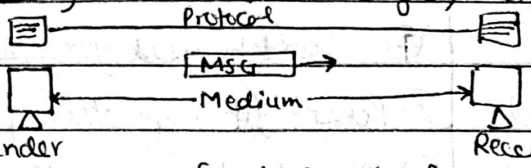
Advanced Computer Networks

Unit-I

Date __/__/____

Network Layer

* Network is a collection of computers that share information and resources such as printers.
* Components of Network: (Message, Sender, Receiver, Medium, Protocol)



* A network is a set of devices (refer to as node) connected by communication links. A node can be computer, printer or any other device.
* ISO-OSI (Open Source Interconnection) and TCP/IP Reference Models

	ISO-OSI Model		TCP/IP		Protocols in TCP/IP
7	Application		Application	4	FTP SMTP DNS HTTP TELENET
6	Presentation				
5	Session				
4	Transport		Transport	3	TCP UDP
3	Network		Internet	2	IP
2	Data Link		Host-to-Network	1	ARPANET SATNET LAN
1	Physical		Network Access		

(i) Physical Layer: Make & break connections, define voltages & data rates, convert digital data bits to electrical signal & decide transmission is simplex or duplex.

(ii) Data Link layer: Synchronization, error detection & frames. To assemble message into frames.

(iii) Network layer: Message into packet, routing of signals.

(iv) Transport Layer: Decide transmission parallel or single path, multiplexing, splitting or segmenting data etc.

(v) Session Layer: Manage & Synchronize conversation b/w two systems logging on/off, user identification etc.

(vi) Presentation Layer: Translating layer

(vii) Application Layer: Retransferring files of information, login etc.

Punk

ISO - OSI	TCP/IP
① 7 layers	① 4 layers
② Transport layer guarantees delivery of packets	② Transport layer doesn't guarantee delivery of packets
③ Horizontal Approach	③ Vertical Approach
④ Separate session & presentation layer	④ No separate session & presentation layer
⑤ Network layer provides connectionless & connection-oriented services	⑤ Network layer only provides connectionless services
⑥ Easy to replace protocols	⑥ Not easy to replace protocols
⑦ Truly a general model	⑦ Can't be used for other applications
⑧ Problem of protocol fitting into model	⑧ Doesn't fit any other protocol stack
⑨ Defines services, interfaces & protocols very clearly (Network layer Intro)	⑨ Doesn't clearly distinguish b/w services, interfaces & protocols

Date __/__/____

* The network layer is a host to host delivery layer, i.e., carrying packet from source to destination.
* The main functions of network layer are as follows:
  - (i) Addressing: To identify each device on Internet uniquely
  - (ii) Internetworking: Provide logical connection b/w different networks
  - (iii) Routing: Decide route to be taken to reach destination from source
  - (iv) Packetizing Data: Encapsulate upper layer protocol packets into new packets
  - (v) Fragmenting: Datagram processing & encapsulation in another frame
  - (vi) Cost & Billing Information: Maintaining statistics of related to data usage
* Network layer design issues / Issues related to services offered by Network layer
  - (i) Providing a link b/w data link layer & transport layer
  - (ii) Providing routing & delivery services to end destination
  - (iii) Maintaining accounting & statistical information for billing purposes
  - (iv) Handling different packet formats
  - (v) Handling different addressing schemes used in different networks
  - (vi) Providing error recovery at end services, if error is detected during transmission
  - (vii) Providing Connection-oriented as well as connectionless services
  - (viii) Providing unique addressing to different nodes & sub-networks
* Address Resolution Protocol (ARP)
  - To reach destination, a packet has to travel through multiple networks & devices such as routers. At network level, they are recognized by their IP address. At physical level, they are recognized by their MAC address.

Punk

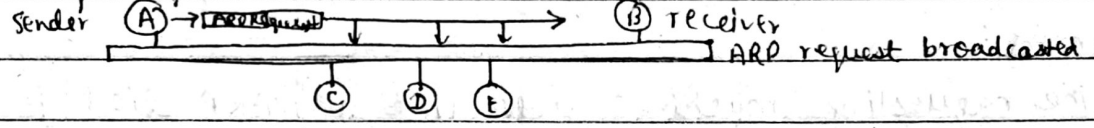
- Both IP & MAC addresses are required for communication. A mapping of IP addresses & into a corresponding MAC address & vice versa is required. This mapping can be static or dynamic.

Date __/__/____

- Static Mapping: It uses a table to store physical address corresponding to every IP address. The problem is that MAC addresses can change. Thus, to implement static mapping, static mapping table needs to be update periodically.
- Dynamic Mapping: In this type of mapping, we use a protocol for finding one address from other. There are two protocols in use: ARP & Reverse ARP (RARP).
- ARP maps an IP address to a MAC address whereas RARP maps a MAC address to a given IP address.
- Working of ARP: (Steps)

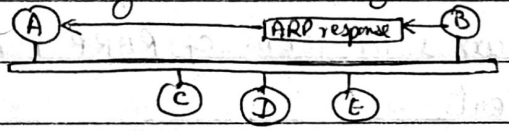
(i) Host A/Router who wants to find MAC address of some other router sends a request packet containing IP & MAC address of sender & IP address of receiver

(ii) This request packet is broadcasted over network.



(iii) Every host & router on network receives & processes ARP request. All host except B (receiver) discards it & B recognizes its IP in request packet. Host B responds back by sending ARP response packet.

(iv) ARP response packet contains IP & physical address of receiver (B). This packet is Unicasted only to A using A's physical address.



- ARP Packet Format

HTYPE (Hardware Length) (16 Bits)	PTYPE (Protocol Type) (16 bits)
HLEN (8 bits) (Hardware Length) / PLEN (8 bits) (Protocol Length)	OPER (16 bits) (Operation) Request 1, Reply 2
Sender Hardware Address (SHA)	
Sender Protocol Address (SPA)	
Target Hardware Address (THA)	
Target Protocol Address (TPA)	

(i) HTYPE: Specifies hardware interface type. value 1 for ethernet.
or
Defines the type of network on which ARP is being run

(ii) PTYPE: Specifies type of high level protocol address such as IPv4.
or
Defines protocol using ARP

Punk

(iii) HLEN: Define length of physical address in bytes. For ethernet, value is 6

(iv) PLEN: Define length of IP address in bytes. For IPv4, value is 4

(v) OPER: Define type of packet, i.e., request or response (reply).

(vi) SHA: Define physical address of sender (MAC address) Date __/__/____

(vii) ~~SHA~~ SPA: Define logical address of sender (IP address)

(viii) THA: Define physical address of receiver. All zeroes if request

(ix) TPA: Define logical address of receiver/target.

Variable Length Field

* Reverse Address Resolution Protocol (RARP)

- In some situations like booting a diskless station or where IP address are assigned dynamically, a machine knows physical address but doesnot know logical address.
- A host needs to know its logical address to communicate with other hosts through a IP datagram
- ~~The~~ RARP ~~has~~ has been designed to address these problems of obtaining IP address from physical address of a device.
- Working:
  - → The requesting machine acts like a RARP client & creates a RARP request.
  - → This request is broadcasted on the LAN.
  - → A machine on the LAN which knows all IP addresses act like a RARP server.
  - → It responds by sending IP address matching the physical address.
  - → This IP address is returned in form of RARP reply which is unicasted to RARP client.
- Drawback:
  - → RARP request is broadcasted on the network & can't pass on to other networks. Therefore, an RARP server is required to be implemented on each different network.
- An alternate to RARP is Bootstrap (BOOTP) or the DHCP protocol, which runs at the application layers.

* Internet Control Message Protocol (ICMP)

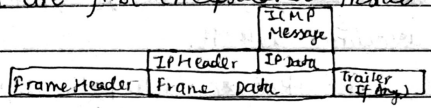
- Internet Communication mostly takes place in form of IPv4 datagrams. IP ~~proto~~ is not designed to be reliable whenever there is some error in data transmission.
- ICMP is an error reporting protocol, where messages are

Punk

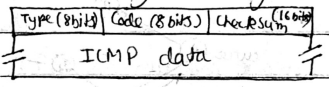
sent to the source IP address to report about some error in delivery
- ICMP messages are used for error reporting and also for diagnosis & troubleshooting purposes.

Date __/__/____

- ICMP doesn't attempt to make IP reliable, just simply attempts to report errors & provide feedback on specific conditions.
- ICMP messages are carried as IP packets & thus are unreliable.
- ICMP also lacks a mechanism for host & management queries. ICMP messages are first encapsulated inside IP datagrams before going to lower layer.



- ping command uses ICMP as a probe to test whether a package is reachable. ping packages an ICMP echo request message datagram & send it to selected destination.
- another utility is trace route, which provides list of all routers along the path to a specified destination.
- ICMP Header is 8 bytes long. The first 4 bytes always have same meaning & the next 4 bytes vary acc^n to ICMP message type.



→ The type field identifies type of message
→ The code field identifies the subtype of a message (if any)
→ The checksum field contains error checking data calculated from header & data
→ ICMP data is a variable length field & contains data specific to type & code fields
→ ICMP Type field: (0-255) (41-255: Reserved)

0 → Echo Reply 1 → Unassigned 2 → Unassigned
3 → Destination Unreachable 4 → Source Quench (Used to ask source to slow down data sending rate if very fast)
8 → Echo 11 → Time Exceeded
17 → Address Mask Request 18 → Address Mask Reply
30 → Traceroute 37 → Domain Name Request 38 → Domain Name Reply

* Routing Basics

- Routing is defined as the process of moving information from a source to a destination. This information is moved in logical units called packets.
- Routers use logical & physical addressing to connect two or more logically separate networks. They accomplish this connection by organizing the large network into logical network segments called as subnets.

Punk

- Each of the subnet is given a logical address. This allows the networks to be separate but still exchange data.
- The role of routers is not only to establish paths between two end points but to do it efficiently. For this, routers need to calculate Optimal path to a workstation on computer.

* How Router Works?

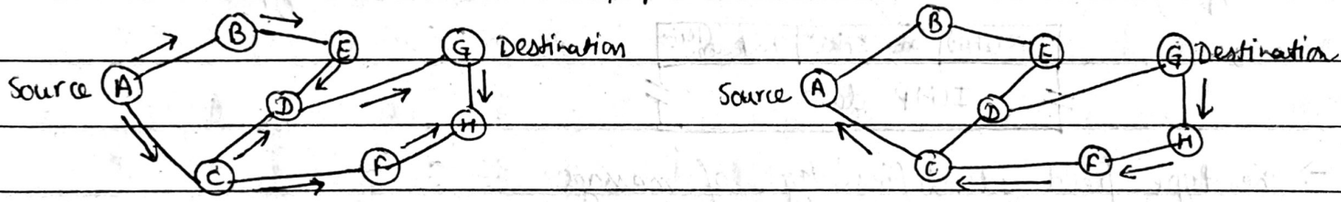
→ Routers maintain information about network in form of tables called Routing Tables.

→ A routing table maintains a row for each destination, the path or next node to be taken and a metric associated with it.

→ Using the next node information, router knows which path a packet must be forwarded to. If router finds one, it simply forwards packet to next node & if not found, a new path is searched:

→ (i) A Route Request (RREQ) Message is generated & broadcast to all neighbours with timestamp

(ii) When this message reaches destination or intermediate node which knows path to destination, it replies by creating a Route Reply (RREP) message. which traverses back to source & path is established.



• (i) RREQ Broadcast (ii) RREP Forwarded Path

~~Routing Algo~~ → When multipath are discovered, the metrics associated with each route are also recorded into table. The metric is the value which describes the path such as delay, hops, bandwidth, jitter etc.

- Routing Algorithm:

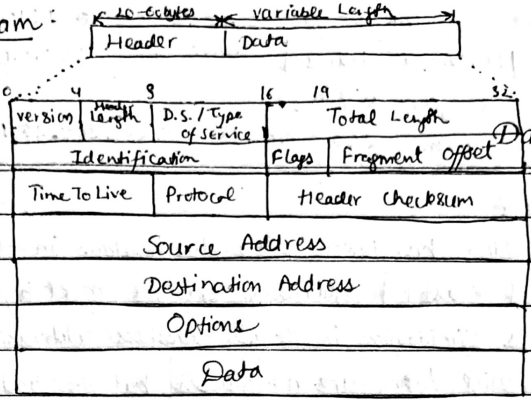
→ Routing algorithm is responsible for deciding the output path over which the packet must be sent. Properties of routing algorithms are:

(i) It's correctness (ii) It's robustness (iii) It's stability
(iv) It's fairness (v) It's optimality (vi) Efficient

* IPv4 Routing Principles:

- IP is a host-to-host network layer delivery protocol designed for internet.
- IP is a connectionless protocol with no reliability assurance as it does not provide any error control or flow control mechanism.
- Packets in IP layer are called datagrams. A datagram is a variable length packet with 2 parts: Header & data.
- Header is 20 to 60 bytes in length & contains info necessary for routing & delivery.
- Other part is data field that is of variable length

- IPv4 Datagram:



Date __/__/____

(i) VER (version) : Defines version of IP

(ii) HLEN (Header Length) : Defines Length of Datagram Header

(iii) D.S. (Differential Service) : Defines class of datagram for quality of service (QOS) purpose

(iv) Total Length : Defines total length of IP datagram (Header + Data)

(v) Identification : Identifies datagram origination from source host

(vi) Flag Bits : 1st bit → reserved & should be '0'

2nd bit → called Donot Fragment bit. If '1' then don't fragment

3rd bit → called More Fragment bit. If '1' then not the last fragment

(vii) Fragmentation offset : Shows relative position of fragement wrt whole datagram.

(viii) Time To Live : Maximum no. of routers visited by datagram (Controls)

(ix) Protocol : Defines higher level protocol which uses IP layer services

(x) Header Checksum : for error checking of header

(xi) Source Address : IP address of source

(xii) Destination Address : IP address of destination

(xiii) Options : Not required for every datagram & used for network testing

- IP addressing : Can be classful or classless

(i) Classful : Three main classes ≡ Class A, Class B & Class C

(A) Class A Address : '0' are MSB of address. Network field is MSB of address (More than 65,534 hosts) & host portion is three byte remainder.

0	Network	Host

Range from 0.0.0.0 to 127.255.255.255

(B) Class B Address : '10' are MS two bits of address. Network field is MS Two (From 255 to 65,534 hosts) bytes of address & host portion is two byte remainder

10	Network	Host

Range from 128.0.0.0 to 191.255.255.255

(C) class C Address : '110' are MS three bits of address. Network field is MS Three. (<255 hosts) bytes & host portion is one byte remainder.

110	Network	Host

Range from 192.0.0.0 to 223.255.255.255

Punk

(D) Class D : First four bits of first octet set to 1110. Reserved for multicasting

1110	Multicast Address

Range from 224.0.0.0 to 239.255.255.255

(E) Class E: Reserved for R&D.

Range from 240.0.0.0 to 255.255.255.254

Date __/__/____

(ii) Classless Addressing

- The address depletion has taken place due to flaws in classful addressing scheme. Class A & Class B addresses are the most affected. An alternate to overcome this limitation is to use classless addressing.
- In classless addressing, there are no classes but the addresses are still generated in blocks. In this scheme, when an entity needs to be connected to the internet, a block range of addresses is granted to it. The size of this block granted is equal to actual requirement, it is not fixed liked classful addressing.
- The following rules are followed while allocating classless address blocks:
  - (a) The address in a block must be continuous
  - (b) The no. of addresses in a block should be a power of 2.
  - (c) The first address should be evenly divisible by the no. of addresses.
- classless addressing treats the IP address as a 32 bit stream of 0s & 1s, where the boundary b/w network & host portions can fall anywhere b/w bit 0 & bit 31.
- A subnet mask is used locally on each host to a network, & masks are never carried in IPv4 datagram. The no. of 1's in the subnet mask determines the network address.

* Classification of Routing Algorithms

(i) Acc^n to their adaptation ability:

(A) Non-Adaptive (or Static) Routing ≡ Routing decisions not based on current traffic & topology
Ex:- OSPF, BGP

(B) Adaptive or Dynamic Routing ≡ Routing decisions changed if any change in traffic or topology
Ex:- Distance vector Routing (DVR) & Link State Routing (LSR)

(ii) Acc^n to their Range (Domain) of Operation:

(A) Intra-Domain (or Interior Routing) ≡ Protocols used within a single Autonomous System
Ex:- DVR & LSR

(B) Inter-Domain (or Exterior Routing) ≡ Protocols used to connect two or more different Autonomous systems.
Ex:- Path Vector Routing

Punk

* Intra Domain Routing

* Link State Routing (LSR):

Principle: LSR must perform 5 basic router operations as follows:

(i) Each router should discover its neighbours & obtain their network addresses

Date __/__/____

(ii) Then it should measure the delay or cost to each of those neighbours

(iii) It should construct a packet containing network addresses & delays of all the neighbours. These packets are called link state advertisements (LSAs).

(iv) Send LSA packet to all other routers in the network.

(v) Each router maintains a database of all received LSAs, which describes network has a graph with weighted edges.

(vi) Each router uses its link state database to run a shortest path algorithm (Dijikstra's algorithm) to produce shortest path to each network.

- OSPF & IS-IS (Intermediate System - Intermediate System) protocol use LSR.

- Features of LSR:

• → In LSR, each node has a complete map of topology.
→ LSAs are flooded to all nodes in the network.
→ Updates are sent only when some changes occur in a neighbour
→ If a node fails, each node calculate the new route
→ Difficulty: All nodes need to have a consistent view of the network.

* Distance Vector Routing (DVR):

Determine path to remote networks using hop count as metric. It has following steps:

→ Initially every node discovers its neighbour nodes & cost associated with them
→ This information is stored in their routing tables
→ A node exchanges this routing table with its immediate neighbours only.
→ If a new destination is received by a node in this exchange, it is also added to its routing table.
→ The cost of new path is calculated as the sum of cost from the current node to its neighbour node & the cost of neighbour to the destination
→ Periodic updates are sent at regular intervals.

- DVR features:

→ With DVR, each node has information only about the next hop.
→ As the info propagates during subsequent cycles, it becomes known to every routers
→ Periodic updates are sent at a set interval
→ Updates are sent to neighbour nodes only.
→ Bellman Ford Algorithm is generally used to find shortest paths.

Difficulty:
→ DVR makes poor routing decisions if directions are not completely correct

Punk Ex of DVR → IGRP & RIP

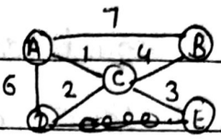
Intra

✱ ~~Intra~~ Domain Routing Protocols:

① Open Shortest Path First Protocol (OSPF)

- ~~DAR SD~~ LSR protocol & uses Dijkstra's algo to build shortest path in H/w.
- ~~OSPF~~ - Steps same as LSR
- Ex:-

Date __/__/____



Shortest paths for Node A:

Step 1:

A	C	D	B	E
0	1	6	7	∞

Node A made permanent & taken out of queue

Step 2: Permanent: A

C	D	B	E
1	6	7	∞

Node C made permanent & taken out of queue

Step 3: Permanent: A, C

D	E	B
3	4	5

Node D made permanent & taken out (cost = 1 (A to C) & from C to other node)

Step 4: Permanent: A, C, D

E	B
4	5

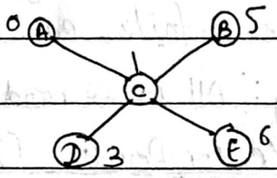
Node E made permanent & taken out

Step 5: Permanent: A, C, D, E

B
5

Lastly B made permanent & queue empty

Destination	Cost	Next
A	0	—
B	5	C
C	1	C
D	3	C
E	4	C



Shortest Path Tree built by Node A

	OSPFv2	OSPFv3
1.	For IPv4 only	For IPv6 & IPv4 both
2.	LSA packet format different	New types of LSA packets introduced
3.	Runs per-subnet	Runs per-link basis
4.	Uses different flooding scope bits.	Separate scopes for flooding LSAs: Link-scope, local scope, area scope, AS scope
5.	We can use only one instance on one link to create a single link in more than one area.	We can use multiple instances on the same link area.
6.	OSPFv2 authentication achieved by implementing a shared secret & MD5 HMAC supported as part of OSPFv2	OSPFv3 does away its own support for authentication & uses the IPsec framework offered by IPv6
7.	IP addressing is not separate of calculating the Shortest Path Tree	Separation of IP addressing from the calculation of Shortest Path Tree. Adding or modifying IP subnets with OSPF domain will not affect integrity of the Shortest Path Trees

Punk

(2) Routing Information Protocol (RIP)

- A DVR protocol & basis is Bellman-Ford Algorithm
- Operation:

Date __/__/____

Phase I: Neighbour Discovery ≡ Initially, every node only knows about its immediate neighbours & stores information about them in their routing tables. Within the same AS, their cost is marked as '∞' (AS ≡ Autonomous system)

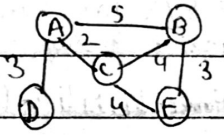
Phase II: ~~Advertisem~~ Advertising ≡ Immediate Neighbours exchange their routing tables to know about other nodes in the network. Path are re-computed if ~~new~~ alternate path available.

Old path updated with new path in two situations:

(A) New path cost less than previous cost.

(B) If there is a change in cost (↑ or ↓) path is always updated as it is possible that some links were lost & therefore cost may increase also.

Ex:-



Initial Routing Table of Node A

To	Cost	Next
A	0	A
B	5	B
C	2	C
D	3	D
E	∞	—

+

Initial Table of Node C

To	Cost	Next
A	2	A
B	4	B
C	0	C
D	∞	—
E	4	E

A's table

Updating A, on receiving C's table,

To	Cost	Next
A	0	A
B	5	B
C	2	C
D	3	D
E	6	C

(Updated Table of A)

- Count To ∞ problem

→ It occurs when some link is lost & its neighbouring discovers it & before it can communicate the revised distance to all neighbours, the neighbour node advertised the previous path, unmindful of the fact that this connection is lost.

→ This problem is resolved only when distance increases to ∞.

→ Soln: Soln to this problem is Split Horizon & Poisson Reverse. When a node advertises its routes to a neighbour which is also Next node, it doesn't pass actual cost value but instead replaces the cost value ~~fo~~ with a special marker to denote that the cost is what I know from you. ∴ The neighbour will come to know that this advertisement is not a new path, but it already has it.

Punk

③ Interior Gateway Routing Protocol

- IGRP is a distance vector routing protocol designed to be used in Gateway for connecting to many different networks.

