3credit

15/07/2024

CN

* Requirement of a traditional network?-
1. Two or more entities 2. commodity/information
3. System

→ Traditional Network is a system that carries info./commodities b/w two or more entities
→ Computer Network is a system that carries information b/w two or more entities in the form of electromagnetic wave or electrical signal.

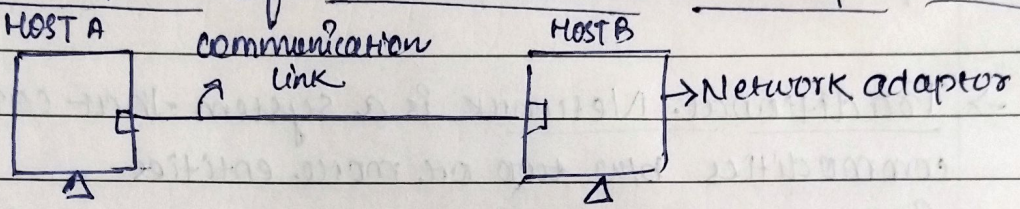
Network	→	Computer Network
→ Vehicle/Driver	→	packet/payload
→ Address of the receiver	→	IP address
→ Route to destination	→	Routing algorithm
→ Intersection	→	Switch/router
→ Traffic jam	→	Network congection
→ Traffic signal	→	flow control
→ Accidents [injury]	→	Packet collision [Packet loss]

* Packet is the small segment of large message.
* IP Address is the unique numerical identifiers given to the device connected to the internet.
* Routing algorithm is responsible for route selection
* Switch connects multiple devices to create a network, a router connects multiple switches to form even large network.
* A hub works in physical layer & switch works in data network layer.
* A hub is a networking device that connects multiple PC, to a

__/__/____

Single network, whereas a switch connects multiple device on a single computer network.

16/7/24 **Requirements for communication in a computer Network.**



* For the communication in computer we required both hardware & software as follows:-

Hardware

1) End devices (any devices)
2) communication link { wireless / wired
   → wired comm. (twisted pair, cabel, fiber optics)
   → wireless comm. (wifi)
3) Network interface control ~~car~~ card (NIC)
   wired (ethernet)
   wireless (wifi)
4) Switches / Router

Software

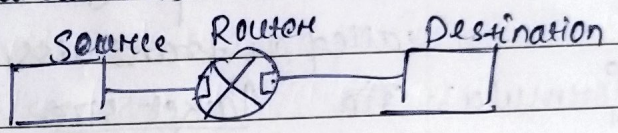
1) Applications

Goals

1) ~~while designing a network~~ 1) Efficient
   → minimum delay → minimum cost → min. packetloss
2) Robust (Strong enough to handle failure & errors)
3) Scalable (expandable)

__/__/__

* Means To Achieve Goal
→ By efficiency designing the hardware and software we can achieve the network goal
→ The Metricies to check whether the goal is achieved or not-
1) Throughput (Datarate / bandwidth)
2) Latency (delay)
3)



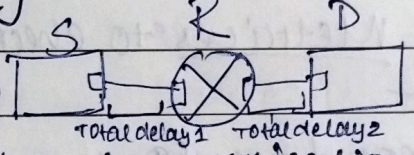
1) Processing Delay → When the sender sends the packet to the router, the router will inspect the packet to check whether the data is correct or corrupted.
→ If the data is corrupted because of packet collision then, router will drop it.
→ If the data is correct, the router will forward it. So, the delay is introduced in the network by the router for the inspection & this delay is termed as processing delay.

2) Queuing Delay → Everey NIC card is associated with a buffer.
→ Suppose the NIC card is having capability of 1MBPS but it is receiving 10MB of data per unit time.
→ If it doesnot have the buffer then first 1MB of data will be sent and rest 9MB of data will be lost in a unit time.
→ Suppose the data is travelling from one NIC card to another, and at that time already some packets are there in the buffer then, the sender has to wait in the

-> Packet consisting headers & data
Bandwidth = data rate

queue for being processed. That introduces a delay in the network (waiting time) in the queue, which is termed as queuing delay.

20/7/24 3) Transmission Delay :- The time taken to send the whole packet into the communication link is called as transmission delay



formula :- Packet size / Bandwidth

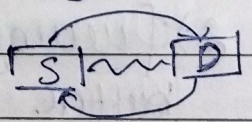
4) Propagation Delay :- Time taken by any bit to travel from one end to other end is called as propagation delay.

-> Propagation delay = distance b/w two ends / Speed of light in that medium

Speed of light in vaccum = 3×10^8 m/s
Speed of light in optical fiber optic = 2.05×10^8 m/s

* Total delay = processing delay + queuing delay + Transmission delay + Propagation delay (oneway)
* overall Total Delay = Total delay 1 + Total delay 2

-> Two way delay -> RTT (Round Trip Time)



Q// What is the propagation time if the distance b/w the two points is 12000km. Assume the propagation speed to be 2.4×10^8 m/s in that cable.

Ans> Distance = 12000km = 1.2×10^6 m
Speed of light = 2.4×10^8 m/s

Propagation time = $\frac{\text{distance b/w two ends}}{\text{Speed of light}}$

$= \frac{12 \times 10^6}{2.4 \times 10^8} = \frac{12}{2.4 \times 10^2} = \frac{12}{240} = \frac{1}{20} = 0.05$ second

or 50 milli second

Q11 If the message is 1KB, bandwidth is 1MBps, Calculate the transmission time in millisecond.

Ans) Packet size = 1KB = 10^{*3}

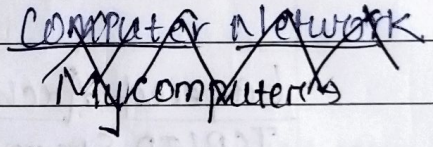
bandwidth = 1MBps = 10^{*6}

Transmission time = $\frac{\text{Packet size}}{\text{Bandwidth}} = \frac{10^{*3}}{10^{*6}} = \frac{1}{10^{*3}} = 0.001$

= 1 ms

22/7/24 Functionalities :- It is required to make the communication possible in a computer network

e.g., Postal System



1) Hostel → Student
2) Student → Genereates letters
3) Letter → Information
4) Office boy → Multiplexing / Demultiplexing.

Multiplexing :- collects the letters from multiple student and post it in the post box.

Demultiplexing :- Delievers letters to the multiple students once letters are received from the postman.

5) Postman { deciding the Path / hop to hop communication
6) Vehicle → physical transmission

__/__/____

Computer Network

1) My computer → Application programs
2) Application program → Generates message (Packet)
3) Packet → Information
4) Transport software → Multiplexing & Demultiplexing
Multiplexing :- Gathering information from multiple applications and sending it to the receiver.
Demultiplexing :- delivering message at the receiver end to the correct application layer.
5) Decides the path → Routing algorithm
Hop to hop communication → Switch / Router
6) wire → cables wireless → (Responsible for physical transmission of data in the form of electromagnetic wave)
wireless → data transfer through air

Layered Architecture / Model

TCP/IP Stack (5 Layers)

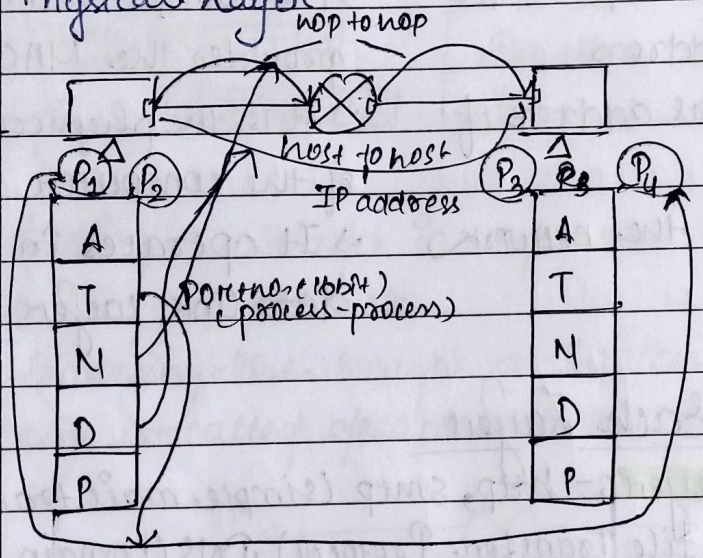
1. Application Layer → Message generation
2. Transport Layer → Multiplexing / Demultiplexing
3. Network Layer → Routing with help of routers & switches
4. Datalink Layer → Hop to hop communication
5. Physical Layer → physical transmission of data in the form of electrical signal. (bit to signal conversion is called encoding) (sing to bit conversion is called decoding)

__/__/____

OSI Model (7 model) [Open System Interconnection]

1) Application Layer
2) Presentation Layer → look & feel of the messages
3) Session Layer → opening, closing & managing session
4) Transport layer
5) Network layer
6) Datalink layer
7) Physical layer

23/7/24



Application layer → Msg generation (processes)

* Application layer → Message generation (Processes run in this layer)
* Transport layer → Process-process comm^n, Multiplexing/demultiplexing.
* Network layer → host to host comm^n, Routing.
→ host will be identify as IP address
IP address size in IPv4 → 32 bits, IPv6 → 128 bits (16 byte)
* Datalink layer → to perform hop to hop comm^n we use MAC address, it is attached to NIC card, which is a 12 digit hexadecimal number.
MAC (Media Access Control)

