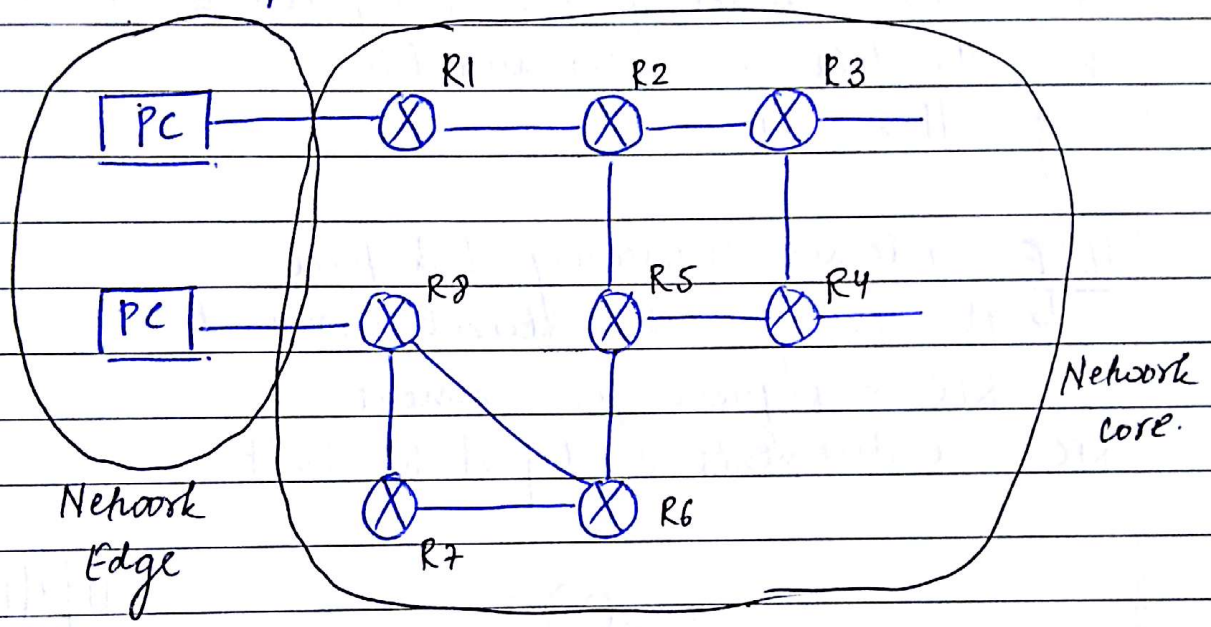
Computer Network – is a group of interconnected computers which allows computers to exchange information and data.

Internet – Millions or Billions of computing devices.

Components of Internet – PCs, smartphones, Routers, Wireless links, laptops, switches.



- Network is divided into two parts.
  Network core & Network edge.
- Network edge consists of devices such as PCs, smartphones, laptops otherwise called as end systems or host.
- Hosts are connected with each other with the help of links and packet switches.

physical media: optical fibre or coaxial cable or copper wire

→ link layer switches } diff. b/w these two. (S/A.
→ Router

Unit of data transfer : bits per second.
Small byles of data in CN packet.

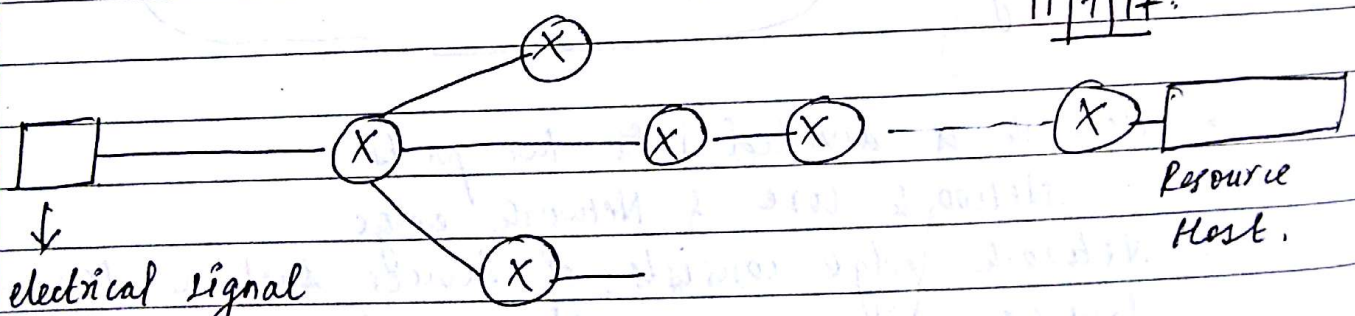
→ The unit of data transfer is bits per second.
→ Packet : A fragment of data with a header.
↳ contains info. about data.
↳ for recognising the data.

$\boxed{\text{data + Header = PACKET}}$

PROTOCOLS - A set of rules or regulations that determine how the data is transmitted.
eg. IP & TCP.

IETF- Internet engineering task force.
↳ It develops the internet standards.
RFC → Request for comment.
RFC are documents developed by IETF

11/7/17.



↓
electrical signal
optical impulse

LAN - Local Area Network
WAN - Wide Area Network
NIC - Network Interface Card.

Scanned by CamScanner

1. Application Layer.

packet of info. in application layer. [Message]

Func: Helps converting data into certain bits.

Protocols in this layer : HTTP, FTP, SMTP, DNS.

2. Transport Layer

packet of info. transport layer is called : Segment.

[Segment : Bit of data + Header]

↳ port no. of sender & receiver.

Protocols : TCP, UDP

Func. End to end delivery of data.

3. Network Layer.

[Datagram : Segment + Header.]

↳ identifier to know where data should reach

Func. Host to host delivery of data.

4. Datalink Layer.

- contains MAC Layer.
- [Frame = Datagram + Header]

info. in this layer is called frame.

5. Physical Layer.

whatever info. received will be converted to bits.

Scanned by CamScanner

Router : just gives packet a Route / path.

Router : Network Layer Works in Router.
But data has to be in slide form.

We can't just transfer using datalink layer coz we need port number.

Q) Which packet transmits from Sending Host & Receiving Host.
OR.
How many times it goes through any layer.

Switch.	Receiving Host	Sending Host	Router.
2 layers P and D	5 layers (ALL) A T N D P Start.	5 layers (ALL) P P N T A Start.	Network Layer - 1 Datalink Layer - 2 Physical Layer - 2 ↓ as many routers there are.

Switch is a type of link where many devices can be connected.
No Network Layer.

Scanned by CamScanner

Q. How many layers of functions performed in Router & Switch.

3 layers — 2 layers (coz no network layer).

Switching

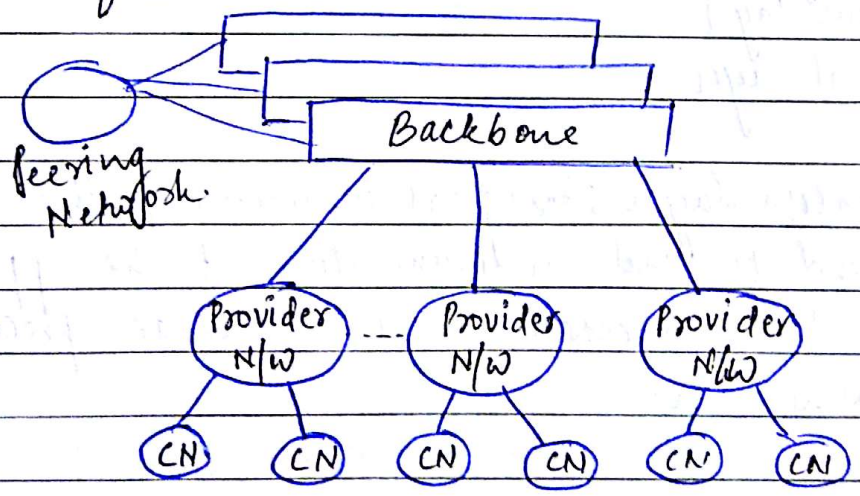
1) Circuit Switch. eg: telephone.

2) Packet Switch.: used in Routers.

In circuit switched network a dedicated connection called as a circuit is always available b/w the two end systems.

In packet switched network, In computer network, communication b/w 2 systems is done in blocks of data called packets. The packets can be stored and forwarded later. eg. Router is a packet switched N/w.

Structure of Network



Scanned by CamScanner

TCP/IP has 5 layers
OSI has 7 layers.

Internet Protocol Stack OR TCP/IP Suite.

↳ All layers & fns & rules in this suite.

TCP/IP Suite ⇒ Basically fns. of these 5 layers.

1. Application Layer
2. Transport Layer
3. N/W Layer
4. Datalink Layer
5. Physical Layer.

14/7/17.

OSI Model.

1. Application Layer
2. Presentation Layer.
3. Session Layer.
4. Transport layer
5. N/W layer.
6. Datalink layer
7. Physical layer

1. Application Layer : ⇒ Logical connection b/w the application layers are end to end, communication at the application layer is b/w two processes, hence called as process to process communication.

Scanned by CamScanner

Program is not active while process is active.

- There are various types of protocols used in application layer. eg HTTP - hypertext transfer protocol.
  SMTP - simple mail transfer protocol (used for electronic mail).

  FTP - used for transferring file from one host to another. [File Transfer Protocol].

DNS - Domain Name Server/System.
Used by the other protocols to find the Network Layer Address.

2. Transport Layer: ~~These are the source of gets the~~
- At the source host gets the message from the application layer and encapsulates the message with transport layer header called as segments.
- There are 2 protocols used in transport layer -
TCP - Transmission Control Protocol
UDP - User Datagram Protocol.
TCP is a connection-oriented protocol that establish a logical connection b/w the transport layers of 2 host.
UDP is a connection-less protocol that transmit user datagram without creating any logical connection.

3. Network Layer: - It is responsible for creating connection b/w source computer and destination computer, otherwise called as host to host communication.
- Protocol that are used in Network Layer are -
IP - Internet Protocol.
ICMP - Internet Control Message Protocol.

Scanned by CamScanner

IP defines the format of the packet called as datagram. Provides flow control, no error control and no congestion control.

ICMP is used to report the problems when routing a packet.

ARP - Address Resolution Protocol.

ARP helps IP to find the link layer addresses of a host or router.

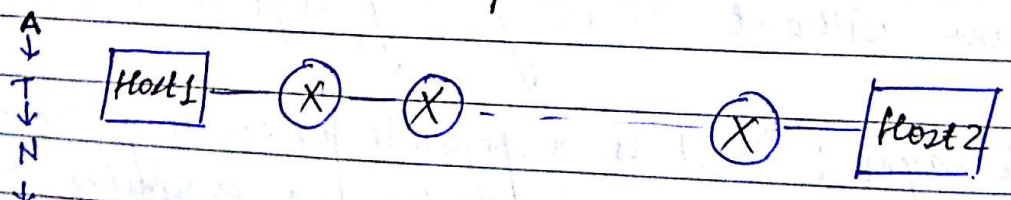
4. Datalink Layer: ⇒ Function of this layer is taking the datagram and moving it across the link. The packet of information in this layer is called as frame.

5. Physical Layer: ⇒ It is responsible for carrying individual bits in a frame across the links.

OSI Model - Open System Interconnection Model.

It is proposed by ISO ~~(Internation Standard of Organisation)~~ (International Organisation for Standardization).

Encapsulation and Decapsulation.



Q. What are the places where encapsulation process is done.

⇒ Sending Host & Router.

Scanned by CamScanner

Encapsulation at the source host – At the application layer the data to be exchanged is called message, the message is transmitted to transport layer. At transport layer a header is attached to the msg called as a segment. The segment is sent to network layer and the network layer header is attached which is called as a datagram. The datagram is then sent to the datalink layer. In datalink layer the header of the datalink is attached to the datagram known as frame. The frame is passed to the physical layer for transmission. The process of passing the msg to various layers and finally transmitting the data is called as an encapsulation process.

Decapsulation at the receiving host – At the destination host, each layer decapsulates the packet received, removes the header and delivers the data to the next higher layer until the message reached to the application layer

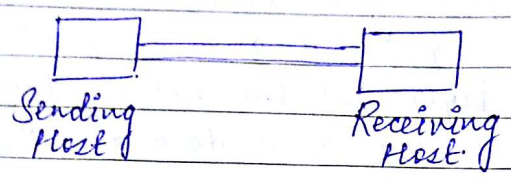
Packet Name	Layers	Address
Message	Application	Name
Segments	Transport	Port Number
Datagram	Network	Logical Addressing
Frame	Datalink	Link layer Address.
Bits	Physical	–

Imp * Q. OSI Model. Diff. b/w OSI Model and TCP/IP Protocol suite?
Q. What are the layers in OSI Model and TCP/IP Protocol Suite?

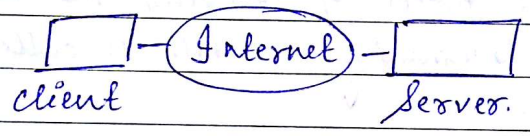
Scanned by CamScanner

18/7/17.

APPLICATION LAYER.



① Client - Server.
② Peer - Peer.



Application Layer - provides services to the user.
There are 2 types of application layer paradigms wed-

1.) Client-Server Paradigm - It is the traditional paradigm. In this the service provider is an application program called as server process. Server process waits for another application program called as client process to make a request. Server should be a powerful computer.
Disadvantage - If a large no. of client try to connect to the server at the same time. The server may be overwhelmed.
Another problem is that there should be a service provider willing to accept the cost.

2.) Peer - Peer Paradigm (P2P) - In this paradigm the responsibility is shared by the peer. A computer can

provide and receive services at same time.
Drawback – ① It is more difficult to create a secure communication b/w distributed services – Security.
② It appears that not all the applications can use P2P paradigm – Applicability.

CLIENT-SERVER PARADIGM.

In client-server paradigm, communication at the application layer is b/w 2 application programs called as processes.
1) Client process.
2) Server process.

A client is a running program that initialises the communication by sending a request.
A server is another application program that waits for request from a client.

Application Program Interface (API) – is a set of instruction b/w two entities. eg. socket / socket interface.
Socket interface lies b/w application layer and transport layer, to transmit the message from application layer to transport layer.
Socket is a data structure that is created and used by application programs.
Communication b/w client process & server process is b/w 2 sockets and 2 hosts.
For each socket there is a socket address.

Scanned by CamScanner

Socket address consists of port no. + IP address
(16 bits) (32 bits).

Q. What is P2P ? Give one eg.

Services of Transport Layer used by Application Layer.

2 protocols of transport layer are used by application layer.
TCP & UDP.
TCP is the connection-oriented, reliable and secured data transmission protocol where UDP is connection-less, unreliable and not secured.

WEB & HTTP.

Repository of information in which documents are stored are called as web pages.
Linking of the web pages was achieved using the concept of hyper text.
Each web page can contain links to other webpages.

Web client are the browsers.
Web client contains a controller, client protocols and interpreters.

Scanned by CamScanner

20/7/17

URL.

URL consists of 4 parts -

1) Protocol
2) Host
3) Port No.
4) Path.

1) Protocol : It is the first identifier. Protocols may be http or ~~fttp~~ ftp.
2) Host : Each host identifier can be the ip address of the server or a unique name given to the server.
3) Port : It is a 16 bit integer defined for the client-server application. If protocol is http, then port no. is 80.
4) Path : It identifies the location & name of the file.

Web Document.

These are of 2 types - 1) Static document
2) Dynamic document.

Static documents are fixed content documents that are created and stored in the server.

Dynamic documents are generated by server, when browser requests them.

HTTP - Hyper Text Transfer Protocol.

HTTP connections are of 2 types -

i) Persistent ii) Non-Persistent.

Scanned by CamScanner

In non-persistent, one TCP connection is made for each respone and request.
In persistent connection, all the data transfer occur in one TCP connection

HTTP Message.

1) Request Message.
   a) Request Line - (Message, URL, Version)
   b) Header Line
   c) Body.

2) Responce Message.
   a) Status Line (Version, Status Code, Phrase)
   b) Header line

Types of method in HTTP request :

1) GET - Requests a document from the server.
2) HEAD - Requests information about a document.
3) PUT - Send document from client to server.
4) POST - Sends information from client to server.
5) DELETE - Removes a webpage.

Q. What is there to separate Method, URL and version?
   Ans - Space.

Q. What do you use to separate Header line from Body?
   Ans - Blank line.

Scanned by CamScanner

Header Line

There are different header lines with values like : user agent, accept, host, upgrade, date, cookie, if modified since.

Response Message.

200 → Successful request
300 → Redirect the client to another URL.
400 → Error at client site.
500 → Error at server site.

Response Header Line

Data, upgrade, server, location, accept Range, Modified.

Proxy Server:

HTTP supports proxy servers :-
A proxy server is a computer, that keeps the copies of the response to recent request. When HTTP client sends request to proxy server, the proxy server checks it's cache, if the response is not stored in cache, the proxy server sends request to original server. Proxy server acts as both server and client. It reduces the load on original server and reduces the traffic.

Scanned by CamScanner

21/7/17.

FILE TRANSFER PROTOCOL.

FTP is used for file transfer. FTP client has 3 components- Client control process, client data transfer process & user interface.

Control connection : It uses port no. 21. In control connection, commands are send from client to server and response are send from ~~cli~~ server to client. Every FTP command generate atleast one responce. Response has 2 parts :- a 3 digit no. followed by a text. eg. 125 - data connection open; 150 - file status ok.

Data connection: It uses port no. 20. The client ~~uses~~ issues a passive open. Client sends the port no. to server. Server receives the port no. and issue an active open.

Data Structure: FTP transfer file uses the following structure of data —

1) File Structure
2) Record Structure
3) Page Structure

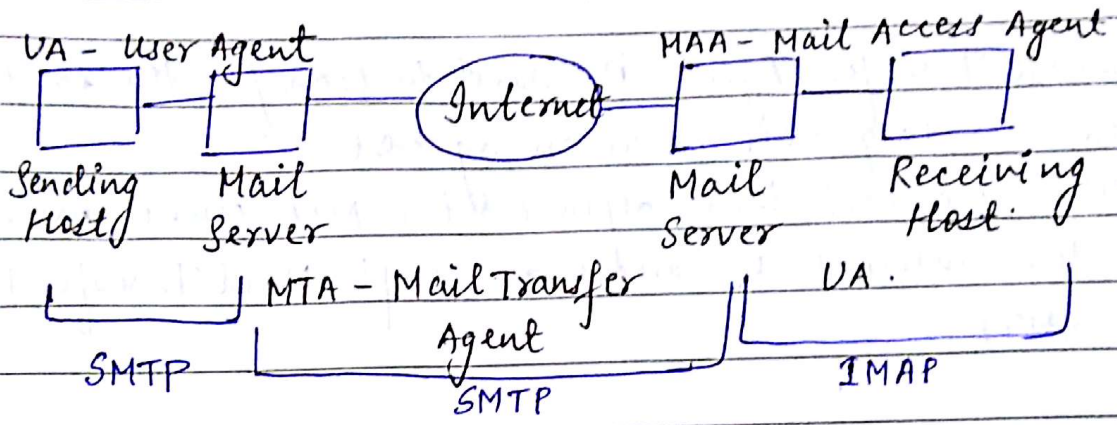
1) File Structure - It is a continuous stream of bytes.

2) Record Structure - The file is divided into records.

Scanned by CamScanner

3) Page Structure: File is divided into pages. Each page has a page no. and a page header.

E-Mail (Electronic Mail)



SMTP - Simple Mail Transfer Protocol.
POP - Post office Protocol.
IMAP - Internet Mail Access Protocol.

There are basically 3 agents used for mail transfer -

1) User Agent : Provides service to the user to make the process of sending and receiving a message easier. User Agent is a software package that composes, reads, replies to and forward message.
User Agent are basically of 2 types -
1) Command Driven
2) GUI Based.

Structure of the E-Mail

1. Envelope → Address

2. Message – Header & Body.

E-Mail Address has 2 parts – i) Local Part
ii) Domain Part.

Message Transfer Agent is used to transfer the email from sending host to receiving host.
The protocol that defines the MTA client and server in the internet is called as Simple Mail Transfer Protocol or SMTP.

Mail Transfer has basically 3 phases –
Connection Establishment, Mail Transfer and Connection Termination.

Message Access Agent – There are basically 2 mail access protocols used i.e. POP and IMAP.
POP – Post Office Protocol
IMAP – Internet Mail Access Protocol.

1) POP – It is very simple but has limited functionality.
First, you have to send the username and p/w to access the mail-box, then only you can retrieve the mail.
It has only 2 modes – 'keep' and 'delete'.
It does not allow users to organize the mail on the server.
It does not allow users to partially check the contents of the mail.

Scanned by CamScanner

2) IMAP- It has more features than POP.
User can check the email header. User can partially download email. User can create, delete or rename the mail-box.

MIME - Multipurpose Internet Mail Extension.
It is a supplementary protocol that allows non-ASCII data to be sent through email. It transforms non-ASCII data at the sender's side to ASCII data.

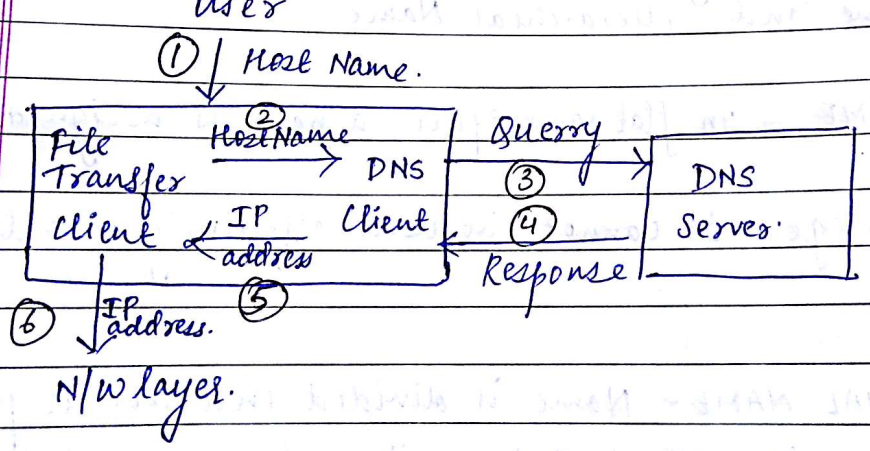
Scanned by CamScanner

2) IMAP- It has more features than POP.
User can check the email header. User can partially download email. User can create, delete or rename the mail-box.

MIME - MultiPurpose Internet Mail Extension.
It is a supplementary protocol that allows non-ASCII data to be sent through email. It transforms non-ASCII data at the sender's side to ASCII data.

24/7/17.

DOMAIN NAME SYSTEM.



→ Domain Name System (DNS) helps in mapping corresponding name to ip address.

→ TCP/IP protocol suite uses DNS client and DNS server to map a name to a ip address.

Scanned by CamScanner

Steps involved are —

i) User passes the host name to file transfer client.
ii) The file transfer client passes to DNS client.
iii) DNS client sends a message to DNS server with a query that gives the file transfer server name.
iv) DNS server respond to DNS client with a ip address.
v) DNS client pass the ip address to the file transfer client.
vi) The file transfer client can now use the received ip address.

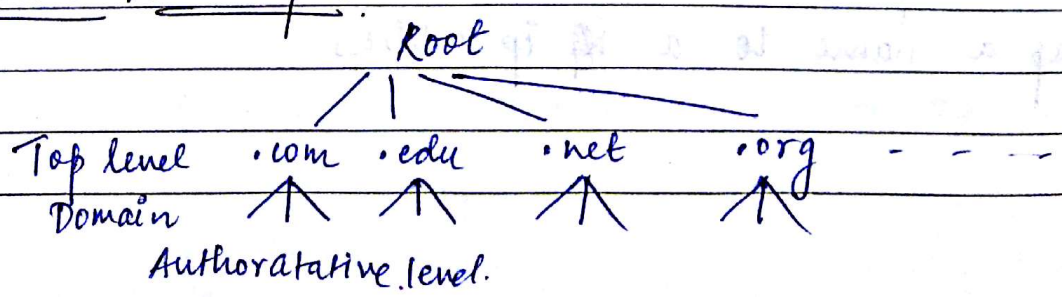
Name Space

Basically of two types —
Flat name and Hierarchial Name

1.) FLAT NAME – In flatname space, a name is assigned to a address.
Disadvantage – It cannot be used effectively in a large system.

2.) HIERARCHIAL NAME – Name is divided into several parts.
eg mycomputer . CE . KIIT University . edu

Domain Name Space.



Scanned by CamScanner

Date
Page

Basically DNS servers are divided into 3 levels —

i) Root Servers
ii) Top Level Domain Servers
iii) Authoratative Servers.

Domain Name - A full domain name is a sequence of levels separated by dots.

A domain is a subtree of domain name space.

There are 2 types of domain name —

1.) FQDN - Fully Qualified Domain Name.
2.) PQDN - Partially Qualified Domain Name.

If a label is terminated by a null string it is called FQDN.
If a label is not terminated by a null string it is called PQDN.

i) Root Server - It is a server whose zone consists of a whole tree.
Basically of 2 types — primary and secondary.
Primary Root Server is a server that stores a file for which it is an authority. It is responsible for creating, maintaining and updating the files.
Secondary Root Server is a server that transfers the complete info. about a zone from another server. It neither creates nor updates the file.

DNS in the internet is divided into 2 domains —.
Generic Domain and Country Domain.

Scanned by CamScanner

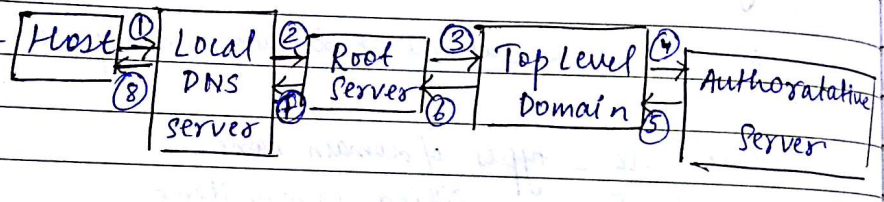
eg. of generic are : edu, org, net, com
eg. of country are : in, us, uk, fr

Resolution OR Address Resolution

1.) Recursive
2.) Iterative.

(In words to be done from book)

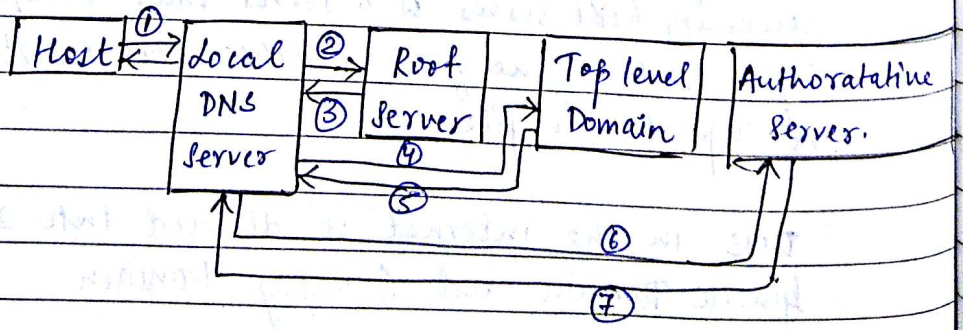
Recursive –



Mapping a name to an address is called name address resolution.
A host that needs to map ~~to~~ an address to a name or a name to an address calls a DNS client; also called as a resolver.
The resolver also called as DNS client, accesses the closest DNS server to find the solution to the request.
There are basically 2 procedures used –
Recursive and Iterative

(In works to be done on own)

Iterative –



DNS Caching.