Date __/__/____

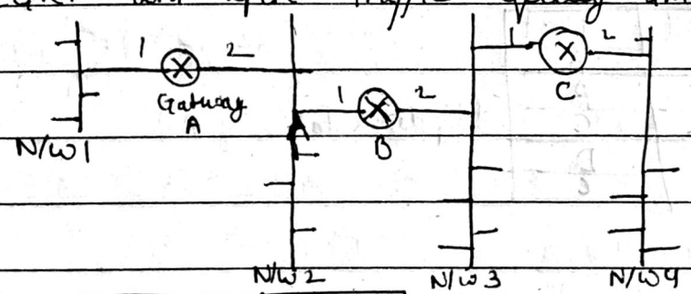
- Features: (i) Dynamic Routing, fast response to Network changes
  (ii) Stable routing ever in complex networks network
  (iii) Low overhead
  (iv) Division of load among different parallel routes for better Network
  (v) Traffic load & error rates taken into consideration to decide flows.
- Operation: Step 1: Initialization ≡ When gateway turned on, routing table initialized
  Step 2: Advertising ≡ Each gateway processes routing table that it receives from other gateways & uses it to modify its own routing table.
  A single composite metric is used to evaluate different links.

$$M = \left(\frac{K_1}{Be} + \frac{K_2}{De}\right) \cdot r$$

K_1 & K_2 ≡ constants
Be ≡ Effective Bandwidth
De ≡ Composite Delay
r ≡ fraction reliability (% of successful packets transmissions)

Step 3: Optimization ≡ Based on composite metrics, link evaluated in terms of its quality. If two links with equal 'M' to a destination are available then IGRP will split traffic equally among two.

Ex:-



⊗ ≡ Gateway

Network	Gateway	Interface
1	None	1
2	None	2

Initial Routing table of A

Initial Routing table of B

Network	Gateway	Interface
2	None	1
3	None	2

Routing Table of C

Network	Gateway	Interface
4	None	2
4	None	2

B receives R.T. of A & C ✱, it updates & create R-T by merging

Network	Gateway	Interface
1	A	1
2	None	1
3	None	2
4	C	2

Final optimized table of Gateway B

Punk

④ Enhanced IGRP (EIGRP)

- Cisco introduced an enhanced version of IGRP that combines advantages of link state protocols & distance vector protocols.
- EIGRP incorporates the Diffusing Update Algorithm (DUAL) ~~developed at SRI International~~

-Features: ① EIGRP & DUAL to achieve fast convergence. In EIGRP, a router stores its neighbours tables so that it can quickly adapt to the network

② EIGRP can also request other routers to discover routes to a particular network if it does not exist. These requests propagate until an alternate route is found.

③ Periodic updates not used as in IGRP. Updates only sent to those nodes which require them

④ EIGRP consumes less bandwidth than IGRP.

⑤ EIGRP supports not only IP but also other networks like Apple Talk & Novell Net Ware

⑥ EIGRP supports variable length subnet masks.

- How EIGRP works?

→ When a router discovers a new neighbour, it records the neighbour's address & interface as an entry in the neighbour table. (Neighbour Discovery Scheme)

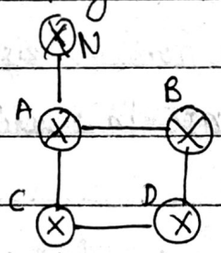
→ Each router periodically sends Hello packets to all nodes connected to it.

→ DUAL module tracks all routes advertised by all neighbours

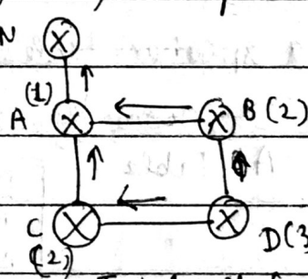
→ DUAL selects routes to be inserted into a routing table based on feasible successors (least cost path to destination) router that has

→ When a neighbour discovers change in metric or topology change occurs, DUAL tests for feasible successors. If one found, DUAL avoid recomputing unnecessarily but when no successors found, recomputation done.

Ex:-



Using EIGRP → successor nodes marked when A discover N



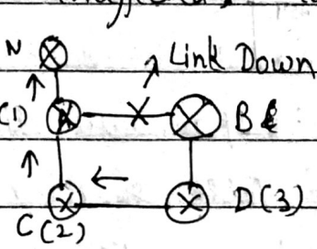
⊗ = Router

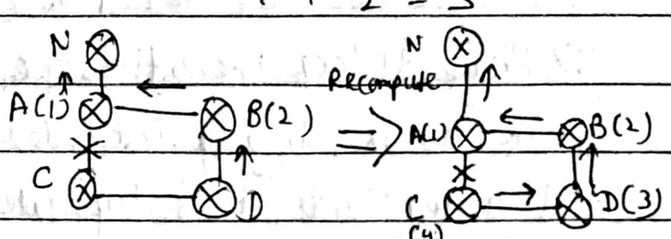
Let AB link lost then ~~recomputation~~ successor found for D to N

Total ~~cost from D to N = B to D cost~~ cost

A & C unaffected. Total Cost of D to N = C to D + C to N

= 1 + 2 = 3





Let AC is lost then C checks successors, no successor to N so recomputation required. Now cost of C = C to D & D to N

Punk

* Inter-Domain Routing Protocols:

- Border Gateway Protocol (BGP)

→ Based on Path Vector Routing.

→ Exterior gateway protocol (EGP) unlike RIP, OSPF & EIGRP.

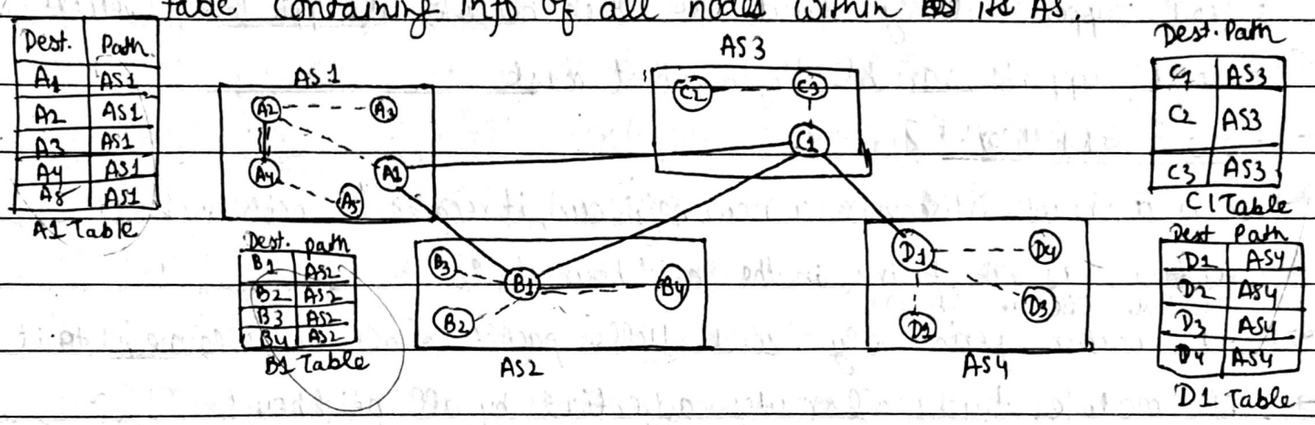
→ Current BGP protocol is BGP version 4 (BGPv4).

→ BGP has been designed to route packets b/w different AS's (Autonomous systems).

→ BGP maintains a routing table based on shortest AS path.

→ Operation: we assume that there is one node in each AS that acts on behalf of entire AS. This node is called speaker node & all communications within an AS is done through this speaker node.

⇒ Phase 1 (Initialization): # Initially the speaker node creates a routing table containing info of all nodes within its AS.



⇒ Phase 2 (Advertising): # Every speaker nodes advertises its routing table with adjacent speaker nodes. Every speaker advertises info about different nodes in its AS & their path.

Ex:- A1 with B1 & C1 / C1 with A1, B1 & D1 /
B1 with C1 & A1 / D1 with C1

when a speaker table node receives a table from a neighbour, it updates its own by adding nodes that are not in routing table.

Ex:- A1 Table

Dest.	Path
A1	AS1
⋮	⋮
A5	AS1
B1	AS1 – AS2
⋮	⋮
B4	AS1 – AS2
C1	AS1 – AS3
⋮	⋮
C3	AS1 – AS3
D1	AS1 – AS3 – AS4
⋮	⋮
D4	AS1 – AS3 – AS4

⇒ Phase 3 (Loop Prevention & Optimization): # If a router discovers that its AS is already included in Routing Table of Advertised message, it understands that it is duplicate & simply discards the message & ignore it. This prevents infinite looping problem.

Punk

Date __/__/____

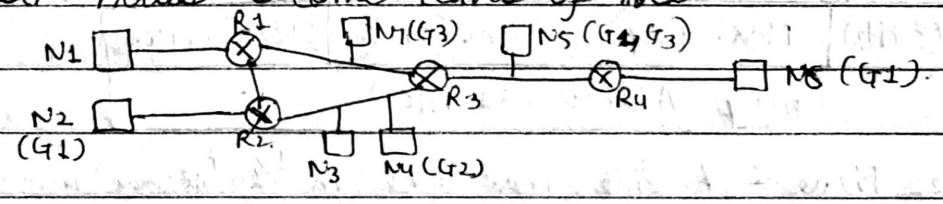
Multicasting in IP Environments

* Unicast, Multicast & Broadcast

- Unicasting is process of serding a message from single source to single destination.
- Multicasting is defined as process of sending a message to a group containing more than one destinations.
- In multiple unicasting, sender creates multiple copies of same packet for each destination whereas in multicasting sender creates a single copy which is transmitted to all nodes in a group.
- Broadcasting is the process of sending a message to all nodes of a network. Only a single copy of packet originates from sender & each router recreates multiple packets, one for each path connected to the router. Even router transmits the packet only once & duplicate packets are discarded.
- Applications of multicasting
  - (i) Teleconferencing
  - (ii) Virtual Classroom
  - (iii) Banking & Distributed Databases
  - (iv) Business Applications
  - (v) Group Messaging

* Shortest Path Trees

- For multiple routing, a router donot need shortest path to only one node but shortest path to all nodes of a group.
- The shortest path tree consists of the source as its roots & all member nodes become leaves of tree
- Ex:-



If N1 needs to send a message to G1, router R1 builds following R.T.

Group	Next Hop
G_1	R_3, R_2
G_2	R_2
G_3	—, R_3

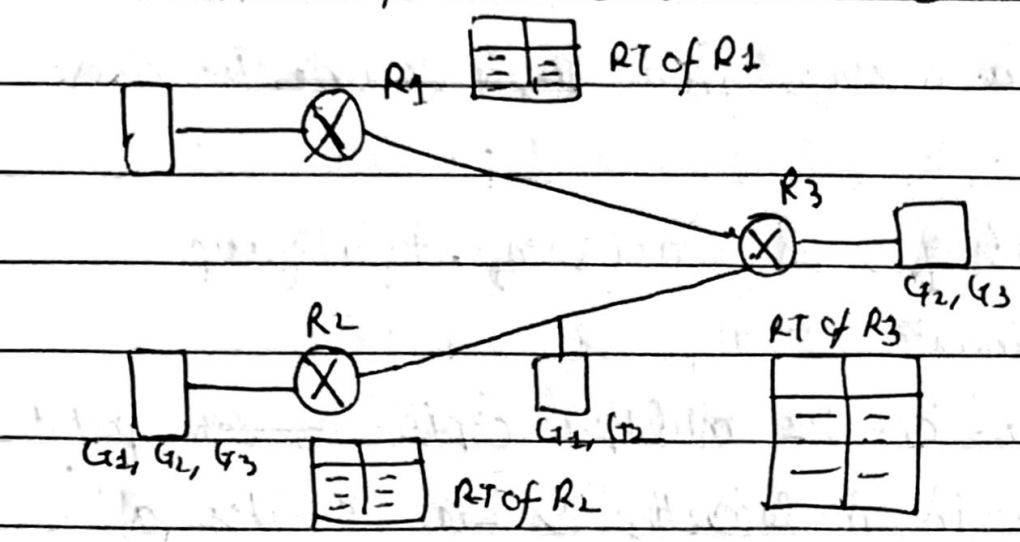
Punk

- Two approaches to store these trees:

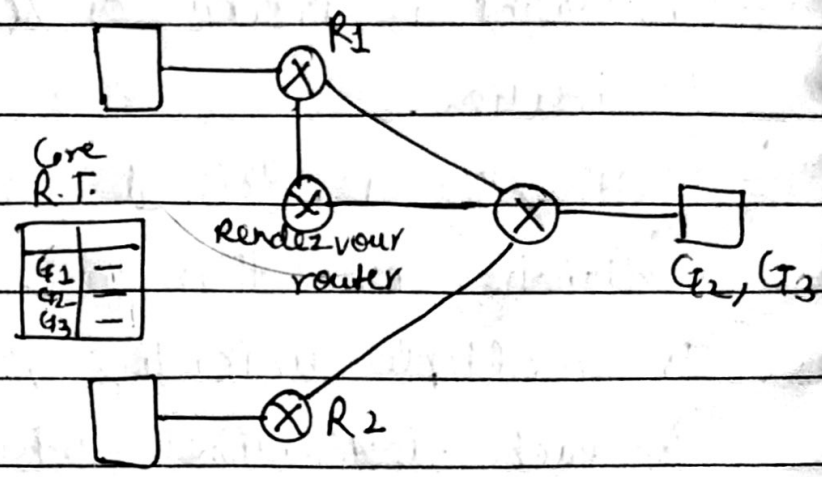
(i) Source based Trees: In these, every router produces & stores its own Shortest Path Tree (SPT) for every group. The no. of SPTs for a router is equal to no. of groups.

Date __/__/____

(ii) Group Shared Trees: In these, every router doesn't maintain & store trees. Rather, a dedicated router called rendezvour router builds SPTs for every group.



Source Based Tree Model



Group Shared Tree Model

* Internet Group Management Protocol (IGMP) & Multicast Listener Discovery (MLD) are the prominent Multicast Group Management Discovery protocols.

* IGMP

- It is a protocol to manage the group membership of hosts and routers. Every network may have one or more Centre Point Router (Rendezvous Router). These centre points are responsible for creation of shortest path trees.
- All multicast packets are unicasted to centre points, which forward them on efficiently. The creation of trees for each group is done with the help of IGMP protocol.
- Format of IGMP message:

Type (8 bits)	Max. Response Time (8 bits)	Checksum (16 bits)
Group Address (32 bits)		

(i) Max Response Time: Define max time (in $\frac{1}{10}^{th}$ seconds) in which a query message must be answered.

(ii) Checksum: 16 bit checksum for error detection

(iii) Group Address: Set to group address in case of special query, membership report & leave report messages
In case of general query, its value is set to 0

(iv) Type: Defines type of packet. There are 4 types of IGMP messages:

Punkit

(A) General query Message ≡ # Used to monitor group membership status over time.
Sent periodically by Centre Point.
Address field in this query message is set to 0.0.0.0

Date __/__/____

(B) Special query Message ≡ # When a router receives a leave report from some of its members, it wants to be sure that some other hosts or router is not wing this group. For this it sends a Special query Message to that router/host.
If host is still interested in group, it sends back Membership Report Message

(C) Membership Report Message ≡ # When a host wants to join a group, it sends a Membership report message to the Centre point.

(D) Leave Report Message ≡ # When a host is no longer interested in a group, it can send a leave Report message to the Centre point.

* Multicast Linear Discovery (MLD) protocol

- Same responsibility as IGMP, i.e., to decide & discover group membership among different hosts of a membership.
- IGMP is used in IPv4 & MLD is used in IPv6.
- A multicast message is sent ~~only~~ to only those links/routers, which have some active members, as per information provided by MLD.
- Format of MLD header:

Type (8 bit)	Code (8 bit)	Checksum (16 bit)
Max. Response Delay (16 bit)		Reserved (16 bit)
Multicast Address (128 bits)		

(i) Max. Response Delay: Specifies max time (in millsec) to response
(ii) Code: To further identify/qualify a packet
(iii) Checksum: For error detection
(iv) Reserved: For future use. Cleared to 0 by sender & ignored by receiver
(v) Multicast Address: Address of multicast group & set to 0 in case of general query
(vi) Type: Define type of packet. Different types of MLD packets are: (sent by routers)
(A) Listener Query ≡ #, to enquire group states of neighbouring hosts
(B) Listener Reports ≡ # Sent by host to report to their neighbour routers about current group status or change in group membership status
(C) Listener Done ≡ # Sent by host to multicast routers to signal that there may not be any further group members in the local subnet.

Punk

* Multicast Routing Protocols

(i) Multicast Link State Routing (MLSR) protocol

- Extension of Unicast LSR protocol & uses source based tree method
- Each router records the membership of its neighbour nodes to different groups. This membership info is recorded & transmitted to all other routers in form of LSAs.
- When other routers receive all LSAs, use this information to create a Network Topology map for each different group.
- If M groups then m different topologies built
- Dijkstra's algo applied on each topology to build M different SPTs.
- Limitation: Processing & Storage required to build these M different SPTs

(ii) Multicast Open Shortest Path Protocol (MOSPF)

- Direct extension of OSPF protocol to multicast environment.
- It is a multicast link state routing protocol.
- Every router determines groups associated with nodes attached to it. This information is stored in different LSA packet called 'Group Membership LSA'.
- This GM LSA is propaged to other routers & in this way every router builds info about all members of particular group.
- Dijkstra's algo applied to build shortest path to each member of a group.
- Unicast address of node used for calculation purposes in Dijkstra algo.
- All shortest path to members of a particular group are combined to create a SPT. These SPTs are stored in cache for future use.
- To increase efficiency, these SPTs are built & are not computed & stored automatically. They are computed only when the first request for multicasting to that group arises

(iii) Distance Vector Multicast Routing Protocol (DVMRP)

- An extension of DVR protocol to multicasting environment
- While forwarding a packet, following considerations must be kept:
  - (A) Loops must be prevented
  - (B) Duplicate packet should not be transmitted
  - (C) Membership information of a node must be dynamically updated
  - (D) Shortest paths must be explored.
- To fulfil above objectives, DVMRP uses one of the following four approaches:

Punk

(A) Flooding : In this strategy, a router simply forwards an arriving packet to all links except arrival link. Problem is that duplicate packets are created unnecessarily which may cause looping.

(B) Reverse Path Forwarding (RPF) : Whenever a packet arrives at a router, the router verifies if it has travelled the shortest path while reaching it or not. If the packet has travelled shortest path to it, only then the packet is forwarded to other links, otherwise it is discarded. The shortest path is verified by the router by looking at the routing table for the address of source

(C) Reverse Path Broadcasting (RPB): While RPF prevents looping, but multiple packets can still reach a node because after checking RPF simply forwards a packet on all links. To prevent this, a packet router is designated for each network. After checking shortest path, a router now sends the packet to only that line for which it is parent. This way flooding is prevented.

(D) Reverse Path Multicasting (RPM) : To limit transmission to networks where there are no active members of group, there exists a parent router maintaining group membership info of all its node. This info is gathered by parent router using IGMP. This protocol works by defining 2 operations:

1. Pruning : If none of the nodes of router is a member of a group, this parent router sends a prune message to its upstream router which in turn records this message to this router. Also, a router which receives prune message from all its downstream routers sends a prune message to its upstream router. Thus unwarranted message to non-member groups never sent

2. Grafting: If a router has already sent a prune message to its upstream router but later it discusses that one of its node is now associated with that group (due to new info by IGMP), then this router sends a graft message to its upstream router which will now again start sending messages of that group to this group.

Using Pruning & grafting, one can easily control sending unnecessary packets to non-member network. This increases efficiency of RPM scheme of DVMRP.

(iv) Core Based Tree Protocol (CBT)

- In CBT, each AS is divided into regions & we elect one router from each region as core router. A tree is created for transmission to each group, where the core becomes the root of the tree.

Punk

- Initially all routers which want to join a group, send a unicast join message to the core. All intermediate nodes forward this message to the core.
- When all these join messages reach the core, the core constructs a tree to reach all member routers.
- Now the multicast tree is constructed. Any node which want to multicast to the group, now unicast the message to the ~~to~~ core. The core router then forwards that message to all member routers of the tree.

Date ~~/ / /~~

(v) Protocol Independent Multicast (PIM)

- PIM refers to two different protocols: Protocol Independent Multicast-Dense Mode (PIM-DM) & Protocol Independent Multicast-Sparse Mode (PIM-SM)

(A) PIM-DM

→ Used when most of the routers are part of multicasting tree
→ Works like DVMRP, ~~Features~~
→ Uses RPM strategy of DVMRP along with pruning & grafting to construct the multicast tree.
→ A packet is multicasted by a Parent-router if:
① The packet has travelled the shortest path in reaching it
② The packet is forwarded only to those links where some active members of the group exist. If none of its members is an active member of the group, the packet is not multicasted.
→ Difference b/w PIM-DM & DVMRP is that PIM-DM doesn't use a specific unicasting protocol (either RIP or OSPF) unlike DVMRP.

(B) PIM-SM

→ Used when network operates in Sparse mode, i.e., not all routers participate in a group.
→ A group-shared tree approach is more appropriate.
→ Similar to CBT method
→ One of the routers serves as centre point, which stores the multicast tree.
→ All nodes desirous of multicasting, the centre point forwards the packet along the links, as defined by its multicast tree.
→ PIM-SM is more ~~ref~~ resilient to failures, as it provides backup centre point, if there is a failure.
→ One unique feature of PIM-SM is that if the network operates in dense mode, then instead of sharing one centre point b/w all routers of network, it switches to source based tree approach, i.e., every node maintains its own tree information.

Punk

Unit-II

Date __/__/____

Transport Layer

* The main functions of the transport layer are:

(i) Application Addressing / Port Number

Delivery of ~~mess~~ datagram from source port ~~number~~ to destination port using port number.

(ii) Segmentation & Reassembly

This layer breaks info (supplied by application layer) into smaller units called segments. It numbers every byte in segment & maintains their accounting. At destination these segments are recombined to create message.

(iii) Connectionless vs Connection-oriented Service.

Transport Layer provides two types of services: Connectionless & Connection-oriented service.

(iv) Process to Process Flow Control

The transport layer provides ~~two~~ by process to process flow control. ~~upto process level~~

(v) Process to Process Error Control

The transport layer provides process to process error control facility.

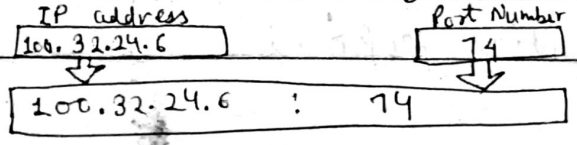
* Port Addressing

- The port numbers are 16 bit integers with a value b/w 0 to 65,535.
- The client process defines itself with a port number randomly chosen. This number is called as an ephemeral port number
- The server process is defined with universal port no. The Internet uses universal port numbers for servers known as well known ports.
- IANA (International ~~Auth~~ Assigned Number Authority) divides the port no. as follows:
  - (i) Well Known Ports: Ports from 0 to 1023 & controlled by IANA
  - (ii) Registered Ports: Ports from 1024 to 49,151 & only registered with IANA to prevent duplication
  - (iii) Dynamic Ports: Ports from 49,152 to 63,535 & neither registered nor controlled by IANA

- Socket Address

The combination of IP address & port address defines a unique host/process combination known as socket address

Ex:-



Punk

* Connectionless vs Connection-Oriented Service

- In connection oriented service, a dedicated connection is established, used & then released. All packets follow the same path.
- In connectionless service, no connection is established. All packets are independent & they can follow different paths to reach a destination.