* Physical layer → encoding & decoding

* IP Address V/S MAC Address

→ It stands for Internet Protocol Address
→ It is either a 4 byte (IPV4) or a 16 byte (IPV6)
→ Internet service provider provides IP address
→ It is the logical address of the computere
→ It operates in the network layer

→ It stands for Media Access control
→ It is a 6 byte hexadecimal address
→ NIC card's manufacturer provides the MAC address
→ It is the physical address of the computer
→ It operates in the data link layer

Protocols Of Each Layer

1) Application Layer :- http, smtp (simple mail transfer protocol), FTP (File Transfer Protocol), DNS (Domain Name System), DHCP (Dynamic Host configuration Protocol)
2) Transport Layer :- TCP (Transmission control Protocol), UDP (User Datagram Protocol) → connection oriented → connectionless
3) Network layer :- IP (Internet Protocol)
4) Datalink layer :- Ethernet Protocol (wired), 802.11 (wireless)
5) Physical Layer :- 10 Base T (It is representing baseband of 10 MBps), OFDM (Orthogonal Frequency Division Multiplexing)

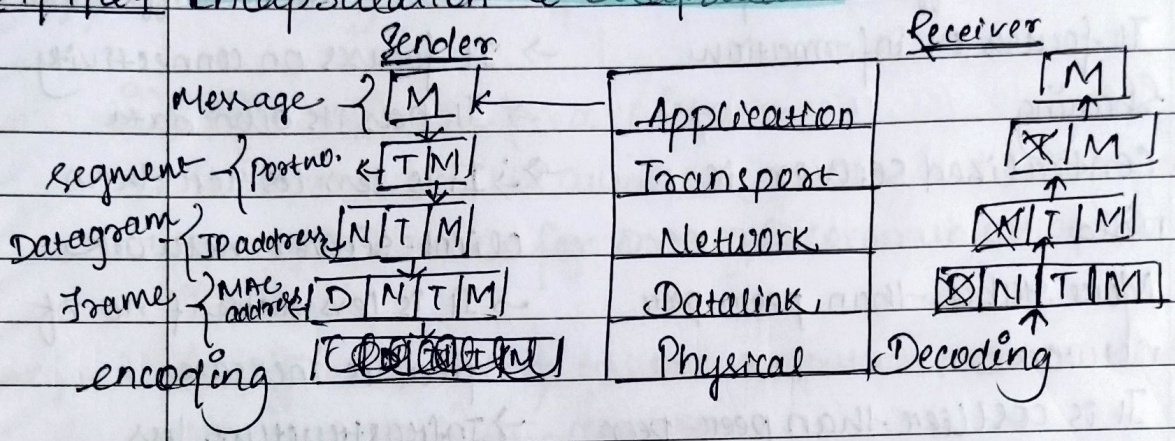
Baseband :- The type of signaling used is digital
Broadband :- The type of signaling used is analog.

* T is the distance travelled by the signal

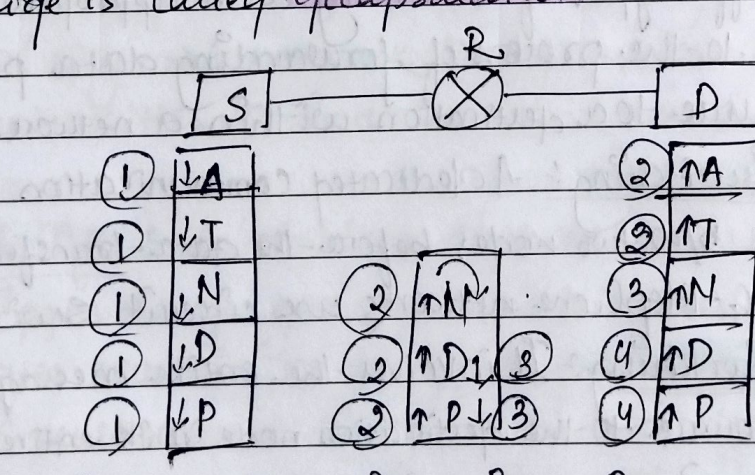
__/__/____

* In TCP/IP stack the router is having Network, Datalink, & Physical layer
* Switch is having two layer; Datalink & physical layer

27/7/24 **Encapsulation & Decapsulation**

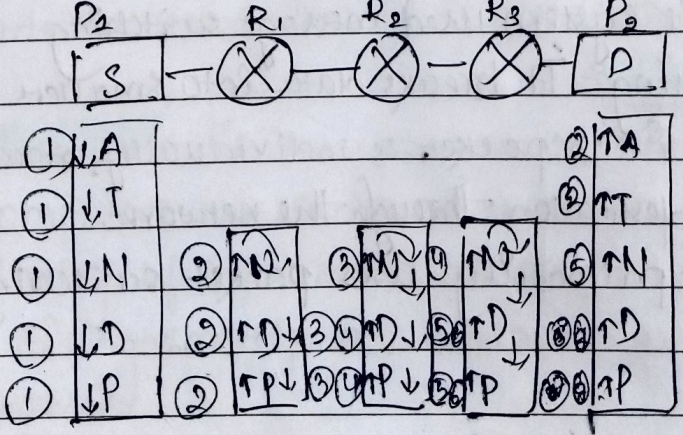


→ Adding the header in sender side at the respective side is called encapsulation.
→ Removing the header at the respective side in the receiver side is called decapsulation



Layer	No. of units
A	2
T	2
N	3
D	4
P	4

eg.,



A	2
T	2
N	5
D	8
P	8

__/__/____

Q// Diff^n b/w client server model & peer-to peer model

Client server model	peer-peer model
→ In this network client & server are differentiated	→ In this network clients & server are not differentiated
→ It focuses on information sharing.	→ It focuses on connectivity
→ centralized server is used	→ It has its own data
→ More stable than peer-peer network	→ It is less costlier than client-server network
→ It is costlier than peer-peer network	→ It is less stable if no. of peer is increase
→ infrastructure oriented	→ Infrastructure less

Q// What is the concept of switching in computer networks. Discuss diff^n types of switching with appropriate example

Ans> It refers to the process of forwarding data packets from a source to a destination within a network.

Types:- 1) Circuit Switching:- A dedicated communication path is established b/w two nodes before the data transfer begins.

eg.: Traditional telephone networks use circuit switching

2) Message Switching:- It involves the entire message being sent from the source to the destination node in its entirety.

eg.: Early e-mail system used message switching

3) Packet Switching:- It breaks data into smaller packets for transmission. Each packet is individually routed from the source to the destination through the network.

eg.: The Internet primarily uses packet switching.

__/__/____

Types of Network

1) **PAN** :- Personal Area Network
:- It allows devices to communicate and share data directly with eachother using technologies like bluetooth or USB
eg :- connecting a smartphone to a laptop via bluetooth

2) **LAN** :- Local Area Network
:- It covers a small area like a single building or campus, connecting devices for internal communication & resource sharing
eg :- An office building where computers, printers & servers are connected to share resources.

3) **MAN** :- Metereopocitian Area Network
:- Covers a city or large campus linking multiple LANs to enable data and resource sharing over a larege area
eg :- A city-wide network, linking various local business and universities to share internet access and resources

4) **WAN** :- Wilde Area Network
:- Spans large geographical distances, connecting LANs across cities, countries or globally via public or private networks.
eg :- A multinational cooperation with offices in diff^{n} countries interconnected through a WAN to share data & resources

5) **Internet** :- It is a worldwide network of interconnected computers and devices that allows communication and sharing of information globally.
eg :- Using smartphone to browse websites like Google or Facebook

29/7/24

__/__/____

Hybrid architecture :- It is a combination of client server & peer-to-peer architecture.

eg., Installation of whatsapp.

Network Topology :-

Q) What do you mean by network topology? Discuss about following topology : 1) point-to-point 2) Bus topology 3) Star topology 4) Ring topology 5) mesh topology 6) tree topology

Ans) It is the arrangement of nodes and connection in a network. It determines how devices are linked & how data flows

1) Point to point topology :- It connects two device directly.

eg., A direct cable link b/w a computer and a printer

2) Bus topology :- All devices are connected to a single central cable. :- It is unidirectional

eg., Ethernet using a linear bus topology where each device connects to a main cable.

3) Star topology :- All devices are connected to central hub or switch.

eg., LAN use star topology where each computer connects to a central switch

4) Ring topology :- Devices are connected in a circular chain, forming a close loop.

eg., Token ring networks where data travels in one direction around the ring.

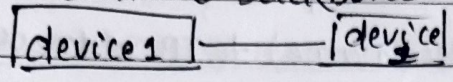
5) Mesh topology :- Each device is connected to every other device in the network.