Caching speeds up the address resolution process but if a server caches a mapping for a long time then it may send an outdated mapping information. Due to this reason, the authoratative server always adds info. to the mapping called as time-to-live (TTL)

DNS Resource Records.

25/07/17.

(Domain Name, Type, Class, TTL, Value)

eg. www.facebook.com → Domain Name; internet → Class.

Domain Name is what identifies the resource record.

Value - Value field defines the information kept about a domain name.

TTL defines the no. of second for which the information is valid.

Class defines the type of network; for computer n/w it is internet (IN).

Type defines how the value should be interpreted.

The types are —

i) A : a 32 bit IPv4 address

ii) NS : identifies the authoratative server for a zone.

iii) CNAME : defines an alias for the official name of the host. (canonical Name)

iv) MX : redirects mail to a mail server.

Scanned by CamScanner

eg (www.facebook.com, A, IN, 5, 101.10.1.9)

DNS Messages.

1.) Request / Query Message.
2.) Response Message.

0	15 16	31
Header	Identification	Flag.
	No. of question records	No. of answer records
	No. of authoratative records	No. of additional record
Values are not fixed for these fields	Question Record	
	Answer Record	
	Authoratative Records	
	Additional Records	

Identification field is used by the client to match a response with a query
The flag field defines whether the message is a query message or a response message.
Next 4 fields defines the no. of each record type.

Peer-to-Peer Networks.

When a peer in the network has a file to share it makes it available to the rest of the peer and interested peer can connect itself to the computer where the file is stored and download it. After the peer

downloads the file it can make it available for other peers to download.

These are of two types –

1. Centralized
2. Decentralized.

1. Centralized – In this network, listing of the peers and what they offer are done using a peer-to-peer paradigm. Listing of the peer is done by client-server paradigm and storing and downloading is done by peer-to-peer. Due to this reason, sometimes it is known as hybrid p-2-p network. eg: Napster.

2. Decentralized – It is of 2 types
   i) Structured
   ii) Unstructured.

A decentralized P-2-P network does not depend upon a centralized directory.

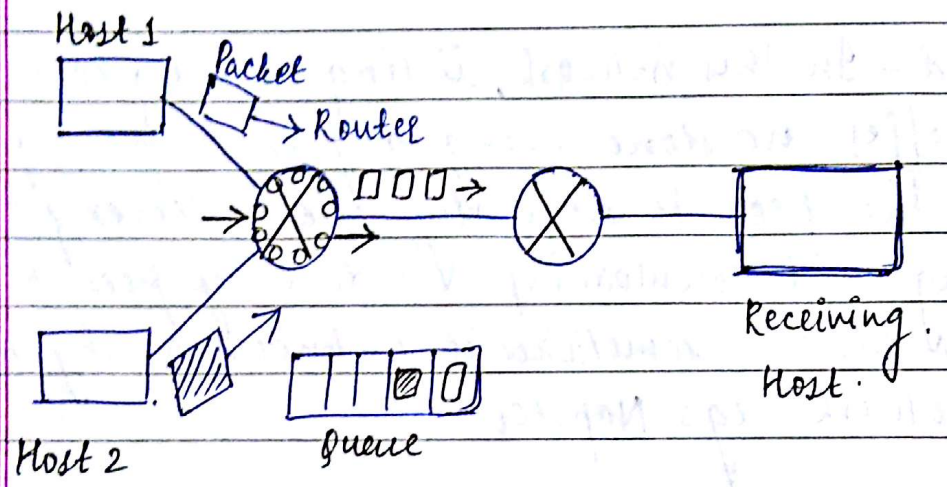
i) Unstructured n/w – The ~~networks~~ nodes are linked randomly.
eg: Gnutella and Freenet.

ii) Structured n/w – It uses predefined setup rules to link the nodes so that a query can be effectively and efficiently resolved.
eg: BitTorrent.

Scanned by CamScanner

31/7/17

(Introduction) PACKET DELAY AND LOSS.



1) PROCESSING DELAY- The time required to examine a packet header, examine the error level and to direct the packet.

one ques. in exam 2.) QUEUING DELAY- The time for which the packet waits in the queue to be transmitted onto the link is called as queuing delay.

3) TRANSMISSION DELAY- The amt of time required to transmit all the bits of a packet into the link is called as transmission delay.

Suppose L = length of the packet.
R = the transmission rate.

then, transmission delay $= \frac{L}{R}$.

Scanned by CamScanner

4) PROPAGATION DELAY – The time required to transmit the packet in the medium is called as propagation delay.

Suppose D = dist. b/w the 2 links.

S = speed of the medium

then, propagation delay $= \frac{D}{S}$

$$\boxed{\text{Delay} = d_{proc.} + d_{queue} + d_{trans.} + d_{prop.}}$$

Q i) How long does it take for a packet of L = 1000 bytes to propagate over a link of D = 2500 km, propagation speed = 2.5×10^8 m/s and transmission rate 2 mbps.

ii) Does this delay depend upon packet length and transmission rate?

i) L = 1000 bytes

D = 2500 km

S = 2.5×10^8 m/s.

R = 2 mbps.

$$d_{prop.} = \frac{D}{S} = \frac{2500 \text{ km}}{2.5 \times 10^8 \text{ m/s}} = \frac{2500 \times 10^3 \text{ m}}{2.5 \times 10^8 \text{ m/s}}$$

$$= 10^{-2} \text{ s.}$$

$$= 10 \text{ ms.}$$

ii) No.

Scanned by CamScanner

FLA

Q. Suppose 2 hosts A and B are separated by 20,000 km and are connected by a direct link of R = 2 mbps. Suppose the S over the link is 2.5×10^8 m/s.

i) Calculate the d_{prop}.

ii) Calculate the max. no. of bits that can be in the link

iii) Consider sending a file of 80,000 bits from host A to host B. Suppose the file is sent continuously as one large file. Calculate the total time taken to send the file.

T+Prop

i) $d_{prop.} = \frac{D}{S} = \frac{20,000 \text{ km}}{2.5 \times 10^8 \text{ m/s}} = \frac{20,000 \times 10^3 \text{ m}}{2.5 \times 10^8 \text{ m/s}}$

=

ii) Bandwidth Delay Product.

$d_{prop} \times R$ = No. of bits in the medium.

iii)

Scanned by CamScanner

THROUGHPUT

Throughput = Minimum [R1, R2, ---- Rn]
n = No. of links.

It is the rate at which bits are transferred b/w sender and receiver.

Q. i) Suppose Host A wants to send a large file to Host B. The path from Host A to Host B has 3 links of rates R1 = 500 kbps, R2 = 2mbps and R3 = 1 mbps. What is the throughput of the data transmission?

Throughput = Min. [500 kbps, 2 mbps, 1 mbps]
= 500 kbps.

ii) Suppose the file is 400 million bytes. How long will it take to reach the receiving host?

$\frac{\text{Packet length}}{\text{Throughput}} \Rightarrow \frac{400 \times 10^6 \times 8}{500}$

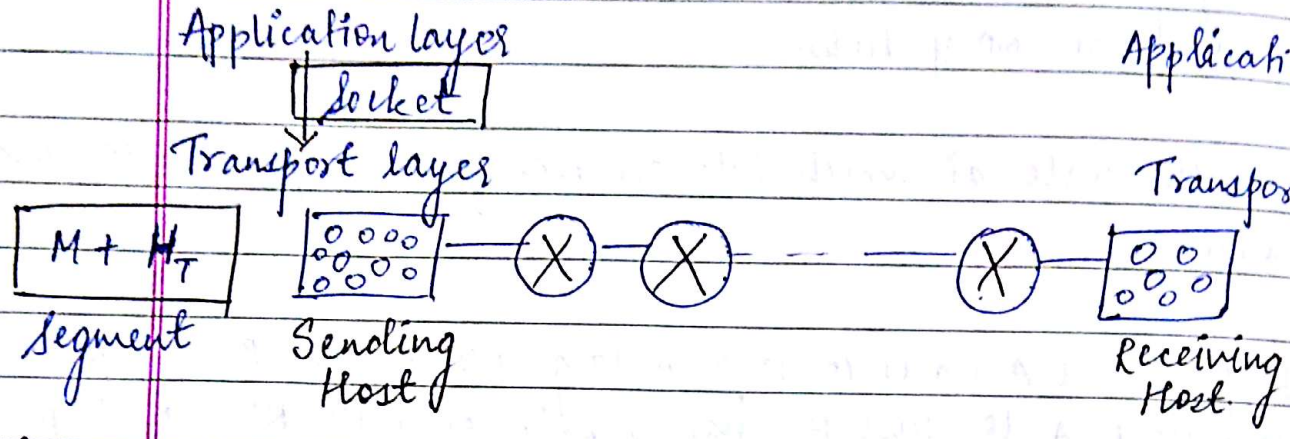
Scanned by CamScanner

if 16 bit then 2^{16} ports are there.

$2^{16} = 65535$.

01 | 08 | 2017

TRANSPORT LAYER.



Imp. (All 8 points) # Services provided by transport layer :-

1. Process - to - Process Communication.

→ The first duty of transport layer is to provide process-to-process communication.

→ A process is an application layer entity which uses transport layer services.

→ A transport layer is responsible for delivery of the message to application layer.

2. Addressing.

1.) Well known port no. → 1024 (0 - 1023) → can't be used
2.) Registered port no. → 1024 - 49251 } can be used
3.) Dynamic port no. → 49252 - 65535 }

Internet Co-operation for Assigned Name and Number - ICANN
Ports nos. are given by ICANN.

Scanned by CamScanner

The port no. of socket address is provided by transport layer.

3. Encapsulation and Decapsulation.

Encapsulation happens at the sender's site and decapsulation happens at the receiver's site.

4. Multiplexing and Demultiplexing.

→ When an entity accepts items from more than one source is called as multiplexing.
→ When an entity delivers item to more than one source it is called as demultiplexing.

5. Flow Control

The sending process at the application layer is only a producer, it produces message and push them to transport layer.
The sending transport layer has 2 roles i.e. producer and consumer.
It consumes the message pushed by application layer.
It encapsulates the message in packet and push them to receiving transport layer.
The receiving transport layer also has 2 roles - producer & consumer.

A buffer is a set of memory location that can hold the packet at sender and receiver.
When buffer of the sending transport layer is full it

Scanned by CamScanner

stops accepting messages from application layer. When buffer of receiving transport layer is full it stops accepting message from sending transport layer.

6. Error Control.

SEQUENCE NUMBER- Each packet is assigned one sequence no. If the header of the packet allows 'm' bit of sequence no, then the sequence no. can range from 0 to $2^m - 1$.
Sequence nos. are modulo 2^m.

~~Ack~~ Acknowledgment : Receiver sends an acknowledgement each time a packet arrives at receiver.

A window is a buffer to store a no. of packet.

7. Congestion Control.

Congestion control helps in keeping the network load below the capacity.

8. Connection-Oriented and Connection-less Service.

Connection-less services uses the protocol UDP.
Data maybe delivered out of order so in connection-less service, there is no flow control, error control or congestion control. In connection oriented service, a

Scanned by CamScanner

connection is setup b/w sender and receiver.
TCP protocol is used for connection-oriented services.

Scanned by CamScanner

connection is setup b/w sender and receiver.
TCP protocol is used for connection-oriented services.

03/08/2017.

TRANSPORT LAYER PROTOCOLS.

1. Simple Protocol.
2. Stop-and-Wait Protocol.
3. GO-BACK-N Protocol.
4. Selective Repeat Protocol.

1. Simple Protocol – It is a connection-less protocol. It does not have flow control and error control. Transport layer at the sender's side gets the message from application layer and makes a packet out of it and sends the packet. Transport layer at the receiver's side receives the packet from network layer, extracts the message and delivers it to the application layer.

2. Stop-and-Wait Protocol – It is a connection-oriented protocol which uses flow control and error control. The sending window size is 1, the receiving window size is also 1. To deduct the corrupted packet, a check~~tone~~sum is added to the header.

To prevent the duplicate packet, sequence no. and acknowledgement no. are used in this protocol.
Three things can happen :-

Scanned by CamScanner

1. The packet arrives safe and sound.
Receiver will send the acknowledgement
Acknowledgement arrives safe at sender and sender sends the next packet.

2. The packet is corrupted and never arrives at the receiver. Sender resends the packet after timeout.

3. Packet arrives safe and sound. Receiver sends an acknowledgement but the acknowledgement is lost. After timeout the packet will be resend, but it will be discarded because it is a duplicate packet.

(Round Trip Time) $RTT = 2 \cdot d_{prop.}$

$$d_{trans.} = \frac{L}{R}$$

Link Utilization = U_L

$$U_L = \frac{L/R}{L/R + RTT}$$

$$= \frac{1}{1 + \frac{RTT}{L/R}}$$

$$= \frac{1}{1 + \frac{2 d_{prop.}}{d_{trans.}}} \rightarrow a.$$

Scanned by CamScanner

$$\boxed{U_L = \frac{1}{1+2a}}$$

where $a = \frac{d_{prop}}{d_{trans}}$

Q. Assume that in a stop-and-wait protocol, the bandwidth of the line is 1 mbps and 1 bit takes 20 ms to make a round trip. If the system data packets are 1000 bits in length, what is the % utilization of link.

$L = 1000$

$R = 1$ mbps

$RTT = 20$ ms

$d_{prop} = \frac{20}{2} = 10$ ms

$d_{trans} = \frac{L}{R} = \frac{1000}{1 \times 10^6} = 10^{-3}$ s. $= 1$ ms.

$a = \frac{10\text{ms}}{1\text{ms}} = 10.$

$U_L = \frac{1}{1+2a} \Rightarrow \frac{1}{1+20} \Rightarrow \frac{1}{21} \Rightarrow 0.0476.$

$\Rightarrow 4.76\%.$

Scanned by CamScanner

Date
Page

Q1 The distance from earth to a distant planet is 9×10^{10} m. What is the channel utilisation if a stop-and-wait protocol is used for frame transmission on a 64 mbps point to point link. Assume that the frame size is 32 kilobyte and the speed of light is 3×10^{8} m/s.

Q2 Consider the use of 10 kilobit size frames on a 10 mbps satellite channel with 270 ms delay. What is the link utilisation for stop-and-wait ARQ technique assuming $P = 10^{-3}$.

P → % of error in transmitting the frame.

ARQ → Automatic Repeat Request.

$$\boxed{U = \frac{1-P}{1+2a}}$$

when P is given in the question (for stop-and-wait only).

4/08/17

Q. A channel have bit rate of 4 Mbps propagation delay 20 ms for what range of ~~time~~ frame size does stop & wait protocol give an efficiency at least 50%.

Doubt (pic in phone).

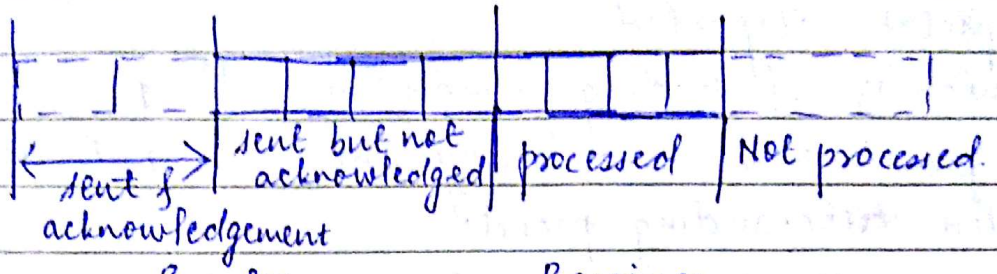
$$U = 50\% = 0.5 = \left[\frac{1}{1 + 2 \times \frac{d_{prop.}}{d_{trans.}}}\right]$$

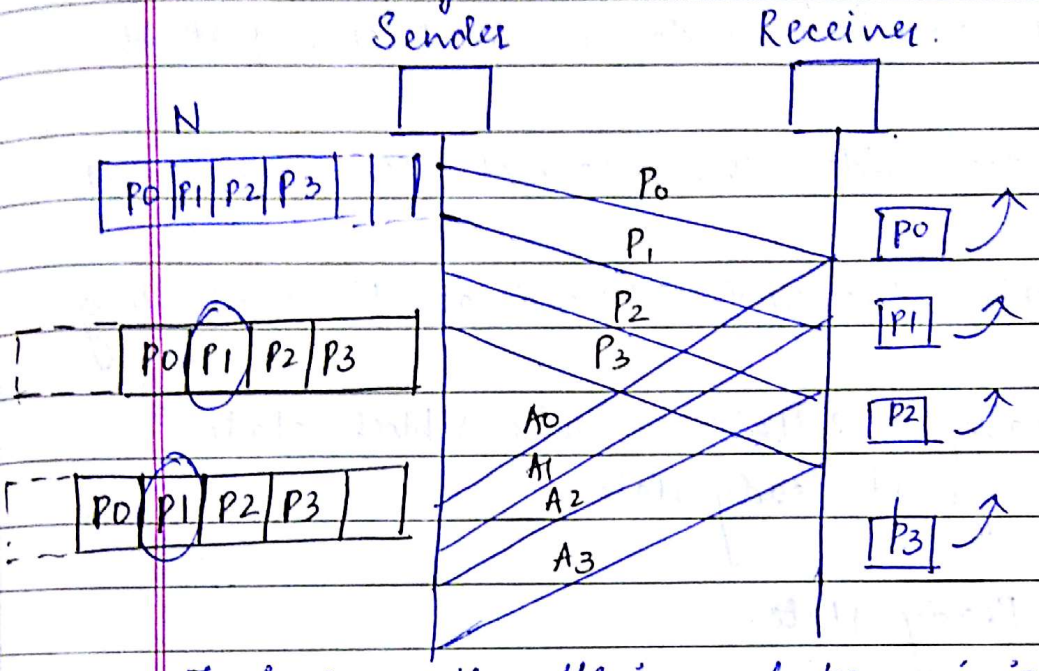
$$= 1 + 2 \times \frac{20 \times 10^{-3}}{L/R} = \frac{1}{0.5}$$

$$\Rightarrow \frac{2 \times 20 \times 10^{-3}}{L/4 \times 10^{3}} = \frac{1}{0.5} - 1.$$

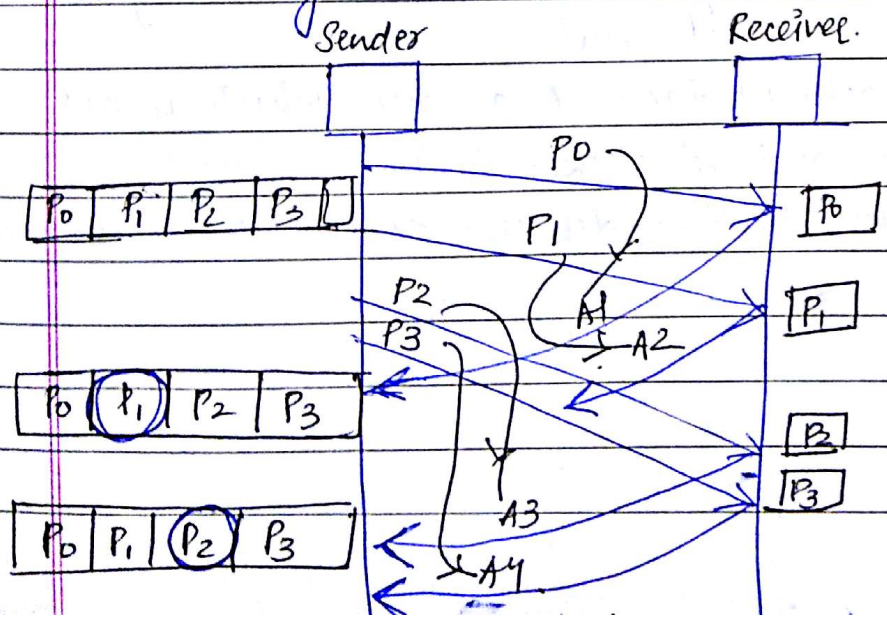
Scanned by CamScanner

3. GO-BACK-N PROTOCOL





To improve the efficiency of transmission multiple packets can be sent while waiting for acknowledgement.
In this protocol sender's sequence no. is in Modulo 2^m where m is the size of the sequence no. filled bits.
Acknowledgement nos. are cummulative.



Acknowledgement: expected next byte because of which it starts from A_1 and not A_0.

Scanned by CamScanner

→ The acknowledgement is cummulative that defines the next packet expected.

→ Maximum size of sending window is $2^m - 1$.
The packet that are already sent and not acknowledged is called outstanding packets.

→ The size of the received window in GO-BACK-N protocol is always one.

→ Receiving window slides when a correct packet arrives and is delivered.

→ When timer expires, the sender resends all the outstanding packets.

→ Sender is basically in 2 states - ready & block state.

→ Receiver is always at Ready State.

Sender's side Ready State.

→ A packet is sent, time started, and the sender goes to blocking state.

→ If an error free acknowledgement arrives the timer is stop.

→ If all the outstanding packets are not acknowledged, timer is restarted & packet sent.

→ If a corrupted acknowledgement arrives which is not related to outstanding packet it is discarded.

→ If timeout occur, the sender resends all the outstanding packets.

Scanned by CamScanner

Sender's side Blocked State.

→ If an error free acknowledgement arrives which is ~~not~~ related to outstanding packet, the sender slides the window.

→ If all outstanding packets are not acknowledgement, the timer starts and sender moves to ready state.

→ If an acknowledgement not related to outstanding packet arrived, acknowledgement is discarded

→ If timeout, sender sends all the outstanding packets.

Receiver's side Ready State.

→ If an error free packet arrives, it is delivered to application layer and an acknowledgement is sent.

→ If an error free packet with sequence no. outside the window arrives the packet is discarded.

→ An acknowledgement which was sent previously is sent.

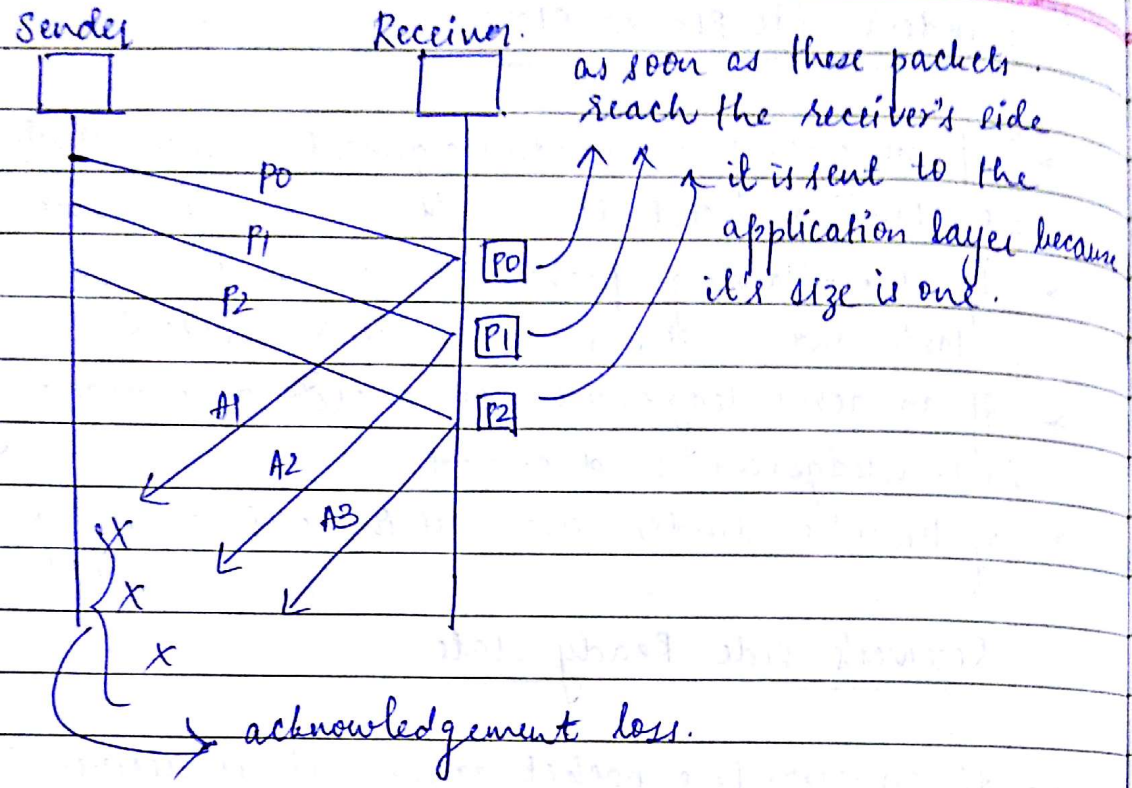
→ If a corrupted packet arrives, it is discarded.

Q. Why GO-BACK-N protocol is called as GO-BACK-N ?

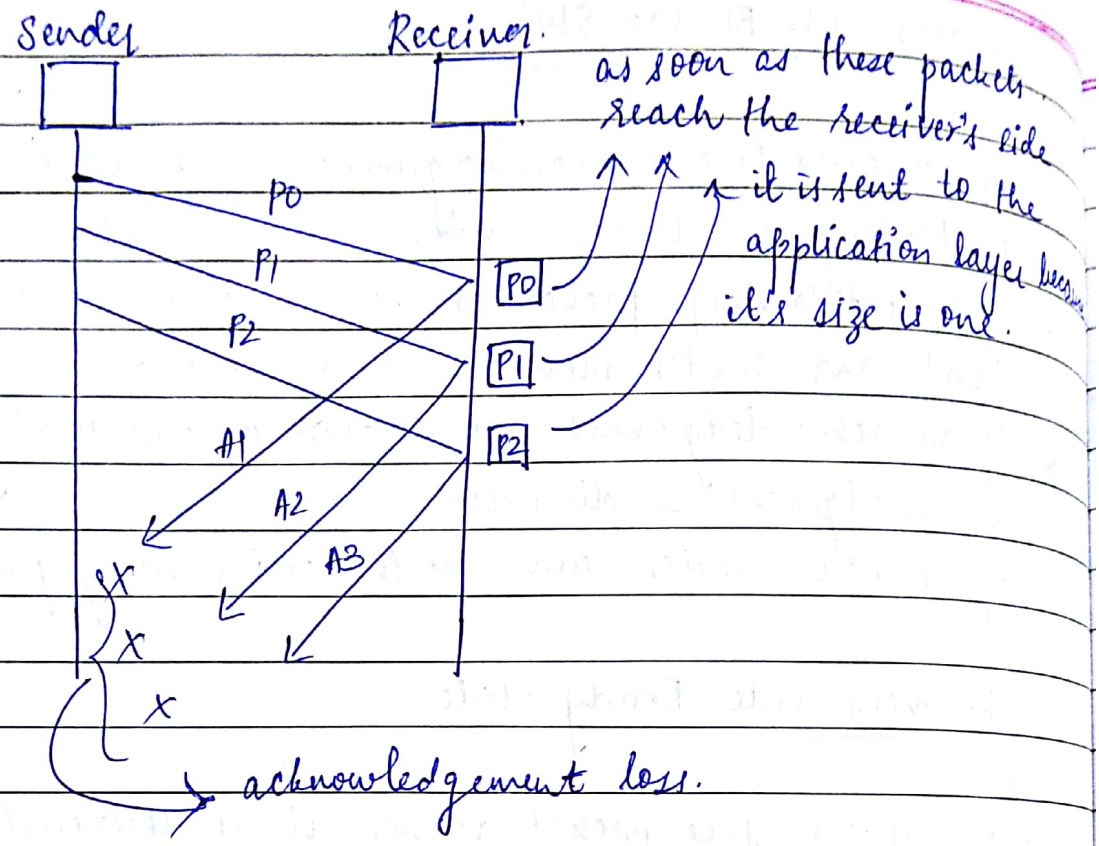
If any packet loss, other packets are also discarded.
if P_0 is loss, then P_1 P_2 P_3 ... are also discarded.
When a packet is lost, it will go back and resend all the packets (n no. of packet) after it.

