDP is unreliable protocol as it does not take guarantee for delivery of data packets.
Speed	TCP is much slower as it provides error checking, flow control and provides assurance of delivery of data.	UDP is mush faster as it does not give guarantee of data delivery.
Head Size	20 bytes	8 bytes.
Flow Control Mechanism	It follows flow control mechanism in which too many packet cannot be sent to the receiver at the same time.	No Flow Control Machanism followed.
Application	This protocol is mainly used where secured and reliable communication is required such as military, email, web page.	This Protocol is used where fast communication is required such as game streaming, music and video streaming.

4. FTP - File transfer Protocol

-> Application layer.

-> Application layer is closest layer of OSI model to end user and programs are based on Clients and Server.

4.1 FTP - File transfer Protocol.

FTP - uses the services of Transmission Control Protocol (TCP). It needs two TCP connections:

① Well known 21 ports for Control Connection

② Well known 20 ports for data Connection.

ⓐ Communication Over Control Connection.

-> It uses 7-bit ASCII character set. Communication is achieved through commands and responses.

-> We send one command or response at a time and each command is only one short line, we we need not worry about file structure and formate.

-> The Control Connection remain connected through out interactive FTP session.

-> Connection is btw Control Process.

ⓑ Communication Over data Connection

-> Data Connection is opened and closed for each file transfered.

-> It opens each time commands that involve transfering files are used, and it closes when the file is transfered.

-> When Control Connection is opened then the data connection can be opened and closed multiple time if several times of several files is to be transfered.

∴ Check steps and diagram on PPT.

#Using data Connection Clients must define

① File type

② data Structure

③ transmission mode.

i) File type

- ASCII file or EBCDIC file.
- Image

ii) Data Structure.

- File Structure (Continuous stream of bytes)
- Record Structure (File divided in records)
- Page Structure.

iii) Transmission mode.

- Stream Mode
- Block Mode
- Compressed Mode.

File Transfer in FTP means :

*The file is to be copied from a Server to Client. This is called retrieving a file. It is done using RETR command

* The file is to be copied from the Client to Server. This is called storing a file. It is done using STOR command.

* list of dictionary or files is to be sent from sever to client. This is done using LIST command.

5. Electronic Mail.

Remarks :

When sender and receiver of an e-mail are on same system, we need only two user agent.

If it is in different system we need two user agent and pair of MTAs (Client & Server)

Different system means when two system are connected by LAN or WAN

Unit 6- Transport and Application layer.

1) Explain E-mail system contain which two subsystem? Write the five basic function provided by e-mail system?

-> E-mail is electronic mail services which gives internet user a method to transfer massage and other formatted files to another internet user in any part of the world.

Two Subsystem:

i) User agent: Program which is used to read, send, and receive mail. Sometimes it is called user agent. It supports variety of command provide service such as:
i) Reply to massage ii) Compose iii) Read iv) Forward
v) Manage mail box.

ii) MTA (Massage Transfer Agent): MTA is actually responsible for transmission of massage over two system. To transfer, system must have Client MTA and system MTA.

Five Basic function provided by e-mail system.

i) Composition: Process to construct messages and answer. For Composition any kind of text editor is used.

ii) Transfer: means procedure of sending mail from sender to recipient

iii) Reporting: refers to confirmation for delivery of mail. It helps user to check whether mail is delivered, lost or rejected.

iv) Displaying: To present the mail in the form that is understand by user.

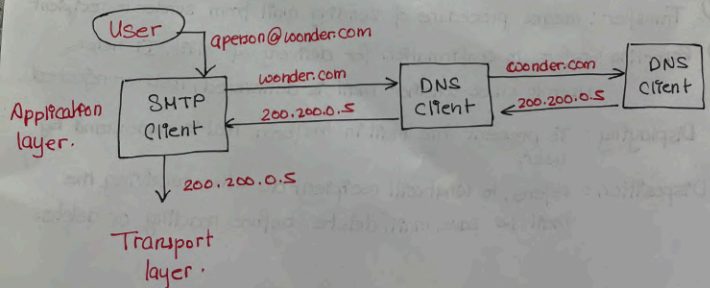
v) Disposition: Refers, to what will recipient do after receiving the mail i.e save, mail, delete before reading or delete.

2/ Explain Working of DNS and its type ?

-> DNS is domain name System and has service that translate the domain name into IP address. Thus, this allows user of network to use user-friendly name instead of remembering numberic IP address.

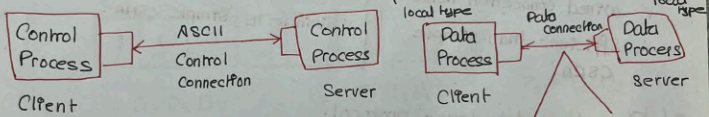
-> If client like web browser sends request containing the host name, then a peiece of software such as DNS resolver send a the request to DNS server to obtain IP address of a hostname. If DNS server does not find any IP address associated with hostname than it pass the request to another DNS server.

Generic Domains	Country Domains	Inverse Domains.
-> Uses three-level Character labels Eg: .com, gov, edu	-> Two level country abbreviation Eg : us (United State) in (India)	-> Mapping Address to name. -> Determine whether client is on authorized list or not.



Q/ Explain FTP and Working of FTP.

Control Connection	data Connection
- Uses 21 Port number	Uses 20 Port number
- Uses very simple rule	- Uses very complex rules as data type varies.
- Connection is made between control processes.	- Connection is made between data process.
- Connection remain connected through out the FTP session	- Connection opens when command come for transfer and closes after transmission.



Q/ Explain 3 Way Handshake ?

Step 1 (SYN): The Client wants to establish the connection with sever, so it sends segment with SYN(Sychronize Sequence number) which informs sever about that client is likely to start communication.

Step 2 (SYN + ACK). The servers respond to client by sending SYN-ACK set of bits. (ACK) Acknowledgement signifies response to segment it received. and SYN signifies with what sequence number it is likely to start.

Step (ACK): Client Acknowledge the response of server and they both establish reliable connection with which they start actual data transfer.