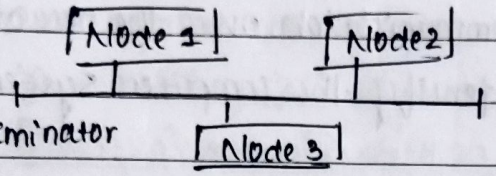
Type :- 1. Full Mesh 2. Partially Mesh

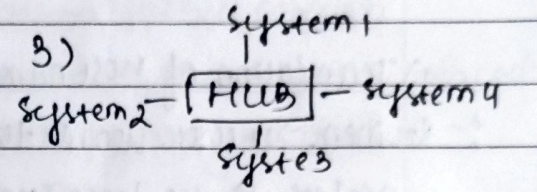
eg.; wireless mesh networks where each node can relay data for other node, improving coverage and reliability.

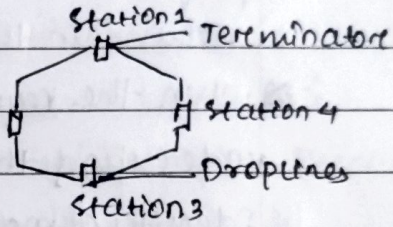
6) Tree Topology :- Devices are arranged in a hierarchical tree structure.

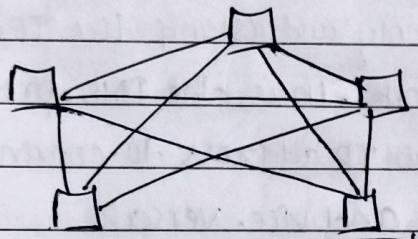
eg.; Large corporate networks in diff² floors or dept - connects to a central backbone.

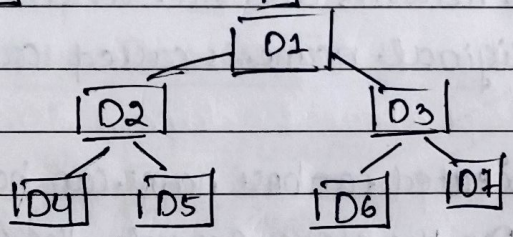
1) 

2) 

3) 

4) 

5) 

6) 

30/7/24 **Application Layer** Unit-02

→ It implements client-server model, peer-to-peer model and hybrid architecture model

→ Socket :- It is an API (Application Program Interface) that'll used for communication b/w application & transport layer. So that the communication will be possible in a computer network

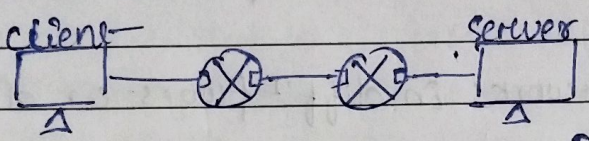
→ Protocol :- It is representing the format and rules for exchanging messages in a computer network.

:- Basically it represents what to send (format), when to send, and

how to act (rules).

Protocols Of Application layer

1) DNS (Domain Name System) :- computers can be identified by the host and the IP address



:- The services provided by DNS protocol :-

1) Translation of host name (domain name) to IP address & vice versa.

:- When, the user want to do a communication over the network, they prefer to use host name to identify the computer system or the machine in the network.

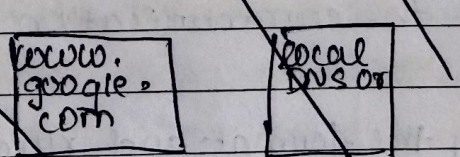
:- When the request is forwarded to the router, the router doesn't understand the host name, it only understand the IP address to identify a machine in a network. Thus, the DNS protocol is invoke to convert the domain name into IP address to continue the communication in the network and vice versa.

2) Host aliasing : Original name is called canonical host name

:- A host with a complicated ~~can~~ host name can have aliases (alternative name), as per the above example, the original hostname is having two aliases.

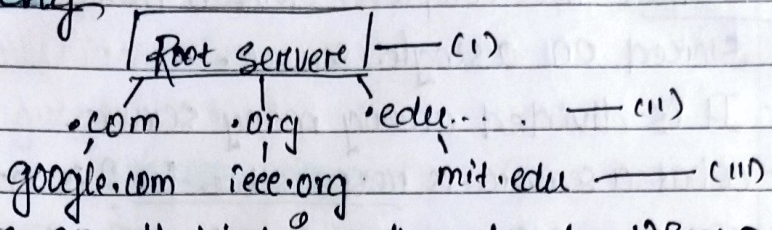
:- The DNS can be evoke by an application to obtain the canonical host name for a supplied alias as well as to obtain IP address of the host.

23/8/24 DNS Query Resolution



3/8/24

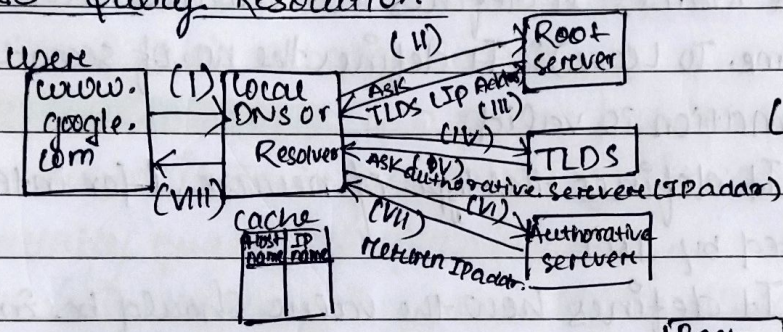
DNS Hierarchy



→ DNS servers are divided into three levels I) Root DNS servers II) Top level domain (TLDS) server III) Authoritative server.

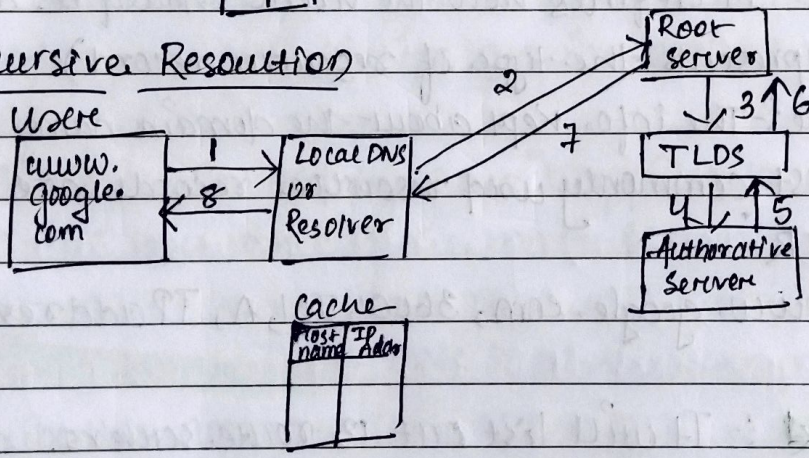
→ There exist 13 route. DNS Root server, strategical placed around the world operated by, 12 diff^n organizations. 10 in USA, 2 in Europe & 1 in Japan

DNS Query Resolution



(Iterative Resolution)

Recursive Resolution



→ ~~Stale Cache~~ It is important to know that once the resolver (Local DNS) receives the IP addr., it will store it in its cache memory, in case it receives another query for google.com, it doesn't have to go through all those steps again. Hence 2 comunications will be required to resolve the query, that is from user to local DNS & local DNS to user.

__/__/____

Zone:- The complete domain name hierarchy cannot be stored on a single server.
:- It is divided among many servers.
:- What a server is responsible for? is called as a zone
:- The zone information associated with a server is implemented as a set of resource record.

Resource Record (RR):- It is a 5-tuple structure as below:
[Domain name, TTL, class, type, value]
I) Domain Name:- It defines the resource record
II) TTL (Time To Leave):- It defines the no. of seconds for which the information is valid.
III) Class:- It defines the type of network. (for internet it is represented by IN)
IV) Type:- It defines how the value should be interepreted (it represents the type of resource record)
V) Value:- The info. kept about the domain name
→ The most commonly used resource records are A, NS, CNAME, MX, PTR
A→[www.google.com, 3600, IN, A, IPaddress]

$dig ↵ :- It will list out 13 route servers.
$dig www.google.com A ↵ :
www.google.com 0 IN A 142.250.182.68
→ Local A resource record will be maintained by authoritative servers, local DNS and TLDs.

A' type record is maintained in IPV4
AAAA " " " " " IPV6

5/8/24

NS Record → It provides the authoratative server names.
:- It stands for Name Server Record
$dig www.google.com NS ↵
google.com. 60 IN SOA ns1.google.com. dns-admin.google.com. 659264433 900 900 1800 60
:- SOA record value marks the begining of the zone information

	Domain name	TTL	class	Type	value
NS Record →	google.com	60	IN	NS	Authoratative Server Name
CName →	google.com	29	IN	CName	Canonical Host Name
MX →	google.com	24	IN		

Mx Record (Mail exchange Record)

3) Mail Server Aliasing :- If a person has an account with gmail then his mail Id will be abc@gmail.com which one is partially qualified domain name.
:- The host name of the gmail server is smtp(simple mail transfer protocol) smtp.gmail.com, which is a fully qualified domain name.
:- DNS can be invoked by a mail applications to obtain the canonical host name of the mail server for a supplied alias mail server as well as the IP addr. of the host.
4) ~~load~~ Distribution :- DNS is also use to perform load distribution among replicated servers.
:- Busy websites as google.com are replicated over multiple servers and with each server running on a diff^n end system and having a diff^n IP addr.
:- For replicated web servers a set of IP addr. is thus associated with one ~~cname~~ canonical host name.
:- DNS distributes the traffic among all replicated servers.