Q. Why sending window size is < 2^m and not 2^m ?

Scanned by CamScanner



Because these acknowledgement's are lost, the sender will resend P0 P1 P2 packets, and then the receiver will resend it to the application layer, which will lead to duplicate packets, which may cause a problem ∴ to overcome such problems the window size is $2^m - 1$.

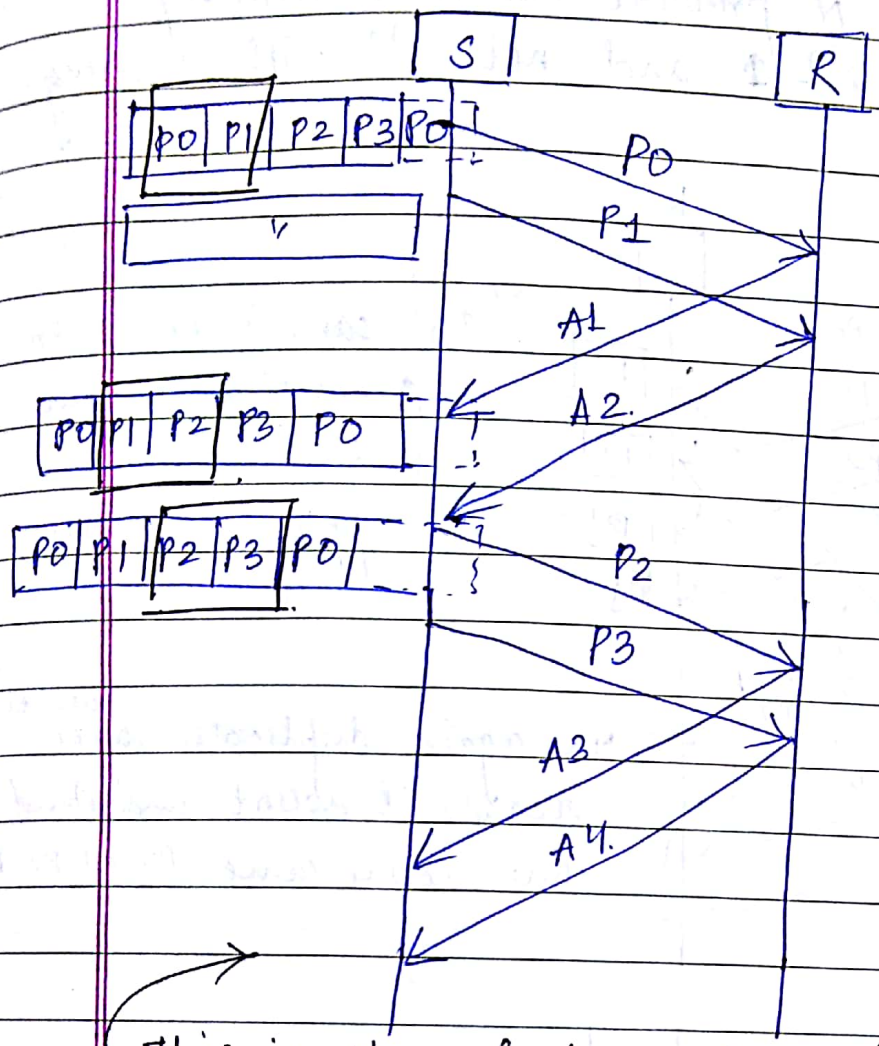


Because these acknowledgement's are lost, the sender will resend P0 P1 P2 packets, and then the receiver will resend it to the application layer, which will lead to duplicate packets, which may cause a problem ∴ to overcome such problems the window size is $2^m - 1$.

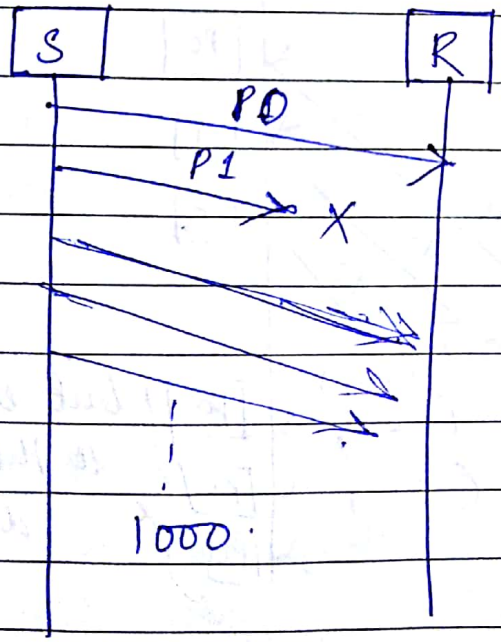
Disadvantage –

If any packet is lost in b/w, all the other packets after that packet has to be retransmitted.

8/8/17



This is Normal transmission (No error).

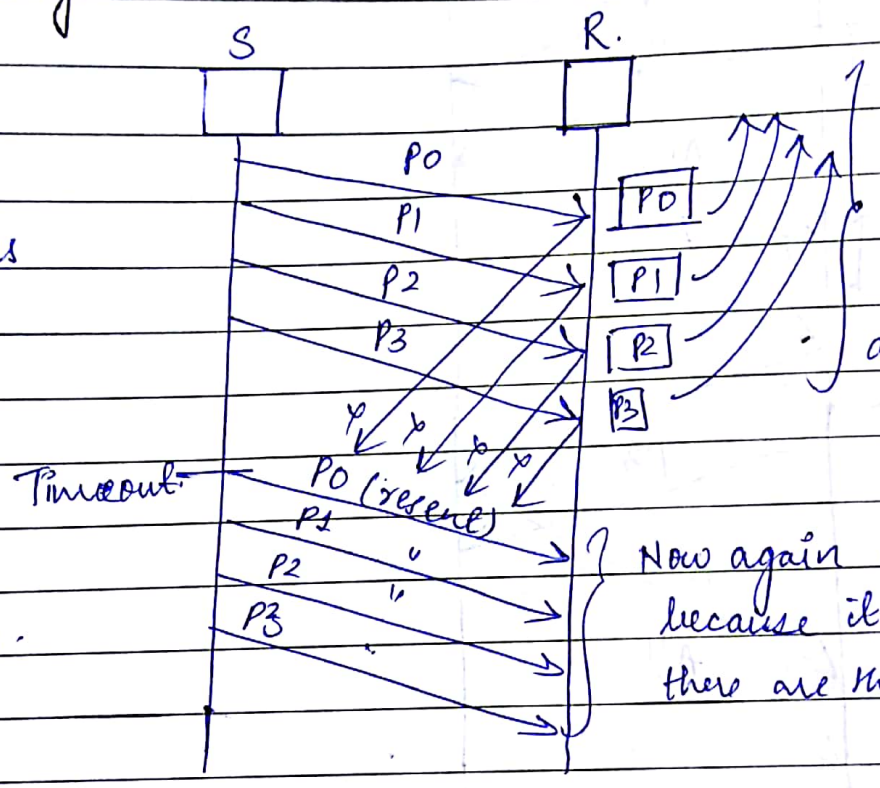


Any out-of-order packet will discard.

Scanned by CamScanner

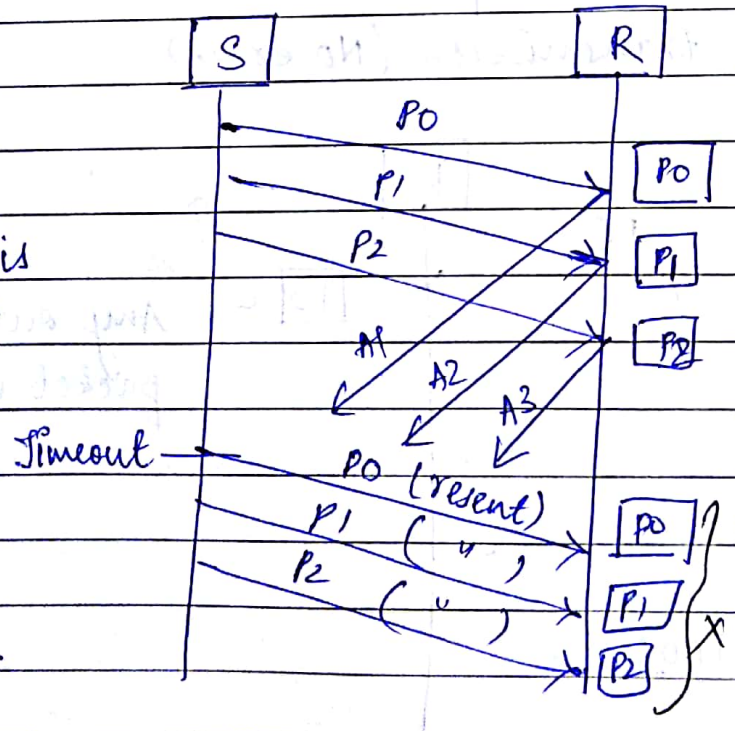
→ Why in GO-BACK-N protocol the max. sending window size is $2^m - 1$ and not 2^m. with timing diagram.

Fig 1: When size is 2^m.



This is an unreliable transmission.

Fig 2: when size is $2^m - 1$



This is a reliable transmission.

Scanned by CamScanner

Assume the max. window size is 2^m in fig. 1
Suppose simultaneously 4 packets are being transmitted.
4 packets send parallelly and all acknowledgement lost.
They'll be delivered to application layer coz they are in order.
When P0 P1 P2 P3 are resend, it will be again delivered → duplicate → unreliable.

Now for fig-2.; it will discard P0, P1, P2 and wait for P3.
Because the next expected packet is P_3.
This is a reliable transmission.

Which is why the max. sending window size is $2^m - 1$ and not 2^m.

Q. Consider the use of 10 kilo bit size frames on a 10 mbps satellite channel with 270 ms delay. What is the link utilisation for go-back-N ARQ with window size 7 assuming $P = 10^{-3}$.

$$\boxed{U = \frac{N(1-P)}{(1+2a)(1-P+NP)}}$$ (for go-back-N protocol)

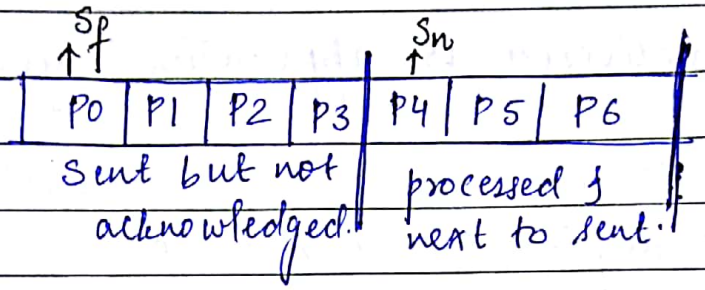
$d_{prop} = 270\,ms$ $\qquad P = 10^{-3}$

$d_{trans} = \frac{10 \times 10^3}{10 \times 10^6}$ $\qquad a = \frac{d_{prop}}{d_{trans}}$

unit is sec

$N = 7$

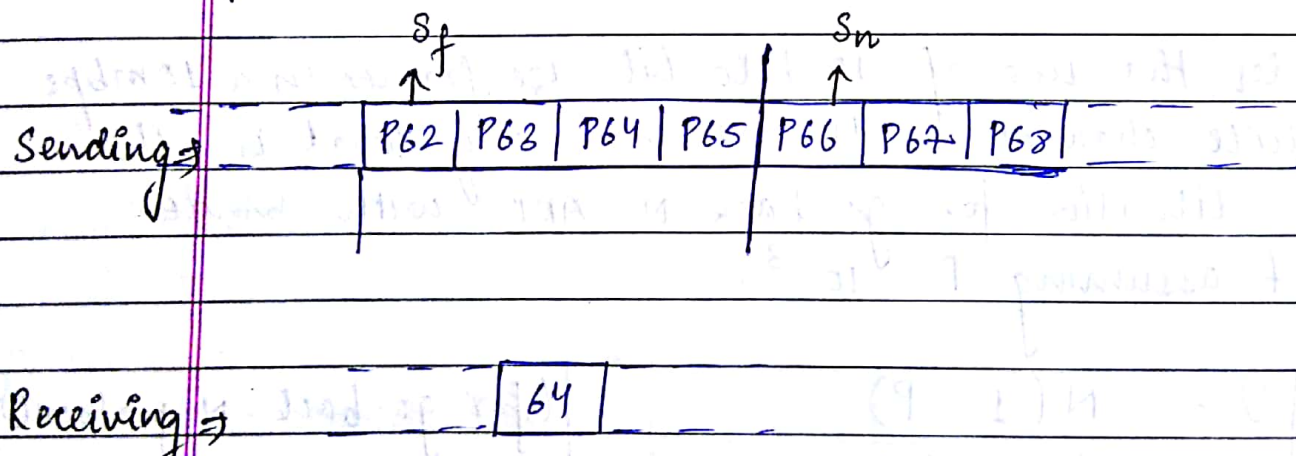
S_f = First outstanding packet.
S_n = next packet to be sent.
R_n = next packet expected at receiver.



$m = 3$. $2^m = 8$
7.

Q. In a network using the go-back-N protocol with $m = 3$ and sending window size 7, the values of variables are $S_f = 62$, $S_n = 66$, $R_n = 64$. Assume that the network does not duplicate or re-order the packets.

i) What are the sequence nos. of the data packets in transit.
ii) What are the acknowledgement nos. of acknowledgement packets in transit.



i) sequence nos. ⇒ 64 & 65 (these packets are expected next)
ii) acknow. nos. ⇒ 62 & 63 (because these have already been sent).

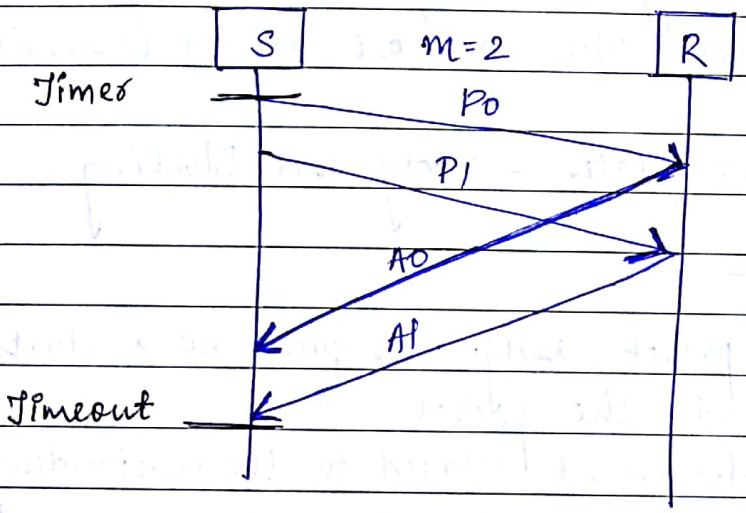
Scanned by CamScanner

Q. A sender sends a series of packets to the same destination using 5 bits sequence no. If the sequence no. starts with 0, what is the sequence no. of 100th packet.

10/08/2017.

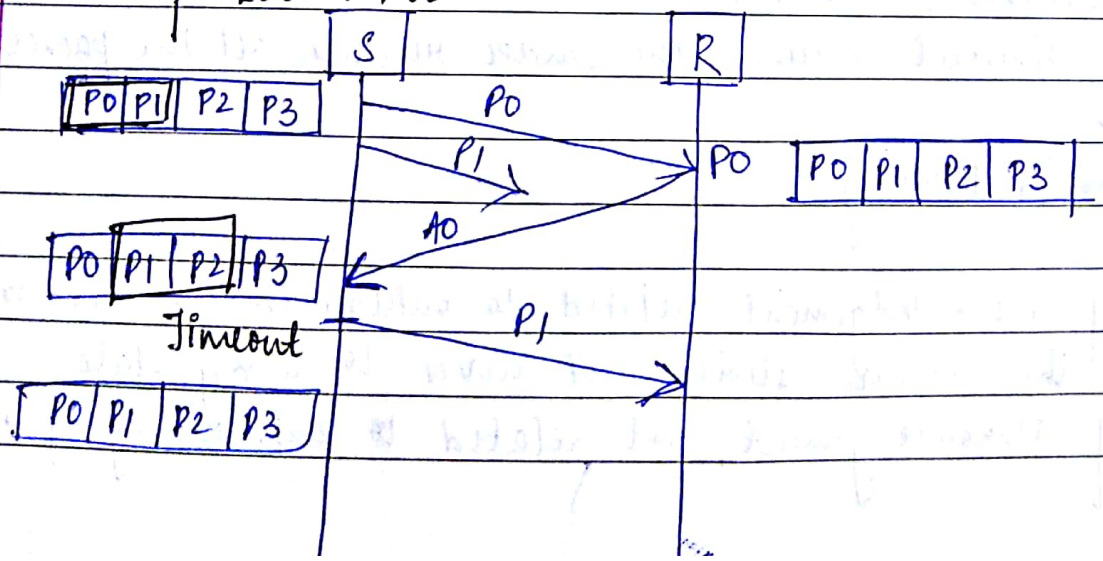
SELECTIVE REPEAT PROTOCOL

The maximum window size in selective repeat protocol is $\frac{2^m}{2}$ where m = no. of bits



Normal Transmission

→ When packet is lost.



Scanned by CamScanner

In selective repeat protocol, the sending window size is equal to the receiving window size.
The maximum window size is $\frac{2^m}{2}$.

Acknowledgement in selective repeat protocol defines the sequence no. of the packet arrived. It allows as many packets as the size of the receiving window to arrive out of order and be kept until there is a set of consecutive packets. And after that, it is delivered to application layer. When the timer expires, only the packet which are lost are re-transmitted.

Sender has two states - ready and blocking.

Sender Ready

→ It creates a packet, assign a sequence no, starts the timer and sends the packet.

→ If an acknowledgement related to the outstanding packet arrives, the window slides.

→ If acknowledgement not related to the outstanding packet arrives, it is discarded.

→ If timeout occurs, the sender resends all the packet.

Sender Blocking

→ If acknowledgement related to outstanding packet arrives, the window slides and moves to ready state.

→ If acknowledgement not related to outstanding packet

arrives, it is discarded.

→ If timeout occurs, re-transmit all the unacknowledged packet.

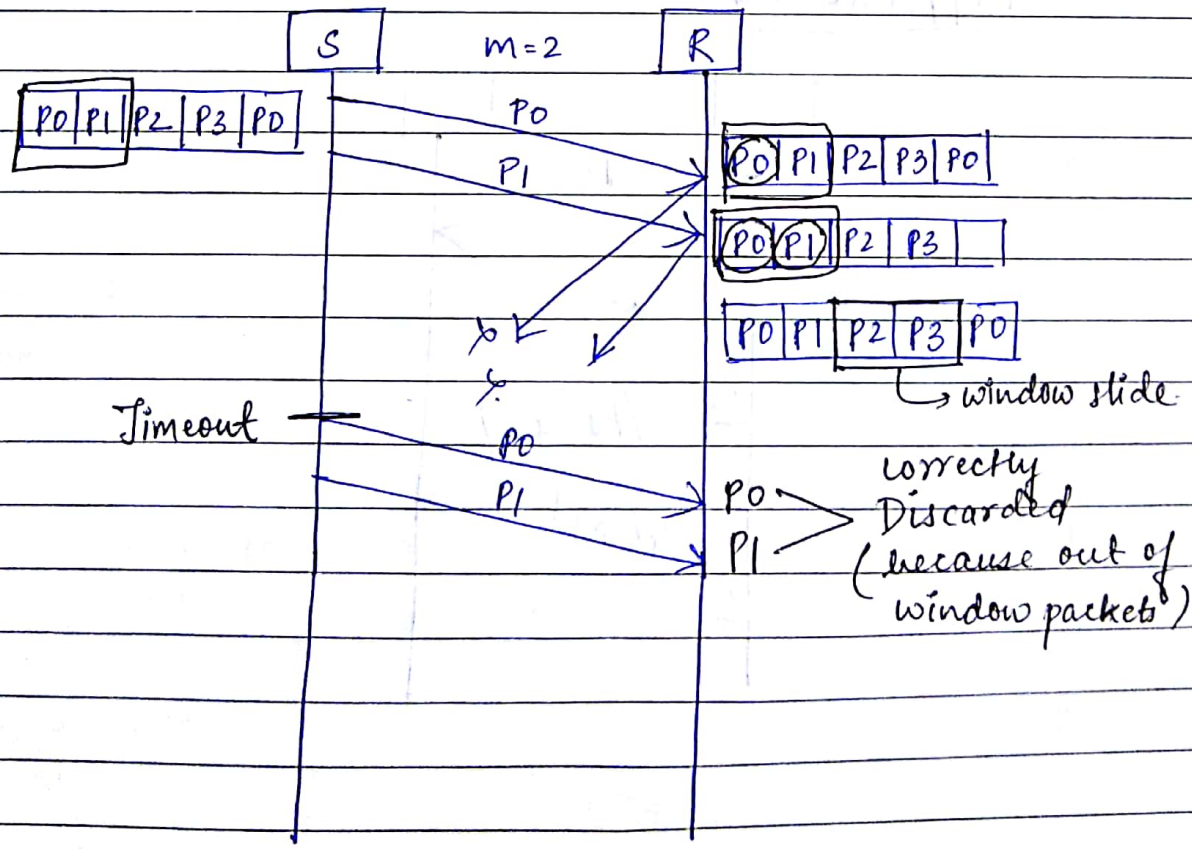
Receiver's Ready State

→ If a packet arrives, acknowledgement will be sent, window slides.

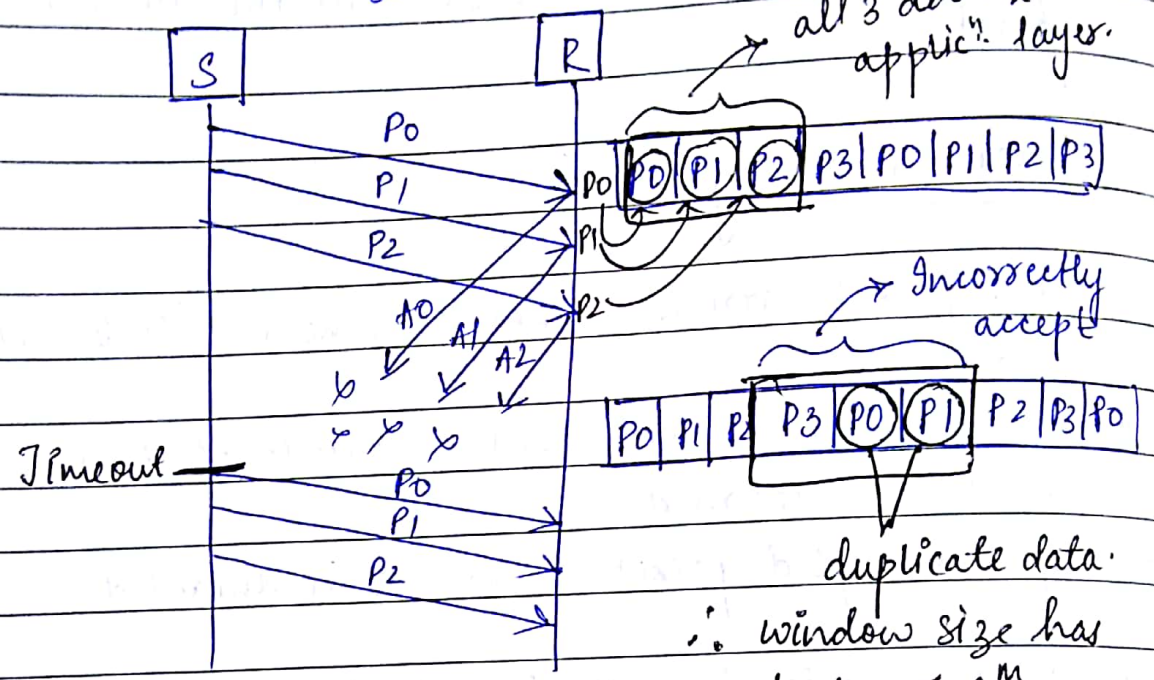
→ If a packet arrives which is outside of the window, the packet is discarded.

→ If a corrupted packet arrives, it is discarded.

Q. Why in selective repeat protocol, the maximum window size is $\frac{2^m}{2}$?

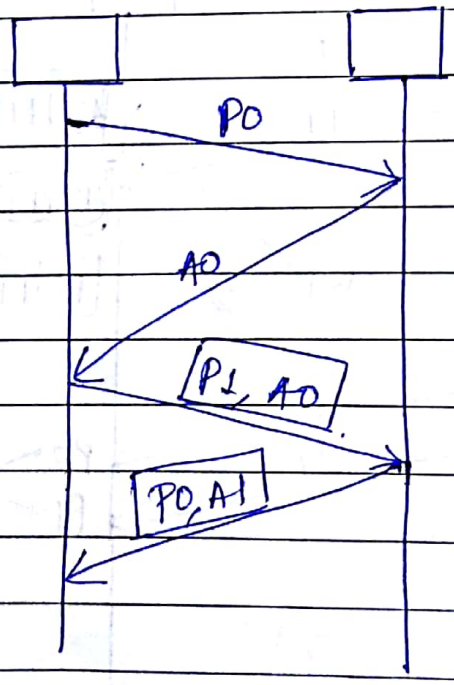


Window size is $\geq \frac{2^m}{2} \approx 3$.



∴ window size has to be $\frac{2^m}{2}$.

PIGGYBACKING



Q. In the previous go back n problem, suppose selective repeat protocol is used instead. Calculate the link utilisation.

$$\boxed{U = \frac{N(1-P)}{1+2a}} \qquad \frac{2^m}{2} = \frac{8}{2} = 4.$$

11/08/2017

Q1 Assume that the timeout values in SR protocol is sufficiently long such that 5 consecutive data segment and their corresponding ACKs can be received. Suppose Host A sends 5 data segment to Host B and 2nd segment is lost. In the end all 5 segments have been received correctly by Host B. How many segment Host A sent to Host B in total and how many ACKs Host B sent in total?

Q2. The value of parameters for stop and wait ARQ are given below :-

Bit rate of transmission channel = 1 Mbps.

Propagation delay from sender to receiver = 0.75 ms.

Number of bytes in packet = 2000

" " " " ACK = 20

Assume that there are no transmission errors. The efficiency (%) of stop-and-wait ARQ is —

↓

link utilization.