Date __/__/____

* Reliable and Unreliable Service

- If application layer program needs reliability then the reliable transport layer protocol (TCP) is used for implementing error and flow control at the transport layer. This will be slow & complex.
- If application layer program doesn't need reliability then an unreliable service (UDP) can be used.

* Some well known ports for UDP & TCP both:

1 → tcpmux (TCP port service multiplier)
7 → echo (echo service)
18 → msp (message send protocol)
20 → ftp-data (FTP data port)
21 → ftp (File Transfer Protocol port, sometimes used by FSP [File Service Protocol])
22 → ssh (Secure Shell Service)
23 → telnet (Telnet Service)
25 → SMTP (Simple Mail Transfer Protocol)
37 → time (Time Protocol)
43 → nicname (WHOIS directory service)
69 → tftp (Trivial File Transfer Protocol)
107 → rtelnet (Remote Telnet)
109 → pop2 (Post office Protocol version 2)
110 → pop3 (Post office Protocol version 3)
123 → ntp (Network Time Protocol)

* User Datagram Protocol (UDP)

- Features:

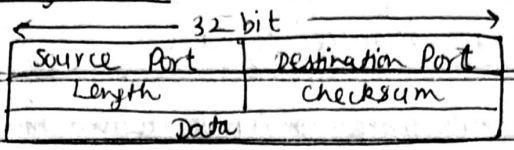
(i) provides a connectionless unreliable service. each UDP datagram contains source & destination socket address.
(ii) no end to end connection is established
(iii) no reliability is assured because no acknowledgement of received datagram
(iv) overheads are very low due to its simple operation
(v) very little error detection performed

Punk

(vi) useful for simple applications which donot require reliability like routing protocols, DNS, etc. & also for real time applications like audio & video

- UDP datagram format: It has a 8-byte header

Date __/__/____



(a) Source port: Optional field indicating port of sending process & if not used, '0'

(b) Destination port: Indicate Internet Destination Address

(c) Length: Size in bytes of UDP packet (Header & data). Min Length is 8 bytes

(d) UDP checksum: Used to verify integrity of UDP header & performed on pseudo header (info obtained from IP header as well as UDP header)

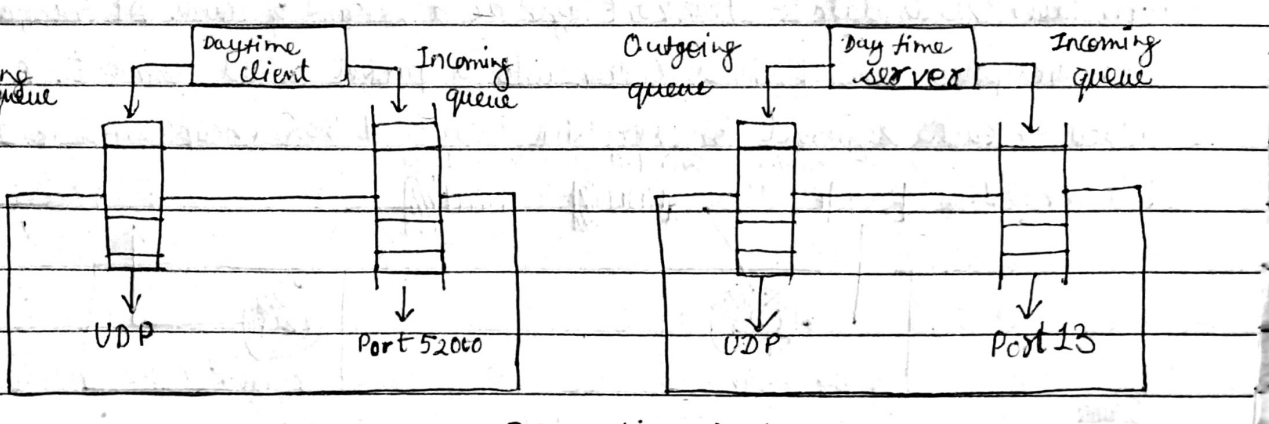
- UDP operation:

(a) Connectionless Service: UDP provides a ~~un~~ connectionless services. Datagrams are not numbered, no connection establishment or release necessary

(b) Flow control & error control: No flow control. No error control mechanism except checksum

(c) Encapsulation & Decapsulation: UDP encapsulates & decapsulates messages in order to send message from one process to another

(d) Queuing: A process starts at client side by requesting port number from OS. Client process is assigned a port no from dynamic port addresses list. One outgoing & incoming queue is also created at client side. The queue function as long as process is running & destroyed as soon as process terminates. Client process can send message to its outgoing queue using source port no. specified in request. UDP removes queue message one by one by adding UDP header & delivers them to IP. If outgoing queue overflow, OS tells client to wait. When client receives message, UDP checks if incoming queue exists. If not, then UDP discards user datagram. If incoming queue overflows, UDP discards datagram & arranges to send "port unavailable" message to server. On other hand, the Server asks for the incoming & outgoing queue using its well known ports as soon as it starts running. The queues exists as long as server is running.



Ex of Queue operation in UDP

Punk

* Transmission Control Protocol (TCP)

- Features:

(i) provides reliable transmission of data in an IP environment

(ii) provides facility of stream transfer of data Date __/__/____

(iii) Stream data transfer makes it possible for TCP to deliver an unstructured stream of bytes to the destination.

(iv) TCP group bytes into segments & passes them to IP for delivery.

(v) TCP provides end-to-end reliable packet delivery

(vi) The reliability mechanism allows devices to deal with lost, delayed, duplicate or misread packets

(vii) TCP offers efficient flow control, i.e., when sending acknowledgements back to source, the receiving TCP process indicates highest sequence no. it can receive without overflowing its internal buffers.

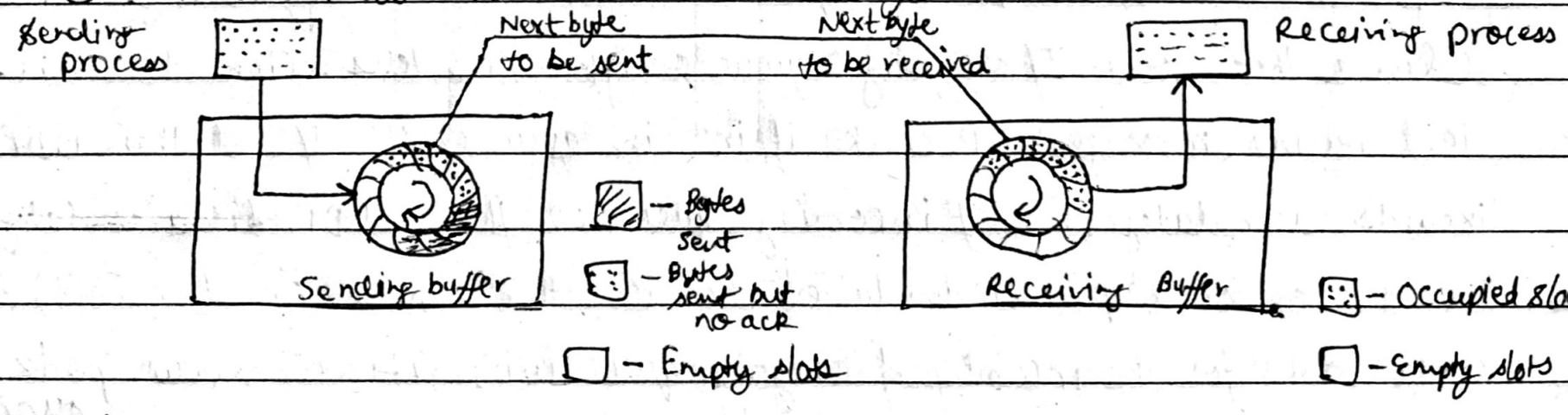
(viii) TCP Buffering ≡ #TCP maintains two buffers at each node → a sender buffer & a receiver buffer.

At the sender node, the buffer contains three kinds of slot →

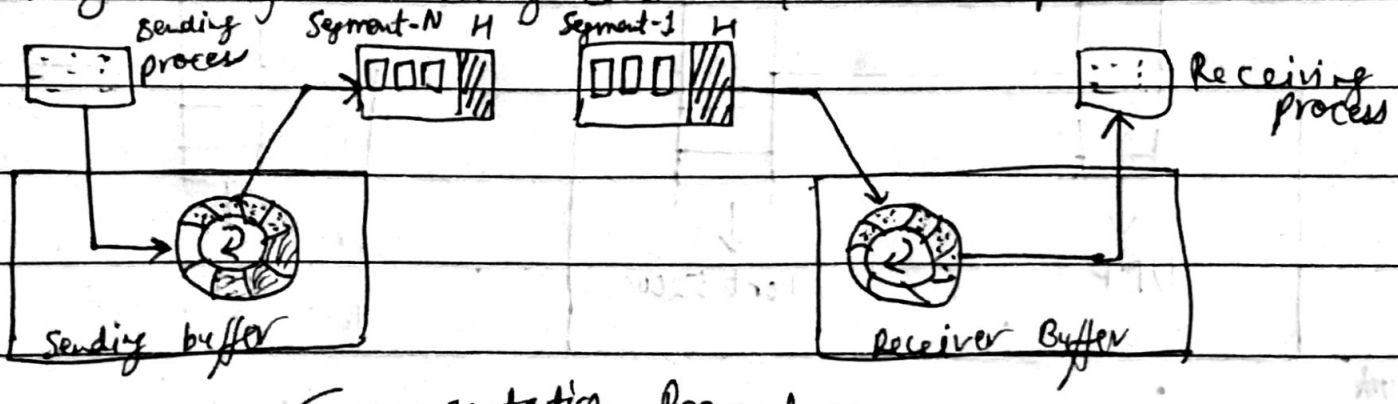
1. Packets sent, but awaiting acknowledgements
2. Packets that are not yet sent
3. Slots which are empty & ready for occupancy

#At the receiver side, buffer consists of two kinds of slot →

1. Slots which are empty & ready for occupany
2. Packets that have not been read yet.



(ix) IP layer sends data in form of packets & not as stream of bytes. However, upper layer sends data to transport layer as a stream of data. At transport layer, TCP groups a no. of bytes together into a packet called segment. A header is added to each segment for exercising control & then encapsulated in IP datagram & transmitted.



Segmentation Procedure

Punk

⊗ TCP always work in full-duplex mode.

– TCP Operation:

Ⓐ Byte, Sequence & Acknowledgement Numbering

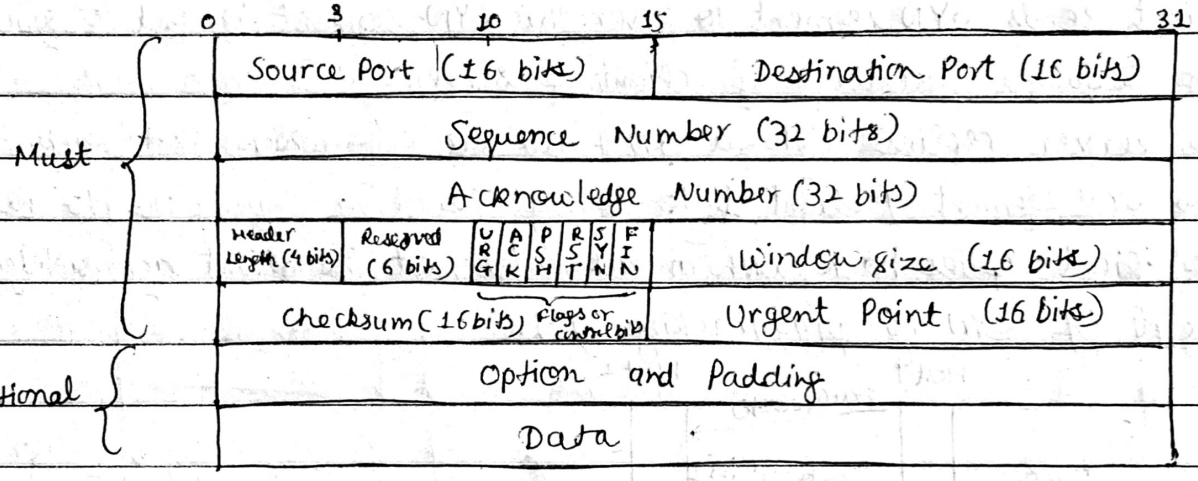
Date __/__/____

① Each byte in TCP is numbered: Bytes in TCP are numbered sequentially. The starting number is a random number & independent in each direction. This starting no. can be any no. b/w 0 & $2^{32}-1$.

② The Segments are also numbered by their Sequence Numbers: The sequence no. for a segment is the byte number of first byte.

③ Acknowledgement Number: Received Bytes are acknowledged in TCP. The acknowledgement no. is the byte no. of next byte, which a node expects to receive. If byte no. x then ack x+1.

Ⓑ TCP Segment Header: TCP segment consists of header & optional data. Header varies from 20 to 60 bytes in length.



① Source Port: Identify sending host application

② Destination Port: Identify receiving host application

③ Sequence No.: Identify current position of 1st byte in segment. After reaching $2^{32}-1$, no. wrap around to '0'.

④ Acknowledgement No.: Identify next byte sender expects from receiver

⑤ Header Length or Offset: Specifies total TCP Header length. Min 20 byte & max 60 byte.

⑥ Reserved: Reserved for future use

⑦ Control Bits or flags: (i) URG (Urgent Pointer): Set 1 if TCP need to interpret urgent pointer field

(ii) ACK (Acknowledgement): Set 1 if ack no. field is valid

(iii) PSH (Push func^n): Set 1 if receiver should deliver this segment to application as soon as possible

(iv) RST (Reset the Connection): Set 1 if signals receiver that sender is a right connection

(v) SYN (Synchronize Sequence No.): If 1 then sender attempting to achieve sequence no.

(vi) FIN (No more data from sender): If 1 then end of stream from current TCP connection

Punk

(8.) Window: Tells sender how much data receiver willing to accept

(9.) Checksum: Used to verify integrity of header

(10.) Urgent Pointer: Used to notify receiver of urgent data

(11.) Options: To provide additional functionality

(12.) Padding: To pad TCP header with '0s' so that segment ends on 32-bit word boundary

Date __/__/__

(13.) Data: ~~Carrie~~ variable length field carrying application data from TCP sender to receiver

(C) TCP Connection Establishment: (Uses three way handshake)

→ Three Way Handshake

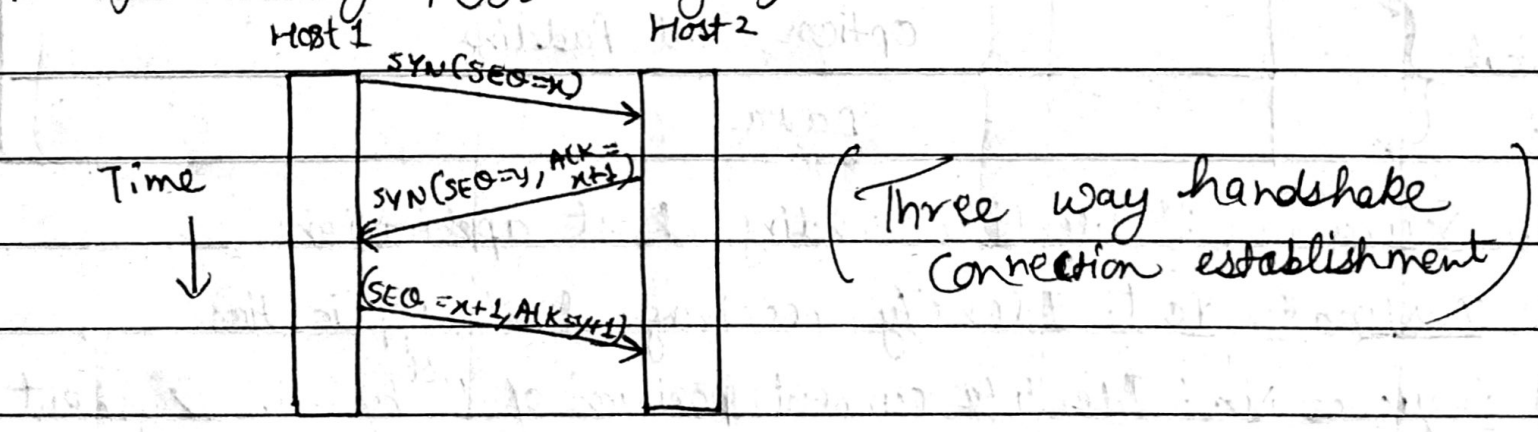
⇒ TCP establishment process is known as Three way Handshaking. When the ~~Stg~~ server is ready to establish a connection, its TCP issues a "Passive Open" request. This "passive open" request is an indication that server is ready to accept requests from clients. A client wanting to connect to this server issues an "Active Open" request.

⇒ Steps:

(1.) Client sends SYN segment to server. This SYN segment is used to synchronise the sequence numbers of client & server.

(2.) The server replies with a SYN + ACK segment which is to acknowledge the SYN segment of client & to convey the Server Sequence NO. to the client

(3.) The client replies back with an acknowledgement. The client acknowledgement receipt of SYN by piggybacking y+1.



(Three way handshake Connection establishment)

(D) Data Transfer

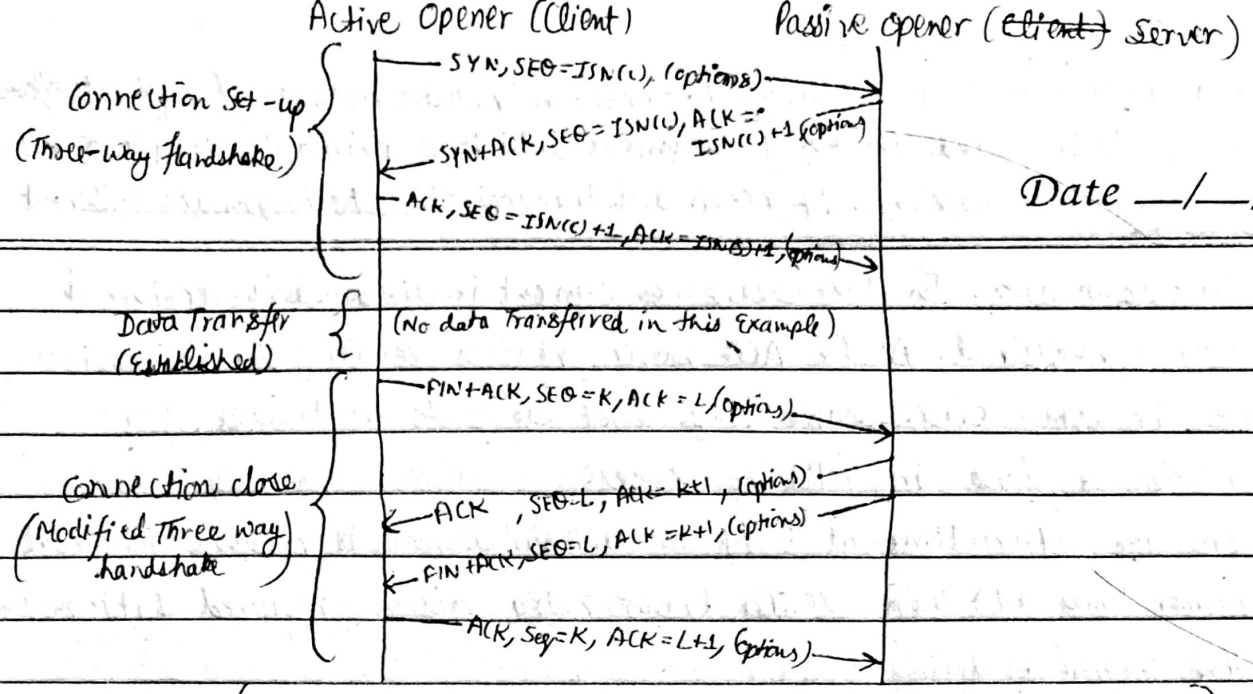
→ After the connection has been established, both server and client can send data to each other in form of segments. Received Bytes are acknowledged by Piggybacking Acknowledgements to the segments. The last byte received is acknowledged by sending the sequence no. of next expected byte.

(E) Connection Termination

→ The connection termination is again a three way handshake process. The client wanting to close the connection sends a FIN (Finish) segment to server.

→ The server responds by sending an acknowledgement of the FIN segment. The server acknowledges the receiving of FIN segment by sending a FIN+ACK segment

→ Finally in the end, the client replies by sending an ACK. This ACK segment Punk acknowledges the receipt of server FIN.



Date __/__/____

(Connection Establishment & Termination of TCP)

– TCP Flow Control

→ TCP flow control mechanism uses a sliding window but different from sliding window of data link layer and is of variable size.

→ TCP flow control sliding window is maintained at senderend but controlled by receiver & the network. Receiver gives instructions about the load that it can receive & sender obey these instructions.

→ The bytes stored in the window are the ones which are transmitted by sender but yet to be acknowledged by receiver.

→ Once acknowledged, these bytes removed from window to may way for new bytes.

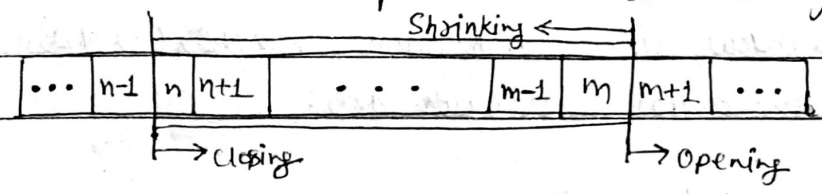
→ Window is variable in size (↑ or ↓) & has left & right wall. Moving left wall towards right is equivalent to closing window & moving right wall towards right is equivalent to opening the window. No. of bytes b/w left & right wall determine the size of window in bytes.

→ The receiver conveys the size of window it expects & this is known as RWND.

→ The network also monitors congestion in network & accly conveys size of window. This is known as CWND.

→ The size of window at any time is equal to minimum of RWND & CWND values. This is used for flow control sliding window as the sender can send bytes without waiting for acknowledgements.

→ Since the sender can only send bytes equal to window size, therefore flow control is maintained. This sender doesn't swamp the receiver with more bytes than it can handle.



Window size = min(RWND, CWND)

Punk

– TCP Error Control

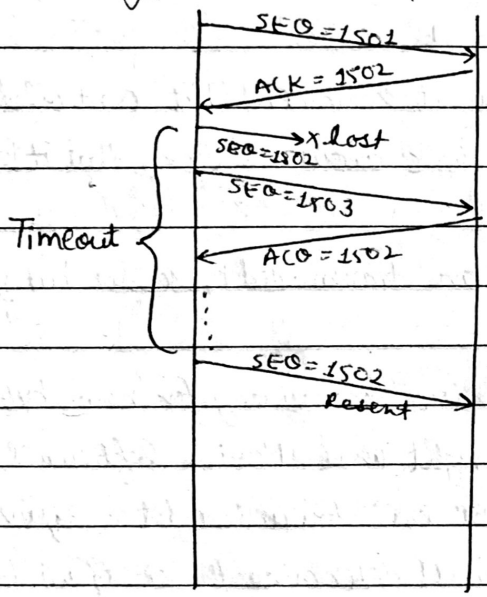
→ TCP uses a mechanism for detection & correction / retransmission of segments affected.