PTR Record → IP addr 20 IN PTR host name

__/__/____

PTR Record → It stores the host name for the IP addr.

6/8/24 → DNS supports client server architecture on CS paradigm.

→ DNS operates over UDP (User Datagram Protocol) for translating host name to IP addr and vice versa.

→ But in case of transferring zone info. from one server to another (which is greater than 512 bytes), DNS operates over TCP.

→ DNS uses the port number 53.
Well known port number range 0-1023

→ ~~Stateful~~ HTTP (HyperText transfer Protocol) :- It is the foundation of www (world wide web) & it is use to load web pages using hyper text links.

:- Web pages are viewed using a program called browser

:- Every web page contains base HTML & it includes several reference objects like other html file, audio, video etc.

:- Each object is addressable by an URL (Uniform Resource Locator) eg :- http://kiit.ac.in/images/logo.gif.

:- ~~It is a protocol~~ It is an application layer protocol used for fetching resources such as html document.

:- It works as a request-response protocol b/w a client and servere to enable communication

:- In this case the client will be web browser & the server will be web server. Hence, it supports client server paradigm.

:- It uses the port number 80 ~~http achieves client server authentication, confidentiality & integrity~~ https

confidentiality & integrity.

HTTPS :- It uses the port number 443

:- It achieves client server authentication, confidentiality & integrity

:- There exists two popular version of HTTP :-

~~i) http 1.0~~ ii) ~~http 1.1~~

i) **http 1.0 (non-persistent)**

→ each object will use a new connection to be downloaded. Thus it is secured. Ex

→ eg., bank transaction

ii) **http 1.1 (persistent)**

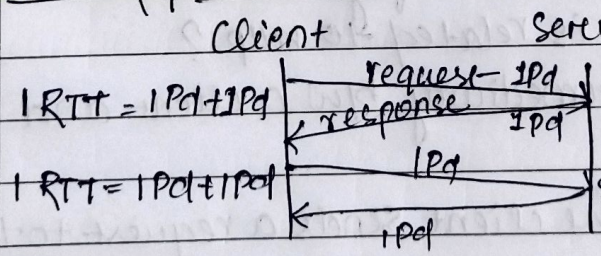
→ same tcp connection will be used to download all objects, thus it is faster but not secured

→ eg., ecommerce

:- HTTP operates over TCP, if the amount of information exchange b/w client & server is greater than 512 bytes

:- It operates over UDP, if the amount of information exchange b/w client & servers is less than 512 bytes

HTTP Response Time



1 RTT = 1Pd + 1Pd

1 RTT = 1Pd + 1Pd

Pd → propagation delay

→ To download one object we required 2RTT

Imp → If we want to access a webpage by default one base HTML file will be downloaded along with other embeded object

Q11 Suppose we want to download a webpage embeded with 5 objects. What will be the overall response time to display the webpage fully using non-persistent &

persistent connection ?

Ans) In this case response time for non-persistent sequential connection.

1 base limit+5 embeded object = 6 objects

RT Non-persistent Sequential → 2RTT + 5 * 2RTT = 12 RTT

RT " parallel → 2RTT + 2RTT = 4RTT

RT Persistent sequential → 2RTT + 5RTT = 7RTT

RT " parallel → 2RTT + 1RTT = 3RTT

Q) What are the diff^n types of webpages ?

Ans) i) Static :- content remains the same unless manually updated eg., personal blogs

ii) Dynamic :- Content changes based on user interaction or other factor eg., social medias

iii) Active :- Allow user interaction, often through forms, games or application. eg., facebook page

Q) What is proxy server? Briefly discuss its working principle & how it is related to http ?

Ans) It acts as an intermediary b/w a client and the internet.

Principle :- 1) Client Request :- The client sends a request to the proxy server.

2) Proxy Processing :- The proxy server forwards the request to the destination server

3) Server Response :- The destination server sends the response back to the proxy server

4) Proxy Response :- the proxy server sends the response to the client

__/__/____

Relation to HTTP :- Proxy servers often handle HTTP requests, providing functions like caching, filtering & anonymity by modifying HTTP headers or blocking certain content based on the request.

10/8/24 Simple Mail Transfer Protocol (SMTP)

→ Connection establishment is known as handshaking.

1st phase :- Handshaking (connection establishment)
2nd phase :- Mail-transfer
3rd phase :- Close connection

→ SMTP uses TCP for reliable transmission of email messages
→ It operates on port number 25
→ The working principle of SMTP comprises of three phases

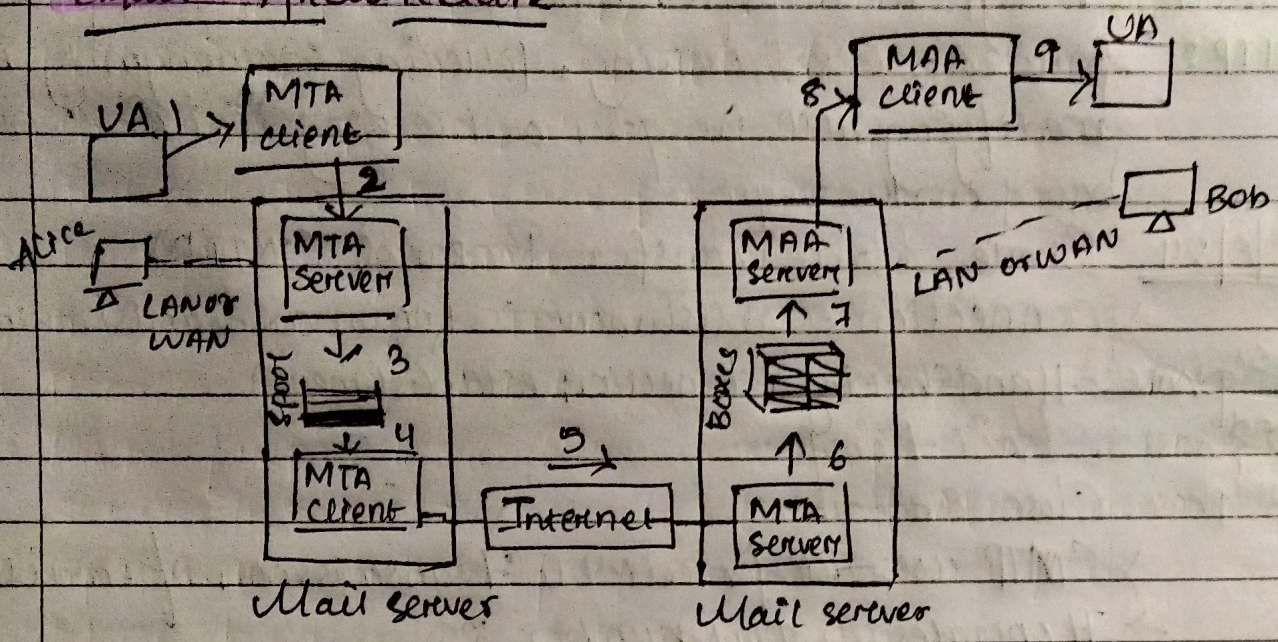
Electronic Mail (E-mail) :- It's architecture uses three measure components :-

1) User Agent (UA) :- It is a local program that composes, reads, replies and forward e-mail ~~process~~ messages
:- It can be text base or GUI base
Sender → Mail Transfer Agent (MTA)
Reader → Mail Access Agent (MAA)

2) Mail server :- It is composed of (i) inbox for users
(ii) message queue will be used for outgoing messages.

3) SMTP :- It is use for sending e-mail messages b/w mail servers.
:- It is of two types :-
i) Sending Mail Server (Client)
ii) Receiving Mail Server (Server)

Email - Architecture



Scenario: Alice sends message to Bob

1) Alice uses UA (User Agent) to compose message and set the "to" field value to bob@gmail.com
2) Alice's UA sends message to her mail sensor; sending mails is a PUSH operation (SMTP or HTTP)/(Microsoft Outlook or Browser); message placed in a message queue.
3) Client side of SMTP opens TCP connection with Bob's mail server.
4) SMTP client sends Alice's message over TCP connection
5) Bob's mail servers places the message in Bob's mailbox (inbox)
6) Bob invokes his user agent to read message; Receiving mail is a PULL operation (POP3, IMAP, HTTP)
   - either one is used to read if we use outlook or Thunderbird.
   - If web browser is used to read

POP3 → Post Office Protocol Version 3.

Transport Layer

UDP	TCP
→ connection less	→ connection oriented
→ It is faster	→ It is slower as compared to UDP
→ Packet oriented	→ stream / byte oriented.

* UDP (User Datagram Protocol)

→ Advantage of UDP :- 1) faster communication 2) Less overhead per packet

header | Payload

→ UDP header size is of 8 bytes whereas TCP header size is 20-60 bytes

12/08/24

UDP Segment Format

8 byte ← header | Payload / data

4 bytes ←	Source port no. (16 bits)	Destination port no. (16 bits)
4 bytes ←	Total length (16 bits)	Check sum (16 bits)
	Variable length data	

→ If the sender wants to communicate with the receiver, then destination port number will be required.