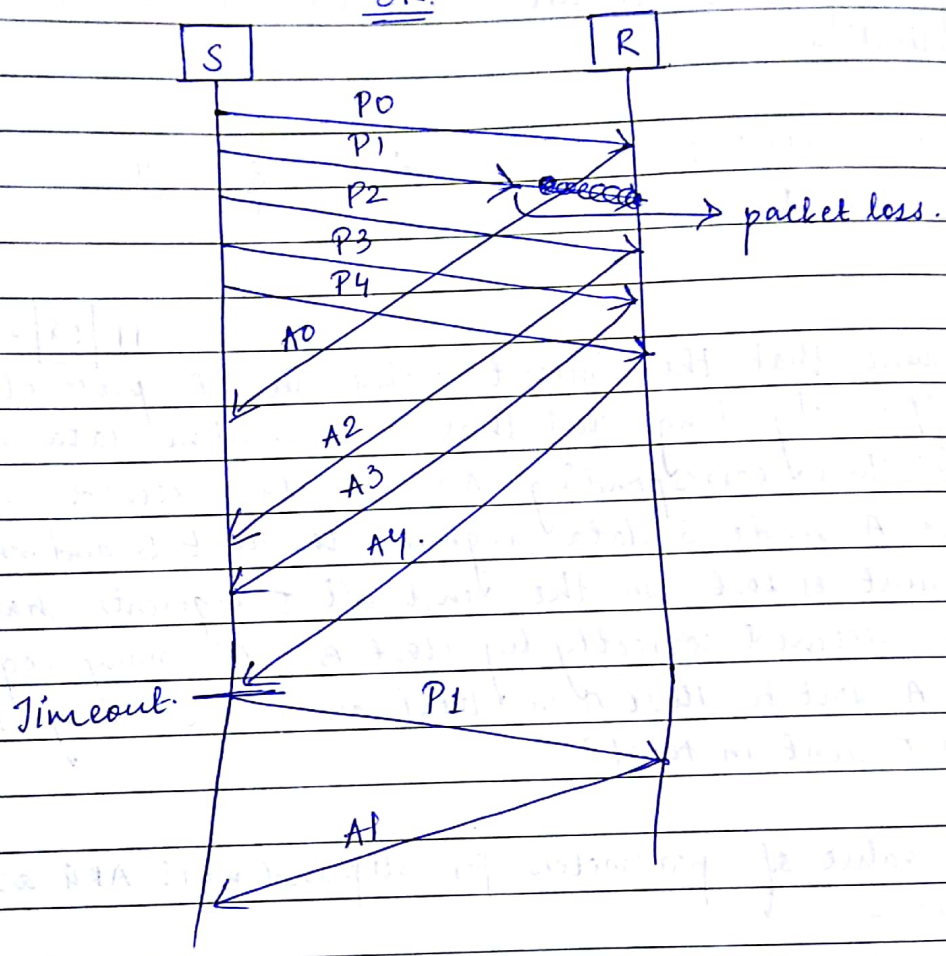
$$U_L = \frac{1}{1+2a} \qquad a = \frac{d_{prop.}}{d_{trans.}}$$

Scanned by CamScanner

Solutions.

SR.

1.



No. of packets sent : 5 P0 P1 P2 P3 P4 P1

" " ACKs " : 5 A0 A2 A3 A4 A1

2. $d_{prop} = 0.75\,ms$

$d_{trans} = \frac{2000 \times 8}{10^6}$ sec. (convert it into ms).

$d_{ACKs} = \frac{20 \times 8}{10^6}$

$d_{processing} = 0.15$ ms.

$$\eta = \frac{d_{trans.}}{\text{total delay}} \times 100 \Rightarrow \frac{d_{trans.}}{d_{prop.} + d_{trans.} + d_{proces} + d_{ACKs.}}$$

Scanned by CamScanner

$d_{processing} = 0.15$ ms.

$$\eta = \frac{d_{trans.}}{\text{total delay}} \times 100 \Rightarrow \frac{d_{trans.}}{d_{prop.} + d_{trans.} + d_{proces} + d_{acks.}}$$

17 | 08 | 2017.

UDP (User Datagram Protocol)

It is connection-less, unreliable and insecure.
The packet of UDP is called user datagram.

* P.T.O.

Header + Data

	0 – 15	16 – 31
Header	Source port no.	Destination port no.
	Total length	Checksum
Data	Data	

this field is not fixed, it is variable.

No. of bytes a UDP header consists of 8.

→ UDP have a fixed size header of 8 bytes made of four fields.

→ Source port no. and destination port no. are of 2 bytes each.

→ 'Total length' field defines the length of the datagram (header + data).

→ 'Checksum' field is used to check if the packet transmitted

Scanned by CamScanner

contains error or is errorfree.

Services Provided by UDP.

1. Process - to - Process Communication.
2. It provides connection-less service.
3. It does not provide flow control.
4. Provides no error control.
5. It does not provide congestion control.
6. Provides encapsulation and decapsulation.
7. Provides queuing facility.
8. Provides multiplexing at the sender and demultiplexing at the receiver.

CHECKSUM.

In UDP, checksum calculation includes a pseudo header, a & UDP header and the data coming from application layer.

*

Pseudo Header

Source IP Address		
Destination IP Address		
All 0s	8 bit protocol	UDP total length

HTTP port no. 20, 21
DNS " 50, 52, 53

eg
```
  1010110110110001
  1010101010101010
 ----------------
 1010110000101101 1
                  +1
 ----------------
  0101100001011100 → sum
(1's complement) 1010011110100011 → checksum.
```

Q. Why there is a need for pseudo header to calculate UDP checksome?

If the checksum does not include the pseudo header, a user datagram may arrive safe and sound. However, if the IP header is corrupted it may be delivered to the wrong host. Value of the protocol field for UDP is 17.

Features of UDP

1. Connection-less Service.
2. Lack of error control
3. Lack of congestion control.

Q. Scenario's where UDP is preferred over TCP.

1. It will be suitable for a process that requires simple request response communication with little concern; for flow and error control.
2. It is suitable for a process with internal flow and error control ~~examination~~ mechanism.

Scanned by CamScanner

3. It is a suitable transport protocol for multicasting.
4. UDP is used for management processes.
5. UDP is also used for route updating protocols; such as routing information protocol (RIP)
6. UDP is normally used for real time application; that cannot tolerate delay.

Scanned by CamScanner

3. It is a suitable transport protocol for multicasting.
4. UDP is used for management processes.
5. UDP is also used for route updating protocols; such as routing information protocol (RIP)
6. UDP is normally used for real time application; that cannot tolerate delay.

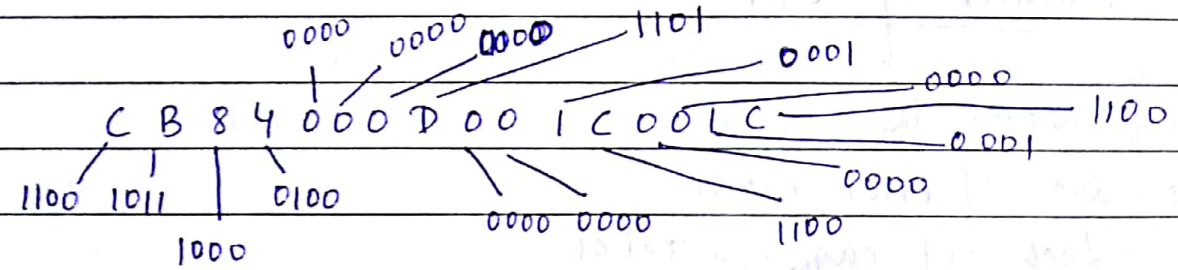
18/08/17

Q. The following is the content of a UDP header in hexadecimal format –

CB84000D001C001C

i) What is the source port no?
ii) " " " destination port no?
iii) " " " total length of datagram?
iv) " " " length of data?

Ans.



Source port no – first 16 bits.

1100101110000100.

$2^{15} + 2^{14} + 2^{11} + 2^{9} + 2^{8} + 2^{7} + 2^{2}$

32768 + 16384 + 2048 + 512 + 256 + 128 + 4

52,100

Destination port no —

0000 0000 0000 1101

= 13

Total length of datagram —

0000 0000 0001 1100

2^4 2^3 2^2

$\Rightarrow 16 + 8 + 4 = 28.$

Length of the data = 28 − 8 = 20 bytes.

Q. Consider a 128 kbps satellite communication link with 1-way propagation delay of 150 ms. Selective repeat protocol is used on this link to send data with a frame size of 1 kilobyte. The min. no. of bits required for the sequence no. field to achieve 100% utilization is?

Ans.

$$U = \frac{N(1-P)}{1+2a}$$ → neglect

$$U = \frac{N}{1+2a}$$

$$N = \frac{2^m}{2}$$

$$U = 100\% = \frac{100}{100} = 1$$

$$a = \frac{d_{prop}}{d_{trans}}$$

$$d_{prop} = 150 \text{ ms}$$

$$d_{trans} = \frac{L}{R} = \frac{1 \text{ kbyte}}{128 \text{ kbps}} = \frac{1 \times 10^3 \times 8}{128 \times 10^3}$$

$$= 0.0625 \text{ sec.}$$

$$= 62.5 \text{ ms.}$$

$$a = \frac{150 \text{ ms}}{62.5 \text{ ms}}$$

$$= 2.4.$$

Scanned by CamScanner

$$1 = \frac{2^m / 2}{1 + 2(2.4)}$$

$$1 = \frac{2^m / 2}{5.8}$$

$$\frac{2^m}{2} = 5.8$$

$$2^m = 11.6 \approx 12 \approx 16$$

no power of 2 is equal to 12.

$$\Rightarrow \boxed{m = 4}$$

Q. A sender uses stop-and-wait ARQ for reliable transmission of frames. Frames are of size 1000 bytes and the transmission rate at the sender is 80 kbps. Size of an acknowledgement is 100 bytes and the transmission rate at receiver is 8 kbps. The one-way propagation delay is 100 ms. Assume no frame is lost. The sender throughput is ___ bytes/sec.

$$U = \frac{1}{1+2a}$$

$$U = \frac{D_{trans.}}{\text{Total delay}} = \frac{D_{trans.}}{D_{trans} + 2D_{prop.} + D_{ack.}}$$

$$D_{trans.} = \frac{L}{R} = \frac{1000 \times 8}{80 \times 10^3} = 0.1 \text{ sec}$$

$$= 100 \text{ ms.}$$

Scanned by CamScanner

$D_{prop} = 100$ ms.

$D_{pack} = \frac{100 \times 8}{8 \times 10^3} = 0.1$ sec $= 100$ ms

$U = \frac{100}{100 + 200 + 100} = \frac{100}{400} = 0.25 = 25\%$

Throughput $= U_L \times$ transmission rate (R)

$= \frac{1}{4} \times 80 \times 10^3$ bps

$= 20 \times 10^3$ bps

$= \frac{20 \times 10^3}{8}$ = bytes per sec

$= 2.5 \times 10^3$ bytes/sec.

$= 2500$ bytes/sec.

8. Suppose that stop-and-wait protocol is used on a link with a bit rate of 64 kbps and 20 ms propagation delay. Assume that transmission time for the acknowledgement and the processing times at nodes are negligible. The min frame size in byte to achieve a link utilization of atleast 50% is ____.

$U \geq 50\%$

Say $U = 50\% = \frac{1}{2}$

Scanned by CamScanner

$$U = \frac{L/R}{L/R + 2d_{prop.}}$$

$L = ?$ $\quad R = 64$ Kbps , $d_{prop.} = 20$ ms

$$\frac{1}{2} = \frac{L/64 \times 10^3}{(L/64 \times 10^3) + 2(20) \times 10^{-3}}$$

$$\frac{1}{2} = \frac{L/64 \times 10^3}{L/64 \times 10^3 + 0.04}$$

$$\frac{L}{64 \times 10^3} + 0.04 = \frac{2L}{64 \times 10^3}$$

$$0.04 = \frac{L}{64 \times 10^3}$$

$$L = 0.04 \times 64 \times 10^3$$

$$= 2560 \text{ bit}$$

$$= \frac{2560}{8} \text{ bytes}$$

$$\boxed{L = 320 \text{ bytes}}$$

Scanned by CamScanner

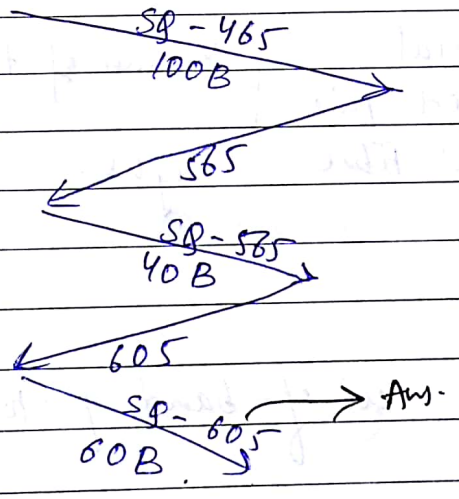
21 | 08 | 17

Q1. 2 Host A and B are communicating using TCP, assume that the sequence no. field starts with 0 and the receiver employeer cumulative ack. A has successfully sent 465 bytes of data which are also ack. by B. Suppose A now sends 3 segments of size 100 bytes, 40 bytes and 60 bytes.

(i) What will be the sequence no. of 3rd segment.

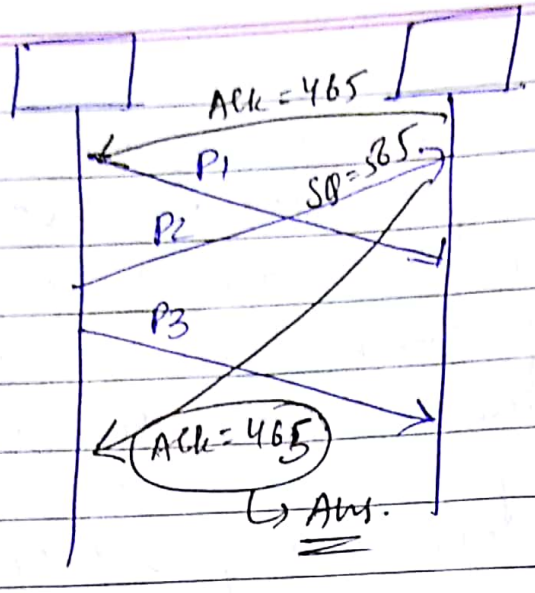
465 bytes transferred — 0 - 464.

Now for 100, 40 & 60.



(ii) Suppose second segment was received before the first and the third segment. What will be the ack. value in the ack. generated as a consequence of receiving the second segment.

Scanned by CamScanner



PHYSICAL MEDIA

2 types –

1) Guided : a) Co-axial
b) Twisted pair.
} Medium of transfer = electricity
c) Optical fibre – light.

2) Unguided

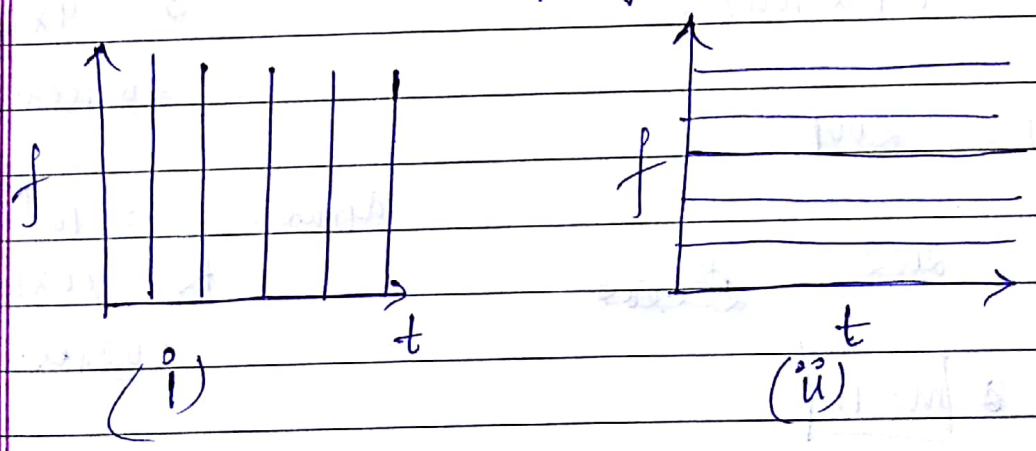
Q. Why FTP is called out-of-band protocol.

HTTP	FTP
Only one TCP connection sending data and control info. both in one. This is why in-band protocol.	2 diff. connection are setup. in 1st data info. sent in 2nd control 2 TCP connection i.e. why out-of-band protocol.

Scanned by CamScanner

Packet Switch	Circuit Switch
1. We don't have to reserve the link.	The link is dedicated and reserved.
2. Transmission capacity can be shared.	Can not be shared.
3. Unpredictable end-to-end delay.	Predictable.
4. Not suitable for real time applications	suitable. eg. telephone & video.
5. Less cost	More cost
6. Efficient	Less.
7. Simple	Complex.

Circuit Switch – i) Time Division Multiplexing (TDM)
ii) Frequency Division Multiplexing (FDM)



Q. Consider a n/w connected to system located at 80,000 km apart. The bandwidth of the n/w is 500×10^6 bits/sec. The prop. speed of the media is 4×10^6 m/s. It is needed to design a go-back-n sliding window protocol

Scanned by CamScanner

for this n/w. The avg. packet size is 10^7 bits. The n/w is to be used to its full capacity. Assume that the processing delays are negligible. The min. size of bits required for sequence no. is ____.

$N = 2^m - 1.$

$U_L = 100\% = \frac{100}{100} = 1$

$U_L = \frac{N(1-P)}{(1+2a)(1-P+NP)}$ $\quad P = 0.$

$U_L = \frac{N}{(1+2a)}.$

$a = \frac{d_{prop.}}{d_{trans.}}$

$1 = \frac{2^m - 1}{1 + 2(1000)}.$

$d_{prop.} = \frac{D}{S} = \frac{80,000 \times 10^3}{4 \times 10^6} =$

$= 20$ secs.

$2^m - 1 = 2001$

$d_{trans} = \frac{L}{R} = \frac{10^7}{500 \times 10^6} = \frac{1}{50}$

$2^m = 2002.$

$= 0.02$ sec.

$\boxed{m = 11}$

$a = \frac{d_{prop.}}{d_{trans}} = \frac{20}{1/50} =$

$= \frac{20}{0.02} = 1000$ sec.

Scanned by CamScanner

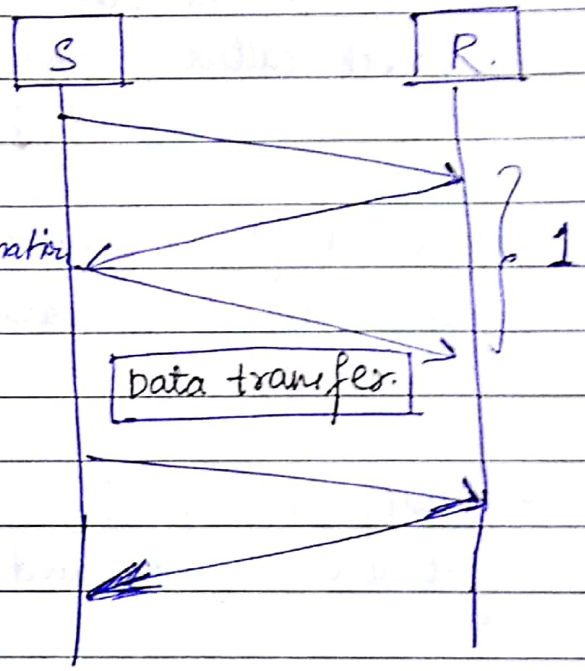
22/02/17

TRANSMISSION CONTROL PROTOCOL (TCP)

TCP is a connection-oriented, reliable and secured protocol.

Phases –

1. Connection Establishment
2. Data Transfer
3. Connection Tear Down / Drop / Termination



TCP uses a combination of Go-Back-N and Selective Repeat Protocol for reliable data transfer. *

2 types of acknowledgement –

(i) Cummulative ack. (Go-Back-N)
(ii) Selective ack. (Selective Repeat).

* It uses cumulative acknowledgement and selective acknowledgement both.

Services Provided by TCP.

1. Process-to-Process Communication : It is achieved using port no
2. Stream Delivery Service : TCP is a stream-oriented protocol

Scanned by CamScanner

It allows the sending process to deliver data as a stream of bytes. It allows the receiving process to obtain data as a stream of bytes. It requires buffers for storage. Buffers are sending buffers and receiving buffers. The stream of bytes group together into a packet called segment.

$\boxed{\text{Data + Header}} \rightarrow$ Segment.

3. Full Duplex Communication : The communication in TCP is bidirectional i.e. data can flow in both direction at the same time.

4. Multiplexing & Demultiplexing : TCP performs multiplexing at the sender and demultiplexing at the receiver.

5. Connection Oriented Service : TCP is a connection-oriented protocol which occur in 3 phases –
   i) Connection Establishment / Setup.
   ii) Data Transfer.
   iii) Connection Termination.

TCP Features.

1. Numbering System – There is no field for a segment no. value in a segment header, instead 2 fields called sequence no. and ack no. is used.
TCP numbers all the data bytes. The no. does not necessarily start from 0, it maybe any no. b/w 0 to $(2^{32}-1)$

TCP header has 32 bits for ack. no and 32 bits for sequence no.

→ 2) Sequence Number: of the first segment is called as initial sequence number. ~~(INS)~~ (ISN).
The sequence no. of any other segment is the sequence no. of the previous segment + the no. of bytes carried by the previous segment.

Q. Suppose a TCP connection is transferring a file of 5000 bytes. The first byte is numbered as 10,001. What are the sequence no. of each segment if data are sent in 5 segments each carrying 1000 bytes.

Sequence No.	Data.
10,001	1000
11,001	1000
12,001	1000
13,001	1000
14,001	1000.

The value in the sequence no. field of a segment defines the no. assigned to the first data byte contained in that segment.

3. Acknowledgement Number – It defines the no. of next byte expected to receive. The ack. in this case is called cumulative.

Scanned by CamScanner

TCP SEGMENT

[Header + Data] = Segment.

Scanned by CamScanner

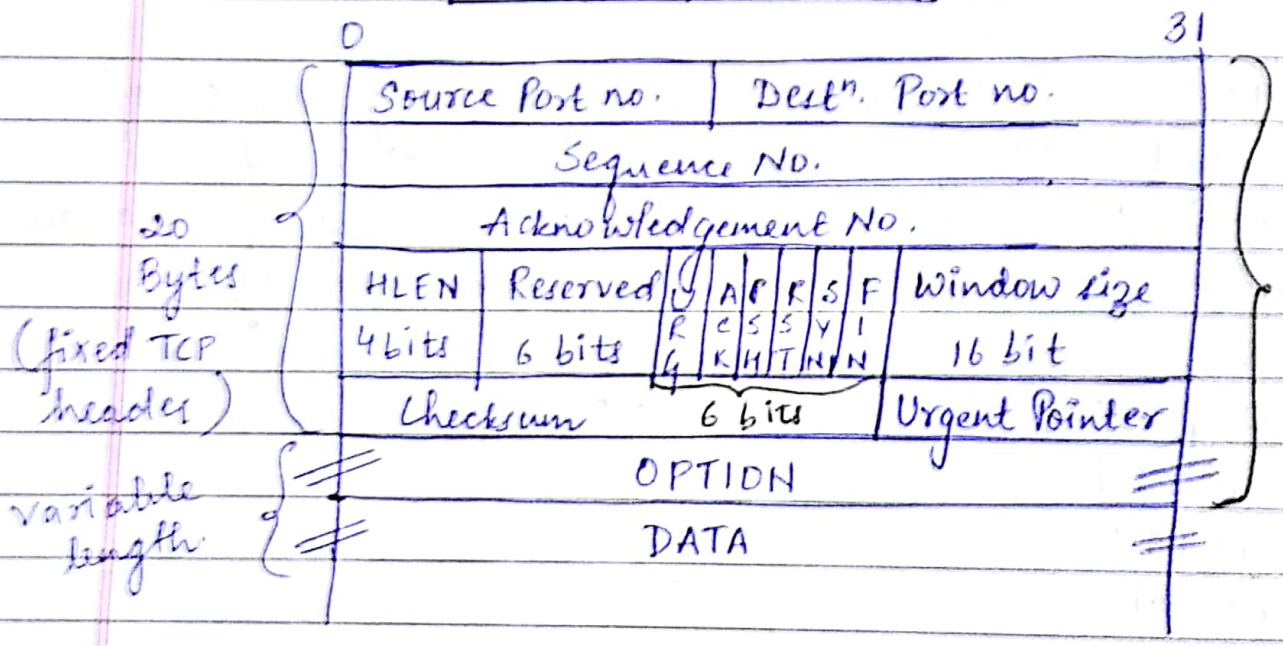
TCP SEGMENT

| Header + Data | = Segment

07/09/2017

Segment

Header	Data



Source Port No - It is a 16 bit field, that defines the port no of the application program of the sending host.

Destination Port No - Defines the port no. of the receiving host.

Sequence No - It is a 32 bit field which defines the no. assigned to the first byte of the data in the segment.

Ack no - It is a 32 bit field that defines the byte no. the receiver is expecting.

If receiver received x byte of data, the acknowledgement send will be x+1.

Scanned by CamScanner

HLEN is the header length. It is a 4 bit field that indicates the no. of 4 byte words in the TCP header.

Q. If HLEN value is 1001. What is the header length?

1001 = 9

9 x 4 = 36 bytes.

Control fields – This field defines 6 different control bits or flags. One or more bit can be set at a time.

URG – Urgent Pointer is valid or not.

ACK – Acknowledgement is valid or not.

PSH – Request for push.

RST – Reset the connection

SYN – Synchronize the ~~ton~~ sequence no.

FIN – Finish or terminate the connection.

If 1 → active

0 → not active

Window size – Defines the window size of the sending TCP in bytes.

Checksum – Exactly same as UDP.

Urgent Pointer – A 16 bit field which is valid only if the urgent flag is set. It is used when the segment contains urgent data.

Scanned by CamScanner

OPTION – can be upto 40 bytes of optional information in the TCP header.

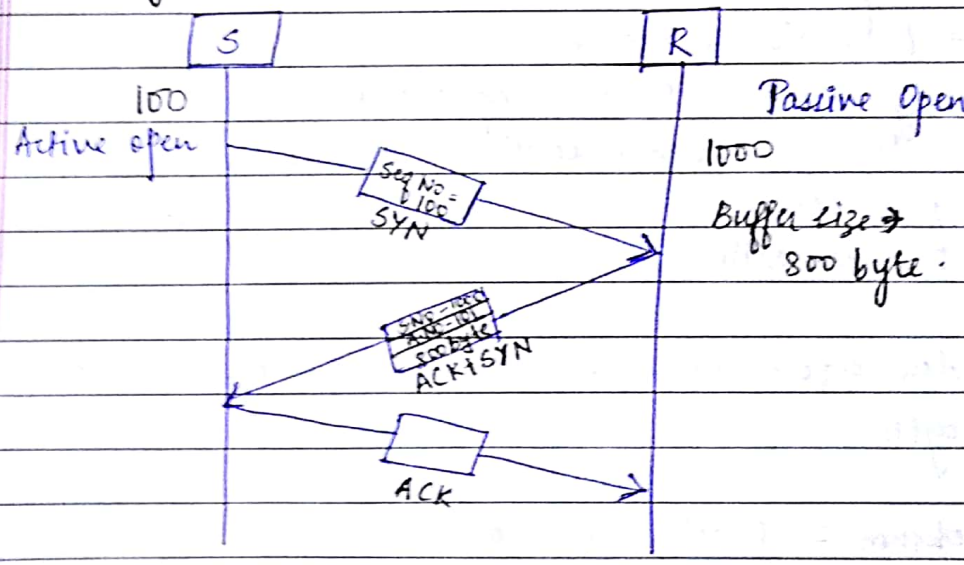
TCP CONNECTION

1. Connection Establishment.
2. Data Transfer
3. Connection Termination / Drop / Teardown.

1. Connection Establishment.

TCP transmits the data in a full duplex mode.

3 way Handshaking.