→ The checksum is included in every segment which is primarily used to detect any error during transmission. If received & transmitted Data checksum are different then error in transmission. In this case, the segment is discarded by receiver & retransmission is required. As the 'ACK' never reaches sender, sender realises that there is some error. Same way lost segments are treated.

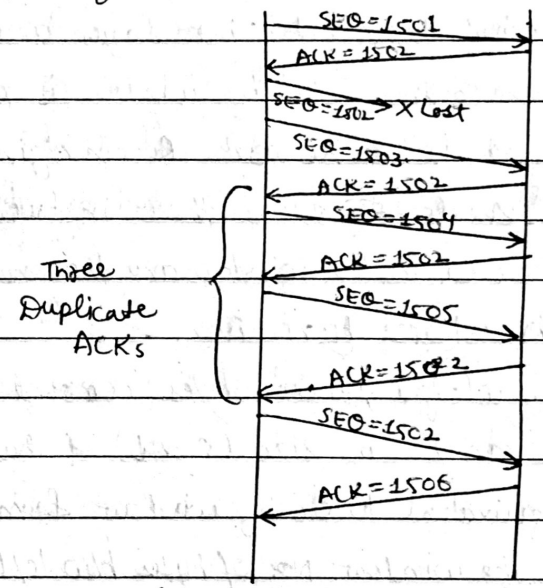
→ A retransmission is done in following cases:

Ⓐ Retransmission After Timeout: If no acknowledgement is received & timeout occurs (Timer times out) then sender know retransmission required & it immediately sends the segment again.

Ⓑ Retransmission after three Duplicate Acknowledgements (Fast Retransmission): If the sender receives three duplicate acknowledgements before its timeout, it immediately retransmits the missing segment. In this case, sender doesn't wait for timeout & responds quickly. This method is known as Fast Retransmission.



(Retransmission After Timeout)



(Retransmission after 3 duplicate ACKs)

– TCP Congestion Control

→ TCP also keeps track of congestion in the network. The TCP monitors congestion, i.e., the maintains a congestion window (CWND). The size of congestion window is decreased whenever some congestion is noticed.

→ The Congestion control also controls the same Sliding Window at the receiver end. The size of the sliding window is taken as minimum of Receiver window (RWND) & the congestion window (CWND).

Sliding window size = minimum (RWND, CWND)

→ Some TCP Congestion Control Strategies are:

Punk

① Slow Start & Exponential Increase : Size of CWND kept minimum, i.e., equal to 1 Maximum segment size (MSS) & on receipt of each acknowledgement the CWND size is doubled. In this way, there is exponential increase

Phase	Initial CWND	Condition Fulfilled	New CWND
1	1	1 ACK received	2
2	2	2 ACK received	4
3	4	4 ACK received	8
4	8	8 ACK received	16
⋮	⋮	⋮	⋮

Thus, Slow start & exponential increase make a cautious start but window size increases rapidly after successful acknowledgements. This process of exponential increase continues until an upper limit known as Slow Start Threshold (ssthresh) is reached. Once the ssthresh is reached, TCP enters Congestion Avoidance Phase.

② Congestion Avoidance (Additive Increase) : In this phase when all segments of a window are acknowledged, CWND is not doubled, but it is incremented by only 1 MSS.

Phase	Initial CWND	Condition fulfiled	New CWND
K	m	m ACK received	m+1
K+1	m+1	m+1 ACK received	m+2
K+2	m+2	m+2 ACK received	m+3
K+3	m+3	m+3 ACK received	m+4
⋮	⋮	⋮	⋮

③ Multiplicative Decrease : Whenever a retransmission is done, the Slow Start Threshold (ssthresh) limit is reduced to 1/2 of current window size. This process is known as Multiplicative Decrease.

* TCP Tahoe

- It is the simplest congestion control algorithm of TCP. Initially, TCP starts with a slow start exponential growth congestion window. Once ssthresh limit reached, CWND grows additively. But in case a retransmission is required following actions taken :

① Tahoe performs a fast retransmission of the missing segment. This missing segment is known from the 3 duplicate ACKs received or retransmission timeout.

② Tahoe set the Slow Start Threshold limit (ssthresh) to half the current window size. Ex:- If current CWND = 256 then $ssthresh_{limit} = 128$

③ CWND size is reset to 1

④ The slow start phase is started again

- The TCP Tahoe doesn't distinguish retransmission due to three duplicate ACKs & retransmission due to Timeout.

Punk

* TCP Reno

Date __/__/____

- It is the most widely used congestion control algorithm of TCP.
- Initially TCP starts with a Slow Start & Exponential Growth Congestion Window. Once upper limit of ssthresh is reached, the congestion window grows additively.
- In case of retransmission, TCP Reno behaves differently depending on retransmission is due to 3 duplicate ACKs or a timeout:

(i) Retransmission Due To Timeout: (Same as TCP Taheo)

(Steps) (A) TCP Reno performs a fast retransmission of the missing segment.

(B) It resets ssthresh limit to half of current window size.

(C) CWND size is reset to 1

(D) The Slow Start phase is started again.

(ii) Retransmission Due To Three Duplicate ACKs: (Different from TCP Taheo)

(Steps) (A) TCP Reno performs a fast retransmission of the missing segment. This missing segment is known from 3 duplicate ACKs received

(B) TCP Reno sets the ssthresh limit to half of current CWND.

(C) CWND size is reset to half of its previous value, i.e., $CWND = \frac{CWND}{2}$, which is equal to new ssthresh

(D) TCP enters the Congestion Avoidance with Fast Recovery Phase. When all bytes of window are acknowledged, then CWND is incremented by 1. This method is known as Fast Recovery because CWND is not reset to 1 like in Tahoe. It assumes that only one intermediate segment is lost, while others may have reached the destination.

Unit-III

Date __/__/____

Optical Networking

* Introduction To Optical Networking

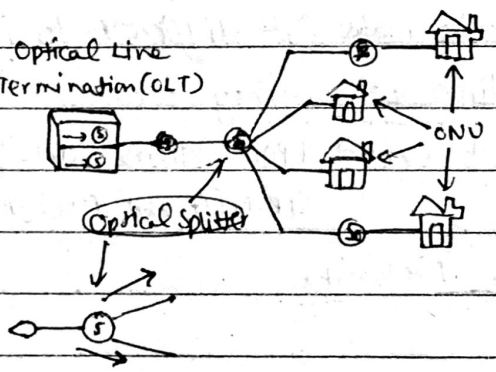
- Optical fibers are very thin glass cylinders or filaments which carry optical signals (signals in the form of light).
- An optical network connects multiple computers & other peripheral devices which can store & generate data in electrical form. During data communication, an optical network utilizes optical devices to generate electrical signals, & amplify & recover the signal that have been transmitted over the network and route the electrical signal
- Theoritically it is possible to send 50x1012 bits per second using a single fiber

	Optical fiber	Copper wire
1.	very expensive hence need optimized installation in network	Not costly
2.	Multiple optical signal may be transmitted by one optical fibre (WDM- Wavelength Division Multiplexing)	Only one signal is transmitted
3.	speed of transmission of optical fiber is far greater that current data processing speed of end terminals	Speed of transmission matches the data processing capabilities of end terminals.
4.	Not easy to maintain	Maintenance is easy

- Characteristics of Optical Network

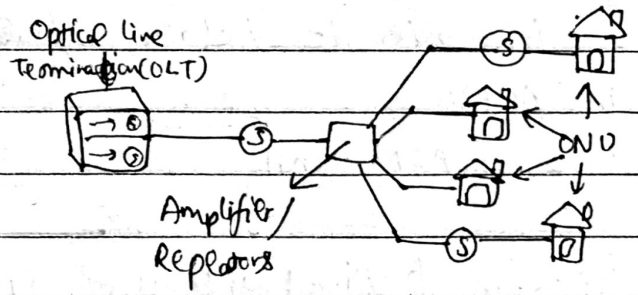
→ Low signal attenuation → Low signal distortion → Low power requirement
→ Low material usage → Small space requirement → Low cost

- Types of Network Designs for Optical Networks



ONU = optical Network Unit

Passive optical Network (PON)



ONU = optical Network Unit

Active Optical Network (AON)

Punk

Date __/__/____

AON	PON
- Active Optical Network	- Passive optical Network
- It requires electricity powered switching equipment like routers or a switch aggregator to manage signal distribution & direction to the correct end users. These switches open & close to ensure that the outgoing & incoming messages are going in the right direction	- It does not require electrically powered equipment & rather makes use of optical splitters to separate & collect optical signals that move through the network.
- Subscribers have a dedicated fiber optic strand	- Shares fiber optic strands for a portion of network
- Uses active components like amplifiers, repeaters or shaping circuits to manage signal distribution	- Uses optical splitters to separate & aggregate the signal
- AON networks can cover a range to about 100 km	- Every time the signal is split two ways, half the power goes one way & half the other therefore PONs have a shorter range of coverage limited by signal strength. A PON is typically limited to fiber cable runs of upto 20km.
- Flexible soln suitable for business	- Rigid soln suitable for residential
- Higher building cost as active networks require more fiber.	- PONs have a Low building cost with lower maintenance costs
- It is easier to isolate a fault in AONs.	- PONs also make it difficult to isolate a failure when they occur
- Types of AON → nil	- Types of PON → EPON (Ethernet PON) (Symmetrical) GPON (Gigabit PON) (Asymmetrical)

* Benefits & Disadvantages of Optical fibers Networks

(1.) ~~Greater~~ (Advantages)

(1) Greater bandwidth: Fiber provides more bandwidth than copper & has standardised performance upto 10 Gbps & beyond.

(2.) Speed & Distance: very little transmission loss & data move at higher speed & greater distances. Distances can range from 550 m (1804.2 ft) for 10 Gbps multimode & upto 40 km (24.8 mi.) for single-mode ~~optic~~ cable.

Date __/__/____

(3.) Security: It doesn't radiate signals & is extremely difficult to tap. If the cable is tapped, it's very easy to monitor because cable leaks light, causing entire system to fail.

(4.) Immunity & Reliability: It provides extremely reliable data transmission. It's completely immune to many environmental factors that affect copper cable.

(5.) Design: Fiber is lightweight, thin, & more durable than copper cable.

(6.) Migration: The proliferation & lower costs of media converters are making copper to fiber migration much easier.

(7.) Easier Field Termination

(8.) Cost: The cost for fiber cable, components & hardware has steadily decreased.

(Drawbacks)

(1.) Higher initial cost in installation

(2.) High cost of connector & interfacing requires specialized & sophisticated tools for maintenance & repairing.

* SONET Architecture :- Digital transmission standard for fiber-optic cable.

- Independently developed in USA & Europe
- SONET (Synchronous Optical Network) by ANSI
- SDH (Synchronous Digital Hierarchy) by ITU-T
- Synchronous network using synchronous TDM multiplexing
- All clocks in the system are locked to a master clock.
- It contains the standard for fiber-optic equipment
- very flexible to carry other transmission systems (DS-0, DS-1, etc)
- Before SONET, DS Digital Carrier System (DS Digital Signal Hierarchy), ISDN & BISDN for optimizing network.
- PCM T-Carrier Hierarchy

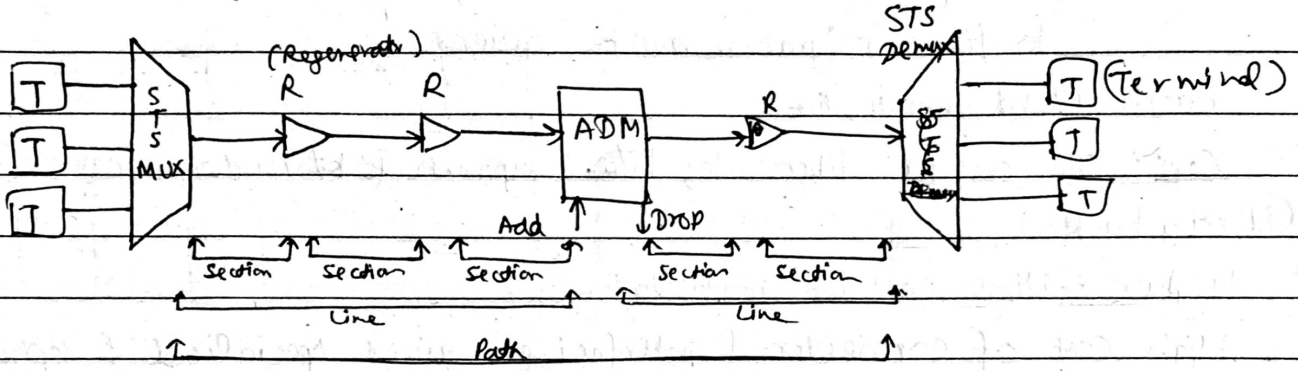
Digital Signal Designation	Line Rate	Channels (DS0)	Line
DS0	64 kbit/s	1	—
DS1	1.544 Mbit/s	24	T1
DS1C	3.152 Mbit/s	48	T1C
DS2	6.312 Mbit/s	96	T2
DS3	44.736 Mbit/s	672	T3
DS4	274.176 Mbit/s	4032	T4
DS5	400.352 Mbit/s	5760	T5

Punk

Date __/__/____

The SONET architecture is as follows:

- Architecture of a SONET system : signals, devices, & connections
- Signals : SONET (SDH) defines a hierarchy of electrical signalling levels called STSs (Synchronous Transport Signals, (STMs)), Corresponding optical signals are called OCs (Optical Carriers)
- SONET Devices : STS multiplex/demultiplexer, regenerator, add/drop multiplexer (ADM), terminals



(Sonet Architecture)

- Connections : SONET devices are connected using sections, lines & paths
- Section : optical link connecting two neighbour devices
- Lines : Portion of network b/w two multiplexers.
- Paths : end-to-end portion of network b/w two STS Multiplexer

SONET Add-Drop Multiplexer

- Complex system of pointers locates channels within a payload, payloads within a frame
- Facilitates rapid access, removal & insertion of data without regenerating SPE

SONET Pointers Frame, SPE payload which can slip or "float" within STS frames.

- POH pointer describes payload channels
- LOH pointer describes entire payload
- Each SONET node recalculates pointers to determine exact payload starting point

Payload can "straddle" more than one STS frame

- pointers in LOH indicate start of payload in each frame.

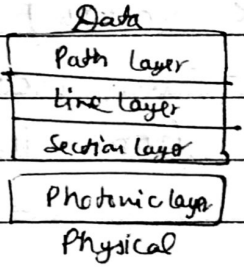
Punk

Date __/__/____

Transportation of T-carrier services within SONET STS-1 frame (51.84 mbps)
- STS-1 designed for DS3 (44.736 mbps) tributary.
- SONET Virtual Tributaries (VT) carry lower data rate signals eg DS1, DS2, E1
- SONET VT resembles STS frame structure
  ⇒ VT carries its own Transport & PO
- VT(s) may be locked or float within STS frame
- VT(s) byte interleaved within respective SPE
- Uses STS-1 SPE

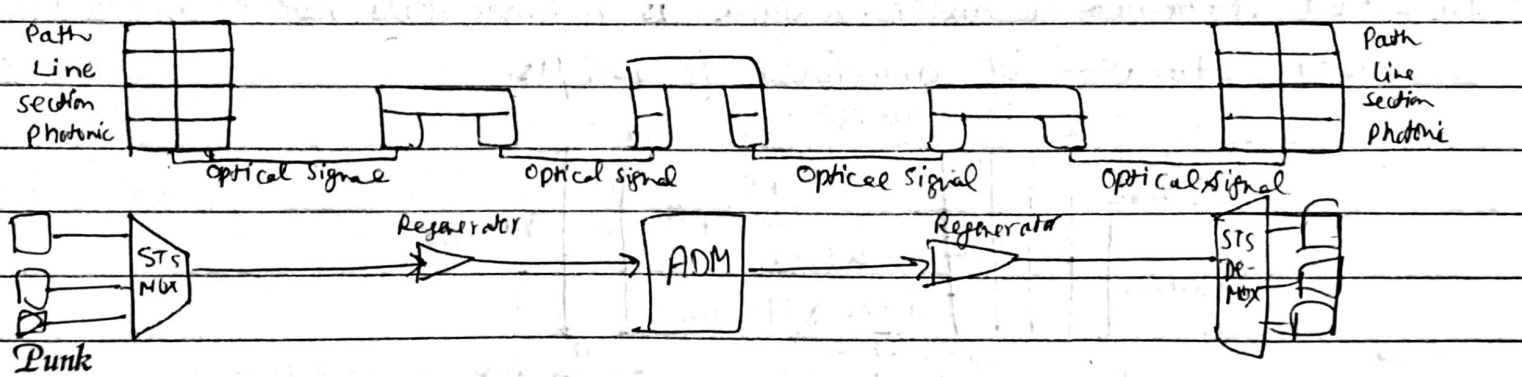
High data rate or broadband tributary signals may require data rates greater that STS-1 SPE capacity (51.84 mbps)
- High capacity STS-N frames assembled from multiple byte interleaved STS-1 frames
- High data rate signals mapped directly into STS-Nc (concatenated frames)
- 3 STS-1 frames concatenated form STS-3c or OC-3c
- 51.84 mbps x 3 = 155.52 mbps

*Sonet Layered Architecture

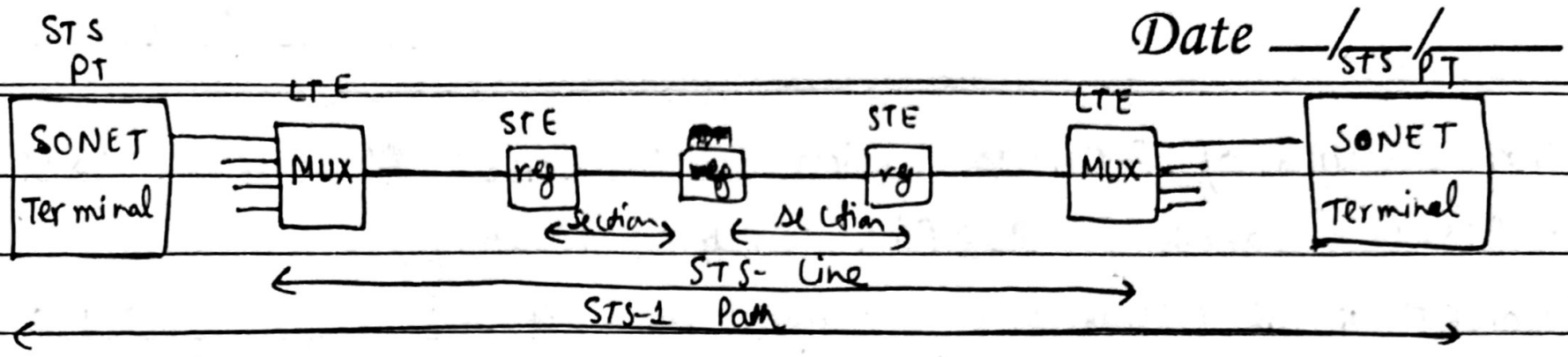


- SONET defines four layers: path, line, section & photonic

Layer	Functions
Photonic	Responsible for conversion b/w STS signal & OC signals
Section	Implements framing, scrambling, error monitoring, section maintenance
Line	Synchronization, Multiplexing, Error Monitoring, Line Maintenance, Protection Switching are functions of Line Layer
Path	Maps signals into format required by line layer. Also read, interprets & modifies path overhead for performance monitoring & automatic protection switch



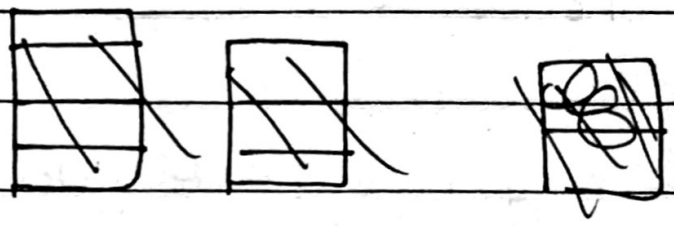
Punk

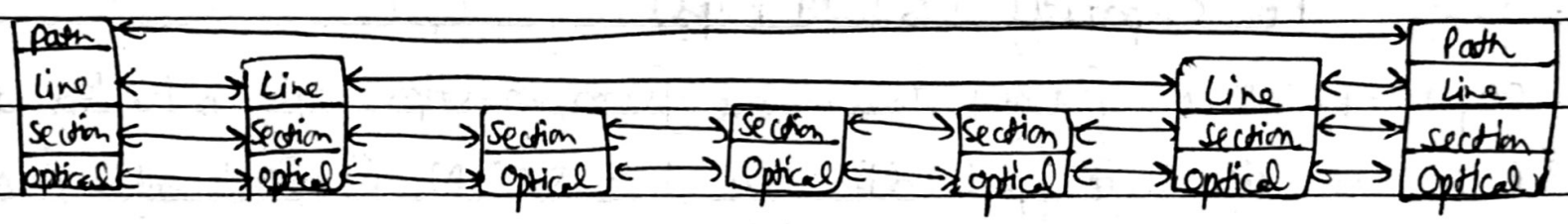


STE: Section Terminating Equipment eg:- repeator

LTE: Line Terminating Equipment eg:- STS-1 to STS-3 multiplexer

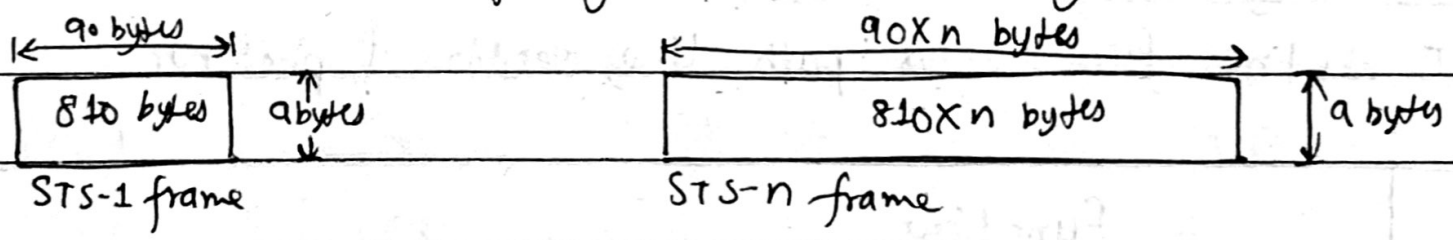
PTE: Path Terminating Equipment eg:- an STS-1 multiplexer



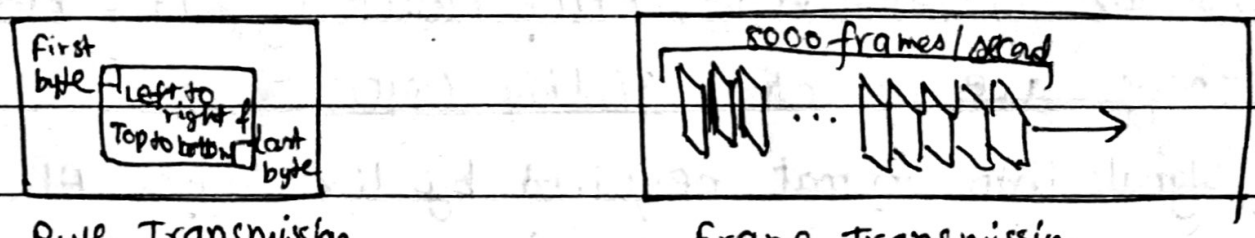


* SONET Frame Format

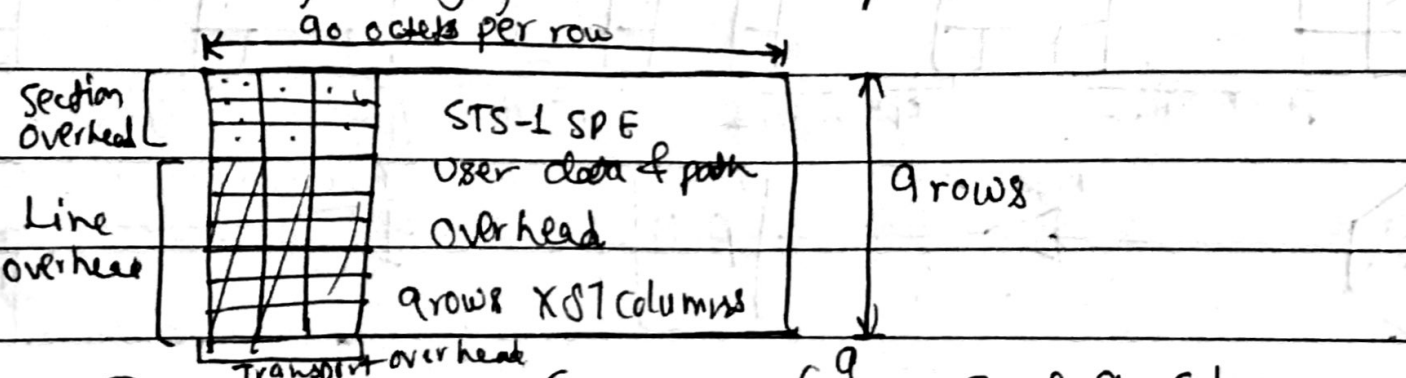
- Each synchronous transfer signal STS-n is composed of 8000 frames. Each frame is a 2D matrix of bytes with 9 rows by 90 x n columns



- A SONET STS-n signal is transmitted at 8000 frames per second
- Each byte in a SONET frame can carry a digitized voice channel



- In SONET, data rate of an STS-n signal is n-times data rate of an STS-1 signal
- In SONET, duration of any frame is 125 μs.