→ If the receiver wants to communicate with the sender, then source port number will be required

→ Hence, to support bi-directional communication. UDP segment is having source port number = 16 bits and destination port number = 16 bits.

→ Total length represents the length of the segment. The range of total length will be $0 - 2^{16} = 0 - 2^{15} / 0 - 65535$. The range of source port number & destination port number will be $0 - 2^{15} / 65535$.

→ The length of the payload/data can be calculated by Total length - header size = Total length - 8bytes

Checksum :- It is an error correction mechanism to check whether the received data is correct or corrupted.

:- It is optional for IPV4.

:- It is mandatory in IPV6

:- It's calculated for both header & data part

:- For header part to calculate checksum, first we need to ~~set~~ set all 16 bits of checksum bit to 0. ~~Aft~~ After calculating, update the checksum field with the calculated checksum.

Steps to calculate checksum:

1) Divide the whole segments into 16 bits chunks
2) Let us consider 64 bit header & 64 bits payload.
3) 64 bit payload for a segment, hence total 128 is segment size
4) Divide this 128 bits into equal number 16 bits chunks (8 chunks each of 16 bits)
5) Add all 8 chunks using 1's compliment addition to yield final sum.
6) Compliment (0→1 & 1→0) the final sum to get the checksum of 16 bits.
1) At the receiver end, receiver will perform all steps to find out the final sum of the received data.
2) Then the receiver will add the calculated final sum and received checksum
3) If the result of the addition is having all one, then the data is correct, else the data is corrupted.

eg.) For simplicity, let us take ~~8~~ three 8 bits chunks. Then first chunk = 11001100 third chunk = 11110000
Second Chunk = 10101010

__/__/____

Ans) adding first & second chunk

```
  11001100          01111010
+ 10101010        +        1
------------      ----------
101110101 0       01111011
```

adding 01111011 with third chunk

```
  01111011          01000111
+ 11110000        +        1
------------      ----------
100101011         01001000
```

Final sum = 01001000

13/8/24 Q) Checksum: 1st chunk = 10100001 2nd chunk = 01010110
3rd chunk = 11001100

A)

```
1st chunk   10100001
2nd chunk + 01010110
            --------
            11110111
3rd chunk   11001100
            --------
            (1)11000011
                   + 1
1's complement -------
            11000100   Final sum
            00111011   Check sum
```

Q) Suppose the receiver receives the data as follows:
10111000 01010110 11001100

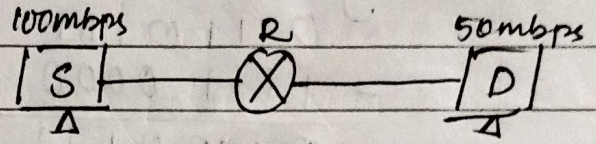
```
  10111000          00001000
+ 01010110        + 11001100
------------      ----------
(1)00010111       11010100   Final sum
                  00101011   checksum
+        1
------------
00001000
```

```
  00111011
  11010100
------------
(1)00011111
         + 1
------------
00010000
```

∴ The data is corrupted

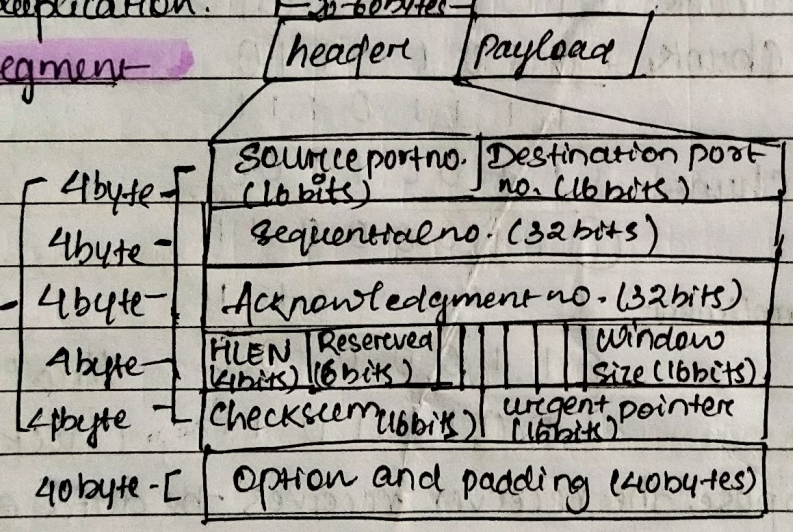
__/__/____

* TCP : Process-to process communication
:- Multiplexing & demultiplexing :- Connection oriented
:- Stream/byte oriented. :- Reliable
:- The realiability in TCP is achieved by
(i) Connection Oriented architecture
(ii) Achieving flow control
(iii) congestion control
(iv) error control



→ Flow control :- synchronizing speed of the sender and receiver
→ Congestion control :- synchronizing speed of the network
→ error control :- This mechanism tells about packet loss/corruption/duplication. how to handle

* TCP segment



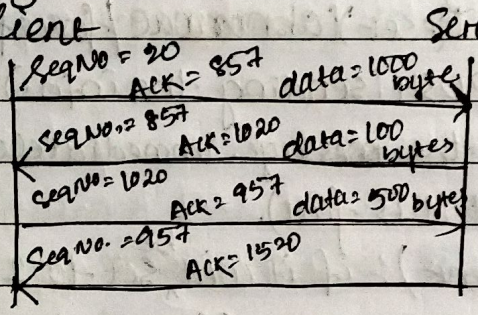
→ Source & destination port no. are use for bidirectional comm° in TCP.
→ Sequence number is 32 bit field defines the no. assigned to the first byte of the data content in the segment
→ TCP is stream/byte oriented protocol. hence, to ensure connectivity is to each byte to be transmitted is numbered. using sequence number
→ The sequence number tells the destination which byte in the sequence is the first byte in the segment.

17/08/24

↳ During connection establishment each party uses a random number generator to create an initial sequence no. (ISN) which is usually different in each direction

Acknowledgement Number (32 bit) :- This will define the byte number that the receiver of the segment is expecting to receive from other party.

:- If the receiver of the segment has successfully received byte no. x from the other party, it returns x+1 as the acknowledgement number



~~HLen~~

HLEN (4 bits) :- Header Length.

:- This 4 bit field indicates the number of 4 byte word in the TCP header.

:- The length of the header in TCP can be b/w 20-60 bytes.

:- Therefore, the value of this field is always b/w 5 (20/4) to 15 (60/4), that means the header length will always be multiple of 4 to make it fit into HLEN which is of 4 bits So, if the header length is 20 byte then HLEN will store 5. & if the header length is 60 byte the HLEN will store 15.

Window Size (16 bits) :- It represents the receiver window size (RWND) to achieve flow control. The maximum size of the window will be $2^{15} = 65535$ bits.

Checksum :- It is used for intigrity check and it is mandatory for TCP header.

Flag bits / control bits :- | URG | ACK | PSH | RST | SYN | FIN |

-> RST, SYN, FIN flag bits are used for connection management.

- Connection management means connection establishment, once the connection is established data transfer, after data transfer ~~teardown~~ teardown occurs once the connection is established.

-> SYN (Synchronizing Sequence Number), FIN (Connection termination), RST (Reset (abnormal / forceful termination).

-> PSH flag means PUSH (sending the info.). This flag is useful in sending the message immediately (no need to wait in the buffer until it is full).

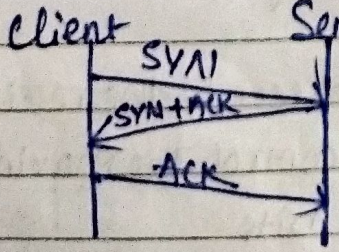
-> ACK (Acknowledgement) :- if it will be set to 1 that means acknowledgement field is there, if only data field is there then it'll be set to 0.

-> URG (urgent flag) :- Suppose the data was already sent and we need to call the abort, then that case abort information should go before the sent data ; that case abort is the urgent data and URG flag should be set to 1.

Urgent Pointer :- It points to the last byte of urgent data

- If the urgent flag is set to 1, then only the urgent point will be populated.

19/8/24 Connection Establishment (3 way handling)



-> ACK will consume 0 seq. number

-> SYN will consume 1 sequence number byte (1 byte).

-> SYN will consume 1 seq. number

ACK → 0 byte will be assigned to the sequences no. of ACK as no. data is associated with it during the connection establishment.

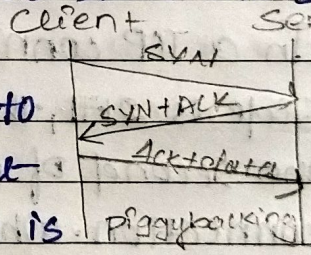
→ but for the third connection, data can be transported along with ACK, which is called as piggybacking.

→ If the data is piggybacked on ACK then ACK sequence no. will be dependent on the data.