The connection establishment in TCP is called as 3 way Handshaking. The process starts with the server, the server program tells its TCP that it is ready to accept a connection with a request called passive open. The client program issues a request called active

open which tells its TCP to connect to a particular server.

i) <u>SYN segment</u> : The client sends first segment called SYN segment in which SYN flag is set. It is used for synchronization of sequence no. The sequence no. is called initial sequence no. A SYN segment cannot carry data but it consumes one sequence no.

ii) <u>SYN + ACK segment</u> : Server sends the second segment a SYN + ACK segment in which two flags are set SYN and ACK. Also defines the receiver's side window. It cannot carry any data but it consumes one sequence no.

iii) <u>ACK segment</u> : The client sends the third segment called ACK segment. It acknowledges the received of the second segment with acknowledgement flag set. It does not consume any sequence no, if it does not carry any data. But some implementations allow ACK segment to carry data.

08/09/2017.

Q. What is SYN flooding? What is the soln. to it?

→ When one or more malicious attackers send a large no. of SYN segment to a server pretending that each of them is coming from a different client is called as SYN flooding attack.

→ Server then send SYN + ACK segment to the fake clients. When server waits for the third segment the resources are allocated without being used.

Scanned by CamScanner

→ If during that time, the server run out of the process, it will be unable to accept request from valid clients.

→ SYN flooding attack belongs to a group of security attack called as <u>denial of service attack</u>.

Soln. to SYN flooding attack –

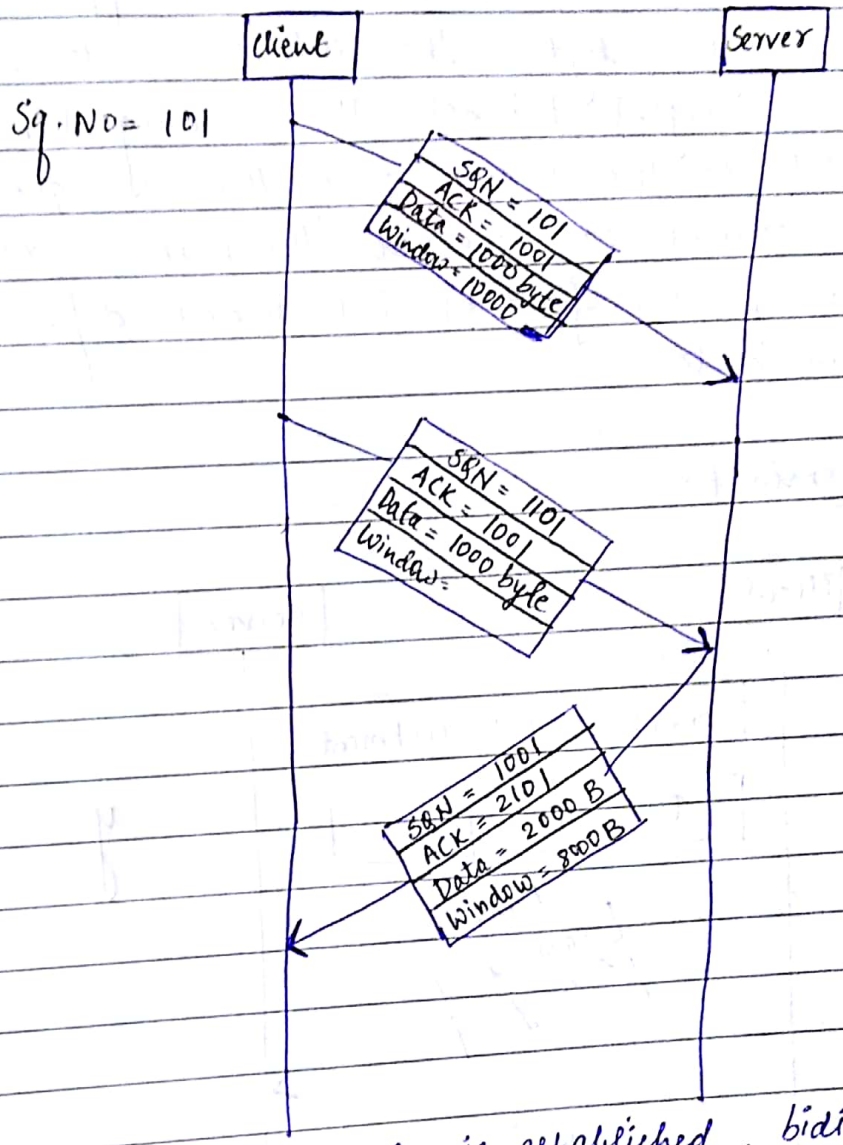
1) Impose a limit of connection request during a specified period of time.

2) Filter out a datagram coming from unwanted address.

3) Postpone the resource allocation until the server can verify that a connection request is coming from a valid IP address.

Scanned by CamScanner

2. Data Transfer.



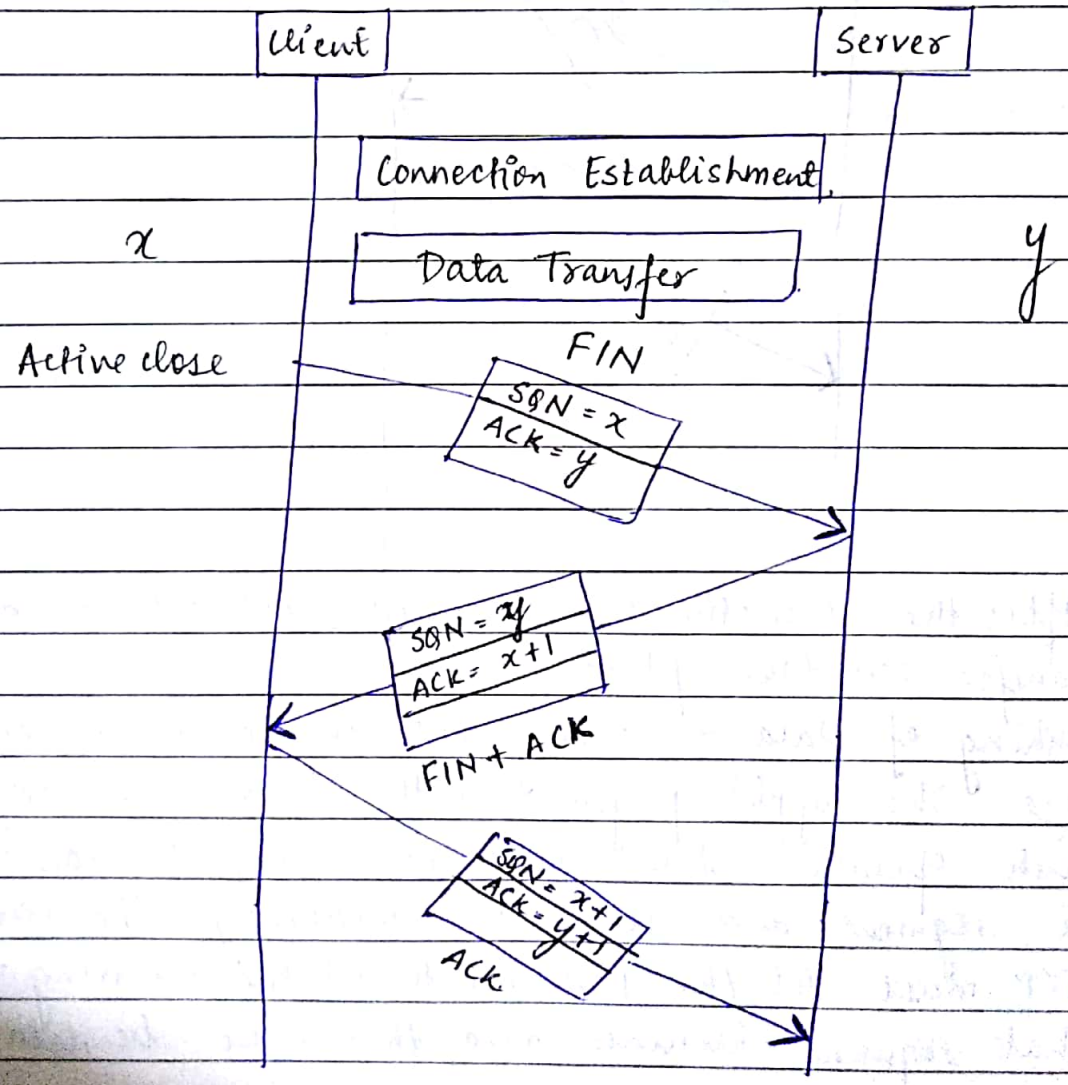
After the connection is established, bidirectional data transfer can take place.

i) Pushing of Data – Sending TCP can select the segment size. The appl^n. program at the sender can request a push operation. This means the sending TCP can create a segment and send it immediately. The sending TCP must set the push bit to let the receiving TCP know that segment includes data that must be delivered

to application layer as soon as possible.

ii) Urgent Data – There are occassions in which appln. programs need to send urgent bytes. The solution is to send a segment with a urgent bit set. The sending TCP inserts the urgent data at the beginning of the segment. Rest of the segment can contain the normal data. The urgent pointer field of TCP header defines end of the urgent data.

3. Connection Termination



Scanned by CamScanner

Connection Termination process of TCP is of 2 types—

i) 3 way Handshaking
ii) 4 way Handshaking with a half closed option.

i) 3 way Handshaking.

a) FIN segment – It is sent to the server by client when client wants to close the connection. FIN flag is set. FIN segment can have some amount of data.

b) FIN + ACK segment – Server confirms the received ~~from~~ of FIN segment from client and announce the closing of the connection. It can carry the last bytes of data from server.

c) ACK segment – Confirms the received ~~from~~ of FIN segment from TCP server. It does not carry any data.

Q. In a TCP connection which of the following segments are used to exchange only control info.

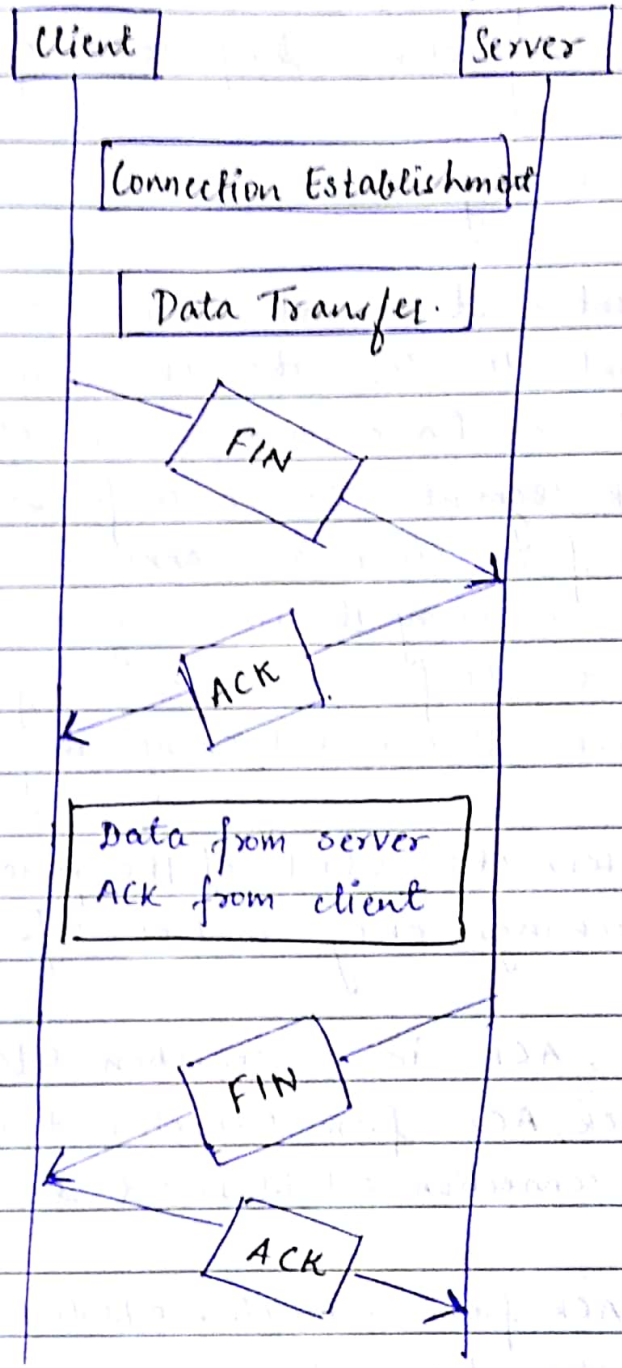
a) SYN + ACK, ACK in a connection establishment phase.
b) SYN, FIN, FIN+ACK, ACK from connection termination phase
c) SYN from connection establishment & ACK from connection termination.
d) SYN+ACK, ACK from connection establishment & FIN, FIN+ACK from connection termination.
e) None.

SYN, SYN+ACK only control info., ACK ~~only~~ both control and data. — Connection Establishment.
FIN, FIN+ACK only control info., ACK both — Data Transfer.
FIN, FIN+ACK, ACK — only control info — Conn. Termination.

Scanned by CamScanner

11/09/17.

ii) 4 way Handshaking with a half closed operation.



In TCP, one end can stop sending data while still receiving the data; this is called as half-closed. Either the server or the client can issue a half-closed operation. The client half-closes the connection

by sending a FIN segment. The server accepts the half-closed by sending the ACK segment. The server can still send data. When server sends all the data it sends a FIN segment. Client sends an ACK and the connection is closed.

Imp. **TCP STATE TRANSITION**

i) CLOSED → No connection exist
ii) LISTEN → Passive open received, waiting for SYN.
iii) SYN-SENT → SYN segment is sent, waiting for acknowledgement.
iv) SYN-RCVD → SYN+ACK segment is sent, waiting for ACK.
v) ESTABLISHED → Connection is established, data transfer in progress.
vi) FIN-WAIT 1 → First FIN segment is sent, waiting for ACK.
vii) FIN-WAIT 2 → ACK. to first FIN received, waiting for second FIN.
viii) CLOSE-WAIT → First FIN received, ACK. sent, waiting for application to close.
ix) TIME-WAIT → Second FIN received, ACK. sent, waiting for 2MSL timeout.
↓
maximum segment life.
x) LAST ACK → Second FIN sent, waiting for ACK.
xi) CLOSE → Both side closed.

Scanned by CamScanner

Q. Diff b/w FIN-WAIT 1 and FIN-WAIT 2?

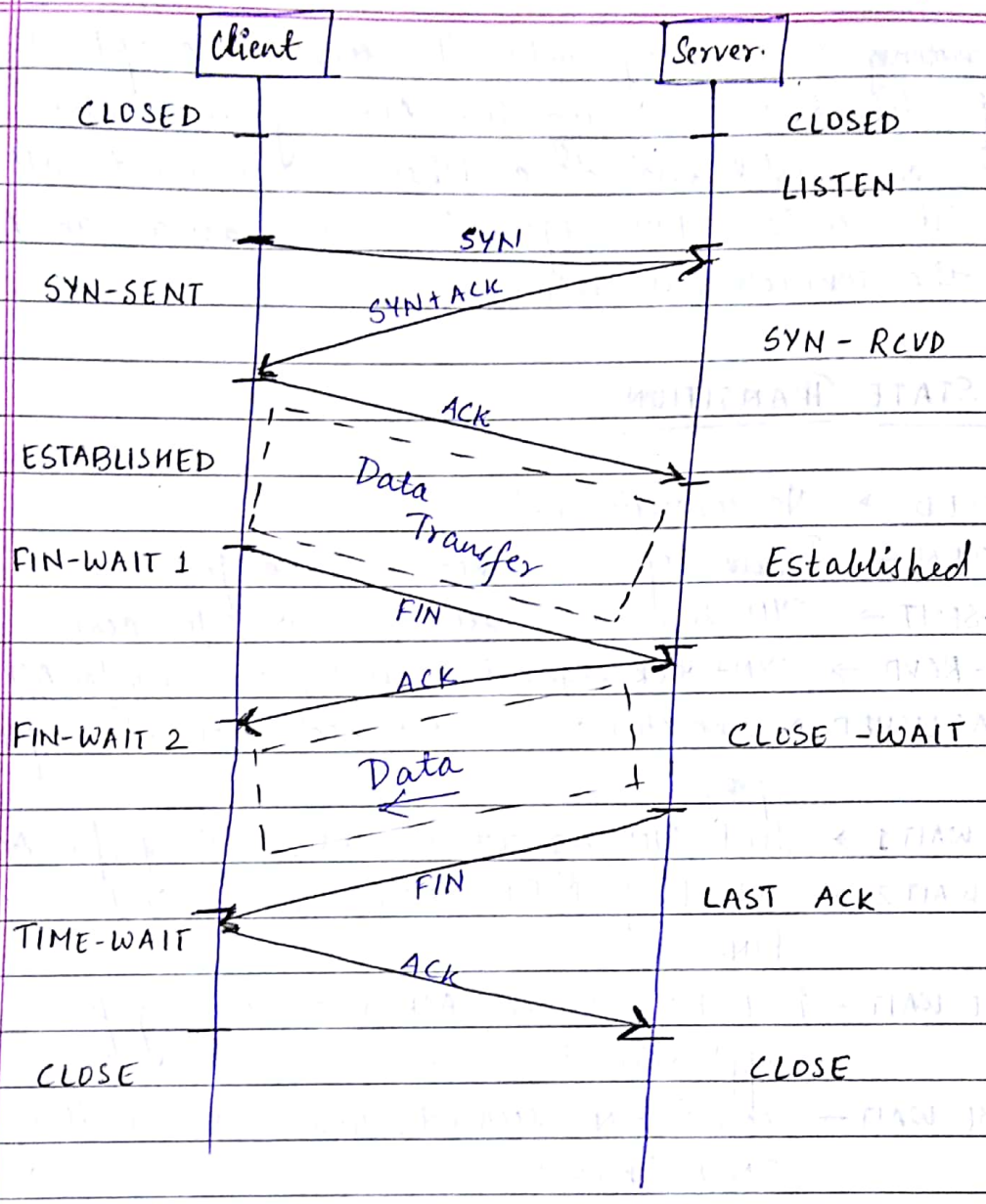


Figure: TIMING DIAGRAM OF TCP CONNECTION.

(Explanation read from book)

Q During half-closed oprn., why client waits for 2MSL time in time-wait state?

Scanned by CamScanner

Client ——— Server - - - - - -

12/09/2017.

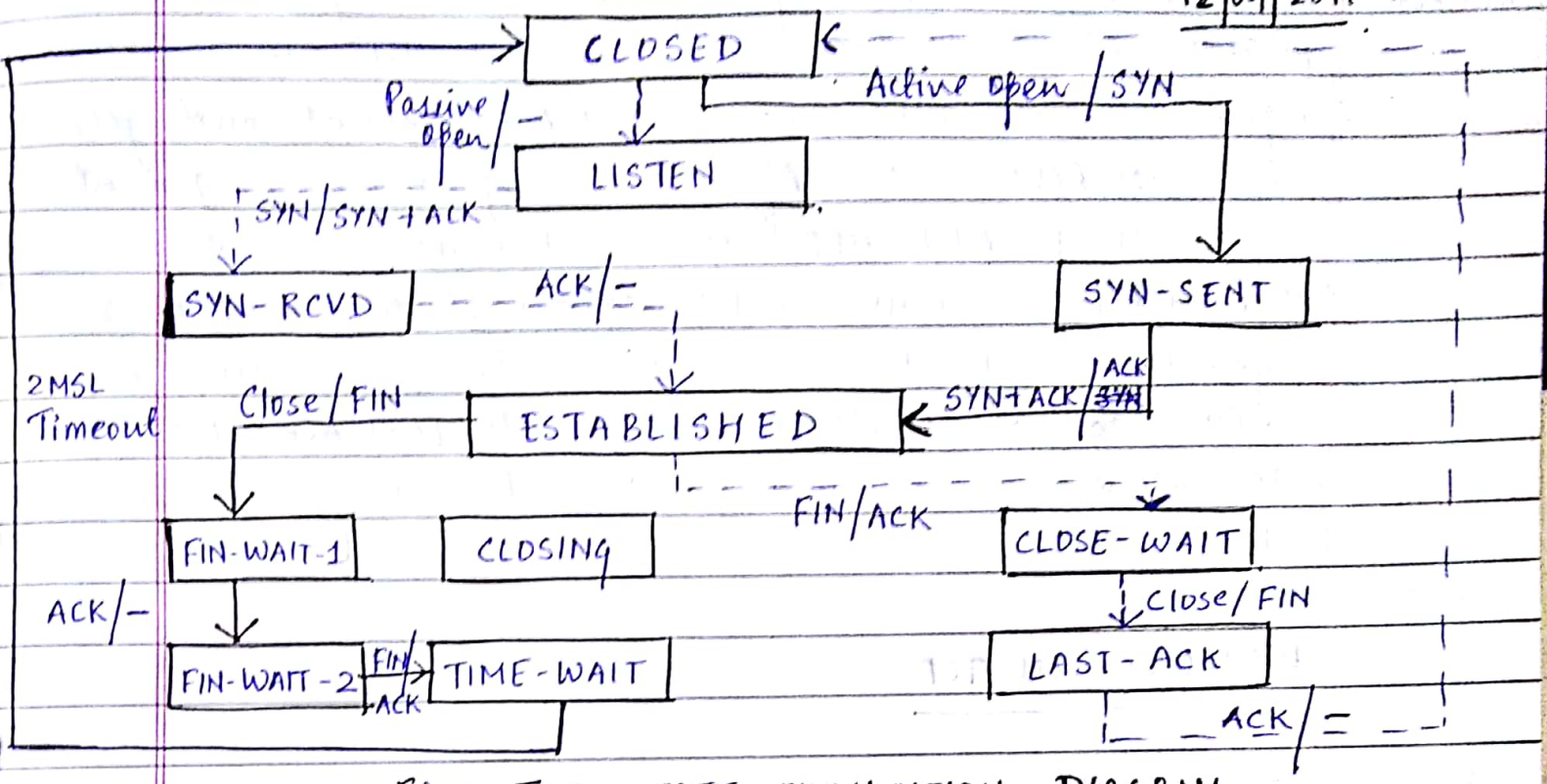


Fig: TCP STATE TRANSITION DIAGRAM.

(Explanation from book).

Explanation for both—

CLIENT— The client process issues an active open command and requests for a connection. Client TCP sends a SYN segment and moves to SYN-SENT state. After receiving the SYN+ACK segment, client TCP sends an ACK segment and goes to ESTABLISHED state. Data transfer occurs and acknowledgements are sent. When client process have no data to sent it issues an active close command. Client TCP sends a FIN segment and goes to FIN-WAIT-1 state. When the client receives the ACK segment it goes to FIN-WAIT-2 state. When client receives the FIN segment it sends an acknowledgement and goes to TIME-WAIT state. After 2MSL time the client goes to CLOSED state.

Scanned by CamScanner

SERVER- Server issues a passive open, the server TCP goes to LISTEN state and stays there until it receives a SYN segment. Server TCP sends SYN + ACK segment and goes to SYN-RCVD state. After receiving acknowledgement it goes to ESTABLISHED state. TCP remains in this state until it receives a FIN segment. It sends an ACK segment and goes to CLOSE-WAIT state. Server sends a FIN segment to client and goes to LAST-ACK state. When acknowledgement received from client it ~~to~~ goes to CLOSED state.

WINDOWS IN TCP

In TCP there are basically 2 types of windows –

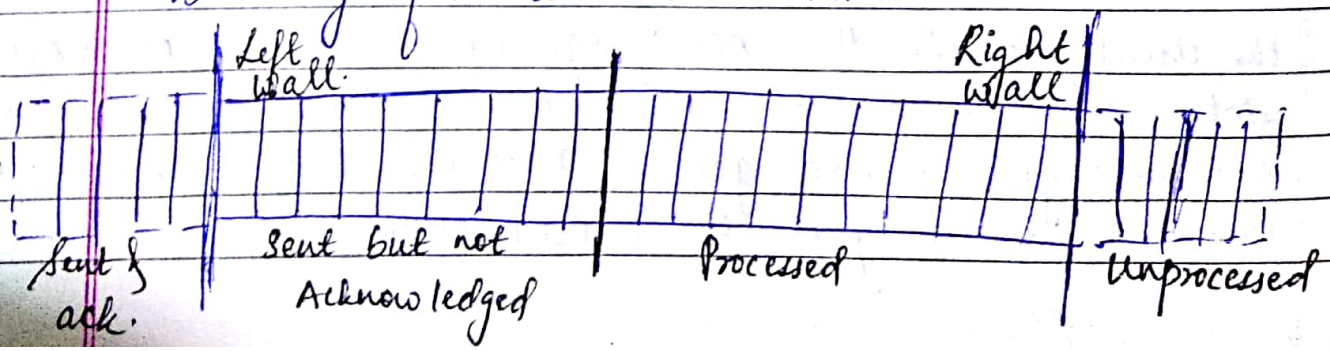
1) Sending Window
2) Receiving Window

1) SENDING WINDOW –

i) OPEN : The send window opens when the right wall moves to right. This is called opening of the window.

ii) When the left wall moves to right it is called closing of the window – CLOSE

iii) If both these operations do not occur it is called shrinking of the window – SHRINK



Scanned by CamScanner

Window size is the no. of bytes. The transmission in TCP occurs segment by segment. TCP can store data, received from the process and send them ~~latter~~ later. TCP uses only one times.

Q. What is the difference b/w sending window of selective repeat protocol and sending window of TCP?

2) RECEIVING WINDOW —

TCP allows the receiving process to pull the data at its own pace. The receiving window size is always smaller or equal to the buffer size.

Receiving window size determines the no. of bytes the receiving window can accept from sender before being overwhelmed.

rwnd = buffer size − the no. of waiting bytes to be pulled.

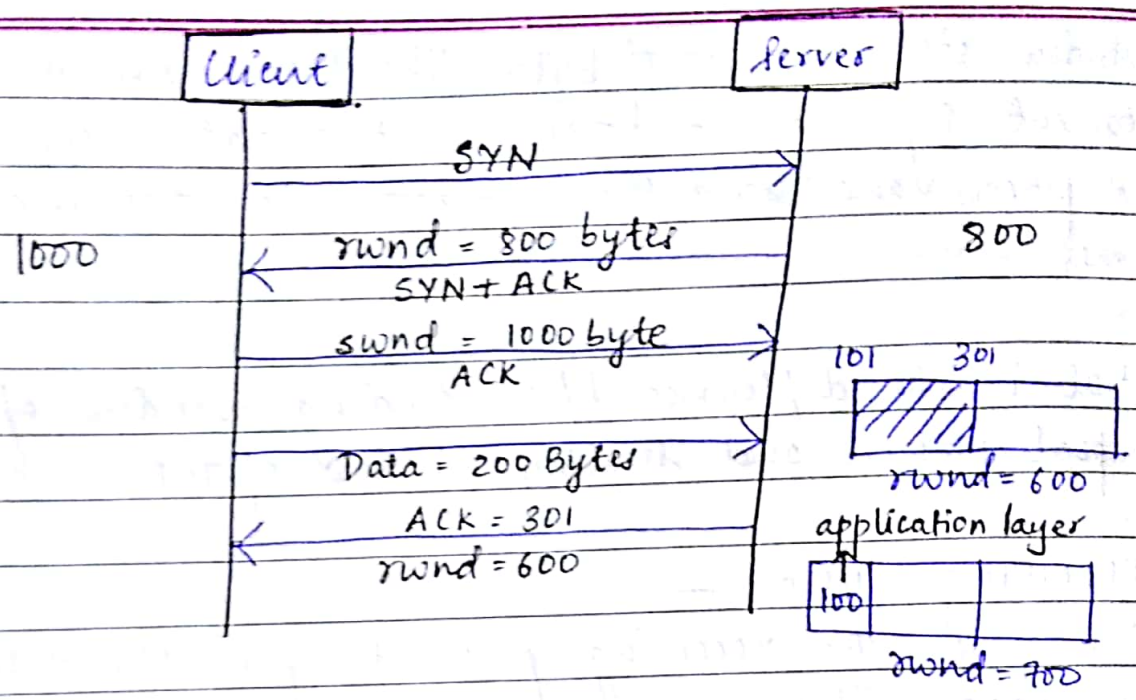
receiving window

The acknowledgement mechanism in TCP is cummulative, but some new implementation of TCP have both cummulative and selective acknowledgement.