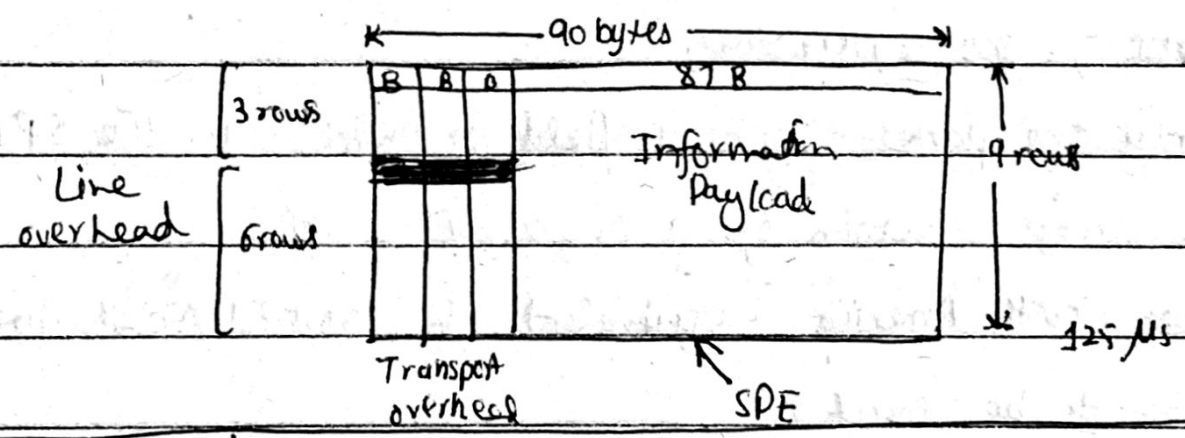
Basic STS-1 frame of 9 rows & 90 columns

Punk

Date __/__/____

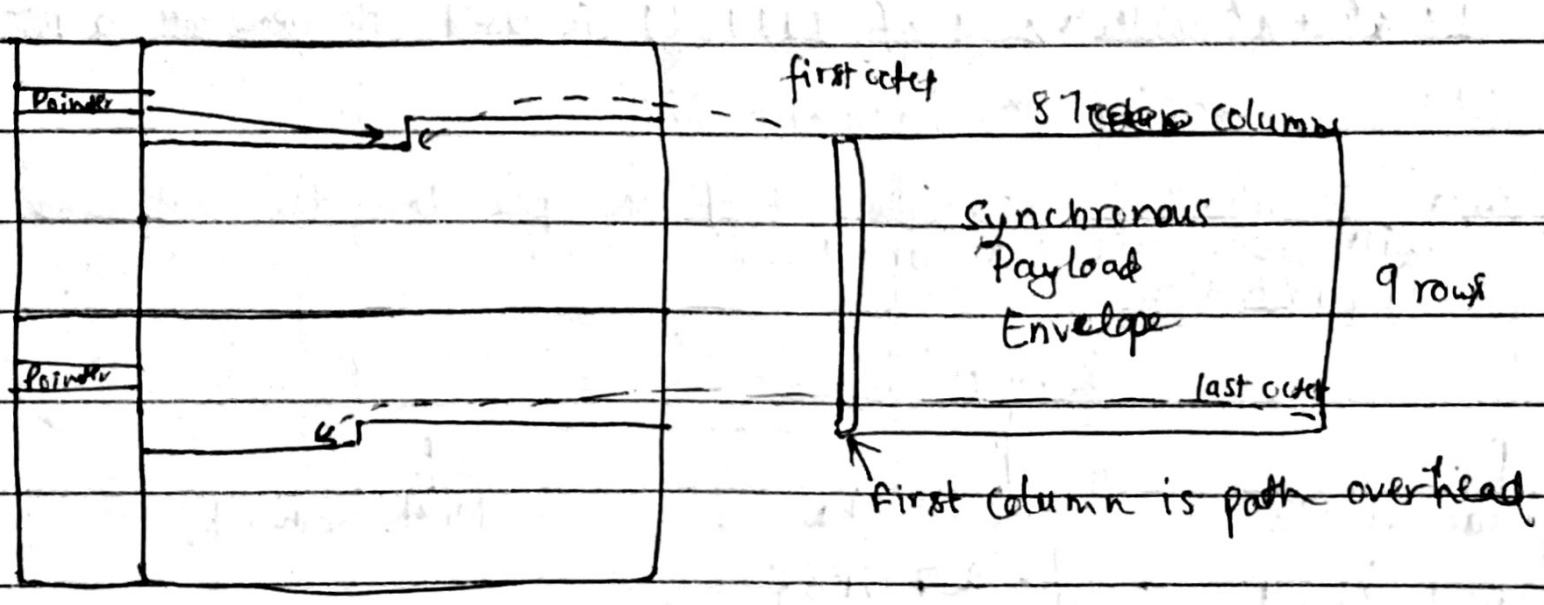
- Transmission is carried out row wise from left to right & from top to bottom. Bits are transmitted serially.
- STS-1 frame of SDH is composed of section overhead, transport overhead, payload overhead & data part
- SONET/SDH is referred as octet synchronous. The first three columns of SONET frame is referred as transport overhead. The next 87 columns of frame are referred as Synchronous Payload envelope (SPE). Payload overhead is part of SPE
- STS-1 is referred as OC-1 (Optical Carrier) after scrambling is done on STS-1.

SONET frame



overhead	Function
Section	Performance monitoring (STS-n signal), Local overwire, Data communication channel to carry info on OAM&P, framing
Line	Locating SPE in frame, multiplexing or concatenating signals, performance monitoring, automatic protection switching & line maintenance
STS Path	Performance monitoring of STS SPE, Signal label, Path Status, Path Trace
VT Path	Provide Communication b/w VT SPE & its point of assembly, error checking, signal label & path status

SPE straddling SONET frame



Punk

SPE straddling SONET Frame

Date __/__/____

- SPE (Synchronous Payload Envelope) contains user data & overhead related to user data (path overhead)
- Path overhead is only calculated for end-to-end at STS multiplexer
- All SONET network elements are integrated into a synchronization hierarchy.
- STS-N frame is sent every 125 msec whether there is data to be sent or not.
- SONET integrates OAM&P in the network. SONET has a fix size SPE.
- A standard STS-1 frame is nine rows by 90 bytes.
- The combination of the section & line overhead comprises the transport overhead, & the remainder is SPE.
- In STS-3 frame is nine rows by 270 bytes, the SPE contains three separate payloads & three separate path overhead field. It is the SPE of three separate STS-1s packed together, one after another.
- In STS-3c, there is only one path overhead field for entire SPE. The SPE for an STS-3c is a much larger version of a single STS-1 SPE.
- STM-1 is the SDH (non-North American) equivalent of SONET (North American) STS-3 frame (STS-3c to be exact).
- Interleaving in SONET / SDH

STS-3 frame is formed using three STS-1 frame with the help of interleaving technique. The interleaving is octet type, i.e., A 1 octet from 1st, 2nd & 3rd STS-1 frame is taken first then A 2 octet from all these three frame are taken and transmitted.

- Scrambling in SONET

⇒ SONET uses NRZ coding, 1 = Light on, 0 = Light off

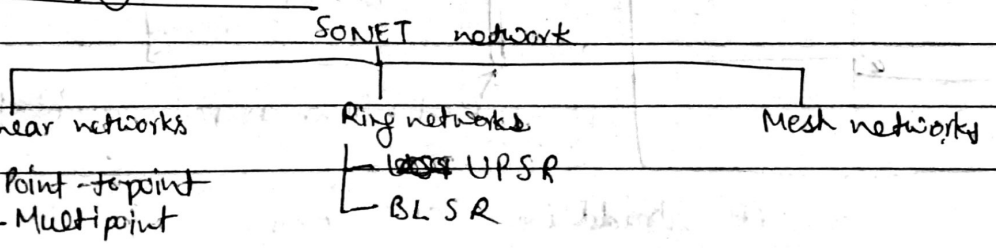
Too many 1's or 0's result in loss of bit clocking information

All bytes (except some overhead bytes) are scrambled

Polynomial $1 + x^6 + x^7$ with a seed of 111111 is used to generate a pseudorandom sequence which is XOR'ed to incoming bits.

If user data is identical (or complement of) the pseudorandom sequence, the result will be all 0's or 1's.

* SONET Configuration

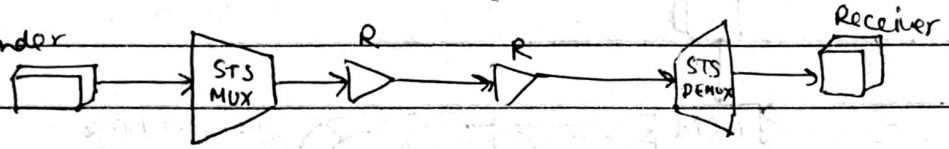


Punk

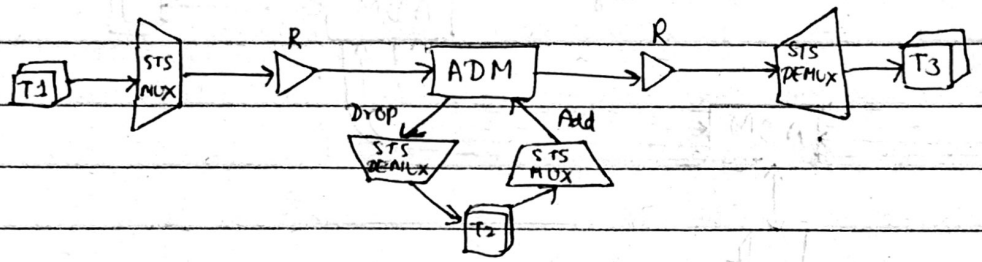
Date __/__/____

- SONET Topologies

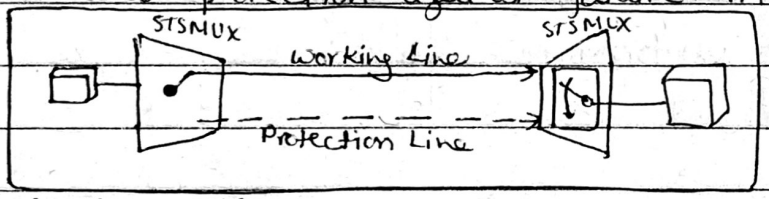
→ Point-To-Point Network : (10-40 Gbs) ultrahigh speed, ultrahigh aggregate bandwidth, high signal integrity, great reliability & fast path restoration capability



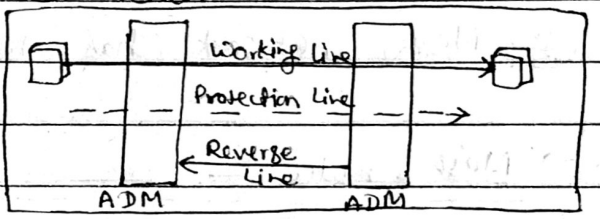
→ Multipoint network.



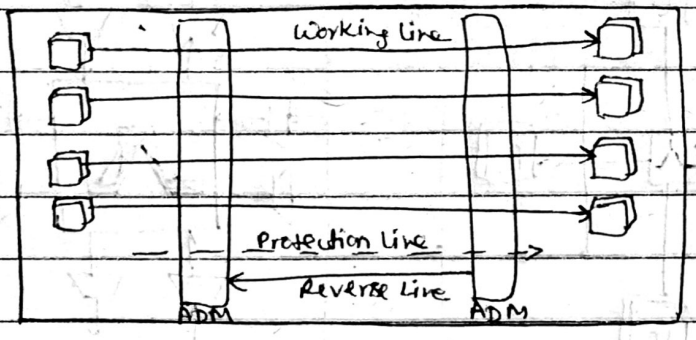
To create protection against failure in linear networks



One-plus-one APS

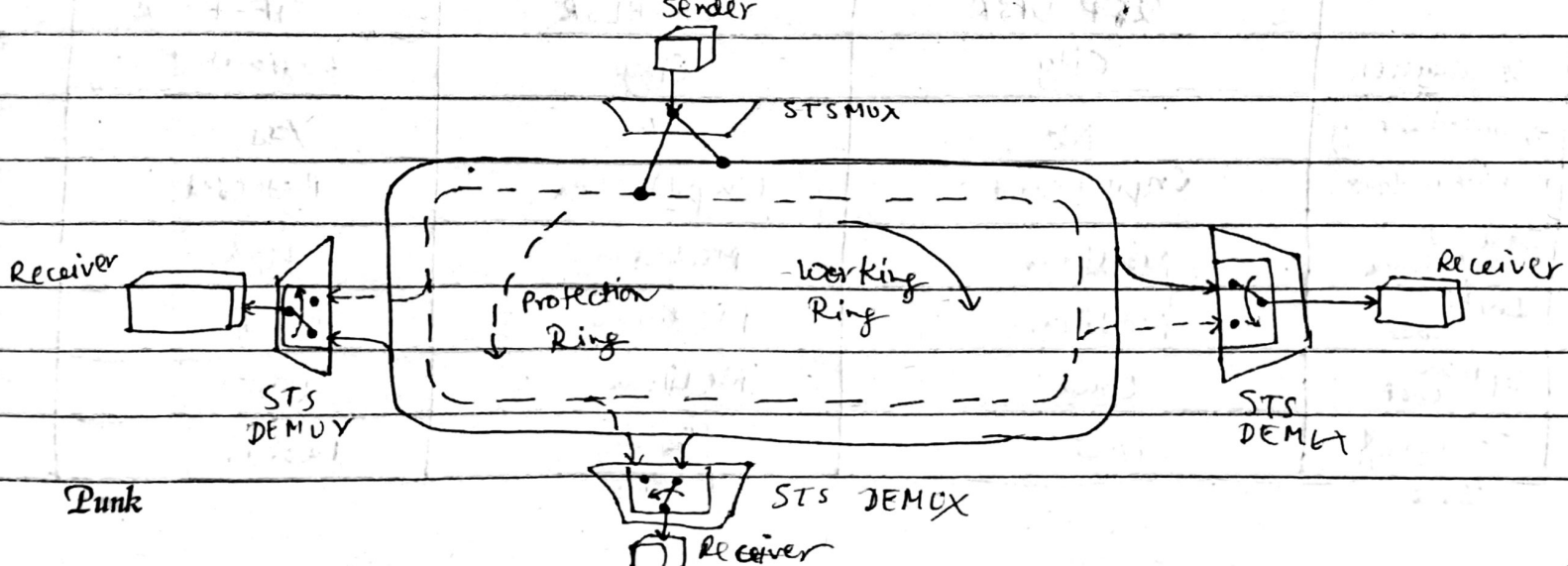


One-to-one APS



One-to-many APS

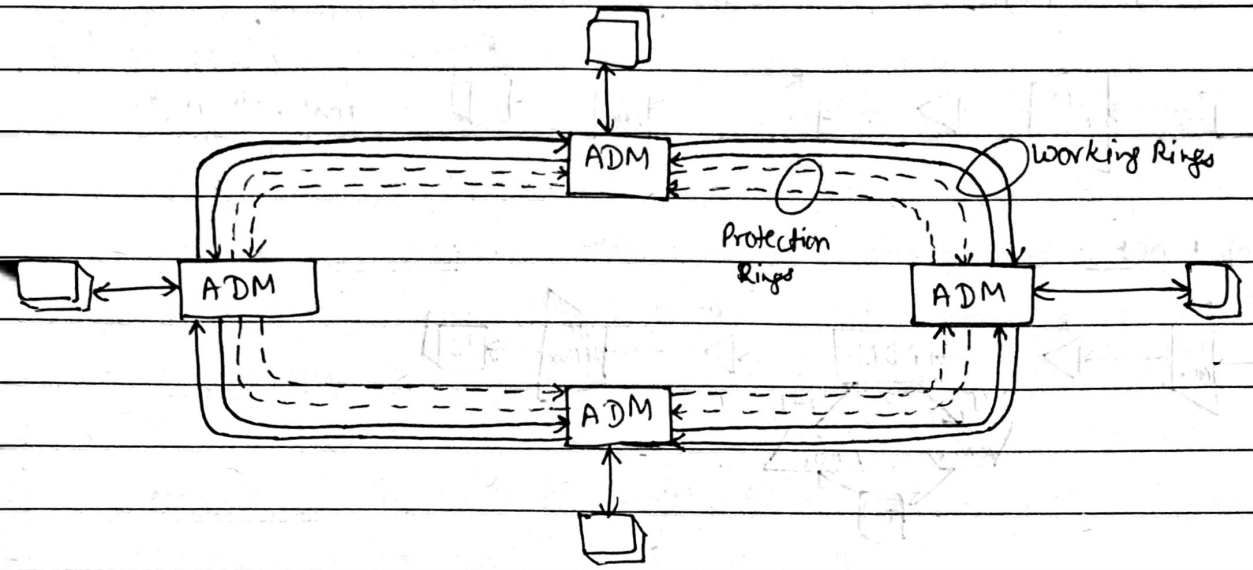
→ Ring Network : UPSR (Unidirectional Path Switching Ring)



Punk

Date __/__/____

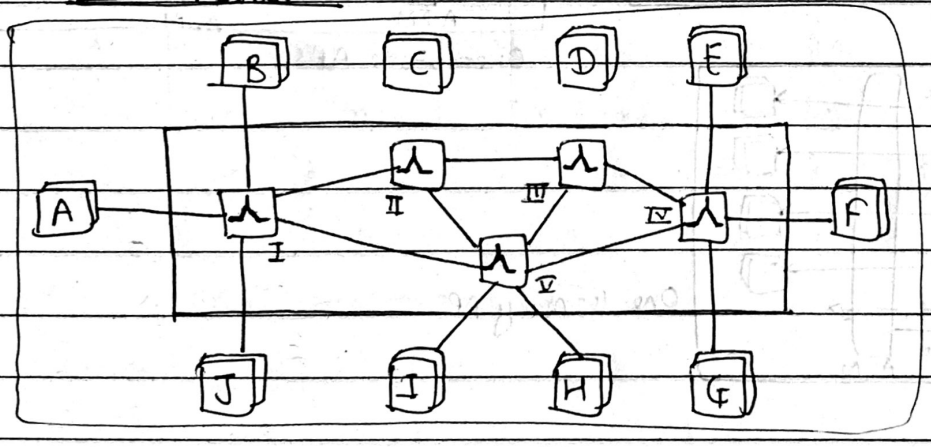
→ Ring Network : BLSR (Bidirectional Line Switching Ring)



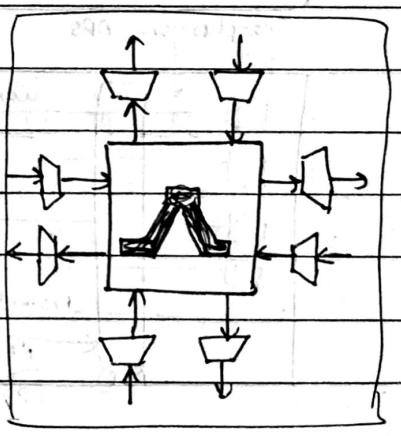
(#) Ring network has lack of scalability

(#) Mesh network has better performance

→ Mesh network



Mesh network



Cross Connect Switch

	UPSR	2f-BLSR	4f-BLSR
Usually seen	City	City	Regional †
Symmetrical Delay	No	Yes	Yes
Multiple failures	Unprotected	Unprotected	Protected
Bandwidth Efficiency	Medium	Medium	High
Initial Cost	Medium	Medium	High
Expansion Cost	Low	Medium	Low
Complexity	Low	High	Medium

Punk

Date __/__/____

Ring Type	Maximum Per Node
All rings	5
BLSRs	2
2-fiber BLSR	2
4-fiber BLSR	1
UPSR	4

* SONET Advantages and Disadvantages.

- The fact that SONET is highly standardized offers benefits of interconnectivity & interoperability between equipment of different manufacturers.
- SONET/SDH is fully extendable to the customer privileges.
- SONET local loop provides many end to end advantages
- SONET supports aggregation of all kinds of traffic, including data, voice & video
- It is attractive for all kinds of traffic including bandwidth intensive applications and its resiliency is a major plus factor.
- It offers high security due to the difficulty of tapping into fiber optic links
- A major disadvantage is its high cost.
- The full advantages of SONET are better leveraged by circuit-switched traffic in comparison to the packet-switched counterpart.