For eg.; Suppose the piggyback data length is 100 bytes the ACK sequence no will be 100

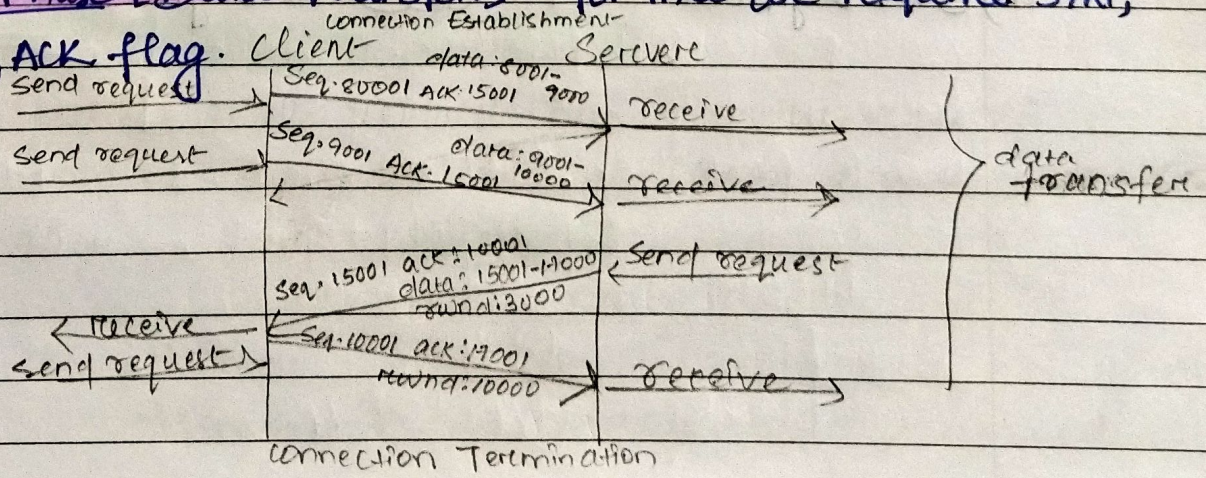
→ The process starts with a servevere. The servevere program thus its TCP that it is ready to accept a connection. This is called a request for a passive open.

→ The client program issues a request for an ~~passive~~ active open. A client that wishes to connect to an open servevere tells its TCP ~~that wishes to~~ that it needs to be connected to that particulares servevere. TCP can now start the 3way Handshaking process.



SYN → One byte will be assigned to the sequence no. of SYN so that client can known that whether the SYN is received by the servevere not. (byte oriented)

20/8/24 2nd Phase [Data Transfer]:- for this we require SYN, PSH, ACK flag.

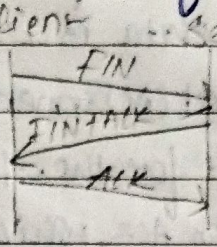


Third phase (Connection Termination):- It is of 2 types

(i) Graceful (FIN)

* 3way Handshaking

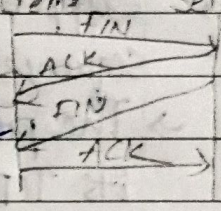
:- The graceful connection teardown is also known as 3 way handshaking.



In the case where client and server finish their work at the same time.

* 4 way Handshaking

:- Half close scenario whoever is initiating half/passive close the connection teardown process by sending FIN request, it'll be in half closed state.



:- In half close state it is not allowed to send further data but it can receive data and send the acknowledgment

:- Half close scenario is a 4 way handshaking process.

Q) In a TCP connection, the initial sequence no. at the client side is 2711, the client open the connection and send 3 segment the second of which carries 1000 byte of data and close the connection. What is the value of sequence no. in each of the following segment sent by the client

(i) SYN segment (ii) Data segment

24/8/24

__/__/____

Abnormal / forceful connection Teardown

↳ RST flag is used in forceful / abnormal connection teardown

Scenario for Abnormal Teardown

1. TCP at one end may deny the connection request
2. May abort an existing connection.
3. May terminate an idle connection

Q1 To make the initial sequence numbers a random number most systems start the counter at 1 during bootstrap and increment the counter by 64000 every half second. How long does it take for the counter to wrap around.

Ans) Seq. number = 32 bit = $2^{32-1} = 2^{31}$ (max value)

The counter will be incremented in 1 sec = $64000 \times 2 = 128000$

∴ Time taken by the counter to wrap around = $\frac{2^{31}}{128000} = 16777.216 = 4.66$ hr

Q2 TCP is sending data at 1MB/sec. If the sequence number starts with 7000 how long does it take before the sequence number goes back to zero.

Ans) Seq. number = 7000

Time taken = $\frac{2^{32} - 7000}{1MB} = \frac{2^{32} - 7000}{10^6}$ = 4295 seconds

ARQ (Automatic Repeat Request)

↳ TCP uses several protocols based on the types of environment that is the channel can be either noiseless or noisy.

Channel

Noiseless	Noisy
↳ simple	↳ stop & wait ARQ
↳ Stop & wait	↳ GBN protocol ↳ selective Repeat

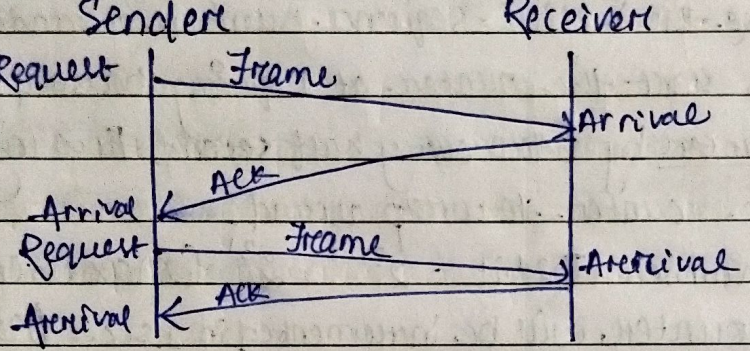
∴ RTT = 2 × PD (PD → Propagation Delay)

Simple Protocol :- It doesnot achieve flow control and errore control.

∴ It is also known as connection less protocol

∴ This channel is ideal

Stop & wait Protocol :- Simple protocol + flow protocol



∴ Implement one's flow control

∴ It is connection oriented

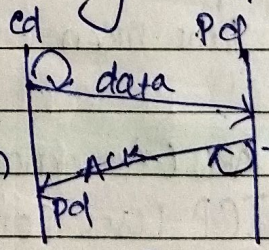
Imp ∴ Stop & wait protocol is very inefficient, if our channel is thick (larger bandwidth) & long (longer RTT)

Imp ∴ Bandwidth delay product = Bandwidth × RTT

∴ The channel utilization or link utilization = $\frac{\text{Packetsize}}{\text{Bandwidth delay product}}$

∴ The channel / link utilization in networking is represented by a symbol ().

∴ Problem associated with stop & wait protocol is poor link utilization



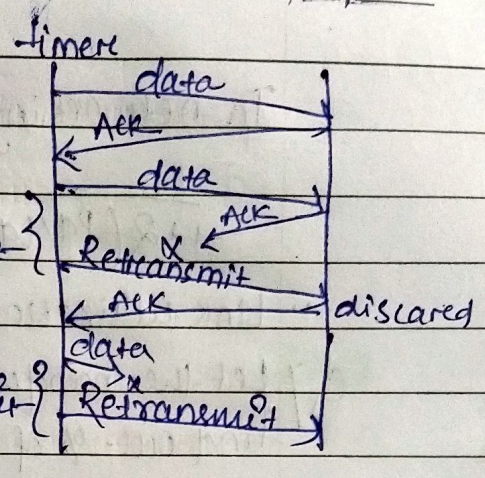
How to find link Utilization () $[t_{dACK} = 0]$

∴ Total end to end delay = $t_d + P_d + t_{dACK} + P_d$

$= t_d + 2P_d$

$\eta = \frac{t_d}{t_d + 2P_d} = \frac{t_d / t_d}{t_d / t_d + 2P_d / t_d} =$

2) Go Back N (GBN) Protocol:-



:- The major problem associated with stop & wait protocol is poor link utilization

:- How to improve efficiency?

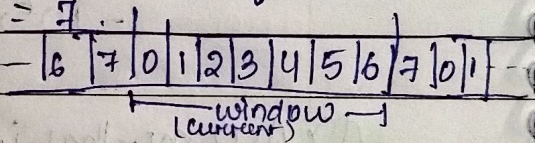
Imp → By introducing the concept of pipelining, we can improve the channel utilization

* Pipelining is implemented using sliding window

:- In this GBN ARQ protocol, which is a sliding window protocol uses send window size $2^m - 1$, where m is the no. of bits required to represent the sequence numbers. Its receive window size is 1.

If $m = 3$, then send window size is 7 (range of seqno. 0–7)

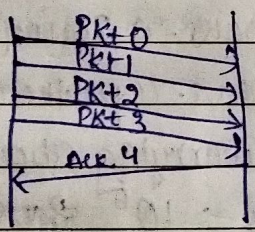
Send window size $= 2^m - 1 = 2^3 - 1 = 7$.



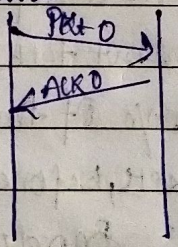
* 2 Types of Ack:

1. Cumulative
2. Selective

eg.



eg.,



:- GBN protocol uses cumulative Ack.