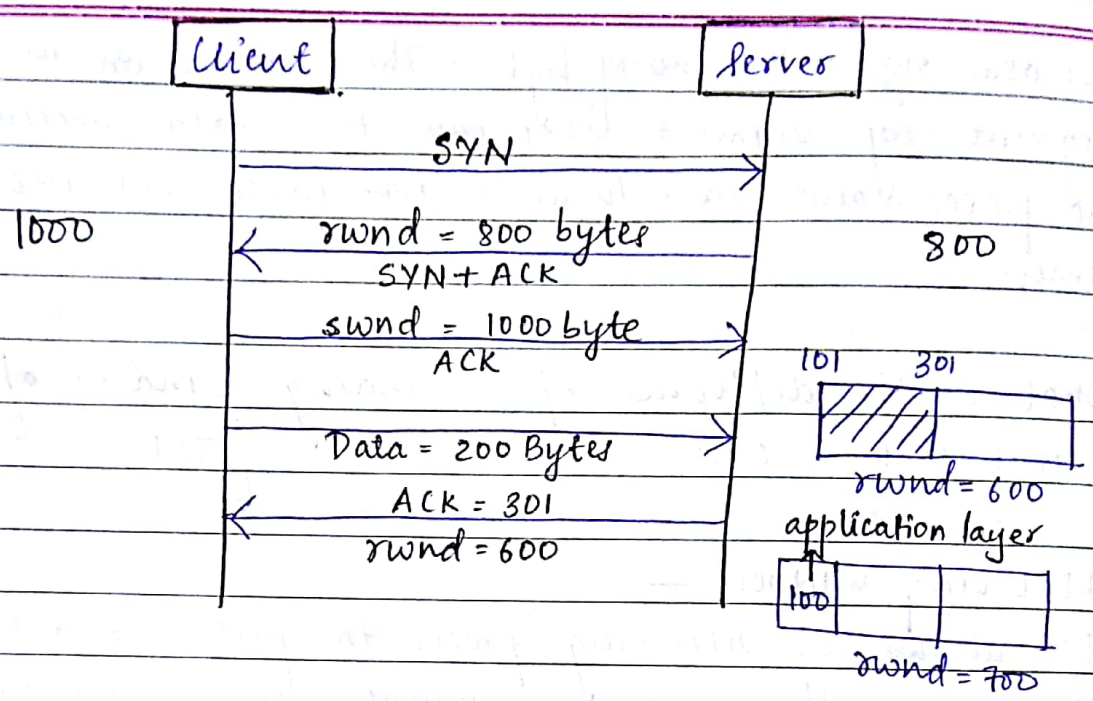
FLOW CONTROL

Flow control balances the rate at which a producer creates a data with the rate at which a consumer uses the data.

Scanned by CamScanner



Scanned by CamScanner



14/09/2017

SHRINKING OF THE WINDOW

The receiver window never shrinks, the sender window can shrink if receiver defines a value of receiving window that resolved in shrinking of the window. The receiver needs to keep the following relationship b/w the last and new acknowledgement, the last and new receiving window to prevent shrinking of the sending window.

(New ack. no. + New receiving window) ≥ (last ack. no. + last receiving window)

WINDOW SHUTDOWN

The receiver can temporarily shutdown the window by sending rwnd = 0. The sender stops sending the data until a new receiving window size arrives but

the sender can send 1 byte of data.

SILLY WINDOW SYNDROME.

Problem arises due to slow transmission of data b/w sender and receiver called as silly window syndrome.

- Syndrome created by sender –

NAGLE'S ALGORITHM.

Step 1: Sending TCP sends the first piece of data even if it is 1 byte

Step 2: After sending the first segment, sending TCP accumulates all the data until it becomes maximum segment size. After that it can send the data.

Step 3: Step 2 is repeated for the rest of the transmission.

- Syndrome created by receiver –

The receiving side TCP may have a silly window syndrome if the application layer at the receiver side consumes the data slowly. Two solns. are given for this –

i) Clark's Solution – Send an ack. as soon as the data arrives, but to announce a window size of 0 until either there is enough space or half of the buffer is empty.

ii) Delay the process of sending the ack.

ERROR CONTROL.

TCP is a reliable transport layer protocol because it provides flow control and error control. Error control is a mechanism for detecting and resending corrupted segments,

Scanned by CamScanner

resending lost segments, storing out-of-order segments, detecting and discarding duplicate segments. Error control in TCP is achieved using 3 tools —

i) Checksum
ii) Acknowledgement
iii) Timeout

i) Checksum — Segment includes a checksum field which is used for corrupted segments checking. TCP header has a 16 bit field for checksum.

ii) Acknowledgement — TCP uses ack. to confirm the receive of data. Acks. are of 2 types - cummulative and selective. Cummulative ack. are the next byte receiver expects to receive also called as positive ack.
There is a 32 bit field for cummulative ack. in TCP header and 1 bit flag field.
Selective ack. reports a block of bytes i.e. out-of-order or duplicate. Since, there is no provision in TCP header for selective ack. it is implemented as an option.

iii) Timeout — When the timer expires or sender receives 3 duplicate ack. the segment is retransmitted.

Scanned by CamScanner

Retransmission after timeout.

Sending TCP maintains one retransmission timeout otherwise called as RTO for each connection. When timeouts the TCP resends the segment. When the timeout period is very large, a second scendrio can be implemented.

Retransmission after 3 duplicate ack.

After 3 duplicate ack. arrives at the sender, it can retransmit the missing segment. It is called as fast retransmission. The out-of-order packets in TCP is stored and marked as out-of-order.

(Pg. 210) — Some scenarios (5-6).

Scanned by CamScanner

Retransmission after timeout.

Sending TCP maintains one retransmission timeout otherwise called as RTO for each connection. When timeouts the TCP resends the segment. When the timeout period is very large, a second scendrio can be implemented.

Retransmission after 3 duplicate ack.

After 3 duplicate ack. arrives at the sender, it can retransmit the missing segment. It is called as fast retransmission. The out-of-order packets in TCP is stored and marked as out-of-order.
(Pg - 210) — Some scenarios (5-6).

15/09/2017.

TCP CONGESTION CONTROL

Congestion Window - Receiver side window is never overflowed because sender and receiver knows each other window size. But congestion in network may occur if the in between routers do not have sufficient buffer to store the packet, ultimately the packets will be dropped and will be retransmitted which will increase the network congestion.
IP Protocol does not provide any error control and congestion control, hence TCP have to provide congestion control.
To provide congestion control, TCP uses a variable called as congestion window. Congestion window is denoted as

Scanned by CamScanner

cwnd. It is controlled by congestion in the network. So the sender window is dependent on 2 variables i.e. rwnd and cwnd. Hence, actual size of sender window is the minimum of rwnd and cwnd.

Q. What are the signs that network is congested?

CONGESTION DETECTION

The sign of congestion in the network is –

i) Time-out. – Stronger sign of congestion.

ii) Three duplicate acknowledgement – Lighter sign of congestion.

i) Time-out : When sender does not receive an acknowledgement for a segment before the timeout occurs, it assumes that the segment is lost and it is due to congestion. After time-out, it has to retransmit the packet.

ii) Three duplicate acknowledgement : When sender receives 3 duplicate ack. it assumes that the packet is not received at the receiver, it occurs due to congestion in the network.

CONGESTION POLICIES

There are basically 3 types of policies used.

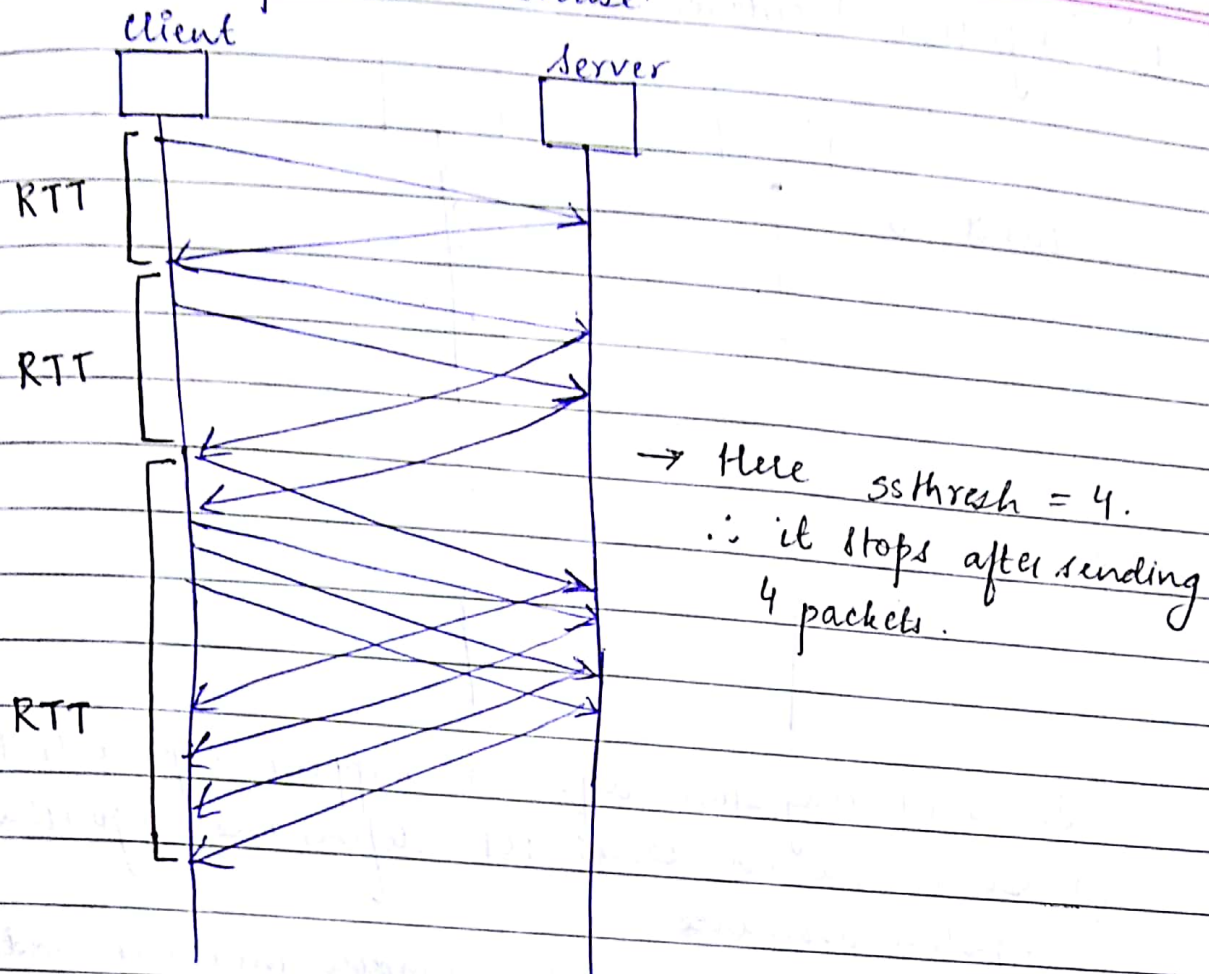
i) Slow Start

ii) Congestion Avoidance

iii) Fast Recovery.

Scanned by CamScanner

i) Slow Start - Exponential Increase.



Slow Start Algorithm is started with one segment and inc. exponentially. It started slow, but grows exponentially. After the acknowledgement for the first segment arrive, 2 segments will be sent, when ack. for 2 arrives, then 4 segments will be sent and so on, until it reaches slow start threshold. (ssthresh)

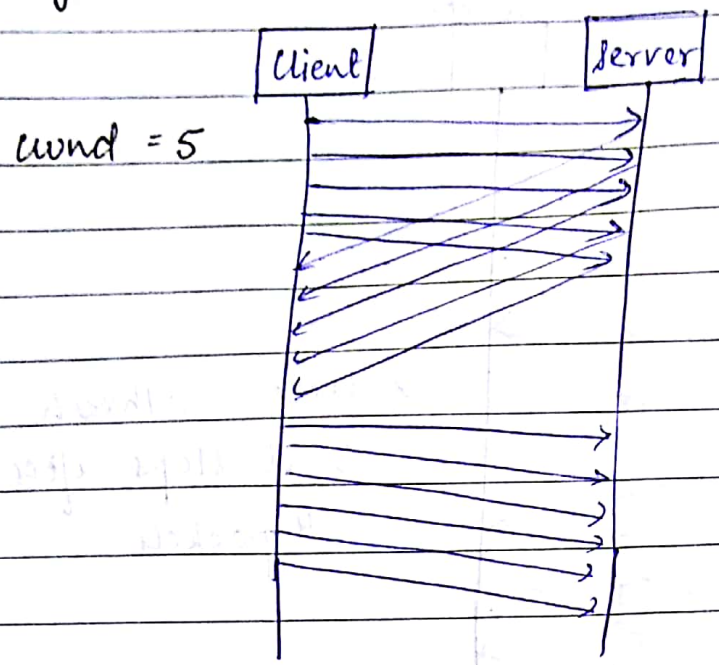
Start	1	2^0
1 RTT	2	2^1
2 RTT	4	2^2
3 RTT	8	2^3

Q. After 5 RTT what will be the size of congestion window?

Ans⇒ $2^5 = \underline{\underline{32}}$.

Scanned by CamScanner

ii) Congestion Avoidance or Additive Increase.



To avoid congestion, before it happens exponential growth must be slowed down. TCP defines one algorithm called congestion avoidance.

In this algorithm congestion window increases additively

	cwnd.
Start	4
1 RTT	4 + 1
2 RTT	5 + 1
3 RTT	6 + 1

iii) Fast Recovery.

Fast Recovery Algo. is optional in TCP. The window size is increased additively. The size of the congestion window is increased when duplicate ack. arrives.

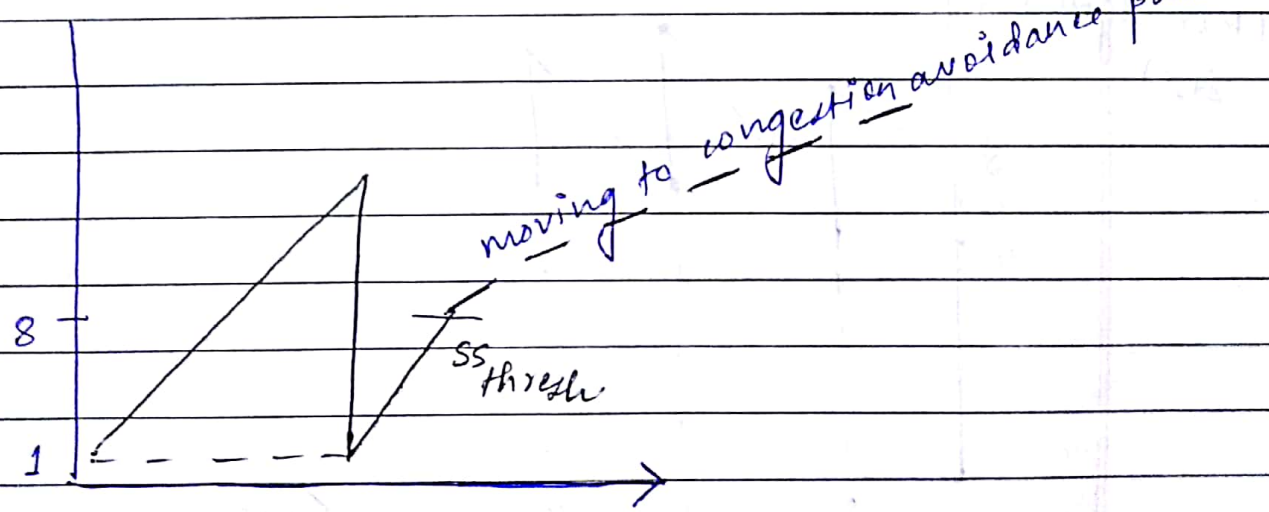
Scanned by CamScanner

16 | 10 | 17.

POLICY TRANSITION

1. Taho TCP
2. Reno TCP
3. New Reno TCP.

1. Taho TCP – The early TCP is known as Taho TCP. It uses only 2 policies : Slow start and Congestion Avoidance. Taho TCP treats the 2 signs of congestion, time-out and three duplicate ACKs. as same way.
When the connection is established, TCP starts with slow start algorithm and set the threshold value.
If congestion is detected, TCP immediately restart the slow start algorithm by setting the threshold value to half of the congestion window and resetting the congestion window to one.



SSthresh = 16

SS thresh = $\frac{16}{2}$ = 8

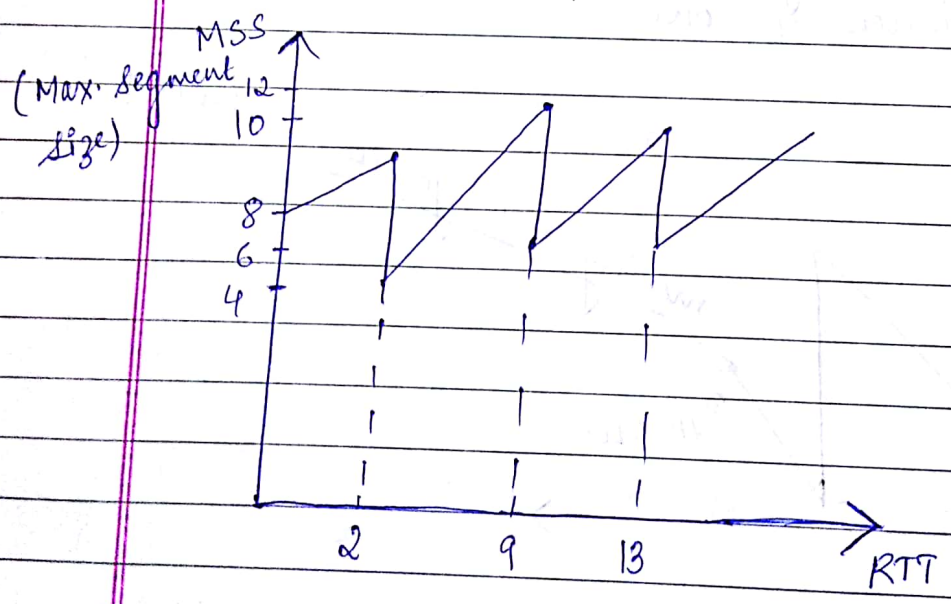
Scanned by CamScanner

In congestion avoidance state the size of congestion window is increased by one upto the end of the communication or the next congestion detection.

2. Reno TCP – The newer version of TCP is called Reno TCP. In this other than slow start algorithm and congestion avoidance algo., there is a new phase called fast recovery. It treats the 2 signs of congestion differently. If time-out occurs, TCP moves to the slow start phase. If 3 duplicate ACK. arrives TCP moves to the fast recovery state.

3. New Reno TCP – Latter version of TCP known as new Reno TCP has an extra optimization on Reno TCP.

THROUGHPUT OF TCP.



$$\boxed{\text{Throughput} = \frac{0.75 \times W_{max.}}{RTT}}$$

W = window size.

Q. If $W_{max.}$ = 10 KB and RTT = 100 ms. What is the throughput of the TCP?

$$\text{Throughput} = \frac{0.75 \times W_{max.}}{RTT}$$

$$W_{max.} = \frac{10+12+10}{3} = \frac{32}{3} = 10.66$$

Scanned by CamScanner

Selecting route is Routing
Selecting interface is Forwarding.

NETWORK LAYER.

→ Services provided by Network Layer –

1. Host to Host Delivery of Data.
2. Packetizing :-
Encapsulating the Payload from transport layer in a Network layer packet is called packetizing. The header of the n/w layer is added to the Payload which contains the source and destination address and some other info. The in-between routers are not allowed to decapsulate the packets unless there is a need for fragmentation.
3. Routing :-
A packet can be transmitted through more than one route from source to destination. It is the function of the network layer to find the best route possible.
4. Forwarding :-
It is defined as the action applied by each router when a packet arrives at one of its interface. The decision-making table of a router helps in forwarding a packet.

17/10

5. Error Control :-
Network layer ignores the process of error control but checksum is used only to check if the header is error free or not.
ICMP protocol is used to provide some error control.

Imp

6. Flow Control :-
Flow control is not provided by network layer. The reason that the designers of the network layer

Scanned by CamScanner

Forwarding Table.

Destination	Interface
160.1.2.1	2

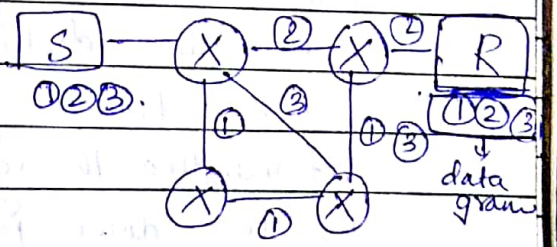
does not or ignores the concept of flow control.
i) Since there is no error control, the receiver may not be overwhelmed.
ii) Buffers may be implemented at the upper layer to receive the data.
iii) Flow control is provided by the upper layer so another level of flow control will make the network complicated.

7. Congestion control :-
Congestion in the network layer is a situation in which too many datagrams are present in a particular area of internet. Network layer provides some amount of congection control.

8. Quality of Service :-
As there are multimedia data transmission, the quality of service should be good.

9. Security :-
Security should be provided by the n/w layer to the packet transmitting.

PACKET SWITCHING.



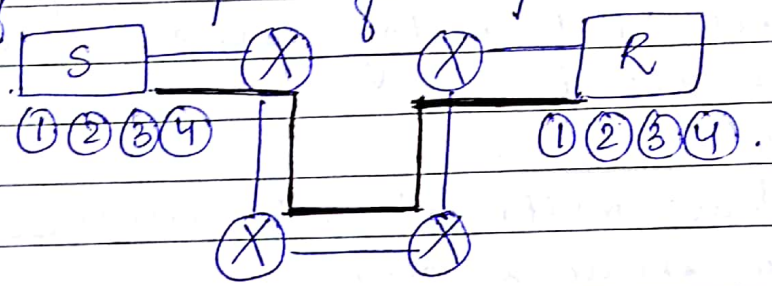
Datagram | Virtual Circuit.

Packet Switching is basically categorized into 2 types — Datagram approach and Virtual Circuit approach.

1. Datagram Approach — It is a connection-less service.

The n/w layer protocols treats each packet independently. The packet may or may not travel in the same path to the destination.
In datagram approach the forwarding decision is based on the destination address of the packet.

2. Virtual Circuit Approach – In this a virtual connection should be setup to define the path of the datagrams. It contains a flow level i.e. a virtual circuit identifier that defines the path of the packet



It consists of 3 phases – connection setup, data transfer and tear down.
It is a connection-oriented service.
In connection setup phase, a virtual path is setup b/w source and destination.
In data transfer phase the data or the packets are transmitted through the virtual path to the destination.
In tear down phase a special packet called tear down packet is sent to delete the virtual path.

[Pg 251 – 255] – Study on your own.
Packet loss, delay, Type of delay, Throughput.

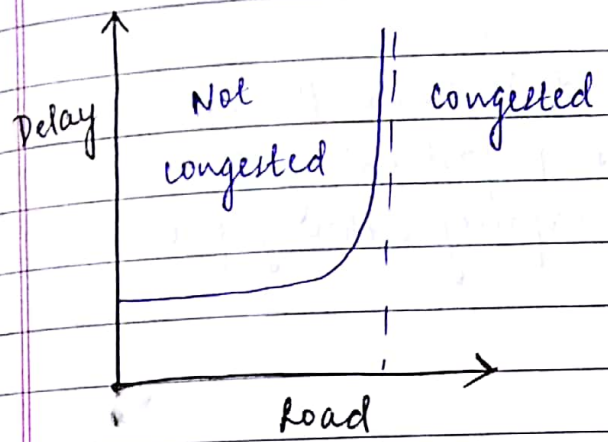
Scanned by CamScanner

NETWORK LAYER CONGESTION

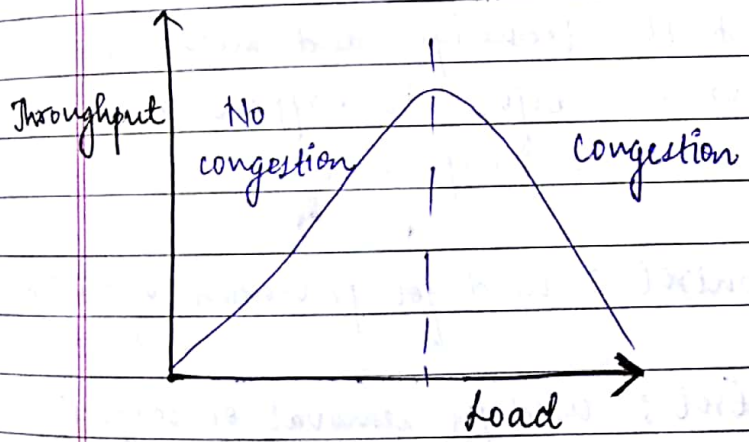
21/10/17.

Network layer congestion depends on 2 factors:

1) Delay
2) Throughput.



Load is the capacity of network.
Delay moves towards infinity.



Congestion in the network depends on 2 factors – Delay & Throughput.

Delay – when the load is much less than the capacity of the network the delay is minimum. This minimum delay compose of 2 delays :- propagation and processing delay.

Scanned by CamScanner

When the load reaches the network capacity, the delay increases sharply. This delay consists of queuing, propagation & processing delay.

The delay becomes infinite when the load is greater than capacity.

Throughput - When the load is below the capacity of the network, throughput increases proportionately to the load. After the load reaches the capacity, throughput decline sharply.

CONGESTION - CONTROL

Congestion control refers to the technique and mechanism that can prevent congestion before it happens or remove congestion after it has happened.

2 types -

i) Open-loop congestion control : used for prevention of congestion.

ii) Close-loop congestion control ; used for removal of congestion.

OPEN - LOOP CONGESTION CONTROL POLICIES

Applied to prevent congestion before it happens. Congestion control is handled by either the source or the destination. Various types of open-loop congestion control are :-

Scanned by CamScanner

i) Re-transmission Policy - If a sent packet is lost or corrupted, the packet must be retransmitted. A good retransmission policy can prevent congestion. Re transmission policy must be designed to optimize the efficiency and prevent congestion.

ii) Window Policy - The type of window at the sender also effect congestion. Selective repeat window is better than Go-Back-N window.

iii) Acknowledgement Policy - Acknowledgement Policy at the receiver may effect congestion.

iv) Discarding Policy - A good discarding policy by the routers may prevent congestion.