Punk

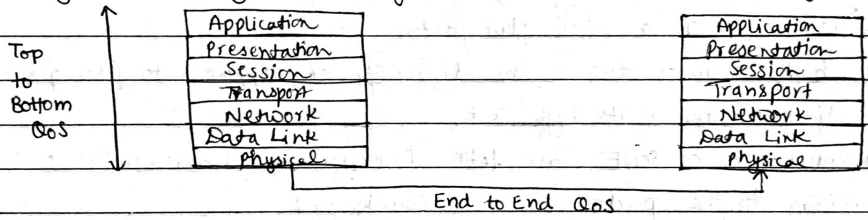
Quality of Service

Date __/__/____

* Introduction To Quality of Service (QoS)

- QoS can be defined as that feature of the computer network which enables the network to differentiate between various classes of network traffic and treat them differently.
- The various parameters to measure QoS of a network are as follows:
  1. Service Availability: The reliability of users' connection to the internet device.
  2. Delay: The time taken by a packet to travel through network from one end to another
  3. Delay Jitter: The variation in the delay encountered by similar packets following the same route through the network
  4. Throughput: The rate at which packets go through the network.
  5. Packet Loss Rate: The rate at which packets are dropped, get lost or become corrupted while going through the network

Any network design should try to maximize 1 & 4, reduce 2, & try to eliminate 3 & 5.



* Queue Analysis

- In any case, projections of performance are to be made on the basis of existing load information or on the basis of estimated load for a new environment. A no. of approaches are possible:
  1. Do an after-the-fact based on actual values
  2. Make a simple projection by scaling up from existing experience to the expected future environment.
  3. Develop an analytic model based on queuing theory.
  4. Program & run a simulation model.
- Option 1. is no option at all as this leads to unhappy users & to unwise purchases. Option 2. sounds promising. The analyst may take position that is impossible to project future demand with any degree of certainty. The problem with this approach is that the behaviour of most systems under a changing load is not what one would intuitively expect.

Punk

Date __/__/____

- Queueing network modelling, is a particular approach to computer system modelling in which the computer system is represented as a network of queues which is evaluated analytically. A network of queues is a collection of service centres, which represent system resources, & customers, which represent users or transactions.
- Analytic Evaluation involves using software to solve efficiently a set of equations induced by the network of queues and its parameters.
- The disadvantage of queuing theory is that a no. of simplifying assumptions must be made to derive equations for parameters of interest. The final approach is a simulation model.
- In most cases, a simulation model is not needed or at least is not advisable as a first step in analysis. For one thing, both existing measurements & projections of future load carry with them a certain margin of error. Thus, no matter how good the simulation model, the value of results are limited by quality of input.
- Despite many assumptions required of queuing theory, the results that are produced often come quite close to those that would be produced by a more careful simulation analysis.
- A queuing model analysis can be accomplished in a matter of minutes for a well-defined problem, whereas simulation exercise can take days, weeks longer to program & run.
- There are two types of queuing models:
  ⓐ Single server queuing models ⓑ Multi server queuing models.

* QOS Mechanisms

- Classification: Each class-oriented QOS mechanism has to support some type of classification.
- Marking: Used to mark packets based on classification and/or metering.
- Congestion Management: Each interface must have a queuing mechanism to priortize transmission of packets.
- Traffic Shaping: Used to enforce a rate limit based on metering by delaying excess traffic.
- Compression: Reduces serialization delay & bandwidth required to transmit data by reducing size of packet headers or payloads.

Punk

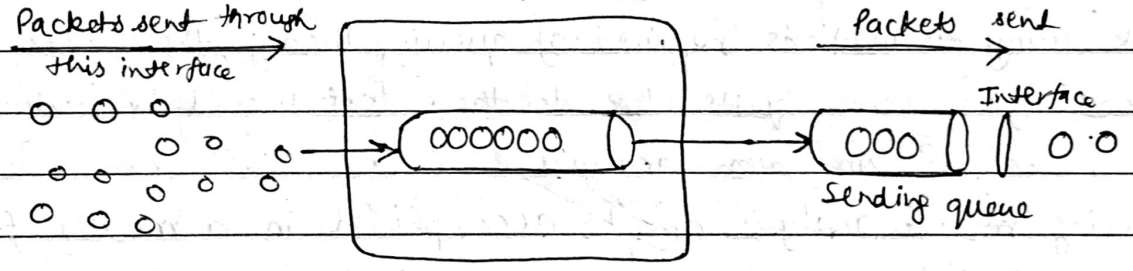
Date __/__/____

- Link Efficiency: Used to improve bandwidth efficiency through compression & link fragmentation & interleaving.

* Queue Management Algorithms

- Queue analysis is implemented in QoS for a network through various Congestion Management Techniques (~~techniques~~ techniques which are implemented in core network router to support various signalling protocols & provide different classes of service).
  - (a) First step in these techniques involving creating different queues for different classes of traffic.
  - (b) Next step involves implementing an algorithm for classifying incoming packets & assigning them to different queues
  - (c) Third step involves scheduling packets out of various network data queues & prepare them for transmission.
- Queuing Techniques can be implemented in four ways:

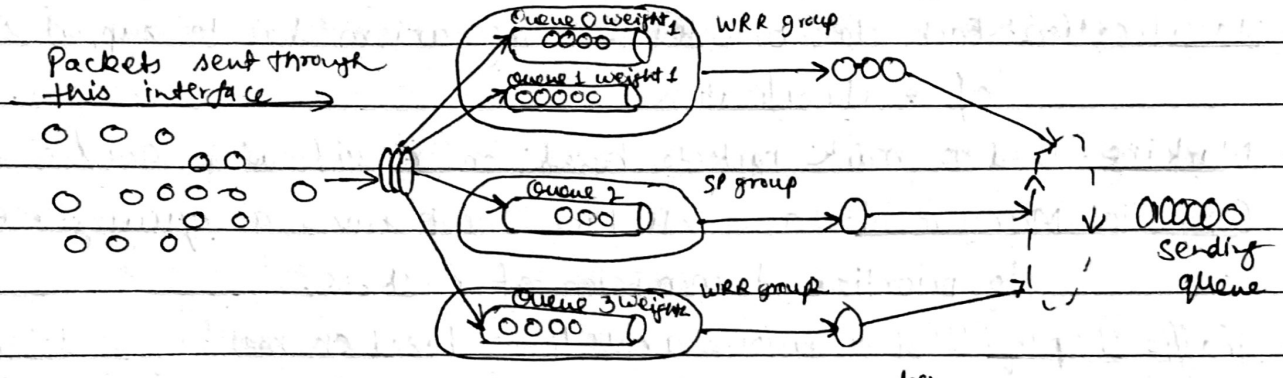
(a) First In First Out (FIFO) queues:



(b) Weighted Fair Queuing

If there are 1 queue each of priority 7 to 0 then division of output bandwidth will be: total = $w_0 + w_1 + w_2 + w_3 + w_4 + w_5 + w_6 + w_7 = Sw$

priority 0 gets $w0/Sw^{th}$ of bandwidth, priority 1 gets $w1/Sw^{th}$ of b.w. etc.



Aim of WFQ is to ensure low volume high priority traffic does get the service level it expects. It also adapts itself whenever network parameter changes. WFQ cycles through fair queues

Punk

Date __/__/____

(c) Custom Queuing: separate queues maintained for separate classes of traffic. Algorithm requires a byte count to be set per queue. That many bytes rounded off to the nearest packet is scheduled for delivery. This ensures minimum bandwidth requirement by various classes of traffic is met. CQ round robins through queues, picking required number of packets from each. If a queue is of length 0 then next queue is serviced.

ex:- 20% for Protocol A, 60% for B & 20% C.

Size of A is 1086 bytes, Size of B is 291 bytes, C is 831 bytes

Steps: (1.) %/size ratio : 20/1086, 60/291, 20/831

(2.) Normalizing : 1, .20619/.01842, .02407/.01842

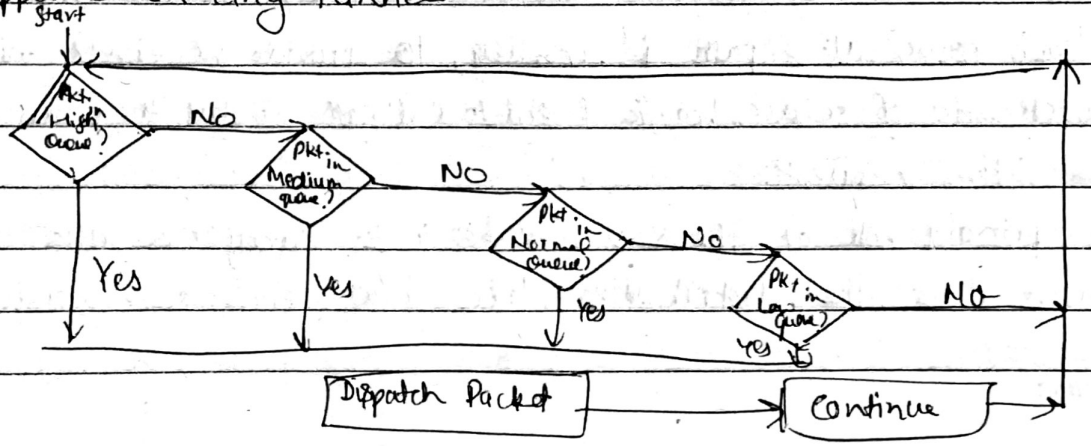
(3.) Round upto nearest int : 1, 12, 2

(4) Multiply each by corresponding byte size: 1086, 3492, 1662

(5) Add them : 6240

(6) 1086/6240, 3492/6240, 1662/6240 or 17.4, 56, 26.6.

(d) Priority Queuing: We can define 4 traffic priorities - high, medium, normal & low. Incoming traffic classified & enqueued in either of 4 queues. Classification criteria are protocol type, incoming interface, packet size, fragments & access lists. Unclassified packets put in normal queue. Queue are emptied in order of - high; medium, normal & low. In each queue, packets in FIFO order. During congestion, when a queue gets larger than a predetermined queue limit, packets get dropped. The advantage of priority queues is the absolute preferential treatment to high priority traffic so that mission critical traffic always get top priority treatment. The disadvantage is that, it is a static schence & does not adapt itself to network conditions & is not supported on any tunnels.



Punk

Date __/__/____

* Resource Reservation Protocol (RSVP)

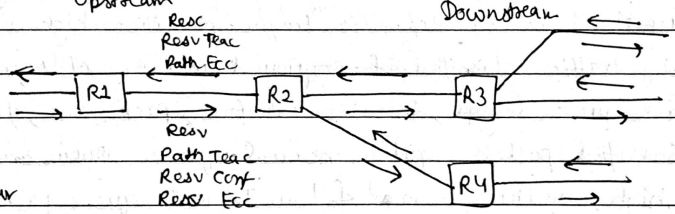
- RSVP was designed to enable senders, receivers & routers of communication sessions (either multicast or unicast) to communicate with each other in order to set up necessary router state to support various router services.
- RSVP is a novel signalling protocol in at least three ways:

(i) It accomodates multicast & point-to-multipoint reservations. To this end, receiver driven request model permits heterogeneity, in principle, & the filter mechanism allows for calls that reserve resources effectively for aggregate traffic flow.

(ii) It uses soft state, which means that it is tolerant of temp. loss of fun^n without enabling fate-sharing b/w end systems & network nodes. This means that QoS routing can be deployed separately.

(iii) RSVP is not a routing protocol, doesn't support QoS-dependent routing itself.

- RSVP identifies a communication session by combination of destination address, transport layer protocol type & destination port number.



Direction of RSVP messages

- RSVP is a signalling protocol ~~merely~~ used to reserve resources along existing route setup by whichever underlying routing protocol is in place.
- The primary messages used by RSVP are Path message which originates from traffic sender & the Resv message which originates from traffic receivers.
- The primary roles of the Path message are firstly, to install reverse routing state in each router along path & secondly, to provide receivers with info about the characteristics of seirder traffic & end-to-end path so that they can make appropriate reservation requests
- The primary role of the Resv message is to carry reservation requests to the routers along the distribution tree b/w receivers & senders.

Punk

Date __/__/____

- RSVP Reservation Types:

(i) Distinct Reservation: The receiver requests to reserve a portion of bandwidth for each sender. In a multicast flow with multiple senders each senders flow can thus be protected from other sender's flow. This style is also called as Fixed filter style.

(ii) Shared Reservations: Here receiver requests network elements to reserve common resources for all sources in multicast tree to share among themselves. This style is important for applications like video conferencing. They are of 2 types:

@ Wildcard Filter Type: The receiver requests resources to be reserved for all the sources in multicast tree. Sources may come & go but they should share resources to send traffic so that sink can receive from all of them.

(b) Shared Explicit Reservation: This is exactly like wildcard filter type except that receiver chooses a fixed set of senders out of all available senders in multicast flow to share resources.

Tunneling

In order for RSVP to operate through non RSVP clouds, RSVP supports tunneling through the cloud.

- Congestion Avoidance Mechanisms

(i) Tail Drop: It simply drops an incoming packet if output queue for the packet is full. When congestion is eliminated queues have room & taildrop allows packet to be queued. The disadvantage is problem of TCP global synchronization.

(ii) Random Early Dropping: RED starts dropping packets randomly when average queue size is more than a threshold value. The rate of packet drop increases linearly as avg. queue size increases until avg. queue size reaches max. threshold. The diff. b/w min & max threshold should be great enough to prevent global synchronization. RED strategies should be employed on top of reliable transport protocols like TCP.

(iii) Weighted Random Early Dropping (WRED): It is a RED strategy where in addition it drops low priority packets over high priority ones when the output interface gets congested. For IntServ environments, WRED drops non-RSVP-flow packets & for Diffserv enviroments, WRED looks at IP

Punk

Date __/__/____

precedence bits to decide priorities & hence which ones to selectively dump. Non IP packets have precedence 0 – highest probability to be dropped. The avg queue size formula is:

$$avg = (old\text{-}avg * 2^{(-n)}) + (current\_queue\text{-}size * 2^{(-n)})$$

where n is exponential weight factor configured by user.

⇒ A high values of n means a slow change in the "avg".

⇒ A very high n implies no WRED effect.

⇒ Low n means WRED will be in synch with current queue size & will react sharply to congestion & decongestion.

⇒ very low n means that WRED will overreact to temp fluctuations & may drop packets unnecessarily.

* Diffserv and Intserv

- Diffserv = Differential Services
  Intserv = Integrated Services
- Different applications require different QOS from network. To address this in IP two approaches have been developed.
- First, Strict QOS guarantees are accomplished by Intserv architecture in conjunction with RSVP for signalling. This framework allows reserving resources on a path through the network to achieve an end-to-end QOS guarantee, but it has shortcomings with regard to scalability.
- Second, the Diffserv architecture, which gives a loose notion of QOS, enables network to optimize transport of data packets acc^n to certain requirements. Diffserv only uses different per-hop behaviours (PHBs) for different class of traffic rather than giving guarantees on these transport characteristics. Several main PHBs are defined - EF Traffic, AF Traffic, & BE Traffic.
  - → EF (Expected Forwarding) Traffic: A high priority service trying to achieve zero packet loss, minimal queuing delay, & minimal jitter.
  - → AF (Assured forwarding): A group of several PHBs giving a variety of different forwarding assurances by defining four classes with three different drop precedences.
  - → BE (Best Effort): A low priority service equivalent to service in Diffserv-unaware networks.

Punk

Date __/__/____

- Intserv

→ A non-scalable (limited to small networks) reservation architecture which consists of Flow Specs & RSVP.

→ Intserv is an architecture, which specifies elements & allows them to request & receive "reservations", which act to guarantee QOS on networks.

→ The two protocols of Interserv are:

⇒ Flow Specs – Describe Intserv reservations

⇒ RSVP – the Interv signaling protocol to transmit reservations across network

→ Intserv vs Diffserv

Intserv specifies a fine-grained QOS system, meaning there are many levels of QOS, which are defined & stored in the routers.

Diffserv is the opposite – it is a coarse-grained control system, with only several QOS levels.

→ Flow Spec

⇒ There are two parts to a flow spec:

ⓘ What does traffic look like? Done in Traffic Specification or TSPEC part.

ⓘⓘ What guarantees does it need? Done in Request Specification or RSPEC part.

⇒ TSPECs include token bucket algorithm parameters. It typically justifies token rate & bucket depth.

⇒ RSPECs specify what requirements there are for flow: it can be normal internet 'best effort' in which case no reservation is needed. The 'Controlled load' setting mirrors performance of a lightly loaded network. The 'Guaranted' setting gives an absolutely bounded service.

→ RSVP (RFC 2205)

⇒ The Resource Reservation Protocol (RSVP) is described in RFC 2205. The RESV message contains flow specs.

⇒ The routers b/w sender & receiver Listener have to decide if they can support the reservation being requested, & if they can't then send a reject msg. Otherwise, they accept the reservation they have to carry the traffic.

Punk

Date __/__/____

→ Why IntServ with its RSVP signaling failed

⇒ The problem with IntServ is that many states must be stored in each router. As a result, IntServ works on a small scale, but as you can upscal to a system the size of Internet, it is difficult to keep track of all of the reservations. As a result, IntServ is not popular.

Reservations in each device along path are "soft" which means need to be refreshed periodically, adding complexity to RSVP sol^n.

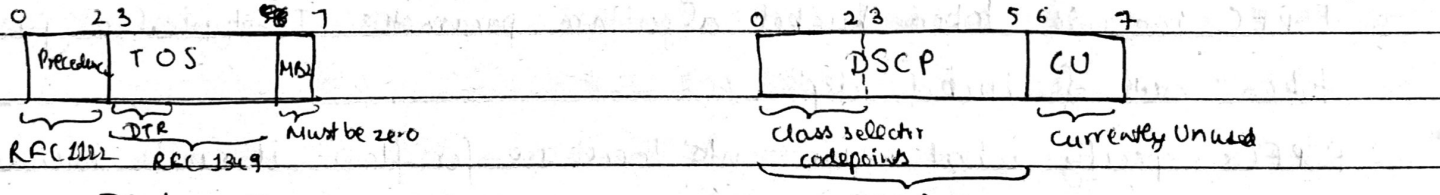
Maintaining soft states in each router adds complexity

Scalability becomes an issue due to maintaining states.

— DiffServ

→ DiffServ (RFC 2474, 2475 & 3270) addresses clear need for relatively simple & coarse methods of categorizing traffic into different classes, also called class of service (COS) & applying QOS parameters to those classes. For making DiffServ a guaranteed service it may be used with CAC - Connection Admission Control.

→ To accomplish this, packets are first divided into classes by marking the type of service (TOS) byte in IP header. A 6-bit bit-pattern (called Differentiated Service Code Point [DSCP]) in IPv4 TOS octet or IPv6 Traffic Class Octet is used.



IPv4 Traffic Class Octet

Diffserv Codepoint Field

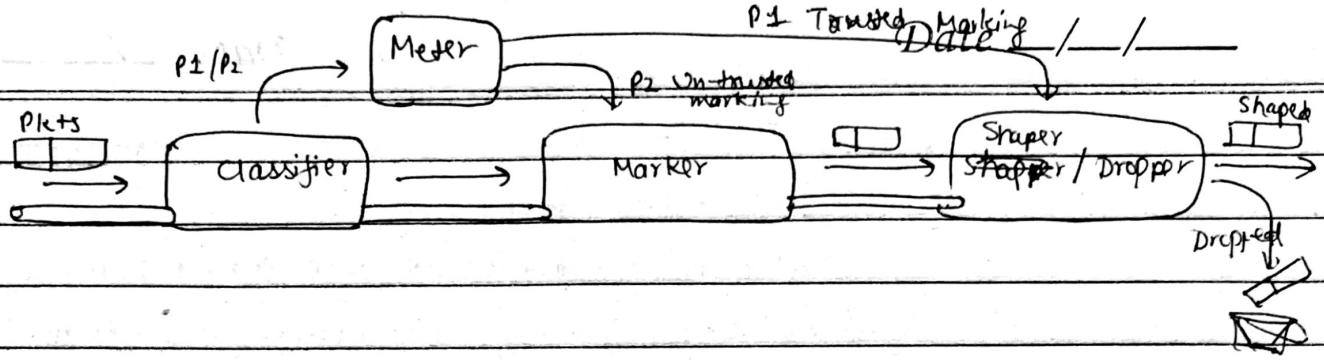
→ TOS byte is completely redefined. Six bytes are now used to classify packets. The field is now called DS (Differential services) Field, with two of the bit unused (RFC-2474). The 6 bits replace the three IP-Precedence bits & is called Differential Services Code point (DSCP). With DSCP, in any given node, upto 64 different aggregate/classes can be supported (2^6).

→ All classifications & QOS revolves around the DSCP in Diffserv model.

→ COS can be applied as Premium, Gold, Silver & Bronze by setting DHCP to a corresponding value.

Punk

Date / /



→ Packets entering Diffserv Domain (DS-Domain) can be metered, marked, shaped, or policed to implement traffic policies (as defined by administrative authority).
→ Marking is done through MOC's class maps.
→ Metering is done using a token bucket algorithm, shaping is done using Generic Traffic Shaping (GSS) or Frame Relay Traffic Shaping (FRTS), and policing is done using class-based policing / Committed Access Rate (CAR)

Punk

Unit-IV

Date __/__/____

TCP/IP Applications

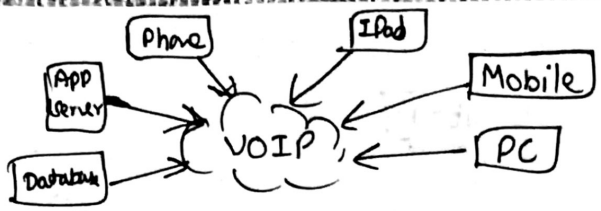
* Introduction

- TCP/IP applications are applications which use TCP/IP protocols in order to func^n. The Internet Model uses client-server architecture.
- TCP/IP Applications & services are generally of two types:
  - (i) The applications which a user uses directly such as Telnet & Email
  - (ii) The applications which are not used directly by a user. These applications provide support to other applications & services. Examples include Domain Name System.
- These applications are as follows:
  - (i) Bootstrap Protocol (BOOTP): It is an application used for providing a dynamic method for connecting workstations with servers. It also makes it provide a dynamic method for assigning workstation IP address & initial program load (IPL) sources.
  - (ii) Internet Setup Wizard: Connecting system to internet (ISP) is possible via use of Internet setup wizard.
  - (iii) Dynamic Host Configuration Protocol (DHCP)
  - (iv) Domain Name System (DNS)
  - (v) E-mail (vi) File Transfer Protocol (FTP) (vii) Remote Access Services: PPP connections
  - (viii) IP filtering and network address translation: IP filtering and network address translation (NAT) work like a firewall to protect network from intruders.
  - (ix) HTTP server: HFS (HTTP File Server) is an application which is used to send & receive file
  - (x) Remote Execution (REXEC): REXEC server is a TCP/IP application that allows a client user to submit system commands to a remote system.
  - (xi) Telnet: It is a protocol that enables users to log on to a user at terminal interacts with local telnet client which in turn interacts with Telnet server.
  - (xii) Trivial File Transfer Protocol (TFTP): It is a simple protocol that provides basic file transfer func^n with no user authentication.
  - (xiii) Virtual Private Networking: A VPN allows a company to securely extend its private intranet over existing framework of a public network such as Internet

* VOIP (Voice Over Internet Protocol).