:- Sf pointer points to first outstanding bit

:- Sn pointer points to next bit

:- If Sf and Sn points to same bit then there is no outstanding bit

Q) In GBN Protocol the send window size should be less than equal to $2^m - 1$. It should not be greater than $2^m - 1$. Why

Selective Repeat Protocol:-

If $m = 2$ Range of Seq. number $= 0 - 2^m - 1 = 3$

SW size : RW size : 2^{m-1}

∴ It uses selective ACK.

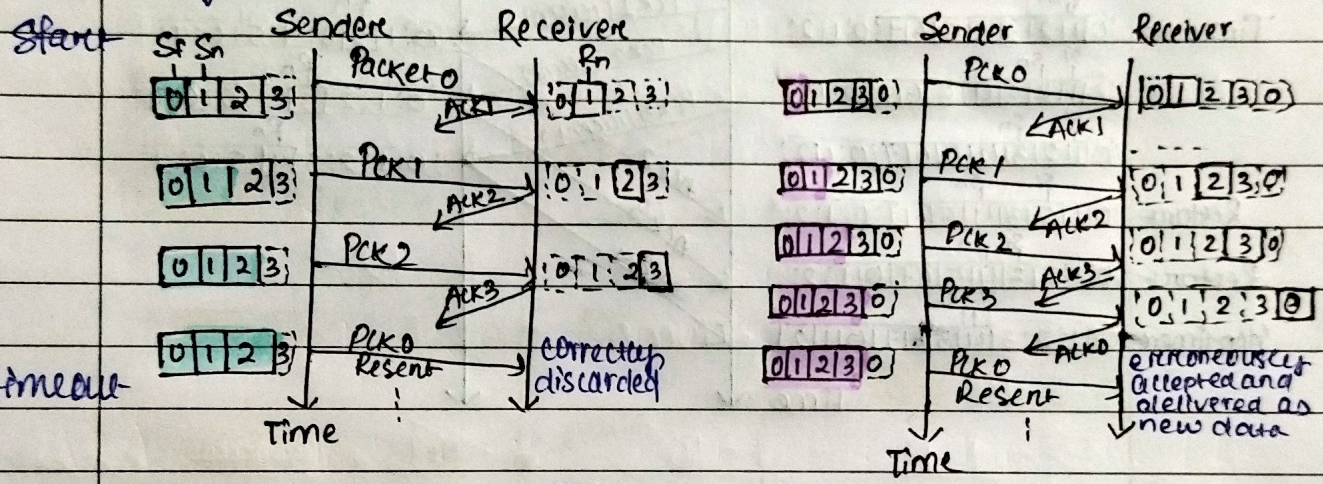
~~ACK~~

Sender Receiver

3|6|24

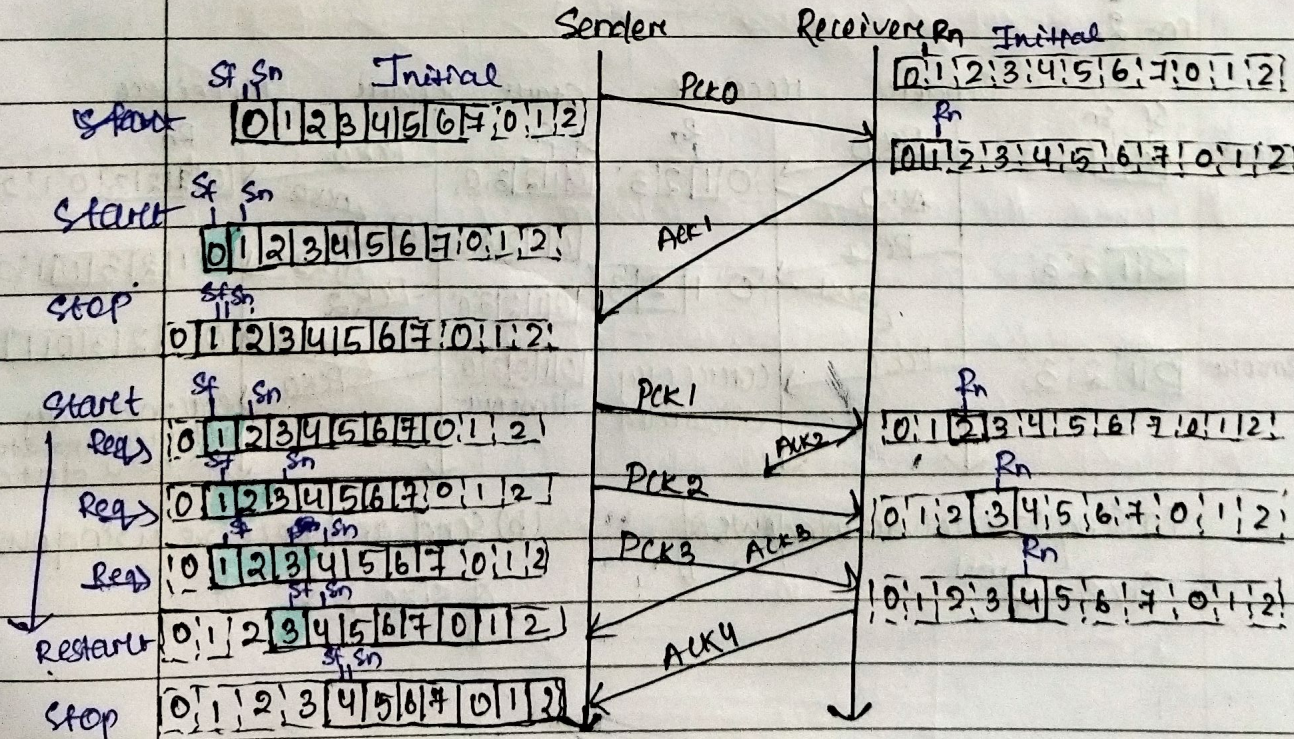
Go-back-N

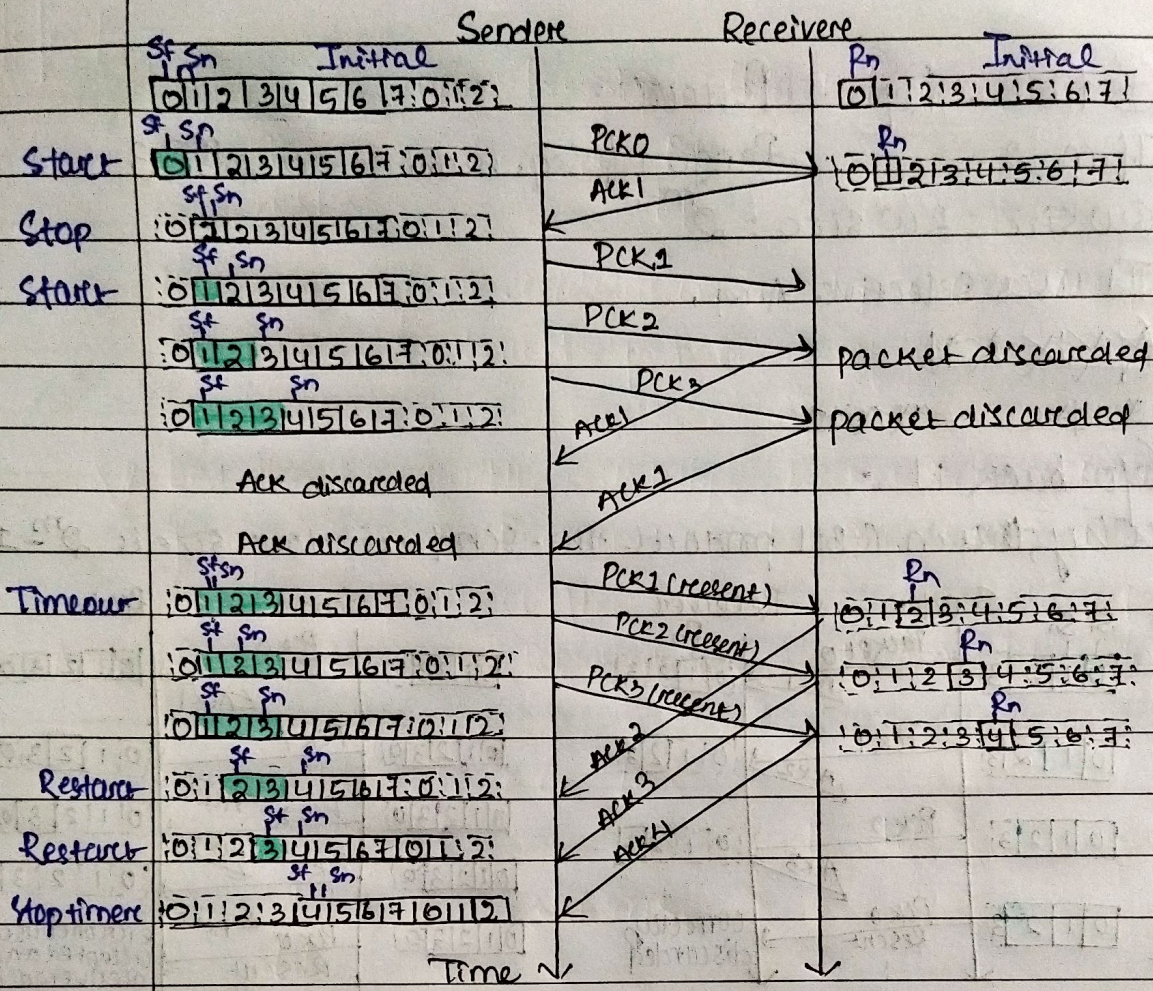
// Why, the in GBN protocol the send window size is $2^m - 1$