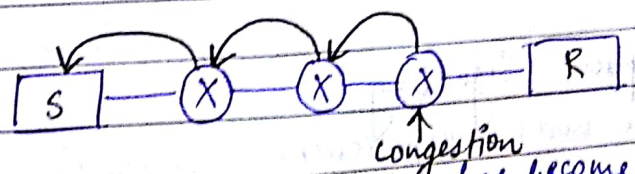
v) Admission Policy - Admission Policy can prevent congestion in virtual circuit network. A router can deny establishing a virtual circuit connection.

CLOSE LOOP CONGESTION CONTROL POLICIES

It is used to alleviate the congestion after it happens. Various types are -

Imp

i) Back Pressure -



(It sends info to previous router that it has become congested and can't receive any more info.)

i) Re-transmission Policy - If a sent packet is lost or corrupted, the packet must be retransmitted. A good retransmission policy can prevent congestion.
Re-transmission policy must be designed to optimize the efficiency and prevent congestion.

ii) Window Policy - The type of window at the sender also effect congestion. Selective repeat window is better than Go-Back-N window.

iii) Acknowledgement Policy - Acknowledgement Policy at the receiver may effect congestion.

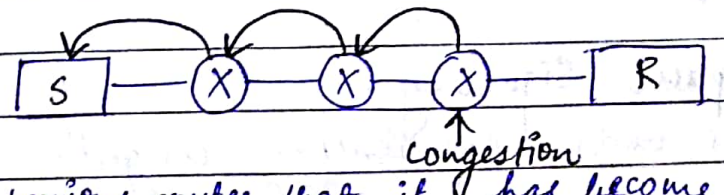
iv) Discarding Policy - A good discarding policy by the routers may prevent congestion.

v) Admission Policy - Admission Policy can prevent congestion in virtual circuit network. A router can deny establishing a virtual circuit connection.

CLOSE LOOP CONGESTION CONTROL POLICIES

It is used to alleviate the congestion after it happens. Various types are -

Imp
i) Back Pressure -

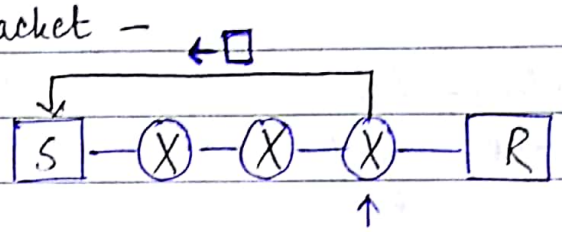


(It sends info to previous router that it has become congested and can't receive any more info.)

Scanned by CamScanner

Back pressure refers to a technique in which a congested node/ router stops receiving data from immediate upstream node. This may cause upstream node to become congested. It also stops receiving data from its upstream node and so on. Back-pressure is a node-to-node congestion control that starts with a node and propagates in the opposite direction of data flow. It can be applied to virtual circuit networks.

ii) Choke Packet –



Congestion

(A packet is directly sent to the sender to tell to stop sending info.)

It is a packet sent by a node to the source to inform that the node is congested.

iii) Implicit Signaling –

In Implicit Signaling, there is no communication b/w congested node & the source. the source guess that there is congestion somewhere in the network from the symptoms. eg. There is no acknowledgement coming for a while

iv) Explicit Signaling –

The node experiencing congestion can explicitly send a

Scanned by CamScanner

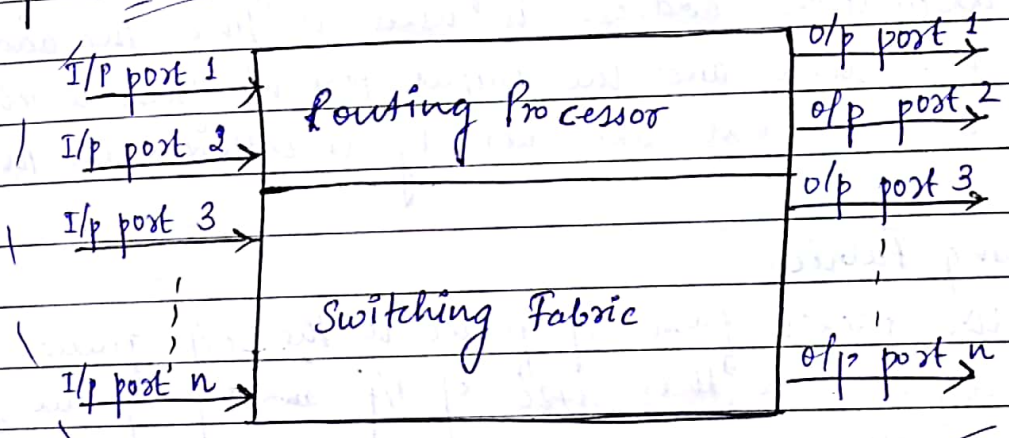
signal to the source.

STRUCTURE OF A ROUTER.

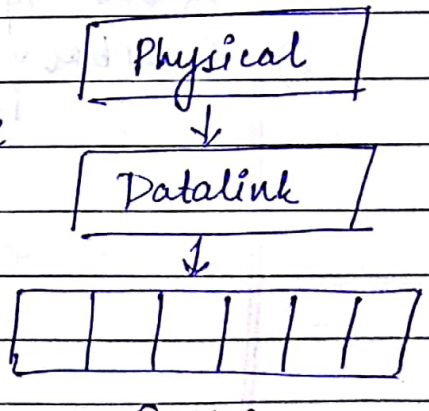
Components of a Router :-

1. Input Port
2. Output Port
3. Routing Processor
4. Switching Fabric.

1. Input Port.



Router

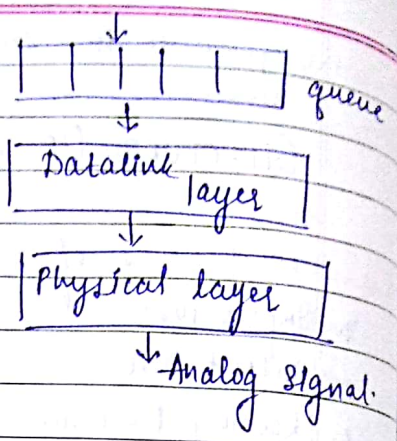


Input port performs the physical & link layer functions of the router. The bits are constructed from received signal. The packet is decapsulated from the frame and discarded if corrupted. If the packet is not corrupted, it is ready to be processed by network layer. The packets are stored in the queue before they are ~~switched~~ directed to switching fabric.

Scanned by CamScanner

2. Output Port.

Output port performs the same function as input port but in reverse order. First, the outgoing packets are queued, then each packet is encapsulated in a frame and physical layer functions are applied to create the signal.



3. Routing Processor.

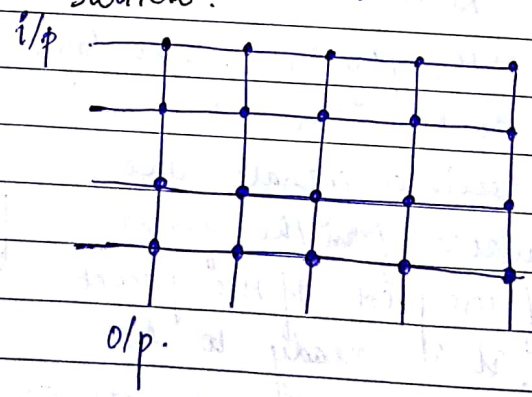
Routing processor performs the functions of network layer. The destination address is used to find the address of the next link and the output port no. from which the packet is sent out. This activity is called table look-up.

4. Switching Fabric.

Moves the packet from i/p queue to the o/p queue. The speed depends on the size of i/p and o/p queue & overall delay.

Various types of switching fabric are :-

i) Crossbar Switch :-



Scanned by CamScanner

It is the simplest type of switch. It connects n i/p to n o/p in a grid, using electronic micro-switches at each cross point.

ii) Banyan Switch –

It is a multi-stage switch with micro-switches at each stage that route the packet based on o/p port represented as a binary string.

For n i/p & n o/p, there are $\log_2 n$ stages with n/2 micro-switches.

I/P = 8 O/P = 8

3 stages, 4 switches

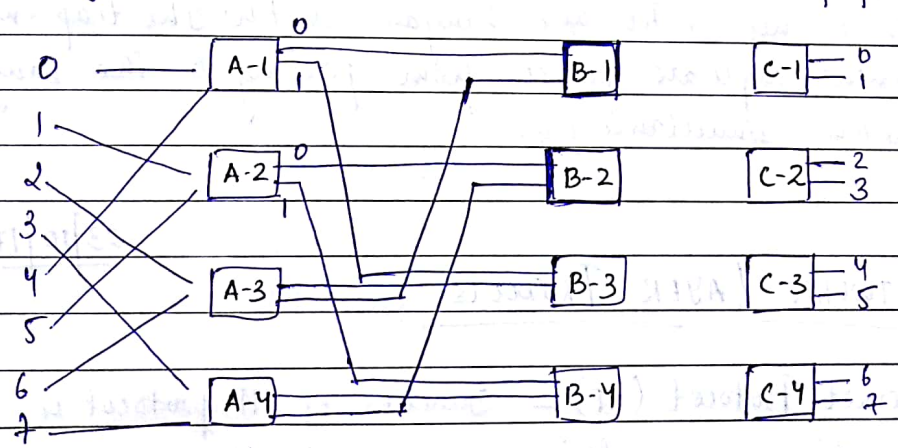
i/p port = 1

o/p port = 6 (110)

LSB

MSB

(1st highest order)



The first stage routes the packet based on highest order bit of binary string.

It is the simplest type of switch. It connects n i/p to n o/p in a grid, using electronic micro-switches at each cross point.

ii) Banyan switch –

It is a multi-stage switch with micro-switches at each stage that route the packet based on o/p port represented as a binary string.

For n i/p & n o/p, there are $\log_2 n$ stages with n/2 micro-switches.

I/P = 8 O/P = 8

3 stages, 4 switches

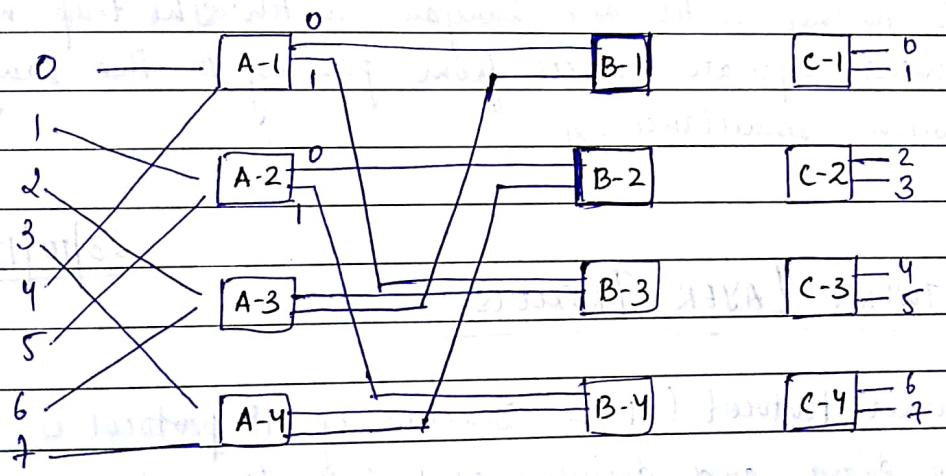
i/p port = 1

o/p port = 6 (110)

LSB

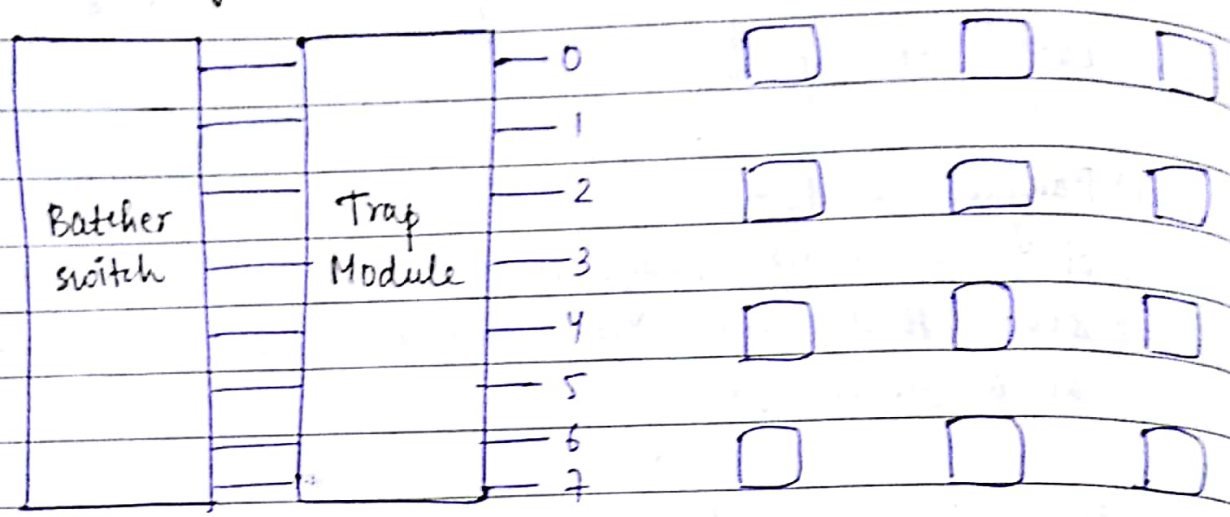
MSB

(1st highest order)



The first stage routes the packet based on highest order bit of binary string.

3. Batcher - Banyan Switch :-



Batcher designed a switch that comes before the banyan switch and sort the incoming packets according to the final destination. The combination is called Batcher-Banyan switch. Another hardware module called trap is added b/w batcher switch and banyan switch. The trap module prevent duplicate packets from passing to the banyan switch simultaneously.

23/10/17.

NETWORK LAYER PROTOCOLS

1. Internet Protocol (IP) – Function of IP protocol is packetizing forwarding and delivery of packets to network layer.

2. Internet Control Message Protocol (ICMP) – Function of ICMP is to handle errors that may occur in network layer delivery.

Scanned by CamScanner

3. Internet Group Management Protocol (IGMP) – Function of IGMP is to help IP in multicasting.

4. Address Resolution Protocol (ARP) – ARP is used for mapping network layer address to link layer address.

IP DATAGRAM FORMAT

Data can be otherwise called as payload.

Header	~~Data~~ (Payload)

Datagram

4 bytes

0	4	8	16	31
VER	HLEN	Service type	Total length	
Identification			Flags 3 bits	Fragmentation offset
Time-to-live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
OPTION				
DATA				

HEADER: Fix, Variable

20-60 bytes ⇒ IP Header size.

Scanned by CamScanner

Version (VER) : Version is a 4 bit field which defines the version of the IP protocol.

Header Length (HLEN): It describes the total length of the header in 4-byte word.

chapter-8

Service Type : Defines how the datagram should be handled.

Total length: It describes the total length of datagram which constitutes data & header.

Identification, Flag & Fragmentation Offset: Related to fragmentation of IP datagram.

Time-to-live : TTL field is used to control the maximum no. of routers visited by the datagram.

Protocol: It is a 8-bit field used to define the underlaying protocol. eg. If TCP is used, the value will be 6. If UDP is used, the value be 17.

Header Checksum : It is used to check the correctness of the header. Checksum is recalculated at each router.

Source & Destination IP Address : These are 32 bit addresses. Datagram should know its source IP address. The destination IP address is provided by the DNS.

Scanned by CamScanner

OPTION : Option field can have upto 40 bytes. It is a variable length field.

DATA or Payload : Payload is the packet coming from other protocols used.

FRAGMENTATION

Maximum Transfer Unit (MTU) – It is the size of the data that can be transmitted in the network. The datagram needs to be fragmented to make it possible for it to pass through the network is called as fragmentation.

Each fragment has its own header. Datagram can be fragmented into many no. of times till it reaches the destination.

Datagrams are reassembled at the destination host.

Fields related to fragmentation:

i) Identification : It is a 16 bit field which identifies a datagram originating from source host. All the fragments have ~~some~~ same identification number.

Identification no. helps the destination in reassembling the data.

ii) Flags : It is a 3-bit field. Left most bit is unused. Second bit is called D-bit or Don't fragment bit.

If D-bit = 0, then it can be fragmented.

If D-bit = 1, then it can't be fragmented.

Third bit is called as M-bit or More fragment bit.

If M-bit = 1, means datagram is not the last fragment.

Scanned by CamScanner

OPTION : Option field can have upto 40 bytes. It is a variable length field.

DATA or Payload : Payload is the packet coming from other protocols used.

FRAGMENTATION

Maximum Transfer Unit (MTU) – It is the size of the data that can be transmitted in the network. The datagram needs to be fragmented to make it possible for it to pass through the network is called as fragmentation.
Each fragment has its own header. Datagram can be fragmented into many no. of times till it reaches the destination.
Datagrams are reassembled at the destination host.
Fields related to fragmentation :

i) Identification : It is a 16 bit field which identifies a datagram originating from source host. All the fragments have ~~some~~ same identification number.
Identification no. helps the destination in reassembling the data.

ii) Flags : It is a 3-bit field. Left most bit is unused. Second bit is called D-bit or Don't fragment bit.
If D-bit = 0, then it can be fragmented.
If D-bit = 1, then it can't be fragmented.
Third bit is called as M-bit or More fragment bit.
If M-bit = 1, means datagram is not the last fragment.

Scanned by CamScanner

If M-bit = 0, means it is the last fragment or only fragment.

iii) Fragmentation Offset : It is a 13-bit field. It shows relative position of the fragment w.r.t whole datagram.

eg: Suppose there is a datagram of size 4000 bytes which is fragmented into 3 fragments.

→ Suppose we want to create fragment length of 1400.

Fragment	Identification No.	Flag	Offset
1	[0 - 1399] I	1	0/8 = 0
2	[1400 - 2799] I	1	1400/8 = 175
3	[2800 - 3999] I	0	2800/8 = 350.

What is DF bit or MF bit.

24 | 10 | 17.

IPv4 Address.

IPv4 addresses are generally 32-bit addresses. IP address is the address of the connection not the address of the device. IP address are unique that means each address defines only 1 connection to the network.

1. Address Space - It is the total no. of address used by the protocol. IPv4 uses 32-bit addresses that means the address space consists of 2^{32} addresses.

Scanned by CamScanner

2. Address Notation.

i) Dotted Decimal – 128 · 11 · 3 · 31

ii) Binary 10000000 00001011 00000011 00011111

iii) Hexadecimal – 8 0 0 B 0 3 1 F

3. Hierarchy in Address.

Addresses are divided into 2 parts – Prefix & Suffix.

Prefix part is the address of the network.

Suffix part are the addresses of the node.

If prefix is n no. of bit then suffix is 32 − n.

Prefix (Network address)	Suffix (Device Address)
n (8 bits)	(32−n) (24 bits) → for class A.

starts with 0. (0–7)

CLASSFUL ADDRESSING – The addresses are divided into 5 category – A B C D E.

i) Class A – The network length is upto 8 bits. The leftmost bit is fixed with a value '0', only 7 bits are remaining for network identifier. Hence only $2^7 = 128$ network addresses possible in class A address.

ii) Class B – In this 16 bit are for prefix and 16 bit are for suffix. From 16 prefix bit, 2 bits have fixed value 10. Hence 2^{14} network addresses are possible.

iii) Class C – 24 bit are for prefix and 8 bit are for suffix. In this 110 is constant. 2^{21} network addresses are possible.

iv) Class D – It is reserved for multicast addressing. There is prefix & suffix part. The leftmost 4 bit are of fixed value 1110.

Scanned by CamScanner

v) Class E – It is reserved for future use. Leftmost 4 bits are fixed value 1111.

Address Depletion – Drawbacks of Class A and Class C.
In Class A – many addresses for device and less addresses for network.
In Class C – many addresses for n/w and less addresses for device.

To overcome the drawback – Subnetting Supernetting.

CLASSLESS ADDRESSING – In this class privilege was removed, variable length block of addresses are used. Prefix length is inversely proportional to the size of the network.

SLASH NOTATION – The prefix length n is added to the address separated by a slash.
eg. 128.11.3.31/22
Slash Notation is otherwise called as Classless InterDomain Routing or CIDR.

Extracting info. from an address, suppose the prefix length is 'n'.
i) The no. of addresses in the block = $N = \cancel{2^{32}} \cancel{/n}. \; 2^{(32-n)}$
ii) The first address of the n/w is, keep the n leftmost bit and set the 32-n rightmost bit to 0.
iii) To find the last address, keep the n leftmost bit and

set (32-n) rightmost bit to 1.

Ques. A classless address is given as 167.199.170.82/27. Calculate the total no. of address, the first address and the last address of the block.

total no. of address ⇒ $2^{32-27} = 2^5$.

first address ⇒ $\underbrace{\underbrace{167}_{8}.\underbrace{199}_{8}.\underbrace{170}_{8}}_{\text{fixed}}.\underbrace{82}_{\text{binary}}$

8 8 8 010|10010

fixed | set it to '0'

$\underbrace{01000000}_{64}$ → first address.

$\underbrace{01011111}_{95}$ → last address

167.199.170.64 – First Address.

167.199.170.95 – Last Address.

26/10/17

Address mask

Block Address

Subnetting

Address aggregation

DHCP (Dynamic Host Config.)

DHCP Message Format

Network Address Translation.

Scanned by CamScanner

27/10/17.

INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

ICMP messages are not passed directly to the datalink layer. It is first encapsulated with IP datagram and passed to the datalink layer.

ICMP messages are
1. Error control messages.
2. Query messages.

Error control messages :-
Error control messages report a problem that a router or a host may encounter when it process the IP packet.

Query messages :-
Query messages help a host to get specific information from host or router.

ICMP MESSAGE FORMAT.

5 fields :-
1. Type
2. Code
3. Checksum
4. Rest of the header
5. Data.

Scanned by CamScanner

Type & Code of Error reporting messages :-

Type	Code
→ 03- Destination unreachable	0 to 50.
→ 04 - Source quench	0
→ 05 - Redirection	0 to 3
→ 11 - Time exceeded	0 and 1.
→ 12 - Parameter problem	01

* Destination unreachable define the type of error message when the datagram has not reached its final destination.

* Source Quench informs the sender that network has encountered congestion and the datagram has been dropped.

* Redirection message is used when the source uses wrong router to send out its message. The router redirects the message to appropriate router and informs the source to change its default router.

* Time exceeded message is sent to the source to inform that the datagram time to live value is now zero.

* Parameter problem message can be sent when there is a problem in the header of the datagram or some percent of the datagram are missing.

Scanned by CamScanner

Query Message-

Type	code
08 - Echo request	0
00 - Echo reply	0
30 - Time stamp Request	0
14 - Time stamp Reply	0

* Query message are used to or test the liveliness of host & routers in the internet.
* Echo request :- A host or router sends echo request message to another host or router to check if it is alive or not.
* Echo reply :- The echo reply message is sent corresponding to echo request message.
* Time Stamp Request & Reply is used to find the round trip time b/w 2 devices or to check whether the clocks of 2 devices are synchronized or not.

UNICAST ROUTING.

If a datagram is destined for only 1 destination, it is called unicast routing.

If a datagram is destined for multiple destinations, it is called multicast routing.

If a datagram is supposed to be delivered to all the host of the network, it is called broadcast routing.

Scanned by CamScanner

Unicast - 1 to 1
Multicast - 1 to many but not all present in n/w.

1 to all - Broadcast host

ROUTING ALGORITHM.

A routing algorithm interpret the least cost and create a least cost tree for each node.
There are 3 types of routing algorithm used in network layer:-

1. Distance - Vector Routing.
2. Link - State Routing.
3. Path - Vector Routing.

Scanned by CamScanner

Unicast - 1 to 1
Multicast - 1 to many but not all present in n/w.

1 to all - Broadcast host

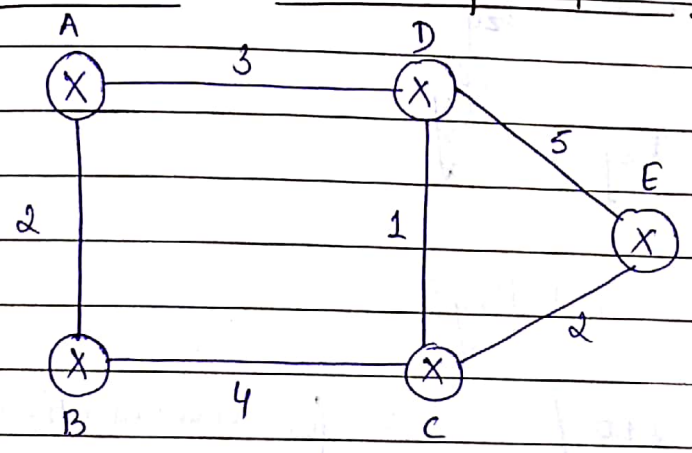
ROUTING ALGORITHM.

A routing algorithm interpret the least cost and create a least cost tree for each node.
There are 3 types of routing algorithm used in network layer:-

1. Distance-Vector Routing
2. Link-State Routing
3. Path-Vector Routing

DISTANCE VECTOR ROUTING ALGORITHM.

3/11/17.



We can't communicate through indirect nodes. (Eg. C can't be communicated through A → B → C). If there is no direct comm^n. b/w the 2 nodes then its distance vector is ∞.

Rudimentary DV Initialization

	B
A	2
B	0
C	4
D	∞
E	∞

	A
A	0
B	2
C	∞
D	3
E	∞

Scanned by CamScanner

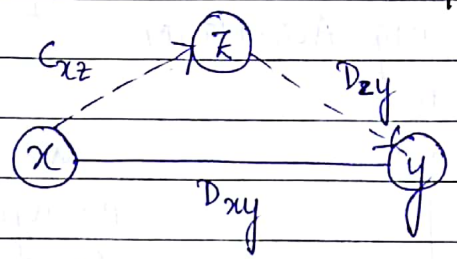
	E
A	∞
B	∞
C	2
D	5
E	0

	D
A	3
B	∞
C	1
D	0
E	5

	C
A	∞
B	4
C	0
D	1
E	2

1. Rudimentary DV initialization.
2. Information (DV) exchange with immediate neighbours.

Q. What is BELMAN-FORD ALGORITHM?



$$D = \min\{D_{xy}, C_{xz} + D_{zy}\}$$

$$\Rightarrow \min\begin{Bmatrix} 2, & 2+0 \\ 0, & 2+2 \\ 4, & 2+\infty \\ \infty, & 2+3 \\ \infty, & 2+\infty \end{Bmatrix}$$

$\Downarrow$

for communication to B through A sends some information to B, so we update B.

new B

A	2
B	0
C	4
D	5
E	8

Scanned by CamScanner

Now, C sends information to B.

$$\Rightarrow \min \begin{Bmatrix} 2, & 4+\infty \\ 0, & 4+4 \\ 4, & 4+0 \\ 5, & 4+1 \\ \infty, & 4+2 \end{Bmatrix}$$

$\Downarrow$

new B

A	2
B	0
C	4
D	5
E	6

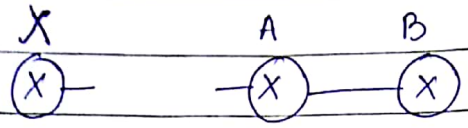
→ Belman-Ford Algorithm is used in distance vector routing. It creates a distance vector that is a one-dimensional array to represent a tree. Each node in the internet creates a rudimentary distance vector when initialized. To improve the distance vector, the nodes exchange information with immediate neighbours. The distance vector is updated using Belman Ford Algorithm.

There is a problem in Distance Vector Algorithm called 'Count to Infinity'.