- It allows a user to receive telephone calls over the internet. It is so called as "IP-telephony". A requirement for a VOIP connection is a high speed internet to offer a connection without packet loss & jitter.

Punk



Date ___/___/___

- VOIP ~~stands~~ is converts voice signal from telephone into digital signal that travels over internet & then converts it back at other end so you can speak to anyone with a regular phone number.
- voice conversations are turned into digitized data & packetized for transmission.
- Working:
  - VOIP looks for IP address & translates phone numbers into IP addresses.
  - The central call processor is a piece of hardware running a specialized database/mapping program called a soft switch.
  - → Soft switch knows:
    - where endpoint is on network
    - what phone no. is associated with that endpoint
    - the current IP address assigned to that end point.
  - → If soft switch doesn't have info, request is handled by another soft switch.
- Protocols used:
  - → H.323: Provides specification for real-time interactive videoconferencing, data sharing and audio applications (VOIP).
  - → SIP (Session Initiation Protocol): Used for signaling & controlling multimedia communication sessions.
- VOIP vs PSTN
  - → PSTN (Public Switched Telephone Network) requires a dedicated line to connect to a network. Compression algorithms can't be implemented in PSTN. Also it is not possible to send video data over traditional PSTN.
  - → VOIP uses Packet Switching which is more efficient than a dedicated line. Also compression algorithms can be implemented in VOIP. VOIP can be used to transmit video data as well.
- Advantages of VOIP:
  - → Cost:
    - Free VoIP to VoIP
    - Low cost VOIP to PSTN
    - Less bandwidth requirements
    - Low cost/no cost h/w & s/w
  - → Mobility:
    - Any internet connection
    - Growing no. of wireless broadband locations
- Disadvantages of VOIP:
  - → Quality:
    - High quality PSTN
    - Variable VOIP dependent on connection
  - → Dependent on wall power
  - → Lost or delayed packet cause drop-out in voice
  - → Emergency Calls:
    - Hard to find geographic location
  - → Security:
    - Most VoIP services donot support encryption

Punk

Date __/__/____

* NFS (Network File System)

- In 1984, Sun Microsystems came up with NFS which allows a server to share directories and files with clients over a network.
- Some common uses include:
  - → Several clients may need access to the /usr/ports/distfiles directory.
  - → To configure a central NFS server on which all user home directories are stored.
  - → Administration of NFS exports is simplified.
  - → Removable media storage devices can be used by other machines on network.
- NFS consists of a server and one or more clients. The client remotely accesses the data that is stored on the server machine.
- These daemon must be running on the server:
  - nfsd : The NFS Daemon which services requests from NFS clients.
  - mountd : The NFS mount Daemon which carries out requests received from nfsd.
  - rpcbind : This daemon allows NFS clients to discover which port NFS server is using.

* Telnet:

- It is a protocol that allows you to connect to remote computers (called hosts) over a TCP/IP network such as Internet.
- Command-line telnet clients are built into most versions of Mac OS X, windows, Unix & linux. Command: Telnet (general protocol) host (Address of service) port (port number)
- A Telnet server generally listens on TCP port 23.
- How it works:
  - → A user is logged in to local system & invokes a TELNET (Telnet client) program by typing.
    telnet xxx.xxx.xxx } host name or IP address
  - → Telnet client is started on local machine if not running. That client establishes a TCP conn. with TELNET server on destination server
  - → Once conn. established, client accepts keystrokes from user & relays them, generally one character at a time, to TELNET server.
  - → The server on the destination machine accepts character sent to it by client & passes them to terminal server (facility provided by OS for entering keystrokes from keyboard)
  - → Terminal server treats remote user as it would any other user logged system.

Punk

Date __/__/____

→ The terminal server passes outputs back to TELNET server, which relays them to the client, which displays them on user's screen.

→ A Telnet server is implemented as a master server with some no. of slave servers.

→ The only things that make TELNET hard to implement is heterogeneity of terminals and OS. that must be supported. To accomodate this heterogeneity, TELNET defines a Network Virtual Terminal (NVT) which maps the 95 printable characters into their defined values - decimal 65 = "A", decimal 97 = "a" etc.

→ The 33 control codes are defined for NVT as:

ASCII value	Decimal value	Meaning
NUL	0	NO-OP
BEL	7	Ring "terminal bell"
BS	8	Backspace
HT	9	Horizontal Tab
LF	10	Line feed
VT	11	vertical Tab
FF	12	form feed
CR	13	Carriage return (move cursor to beginning of current line)
all others		NO-OP

→ NVT defines end-of-line to be a CR-LF combination - the two-character sequence.

→ Telnet Operation: Telnet protocol is based on three ideas:

(i) NVT concept: A NVT is an imaginary device having a basic structure common to a wide range of real terminals.

(ii) A symmetric view of terminals & processes

(iii) Negotiation of terminal options

→ The two hosts begin by verifying their mutual understanding. Once this initial negotiation is complete, they are capable of working on min level implemented by NVT

→ After this minimum understanding is achieved, they can negotiate additional options

→ Because of symmetric model, both host & client may propose additional options.

→ The set of options is not part of TELNET protocol.

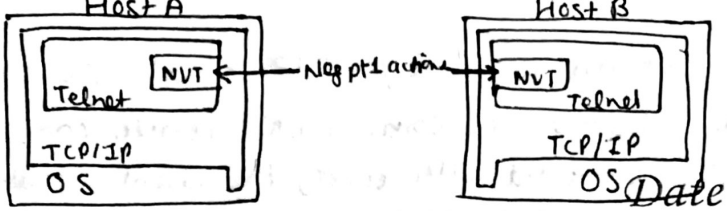
→ All Telnet cmds & data flow through TCP conn. Commands start with a special character called Interpret as Command (IAC) escape character.

→ The IAC code is 255. If 255 is sent as data - it must be followed by another 255.

→ Each receiver must look at each byte that arrives & look for IAC. If IAC is found & the next byte is IAC - a single byte is presented to application/terminal.

→ If IAC is followed by any other code - The TELNET layer interprets this as a command.

Punk



Telnet Architecture

Date __/__/____

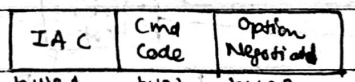
- Telnet Options:

RFC #	Num	Name	RFC #	Num	Name
856 :	0	: Binary Transmission		8	: O/P Line Width
857 :	1	: Echo		9	: O/P Page Size
859 :	5	: Status	698 :	17	: Extended ASCII
	2	: Reconnection	727 :	18	: Logout
861 :	255	: Extended-Options-list	1043 :	20	: Data Entry Terminal
1372 :	33	: Remote Flow Control	779 :	23	: Send Location
1079 :	32	: Terminal Speed	1091 :	24	: Terminal Type
1416 :	37	: Telnet Authentication Option	885 :	25	: End of Record

- Telnet Command Structure:

→ The communication b/w client & server is handled with internal cmds, which are not accessible by users. All internal TELNET cmds consists of 2 or 3 byte sequences

→ The Interpret as Command (IAC) character is followed by a command code. If this command deals with option negotiation, the cmd will have 3rd byte to specify code for referenced option.

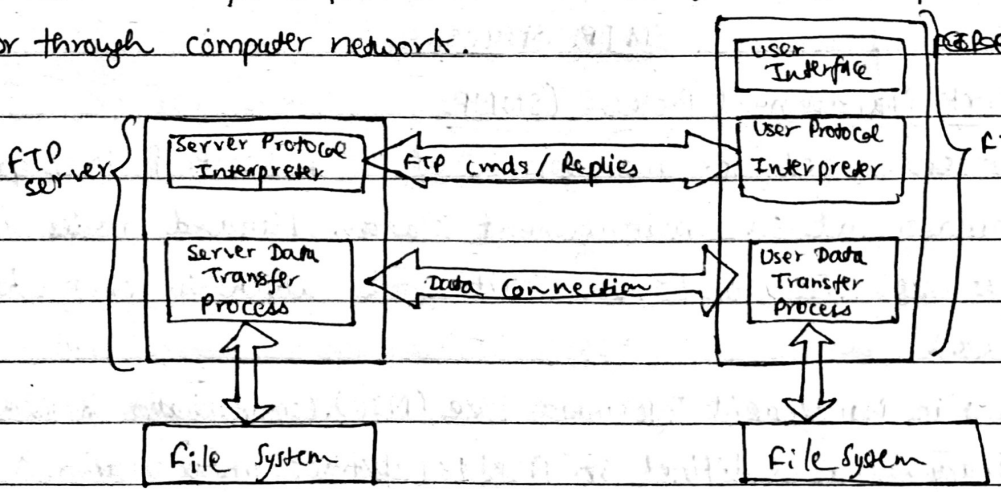


Sample:

255 → IAC 253 → WILL 24 → Terminal type

* File Transfer Protocol (FTP)

- FTP is used to transfer (upload / download) data from one computer to another over the internet or through computer network.



FTP Model

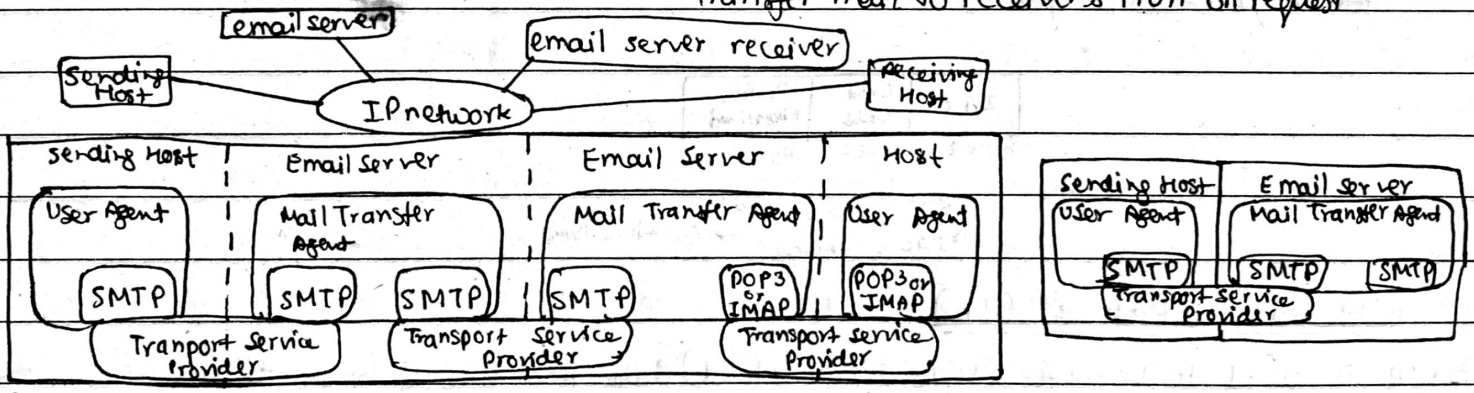
Punk

- The client computer that is running FTP client s/w such as Filezilla & Smart FTP etc initiates a conn. with remote computer (server).
- After successfully connected with server, the client computer can perform a no. of operations like downloading files, uploading, renaming & deleting files, creating new folders etc. Virtually OS supports FTP protocols.

Date __/__/__

* Simple Mail Transfer Protocol (SMTP)

- It is based on end-to-end delivery: An SMTP client contacts the destination host's SMTP server directly, on well-known port 25, to deliver the mail. It keeps the mail item being transmitted until it has been successfully copied to the recipient's SMTP.
- It is possible to exchange mail b/w TCP/IP SMTP mailing system & locally used mailing system. It is done using applications called mail gateways or mail bridges.
- when a mail gateway is used, SMTP end-to-end transmission is host-to-gateway, gateway-to-host, or gateway-to-gateway; the behaviour beyond gateway is not defined by SMTP.
- The agents used in SMTP may be grouped as:
  - MUA - Mail User Agent
    - User's email program
    - User read & write email
  - MTA - Mail Transfer Agent
    - Receives mail from MUA
    - Transfer Mail to other MTA's
    - Transfer mail to receiver's MUA on request
  - SMTP - Simple Mail Transfer Protocol
    - From MUA to MTA
    - From MTA to MUA



SMTP Structure

* Simple Network Management Protocol (SNMP)

- It is a protocol used for management of the network & is implemented by network manager at a management station. Managed nodes consists of router, hosts, etc. It must run SNMP agent which in turn keep objects (statistics etc).
- Objects defined in Management Information Base (MIB). Communication is with binary values Structure of binary values is defined in ASN.1 (abstract syntax notation one). Thus, ASN.1 defines types of objects (int, string, arrays, etc.) & a standard binary representation of these.

Punk

Date __/__/____

* Finger

- Displays info about a user or users on a specified remote computer (typically a computer running UNIX) that is running Finger service or daemon. The remote computer specifies the format & output of user.
- Used without parameters, finger displays help.

Syntax: finger [-l] [User] [@host] [...]

Parameters:
- -l: Displays user info in long list format
- User: specifies user about which you want info
- @host: specifies remote computer running finger service where you are looking for user info.
- /?: Displays help at cmd prompt

Remarks:
- Multiple User@host parameters can be specified.
- must prefix finger parameters with - (hyphen) rather than / (slash).
- this cmd available only if TCP/IP installed as component of network adapter.
- Windows 2000 and Windows XP do not provide a finger service

Ex: finger user1@users.microsoft.com } To display user1 info
finger @users.microsoft.com } To display info for all users

Formatting legend

Format	Meaning
Italic	Info that user must supply
Bold	Elements that user must type exactly as shown
Ellipsis (...)	Parameter that can be repeated several times in a cmd line
B/w Brackets ([])	Optional items
B/w braces ({}); choices separated by pipe (|) Ex:- {even|odd}	Set of choices from which user must choose only one
Courier Font	Code or program output

* WHOIS

- It is a query & response protocol that is widely used for querying databases that store registered users or assignees of an Internet resource such as domain name, an IP address block or an autonomous system.
- The protocol stores & delivers database content in a human-readable format.
- WHOIS protocol is documented in RFC 3912.

Punk

Date __/__/____

- It is based on NAME/FINGER protocol. WHOI services are typically communicated using TCP. Servers listen to requests on well know port no. 43. Clients are simple applications that establish a communication channel to server, transmit a text record with name of resource to be queried & await response in form of sequence of text records found in database.
- This simplicity of protocol also permits an application & a cmd line interface user to query a WHOIS server using Telnet protocol.
- A WHOIS database consists of a set of text records for each resource. These text record consists of various items of info about resource itself & any associated info of assignees, registrants, administrative info such as creation & expiration date.
- Two data models exist for storing resource info in WHOIS database:

(i) Thick Model: A thick-WHOIS server stores complete WHOIS info from all registrars for particular set of data.

(ii) Thin Model: A thin WHOIS server stores only name of WHOIS server of registrar of a domain which in turn has full details on data being looked up.

- Example of WHOIS query: Result of WHOIS query of example.com

```
whois example.com
[Querying whois.verisign-grs.com]
[Redirected to whois.iana.org]
[Querying whois.iana.org]
[whois.iana.org]
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:       EXAMPLE.COM

organisation: Internet Assigned Numbers Authority

created:      1992-01-01

source:       IANA
```

~~* WWW, IPv6 & Next Generation networks~~

* Telnet Basic Commands

- The primary goal of Telnet protocol is provision of a standard interface for hosts over a network.
- To allow conn. to start, it defines a standard representation for some functions:

Punk

- IP : Interrupt Process
- AO : Abort Output
- AYT : Are You There
- EC : Erase character
- EL : Erase Line
- SYNCH : Synchronize
- QUIT : Quit session

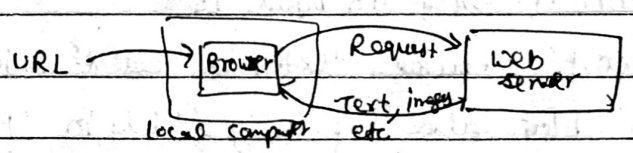
Date __/__/____

Some + imp.
- Telnet Commands:

Cmd name	Code	Comment
SE	240	End of sub-negotiation parameters
NOP	241	No operation
Break	243	NVT & character BRK
Go Ahead	249	The GA signal
SB	250	Indicates sub negotiation
WILL	251	Show desire to use
WONT	252	Show refusal to use
DO	253	Request that other party uses
DONT	254	Demand that other party stop using
IAC	255	Interpret As Command

* WWW, IPv6 and Next Generation Networks

- WWW : World wide Web & Its Components
- The Web: An infrastructure of info combined & network s/w used to access it
- Webpage: A document that contains or references various kinds of data
- Links : A connection b/w one webpage & another
- Website: A collection of related web pages
- Web browser: A s/w tool that retrieves & displays web pages
- Web Servers: A computer set up to respond to requests for web pages
- URL (Uniform Resource Locator): A standard way specifying location of a webpage, containing the hostname, "/", & a file



URL processing

- Search Engine : A website that helps you find other websites
- Instant Messaging:
  - → Applications that allow people to send short messages.
  - → Similar to texting, but based on username not cellular phone no.
  - → Some applications allow more than two users in a chat room.
  - → If participants run app simultaneously, they can have interactive conversation.
  - → Most app use proprietary protocols that dictate precise format & structure of messages.

Punk

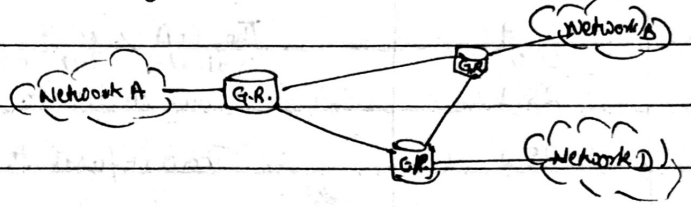
→ Most instant messages are not secure.

- Cookie: A small text file that a web server stores on your local computer.
- Web Analytics: Collection and analysis of data regarding website usage. Typically used by website owners to track no. & behaviour of users visiting their sites.

Date __/__/____

* IP v6 - The next Generation of IP

- All network elements such as routers, switches, gateways, bridges, LAN cards; need to have at least one IP address. Different IP packet networks are normally interconnected by Routers that have added functionality to permit accounting b/w interconnected networks.



G.R. - Gateway Router

Major Benefits of IPv6 - Why Change?

→ The new version of IP v6 was conceived to replace previous IPv4 standard which is being used successfully to support communication systems in emerging info. society & has been updated to extend its useful life (eg: NAT mechanism, IPsec protocol, MPLS, Tunnelling).

→ IPv6 has limited capabilities in following areas:

⇒ Exhaustion of IPv4 address space
⇒ Growth of Internet & maintenance of routing tables
⇒ Auto configuration
⇒ Mobility
⇒ Security
⇒ Quality of Service

→ These limitations are overcome by IPv6 & offers improvement:

- Expansion capability for addressing & routing: From 32 bits to 128 bits address
- Simplified Header format: Only 40 bytes long
- Enhanced options support: Separate "extension headers" which enable flexible support for options
- Quality of Service: Flow Label & priority fields in IPv6 header
- Auto-configuration: Dynamic assignment of part of address space
- Elimination of need for NATs (Network Address Translators)
- Improved security with mandatory IPsec implementation: Integral support for authentication, privacy & data integrity measures.
- Mobility: Mobile computers are assigned with at least two IPv6 addresses whenever they are roaming away from their home networks. One (the home address) is permanent; the other (the IPv6 local link address) is used temporarily.

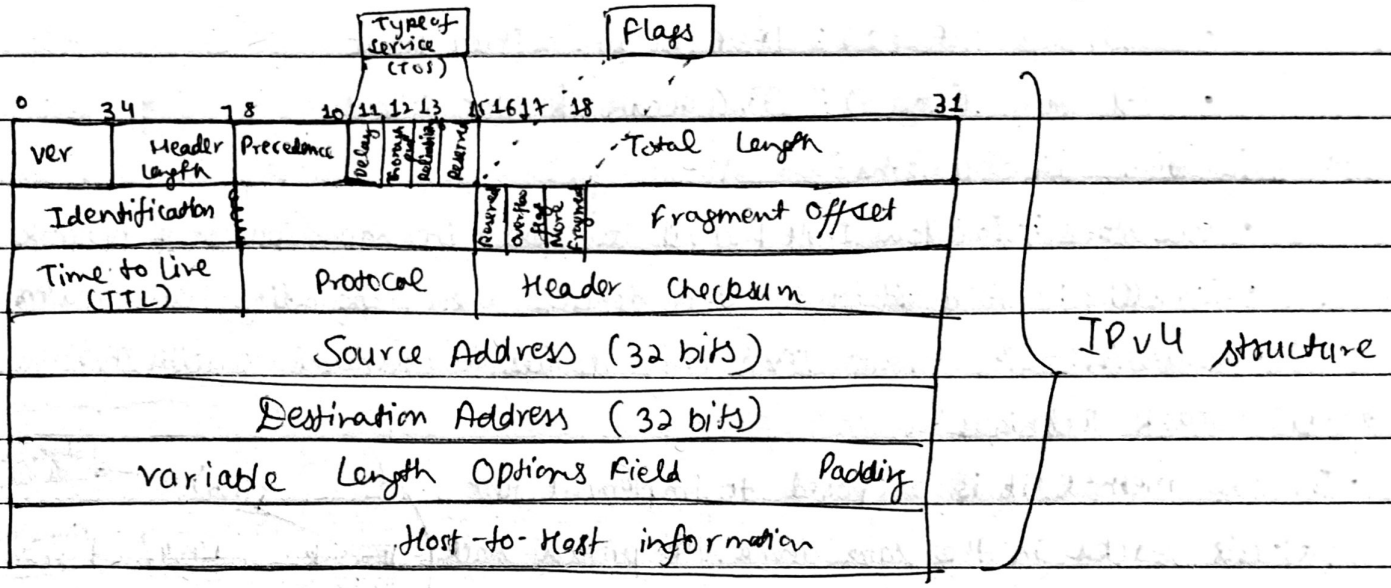
Punk

Date __/__/____

- IP addressing architecture:

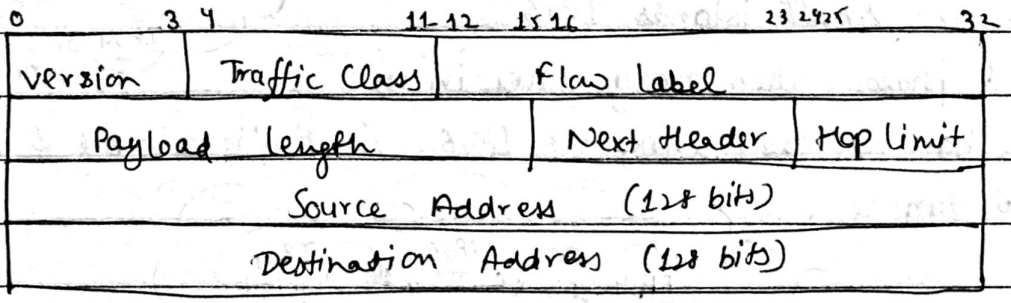
• An IPv4 address consists of 32 bits (group of 4 nos. [8bit hexadecimal]) from 0 to 255 ranges & separated by full stops.