Scanned by CamScanner

Count Infinity Problem.

eg.



A —∞— X

B —∞— X

X	A
	~~X~~
	~~3~~
	8
	⋮
	∞

X	B
	~~2~~
	~~5~~
	13
	⋮
	∞

If a link is broken the router should be aware of this problem. But, in distance vector algorithm, it takes some time which is called as count to infinity.

Solution to Count to Infinity Problem

There are 2 solutions provided :-

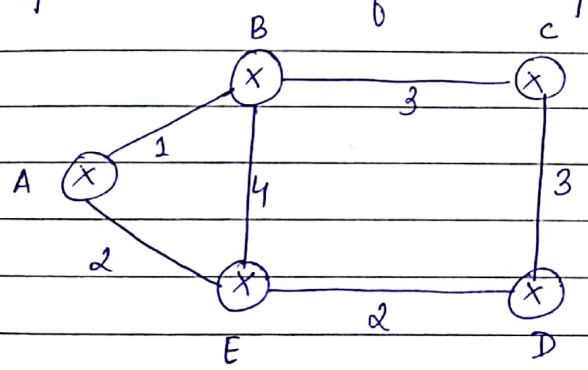
i) Split Horizon - In this only part of the distance vector is sent to neighbouring node. If node B thinks that optimum route to reach X is through A, it does not advertise the information to A. Node B eliminates the information and send it to A. Node A keeps the value as ∞ to distance to X and send it to B.

ii) Poisoned Reverse - Protocols use timer, if there is no news about the node, then the node is deleted from the table. When node B eliminate X & send info. to A,

A will be confused that it is due to split horizon or router is not alive. Hence B can still advertise the value of X but if the source of info. is A, the value can be replaced with ∞. That means Don't use the Value what I know About this Route Comes From You.

2. LINK STATE ALGORITHM

In link state algorithm, least cost trees are created. The characteristics of a link represents a network in the internet. The cost associated with an edge defines the state of the link. Link with lower costs are preferred over link with higher cost. If cost of a link is ∞, it does not exist. The collection of states for all link is called Link State Database. Link State Database is a 2-D Array which represent the cost of the corresponding link.

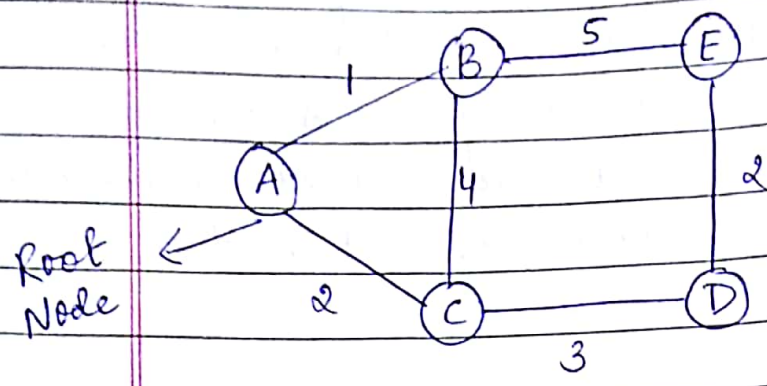


	A	B	C	D	E
A	0	1	∞	∞	2
B	1	0	3	∞	4
C	∞	3	0	3	∞
D	∞	∞	3	0	2
E	2	4	∞	2	0

Scanned by CamScanner

DIJKSTRA'S ALGORITHM

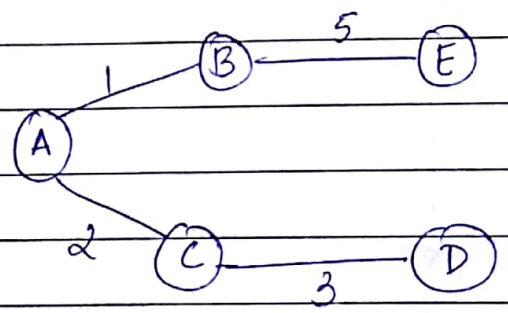
4/11/17.



$$D[x] = \min\{D[x], (D[w] + c[w,x])\}.$$

Steps	Nodes	$D_B P_B$	$D_C P_C$	$D_D P_D$	$D_E P_E$
0	A	1, A	2, A	∞	∞
1	AB		2, A	∞	6, B
2	ABC			5, C	6, B
3	ABCD				6, B.
4	ABCDE				

Least Cost Tree :-



Step 1: ~~If~~ Each node sends its info. to immediate neighbour.
~~If~~ It uses a packet to send the information called as link state packet or LSP.
When the node receives the LSP it compares with the older LSP it has and then choose which LSP to keep.

Scanned by CamScanner

Formation of Least Cost Tree

To create a least cost tree, dijkstra's algorithm is used.

i) The node selects one node among all the nodes as the root.

ii) The nodes closest to the root node is added to the tree. The cost of all other nodes are updated.

iii) Nodes repeat step2 until all the nodes are added.

3. PATH-VECTOR ALGORITHM.

In path-vector algorithm, the goal is not the priority. Priority here is the path followed by the packet. The source can control the path of the packet.

→ Three protocols are used in network layer for routing purpose –

Intra ASRP 1. Routing Information Protocol (RIP) – It uses Distance Vector Routing Algorithm.

Intra ASRP 2. Open ~~Source~~ Shortest Path First (OSPF) – It uses Link State Routing Algorithm.

Inter ASRP 3. Border Gateway Protocol (BGP) –

AUTONOMOUS SYSTEM – Each autonomous system can run a routing protocol. The routing protocol that is used in autonomous system is called as Intra Autonomous System Routing Protocol or Intra Domain Routing Protocol or Interior Gateway Protocol.

The routing protocol that is used in between autonomous

Scanned by CamScanner

system is called as Inter Autonomous System Routing Protocol or ~~Intra~~ Inter Domain Routing Protocol or Exterior Gateway Protocol.

Hierarchial Routing is a routing procedure in which routing process is divided into different steps.

Why Hierarchial Routing is used?

i) Scalibility Problem - The size of the forwarding table becomes huge. Searching for the destination will be time consuming.

ii) Administrative Issues — The administrator needs to have control over the internet.

NEW CH: DATA LINK LAYER

In datalink layer the communication is node to node. Two end hosts and in between routers are called nodes. The network in between are called as links.

Links are divided into 2 types —

a) Point-to-Point : In this link, it is dedicated to two devices.

b) Broadcast : It is shared b/w various devices.

Scanned by CamScanner

Datalink layer is divided into 2 sub-layers :

Data Link Control (DLC)
Media Access Control (MAC

1) Data Link Control (DLC) – In DLC, the link can be point-to-point or broadcast. The functions of DLC include framing, flow and error control, error detection and correction.

FRAMING – Framing in DataLink layer is constituting a frame that can be transmitted in a network.

Framing are of 2 kind – a) Fixed-size Frame.
b) Variable-size Frame.

a) Fixed-size Frame : Does not need to define the boundaries.

b) Variable-size Frame : Defines the boundaries.

There are 2 approaches to constitute a variable-size frame :

i) Byte-oriented

ii) Bit-oriented.

i) Byte-oriented / Character-oriented : In this header carries the source and destination address and control info. The trailer carries error detection, redundant bits. To separate one frame from another flags are added in the beginning and end of the frame.

ii) Bit-oriented : The frame is a sequence of bits.

Flow & Error Control : Flow control is one of the duties of DLC sub-layer. Any time an error is detected in a frame it is re-transmitted. Error control at the datalink layer is node to node.

Scanned by CamScanner

Error Detection & Error Correction

There are various types of errors:

i) Single Bit Error – one bit error. Either 0 becomes 1 or 1 becomes 0.

ii) Burst Error – 2 or more bits are corrupted.

In error detection, we have to only detect the error. In error correction, the bits that are corrupted should be identified and corrected.

Error Correction Techniques.

i) Hamming distance

ii) Cyclic Redundancy Check (CRC).

iii) Parity Check

iv) Checksum.

Scanned by CamScanner

Error Detection & Error Correction

There are various types of error:

i) Single Bit Error – one bit error. Either 0 becomes 1 or 1 becomes 0

ii) Burst Error – 2 or more bits are corrupted.

In error detection, we have to only detect the error. In error correction, the bits that are corrupted should be identified and corrected.

Error Correction Techniques.

i) Hamming distance
ii) Cyclic Redundancy Check (CRC).
iii) Parity Check
iv) Checksum.

(i) HAMMING DISTANCE

6	11	17.

$$
\begin{array}{rl}
 & 0\,1\,0\,1\,1\,0\,1 \rightarrow x \\
\oplus & 1\,0\,1\,1\,0\,1\,0 \rightarrow y. \\
\hline
 & 1\,1\,1\,0\,1\,1\,1
\end{array}
$$

$d(x, y) = 6$ (no. of 1's). → Hamming distance.

The no. of bits ~~ta~~ of error can be detected using hamming distance $d = d-1$.

The no. of bits that can be corrected $= \frac{d-1}{2}$.

Scanned by CamScanner

Q. Suppose the minimum hamming distance is 7. How many bits of error can be detected and corrected.

Detected = $d-1 = 7-1 = 6$

Corrected = $\frac{d-1}{2} = \frac{7-1}{2} = \frac{6}{2} = 3.$

Q. Suppose we have a dataword 101011001110. Find the codeword using hamming code.

1 0 1 0 1 1 0 0 1 1 1 0 → Dataword.

D17 P16 D15 D14 D13 D12 D11 D10 D9 P8 D7 D6 D5 P4 D3 P2 P1

1 P16 0 1 01 1 0 0 P8 1 1 1 P4 0 P2 P1 → Codeword

The position where we have to add parity bit is $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$.

For P1, (1 bit check & 1 bit skip).

P1 0 1 1 0 1 0 0 1 → if no. of 1's is even, P1 = 0.

For P2, P2 0 1 1 0 1 1 0 → even P2 = 0.

P4, P4 1 1 1 1 0 1 0 → odd P4 = 1

P8, P8 0 0 1 1 0 1 0 → odd P8 = 1.

P16, P16 1 → odd P16 = 1.

Codeword, 1 1 0 1 0 1 1 0 0 1 1 1 1 1 0 0 0 → Ans.

(Replacing the parity bit by its value).

Scanned by CamScanner

Q. Suppose the minimum hamming distance is 7. How many bits of error can be detected and corrected.

Detected = $d-1 = 7-1 = 6$

Corrected = $\frac{d-1}{2} = \frac{7-1}{2} = \frac{6}{2} = 3.$

Q. Suppose we have a dataword 101011001110. Find the codeword using hamming code.

1 0 1 0 1 1 0 0 1 1 1 0 → Dataword.

D17 P16 D15 P14 D13 D12 D11 D10 D9 P8 D7 D6 D5 P4 D3 P2 P1

1 P16 0 1 0 1 1 0 0 P8 1 1 1 P4 0 P2 P1 → Codeword

The positions where we have to add parity bit is $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$.

For P1, (1 bit check & 1 bit skip).

P1 0 1 1 0 1 0 0 1 → if no. of 1's is even, P1 = 0.

For P2, P2 0 1 1 0 1 1 0 → even P2 = 0.

P4, P4 1 1 1 1 0 1 0 → odd P4 = 1

P8, P8 0 0 1 1 0 1 0 → odd. P8 = 1.

P16, P16 1 → odd P16 = 1.

Codeword, 1 1 0 1 0 1 1 0 0 1 1 1 1 1 0 0 0 → Ans.

(Replacing the parity bit by its value).

Scanned by CamScanner

(ii) Parity check.

Dataword	Codeword.
1001	10010 (if even, add 0)
1101	11011 (if odd, add 1)
1000	10001 "

It is a error ~~decti~~ detecting code, in this k bit of dataword is changed to n bits of codeword where $n = k+1$.

(iii) Cyclic Redundancy Check. (CRC)

Encoder's side

```
        | 1010
        |-------
1011    | 1001 000   , append extra 3 bits.
        | 1011 ⊕
        | 0100
          0000 ⊕
          -----
           1000
           1011 ⊕
           -----
            0110
            0000 ⊕
            ------
              110
```

Dataword is 1001.

Now append it with remainder which becomes codeword.

1001110 → Codeword.

Scanned by CamScanner

Decoder's side

```
        1010
1011 | 1001110
       1011
       ----
        0101
        0000
        ----
        1011
        1011
        ----
        0000
        0000
        ----
         000 (No error)
```

It means codeword is correct.

```
        1011
1011 | 1000110
       1011
       ----
        0111
        0000
        ----
        1111
        1011
        ----
        1000
        1011
        ----
         011 (error).
```

The remainder obtained at the decoder's side is called as syndrome.

Syndrome - If all the bits in the syndrome are zero, extract 4 leftmost bits and that is the dataword.

If the syndrome contains any no. of 1's then the dataword is corrupted and will be discarded.

k - length of dataword
n - length of codeword
n-k - no. of 0's to be added.

2.) Media Access Control (MAC)

i) Random Access Protocol
ii) Controlled Access Protocol
iii) Chanelization.

a) ALOHA
b) CSMA/CD
c) CSMA/CA.

Scanned by CamScanner

i) a) ALOHA
b) CSMA / CD : Carrier Sense Multiple Access with Collision Detection
c) CSMA / CA : Carrier Sense Multiple Access with Collision Avoidance

ii) a) Reservation
b) Polling
c) Token Passing

iii) a) Time Division Multiple Access
b) Frequency Division Multiple Access
c) Code Division Multiple Access.

i) Random Access Protocol –

Scanned by CamScanner

i) a) ALOHA
b) CSMA / CD : Carrier Sense Multiple Access with Collision Detection
c) CSMA / CA : Carrier Sense Multiple Access with Collision Avoidance

ii) a) Reservation
b) Polling
c) Token Passing

iii) a) Time Division Multiple Access
b) Frequency Division Multiple Access
c) Code Division Multiple Access.

7/11/17

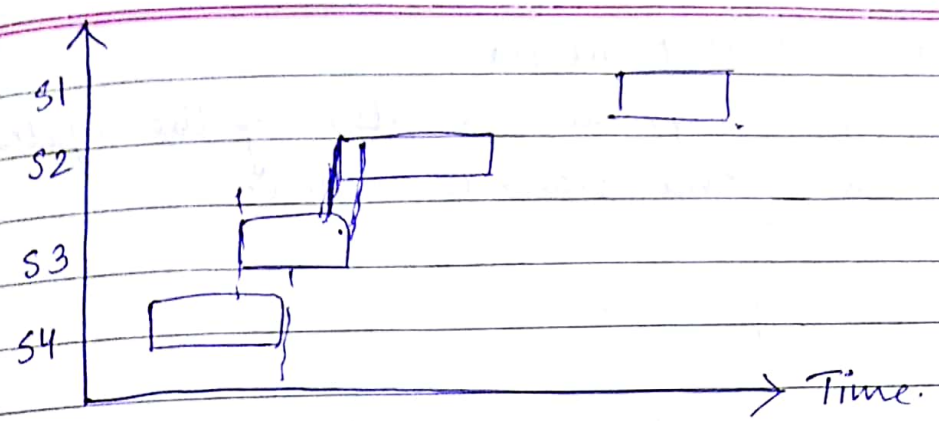
i) Random Access Protocol – The random access or contention methods, no station is superior to another. There is no schedule time to send data. The transmission is random among the stations. The problem with random data transmission, the data may collide. Collision of data either destroy the frames or modify the frames. For this 3 protocols are designed :–

1. ALOHA
2. CSMA / CD
3. CSMA / CA

1. ALOHA
a) Pure Aloha
b) Slotted Aloha.

a) Pure Aloha – The original ALOHA protocol is called as pure Aloha.

Scanned by CamScanner



Each station sends frame when it has a frame to send. If the acknowledgement does not arrive after a timeout period, the frame is retransmitted.
Stations wait for a random amt. of time before resending the frame. This frame is called as Back-off Time (T_B). Time-out period is generally set to round-trip propagation delay (T_p).

Average Frame Transmission Time (T_{fr}) - Time taken by a frame to transmit.
Vulnerable Time - It is the time in which there is a possibility of collision.
Vulnerable time = $2 \times T_{fr}$.

Q. A pure aloha n/w transmits 200 bit frames on a shared channel of 200 kbps. What is the vulnerable time?

$$T_{fr} = \frac{L}{R} = \frac{200 \text{ bit}}{200 \times 10^3 \text{ bps}} = 10^{-3} s = 1 ms$$

$$VT = 2 \times 1 ms = 2 ms.$$

Scanned by CamScanner

THROUGHPUT OF PURE ALOHA.

G = Average no. of frames generated by the system during one frame transmission time.

$$S = G \times e^{-2G}$$

Q. A pure aloha n/w transmits 200 bits frame on a shared channel of 200 kbps. What is the throughput if the system produces 1000 frames per sec.

$G = 1.$

1000 frames – 1 sec

$\therefore$ 1 frame – 10^{-3} sec = 1 ms

$G = 1$ ms

$S = 1 \times e^{-2} = e^{-2}$

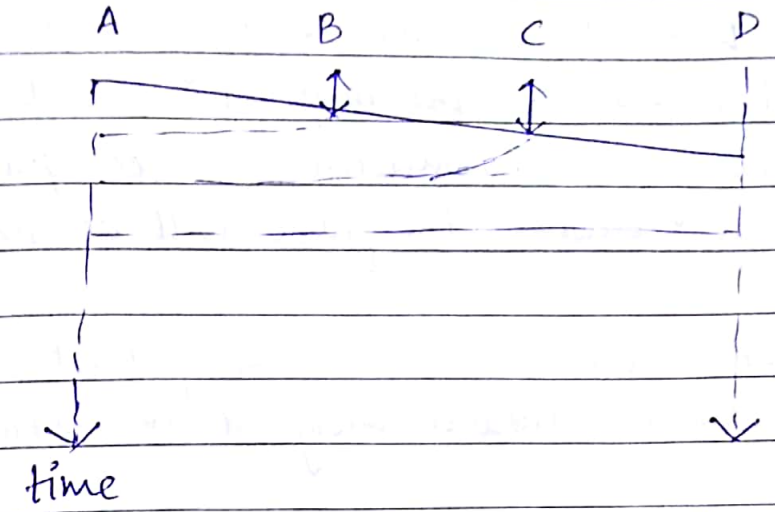
$= 0.1353$ Ans.

b) Slotted Aloha – It divides the time into slots. The station can send data only at the beginning of the slot. The vulnerable time in slotted aloha is T_{fr}. The throughput is $G \times e^{-G}$.

Q. In the previous problem, if slotted aloha protocol is used, what will be the throughput?

$$S = G \times e^{-G}$$
$$= 1 \times e^{-1}$$
$$= e^{-1}$$

2. Carrier Sense Multiple Access (CSMA) – In CSMA, each station first listens to the medium and then send the data. The vulnerable time in CSMA is propagation time (T_p).



Persistent Method – Basically these are of 3 types –

i) 1- Persistent

ii) Non- Persistent

iii) P- Persistent

i) 1- Persistent : It is very simple, after the station finds the line idle its sends the frames immediately.

ii) Non- Persistent : If the line is idle it sends the frames immediately, if the line is not idle it waits for a random amount of time and then sends the line.

iii) P- Persistent : This method is used if the channel has time slots with slot duration equal to or greater than T_p. It reduces the chances of collisions and improves efficiency.

Step1 – With propability P, the station sends the frame

Step2 – With probability $Q = 1-P$, the station waits for the beginning of the next time slot and checks the line

Scanned by CamScanner

again. If the line is idle, goto step 1. If the line is busy it acts as though a collision has occurred and uses the back-off procedure.

Diagram from book

(a) CSMA/CD. – This algorithm is designed to handle collision. A station monitors the medium after it sends a frame, to check if the transmission is successful or not. If there is a collision, the frame will be sent again.

(b) CSMA/CA – It is a random access protocol called as CSMA with collision avoidance designed to avoid collision.

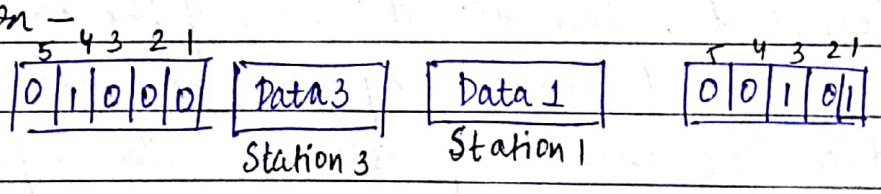
ii) <u>Controlled Access Protocol.</u>

In controlled access protocol, the stations consult one another to find which station has the right to send. A station cannot send data if it is not authorized to send.

3 types of controlled Access Protocol used :-

1. Reservation
2. Polling
3. Token Passing.

1. Reservation –



In this method, a station needs to make a reservation before sending data. A reservation frame preceeds the data frame. If there are n stations, there are n reservation

mini slots in the reservation frame.

Scanned by CamScanner

mini-slots in the reservation frame.

10/10/17.

2. Polling –
Primary
Secondary device
① Select
② Poll

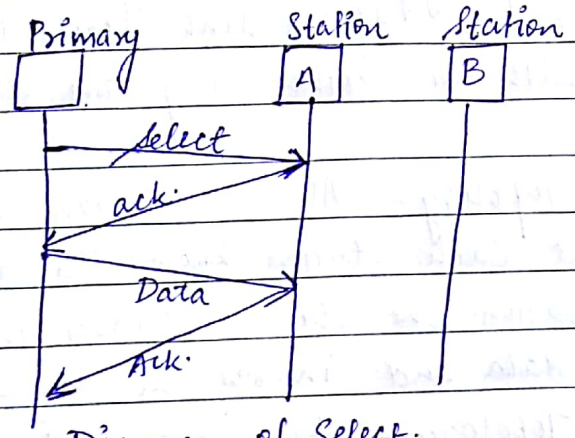


Diagram of Select.

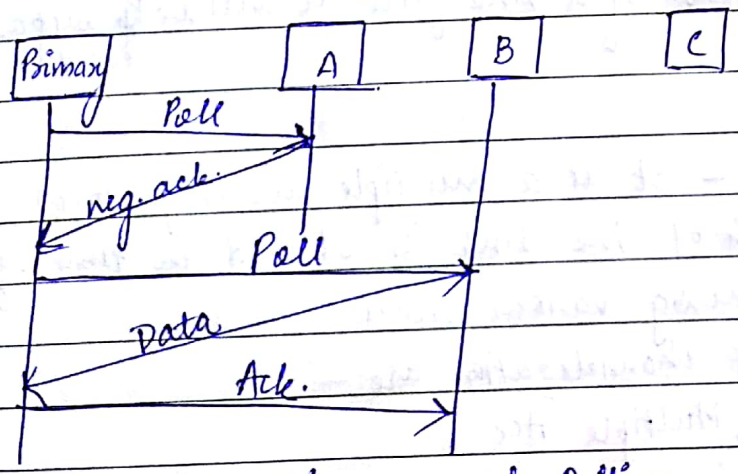


Diagram of Polling.

3. Token Passing – A token is circulated among the station which have some data to send, it will receive the when the station has no more data to send, it will release the token. The stations are organised in

Logical rings is classified into 4 types –

(i) Physical Ring – The station which has some data to send possesses the token. After the data is sent the token is released.

Drawback – If single link fails, the total network fails.

(ii) Dual Ring Topology – A secondary or auxiliary ring operates in reverse. If one link fails the link is combined with the other ring and data transmission continues.

Bus Ring Topology – All the stations are connected to a bus or cable. Each station knows the address of its successor station. The station releases the token after sending the data and inserts the address of the successor.

(iv) Star Ring Topology – There is a hub which connects all the stations. If a link fails it will be bypassed by the hub.

(iii). Channelization – It is a multiple access protocol, in which the bandwidth of the link is shared in time, frequency and code among various stations.

Various types of channelization are –

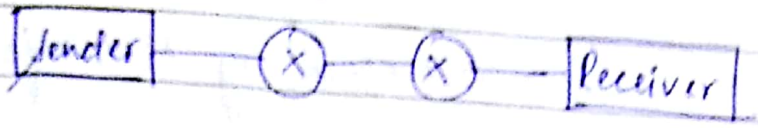
(i) Time Division Multiple Access

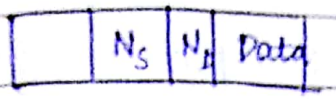
(ii) Frequency Division Multiple Access

(iii) Code "

Scanned by CamScanner

Link Layer Addressing.

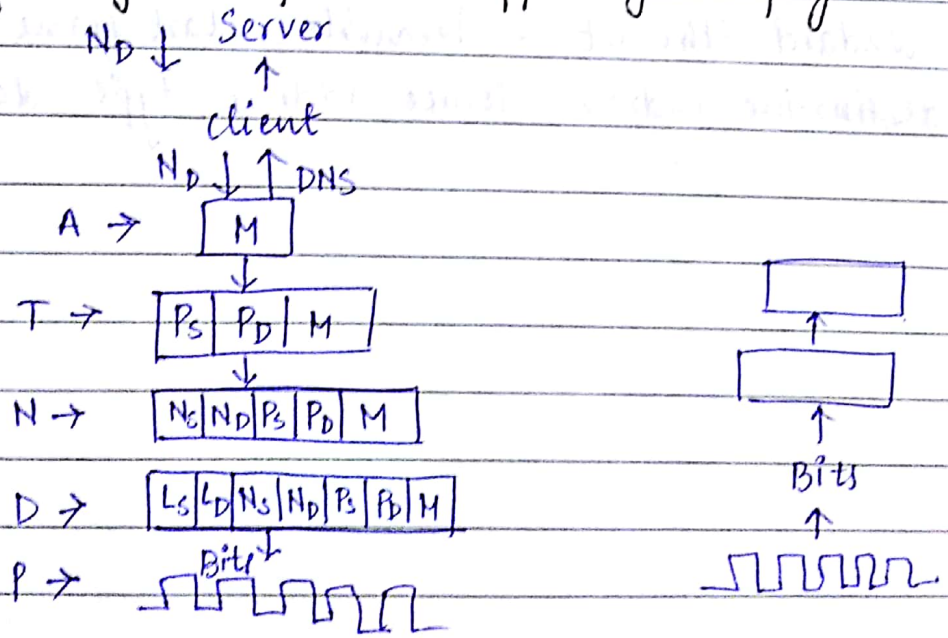




A link layer address is sometimes called as link address, physical address or MAC address. ARP belongs to n/w layer but functions in datalink layer.
ARP maps the corresponding ip address to link layer address.
It has 2 types of messages - Request msg & Reply msg.
ARP packet format include hardware type, protocol type, hardware length, protocol length, source h/w address, destination h/w address, source protocol address, destination protocol address.

ARP Request - From book.
ARP Reply - From book.

→ Process of msg transfer from appl^n layer to physical layer.



Scanned by CamScanner

WIRED LAN'S OR ETHERNET PROTOCOL'S.

Ethernet protocol's are developed by Metcalfe and Bogas in 1970.
From then ethernet LAN's have been developed in different phases. The various generations

(i) Standard Ethernet (10 mbps)
(ii) First Ethernet (100 mbps)
(iii) Gigabit Ethernet (1 gbps)
(iv) 10 Gigabit Ethernet (10 gbps)

} Study short notes from book.

IEEE Project 802 enable intercommunication among equipment with a variety of manufacturer.
It divides the datalink layer into 2 sub-layers –

(i) Logical Link control
(ii) Media Access Control

The framing is handled by logical link control and media access control.

(i) Standard Ethernet – Preamble, start frame delimiter, destination address, source address, type, data, CRC.

Scanned by CamScanner