Ex:- 124.32.43.4



• An IPv6 addresses have 128 bits length & consists of eight nos. in hexadecimal format, from 0 to 65535 (decimal) ranges & separated by a colon ":"

Ex:- FECA:0000:234A:0043:AB45:FFFF:9A3E:000B



- IPv6 services & Equipments:

→ Applications that need or will benefit from IPv6 :

- Mobile broadband IP
- iTV & IPTV
- P2P multiplayer games
- Mobile IP broadcast
- Grids
- Remote manufacturing system
- Peer to Peer VoIP
- RFID
- Sensor networks
- Digital Radio
- Control Networks
- Microsoft (native support of IPv6 in next version of windows — Longhorn)

→ Technologies that will support migration to IPv6:

- Powerline Communication
- Wi-fi
- Wi-Max
- ZigBee
- Unlicensed Mobile Access (UMA)

Punk

Date __/__/____

- Migration: The current IP-based network will gradually migrate from IPv4 to IPv6.

→ Mapping of signalling b/w IPv6 & IPv4 is required. From deployment point of view, there are three stages of evolution scenarios:

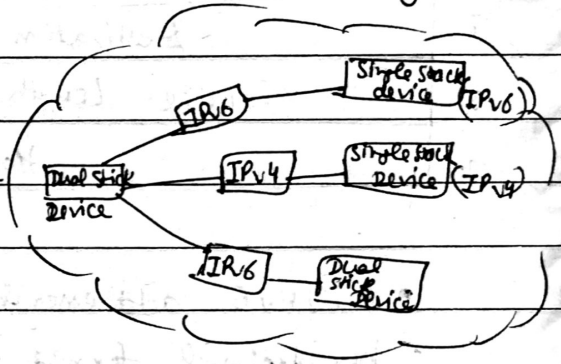
- First stage (stage 1): IPv4 ocean & IPv6 island
- Second stage (stage 2): IPv6 ocean & IPv4 island
- Third stage (stage 3): IPv6 ocean & IPv6 island

→ Migration mechanisms:

- Dual stack :- To allow IPv4 & IPv6 to coexist in same devices & networks
- Tunnelling :- To avoid order dependencies when upgrading hosts, routers or regions
- Translation :- To allow IPv6 only devices to communicate with IPv4 only devices.

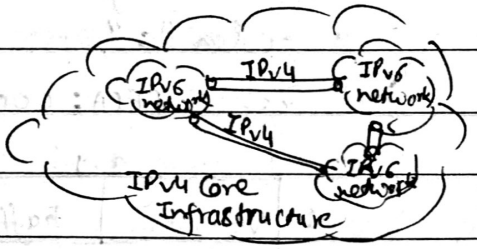
→ Dual Stack Technique:

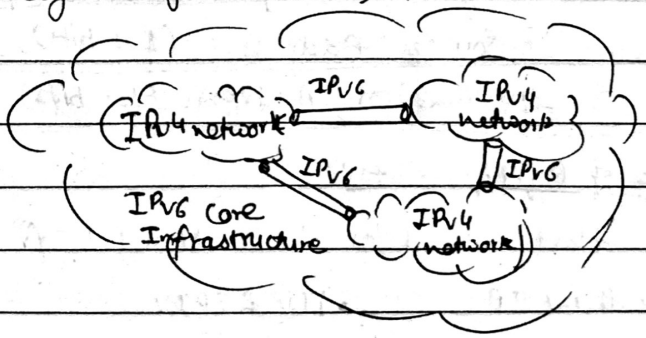
- In this method it is proposed to implement two protocols stacks in the same device. The protocol stack used for each link depends on device used at other end of the link.



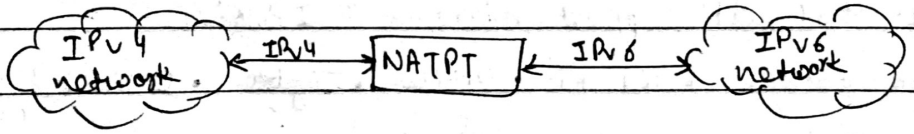
→ Tunnelling Techniques:

- In first phase core of network uses IPv4 protocol & there are small islands IPv6
- In second phase, when many nodes in core network have already changed to IPv6, situation is reversed & IPv4 is encapsulated in IPv6 tunnels





→ Translation Techniques: This technique uses a device, the NAT PT (Network Address Translation - Protocol Translation) that translates in both directions b/w IPv4 & IPv6 at boundary b/w IPv4 network & IPv6 network.

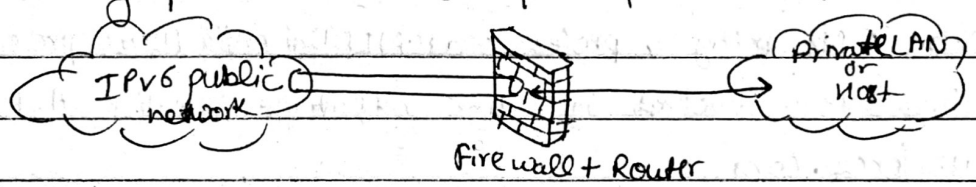


Punk

Date __/__/____

- Some proposals: The most preferable soln on backbone of IP network is the use of dual stack technique by ISPs & network operators.
- Security: IPv6 is considered to have "Native Security" & has following characteristics:
  - It works end-to-end, authentication separate from encryption
  - It has an authentication header (AH)
  - It has an Encapsulating Security Payload (ESP) header

The firewalls have following functions:
- They enforce uniform policy at parameter
- They stop outsiders from performing dangerous operations
- They provide a check point & scalable, centralised control



Combined Firewall and Router

- IPv6 & the NGN: Mobile access networks are one of the major potential application areas for IPv6. From signalling point of view, the IPv6 protocol has many features related to QOS & other capabilities.

Punk

Date __/__/____

* Cloud Computing

- The cloud is IT as a service, delivered by IT resources that are independent of location. It is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet where end users have no knowledge of, expertise in, or control over the technology infrastructure (the cloud) that supports them.

- Key Attributes in Cloud Computing:
  - Service Based: Considered "Ready To Use" or "Off the Shelf"
  - Scalable and Elastic
  - Shared
  - Metered By Use
  - Uses Internet Technologies

- History:

  1961 - John McCarthy, professor at MIT University (USA) presented idea of Cloud

  Since then evolved including grid & utility computing, ASP, SAAS.

  1999 - Salesforce.com

  2002 - Next Development -> Amazon web services

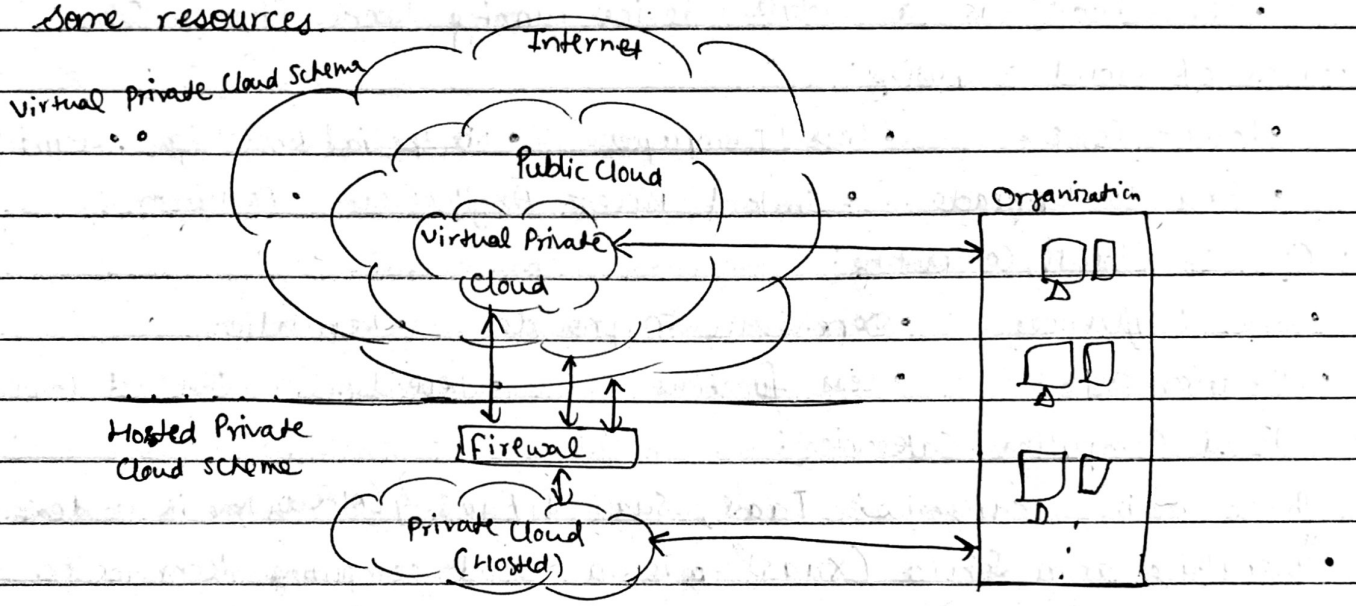
  2009 - Google & other services such as Google Apps.

- Architecture:
  - Virtualization is best described as essentially designating one computer to do the job of multiple computers by sharing resources of that single computer across multiple environments.
  - Cloud Computing architecture divided into two sections, front end & back end, connected together through a network.
  - The Front End includes client's computer and application required to access cloud computing system.
  - The Back End is represented by various computers, servers & data storage systems that create "cloud" of computing services.
  - A central server administrates system, monitoring traffic & client demands to ensure everything runs smoothly using a special s/w called middleware. Middleware allows networked computers to communicate with each other.
  - Public cloud (external cloud) is a model where services are available from a provider over the Internet, such as applications & storage.

Punk

Date __/__/____

- Private Cloud (Internal cloud / Corporate Cloud) is computing architecture providing hosted services to a limited no. of people behind a company's protective firewall & it sometimes attracts criticism as firms still have to buy, build & manage some resources.



- Cloud Computing Design & Integrability

→ Design level

- End to end design : Func^n reside at both ends of network, not within Internet backbone.
- Technical design: Design include end user device, connectivity, Internet & cloud

→ Network level

- Devices : Cloud services should be device agnostic.
- Connectivity: Identify required connections such as enterprise to cloud, cloud to cloud, remote to cloud etc.

→ Reliable, Efficient & Secure Connectivity

- Management: Policies Synchronized
- Security : Evaluate security security
- Access Control: Mechanism to protect critical resources from unauthorized users
- Cryptography: Methods for taking legible, readable data & transforming it into unreadable data while transmitting it.
- Operations Security: Procedures for back ups & change control management.

- The "Cloud computing Manifesto" is a manifesto containing "a public declaration of principles & intentions" for cloud computing providers and vendors; annotated as "a call to action for the worldwide cloud computing" and "dedicated belief that the cloud should be open".

Punk

Date __/__/____

- Examples: Google Apps, MS Outlook or MS exchange services, Cloud X Technology Group, Yahoo, E bay, Facebook, Citric XennApp, AJAX, etc.

- Device using Cloud Computing:
  - "Chromebook" is a mobile device running Google Chrome OS.

- Pros of Cloud Computing:
  - Lower Costs • Less IT employees • No special knowledge • Security
  - Easy To Upgrade • Instant Access Anywhere • Requirements

- Cons of Cloud Computing:
  - Legal Differences • Dependence on provider • Reputation
  - Migration costs • Less functions • Dependance on Internet Connection

* Cloud Computing Categories:

Three main categories: Iaas, Saas & Paas } (Already Done in Cloud Computing)

- "Everything as a Service (Xaas)" is a cloud computing term for the extensive variety of services and applications emerging for users to access on demand over the Internet as opposed to being utilized via on-premises means. Also known as anything-as-a-service facilities the flexibility for users & companies to customize their computing environments to craft experience they desire, all on demand. Xaas is dependent on a strong cloud services platform and reliable Internet connectivity to successfully gain traction and acceptance among both individuals and enterprises.

* Big Data and Data Analysis

- Big data is high-volume, high-velocity & high variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.
- E-commerce, in particular, has exploded data management challenges along three dimensions: volumes, velocity and variety.
- Key Computing Resources for Big Data
  - Processing Capability: CPU, processor, or node
  - Memory
  - Storage
  - Network

Punk

Date __/__/____

- Techniques towards Big Data

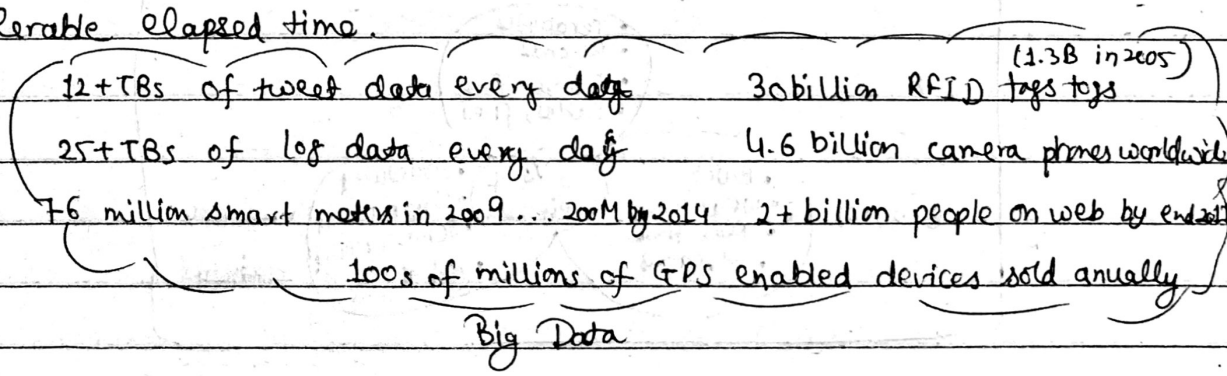
- Massive Parallelism
- Data Distribution
- High-Performance Computing
- Data Mining and Analytics
- Machine Learning
- Huge Data volumes, Storage
- High-Speed Networks
- Task & Thread Management
- Data Retrieval
- Data Visualization

- More About Big Data & Data Analytics

→ "Big Data" is an all-encompassing term for any collection of data sets so large and complex that it becomes difficult to process using on-hand data management tools or traditional data processing applications.

→ Each day, we create 2.5 quintillion bytes of data—so much that 90% of data in the world today has been created in last two years alone. This data comes from everywhere: sensors used to gather climate info, post to social media sites, digital pictures and videos, purchase transaction records, & cell phone GPS signals to name a few. This data is "big data".

- Definition: Big data usually includes data sets with sizes beyond the ability of commonly used s/w tools to capture, create, manage, & process the data within a tolerable elapsed time.



- Big Data Analytics

→ Big (& small) Data Analytics is the process of examining data—typically a variety of sources, types, volumes and/or complexities—to uncover hidden patterns, unknown correlations, and other useful information.

→ Big Data analytics uses a wide variety of advanced analytics to provide

1. Deeper Insights
2. Broader Insights
3. Frictionless Actions

Punk

– Advanced Big Data Analytics

SQL Analytics	Descriptive Analytics	Data Mining	Predictive Analytics	Simulation	Optimization
• Count • Mean • OLAP	• Univariate distribution • Central Tendency • Dispension	• Association rules • Clustering • Feature extraction	• Classification • Regression • Forecasting • Spatial • Machine learning • Text Analytics	• Monte Carlo • Agent Based modeling • Discrete event modeling	• Linear optimization • Non-linear optimization

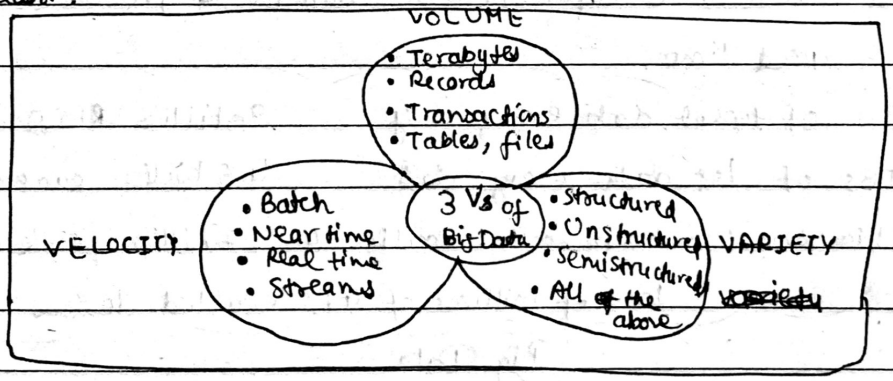
Date ___/___

– Big Data Analytic Applications

	Improves Operation Efficiences	Increases Revenues	Achieve Competitive Compet Differentiation
Mature Analytic Application	• Supply chain optimization • Marketing campaign optimization	• Algorithm trading	• In-house custom analytic application
Maturing Analytic Application	• Portfolio optimization • Risk Management • Next best offer	• Ad targeting optimization • Yield optimization	• In-house custom analytic applicatin
Emerging Analytic Applicatin	• Chronic disease prediction and prevention	• Custom churn protection prevention	• Product design optimization • Design of experiments optimization • Brand • Product market targeting

– 3 Dimensions / characteristics of Big Data

- 3 Vs (volume, variety & velocity) are three defining properties or dimensions of big data.



- Volume: Refers to amount of data. Experts predict that volume of data in the world will grow to 25 Zettabytes in 2020.
- Velocity: Refers to speed of data processing. Data is increasing accelerating the velocity at which it is created & at which it is integrated.
- Variety: Refers to no. of types of data. 80% of world's data is unstructured. The variety of data sources continues to increase. It includes internet data, primary research, secondary research, location data, image data, supply chain data, device data.

Punk

Date __/__/____

- Why Big Data?
  1. Understanding and Targeting Customers
  2. Understanding and Optimizing Business Processes
  3. Personal Quantification and Performance Optimization
  4. Improving Healthcare and public health
  5. Improving Sports Performance
  6. Improving Science and Research
  7. Optimizing Machine and Device Performance
  8. Improving Security and Law Enforcement
  9. Improving and Optimizing Cities and Countries
  10. Financial Trading

- Unstructured Data: Unstructured data is information that either does not have a predefined data model and/or does not fit well into a relational database.

- Mining Unstructured Data: To help with the problem, organizations have turned to a number of different software soln designed to search unstructured data and extract important information.

- Unstructured Data and Big Data:
  - → Structured Data generally resides in a relational database, and as a result, it is sometimes called "relational data". This type of data can be easily mapped into pre-designed fields.
  - → In addition to structured & unstructured data, there's also a third category: semi-structured data. Semi-structured data is information that doesn't reside in a relational database but that does have some organizational properties that make it easier to analyze.
  - → Big data refers to extremely large datasets that are difficult to analyze with traditional tools.

- Implementing Unstructured Data Management
  Variety of different tools to help organize & manage unstructured data
  - Big data tools: S/w like ~~Hadoop~~ Hadoop
  - Business intelligence software: Also known as BI

Punk

Date __/__/____

- Data integration tools : Tools to combine data from disparate sources to analyze
- Information management solutions : Tracks structured & unstructured data.
- Search & indexing tools : To retrieve info from unstructured data files.

* Elements of Social Network

- Social Network Analysis or SNA is the methodical study of collections of social rel"ship. These consists of social actors implicitly or explicitly connected to one another.
- SNA portray world to be composed of entities that are joined together by relationships.
- SNA focuses on relational data. Network analysts focus on patterns generated within collections of many connections.
- For individuals, SNA is more about "who you know" than "what you know" or "why you are". At group level, SNA illuminates how each person's individual connections aggregate form emergent macro-structures like densely connected sub groups. Using the
- Using the mathematics of graph theory, social network analysts calculate & visualize properties of networks & social actors that inhabit them.
- SNA is thus, a method of analyzing data, more than it is a theoritical framework.
- Types of SNA Networks:
  - Directed vs Undirected: Directed networks represent phenomena where the connection between two nodes is not necessarily reciprocated. Undirected networks are always mutual. For example, friends networks (such as on Facebook) and affiliation networks (same wiki page edit)
  - Weighted vs Unweighted: Some edges have values associated with them. for ex, edges in an email network are "weighted" based on no. of message one persons sends to another person, while a wiki co-edit page network is weighted based on no. of pages two people have both edited. Other edges are binary; they either exist or they don't. For example, facebook friendships & Twitter follow rel"ships don't have weights.
  - Multiplex Networks: It includes multiple types of edges. For ex, a network that connects people together based on their communication via email, phone, & face-to-face

Punk

interactions would include 3 distinct types of edges. This could be analyzed and visualized as a single multiplex network or as 3 distinct networks.

- Unimodal and Multimodal Networks: Many social networks, called unimodal networks, include only one type of node for ex:- all nodes represent people. / In / Contrast, multimodal networks include more than one type of node. If there are only two types of nodes we called the network bimodal, which is a subset of more general multimodal concept. Many bimodal networks, called bipartite networks, have one type of node (i.e., people) connected to another type of node (ex:- organizations) without any edges connecting nodes of same type (ex:- people to people). These bipartite networks can be transformed into unimodal networks.
- Partial Networks: In practice, it is not practical or useful to collect data on an entire network. Instead, analysts create partial networks in a variety of ways. One approach is to create an "egocentric network", which includes a single node (called "ego") & all of nodes that ego is directly connected to (called "alters"). when the connections b/w alters are also included, the graph is called 1.5 degree network. Adding ego's "friends of friends" makes it a 2.0 degree network & so forth.

- Network Analysis Tools: SNA requires use of specialized s/w designed to compute network metric & visualize network graphs. The tool landscape is in constant flux

SNA Tool	Description	Expertise Required	Open source	Maximum Network Size
Gephi	Standalone network analysis designed primarily for visualization. Can be extended via plugins.	Designed for novices	Yes	hundreds of thousands
NodeXL	Includes sophisticated graph visualization, social media data importers, & extensibility via formulas & macros but relatively few metrics	Microsoft Excel plugin designed for SNA novices	Yes	tens of thousands
Pajek	Includes comprehensive test of network metrics & statistical tests. Steep learning curve	Designed for sophisticated analysis of large datasets	Yes	millions
R	Open source statistical package with social network analysis functionality via the igraph, sna, network, & statnet packages. Includes comprehensive list of network metrics & statistical tests	Steep learning curve	Yes	millions
UCINet	Includes comprehensive list of network metrics & statistical tests. Designed for knowledgeable SNA researchers but does not require coding	Designed for researchers performing SNA	No	tens of thousa

Punk