(a) Send window of size $< 2^m$

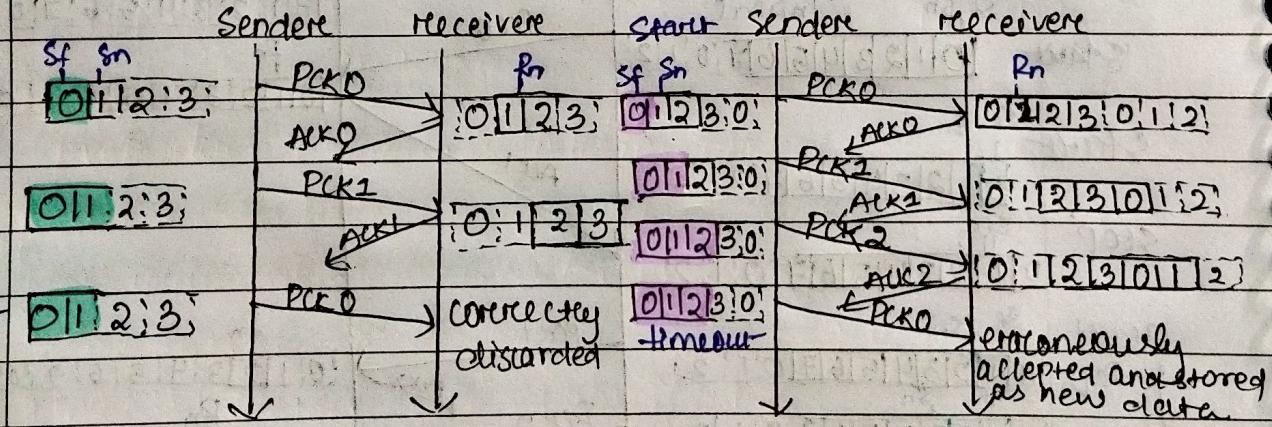
(b) Send window of size $= 2^m$





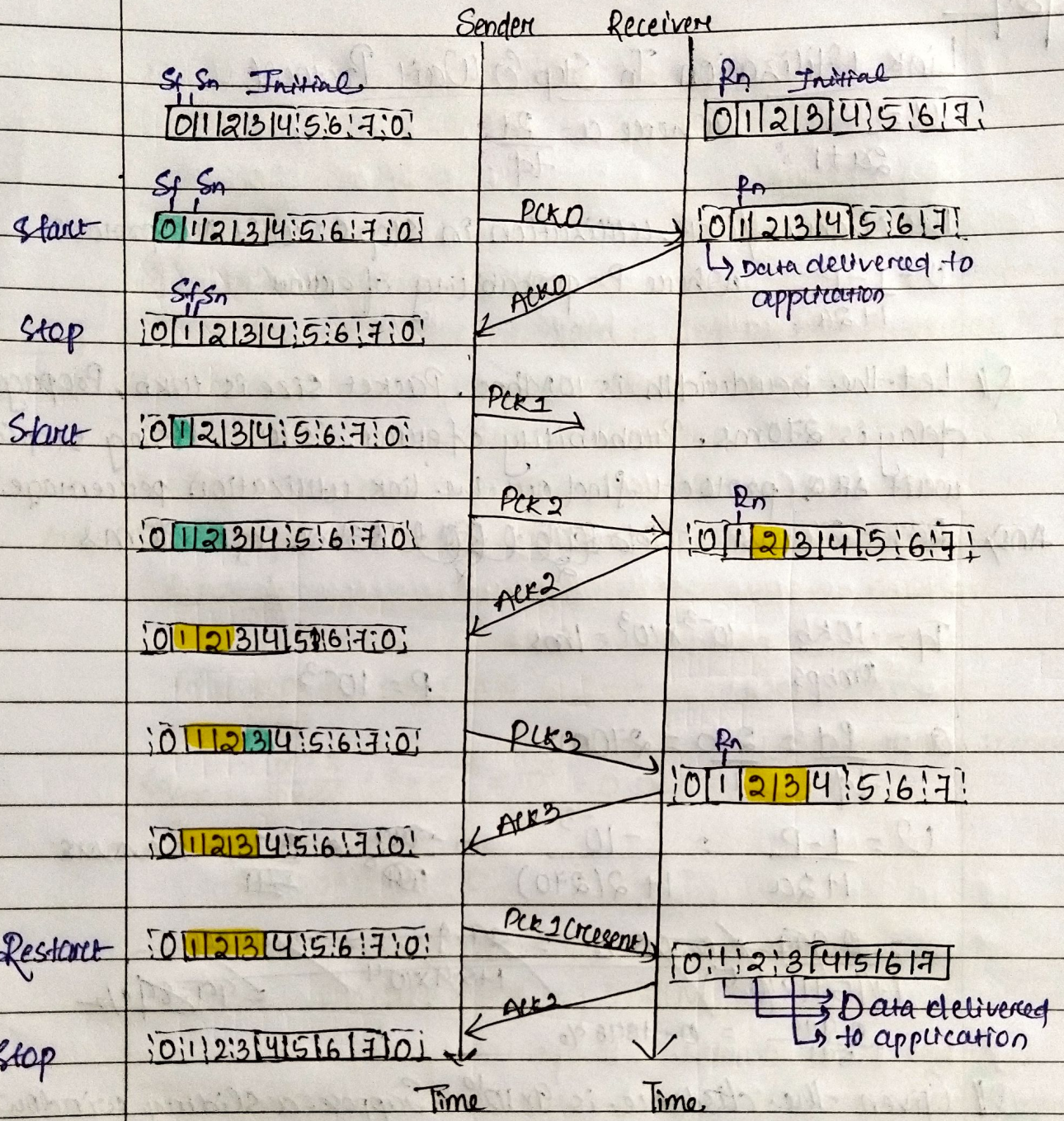
// Why window size is $2^m - 1$ only.

m = 2



(a) Send & receiver windows of size = 2^{m-1}

(b) Send and receive windows of size > 2^{m-1}



$U = \frac{N}{1+2a}$ [without error]

$U = \frac{N(1-P)}{(1+2a)(1-P+NP)}$ [with error]

N = Send window size.

31/8/24

Link Utilization In Stop & Wait Protocol

$U = \frac{1}{2a+1}$ where $a = \frac{Pd}{Td}$

The channel/link utilization in stop & wait ARQ protocol

$U = \frac{1-P}{1+2a}$ where P = probability of error

Q) Let the bandwidth is 10Mbps. Packet size is 10Kb. Propagation delay is 270ms. Probability of error is 10^{-3}. Using stop & wait ARQ protocol find out the link utilization percentage.

Ans) RTT = 270ms Pd = 270ms

$Td = \frac{10Kb}{10mbps} = 10^{-3} \times 10^{3} = 1ms$ $P = 10^{-3}$

$a = \frac{Pd}{Td} = \frac{270}{1} = 270ms$

$U = \frac{1-P}{1+2a} = \frac{1-10^{-3}}{1+2(270)} = \frac{0.999}{541} = 0.1848\%$

Q) Given the distance is 9×10^{10} m. Suppose a sliding window protocol is used. find out the send window size. For which the link utilization will be 100%. Given bandwidth is 64mbps. Frame size is 32KB. Speed of light is 3×10^{8} m/s

Ay) Link utilization 100% means U=1

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

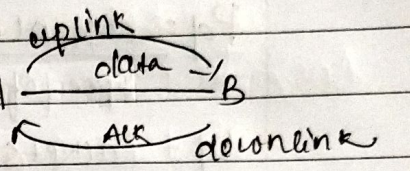
$N = 1 + 2 \times \frac{9 \times 10^{10}}{3 \times 10^{8}}$ $\frac{32 \times 8 \times 10^{-3}}{64}$

Bandwidth → maximum capability of a network
Throughput → current capability of a network

$a = \frac{Pd}{td} = \frac{9\times10^{10}\,m / 3\times10^{8}\,m/s}{32KB / 64Mbps} = \frac{300s}{32\times8\times10^{3} / 64\times10^{6}}$

$= \frac{300s}{0.004} = 75000$

$N = 1+2\times75000 = 150001$



2/9/2024

Q) Let the uplink for the data is 1Mbps and downlink is 10Mbps. The datasize is 1000bytes. Ack value is 100bytes, Propagation delay for the data is 20ms. Propagation delay for Ack is 10ms. What is the throughput achieve by the protocol.

Ans) Throughput = U (link utilization) x Bandwidth

$U = \frac{td}{td + Pd + td_{Ack} + Pd_{Ack}}$

$td = \frac{1000\times8}{1\times10^{6}} = 8\times10^{-3}\times10^{3} = 8ms$

$td_{Ack} = \frac{100\times8}{10\times10^{6}} = 8\times10^{-5}\times10^{3} = 0.08ms$

$td_{Ack} = 0.08ms$
$Pd_{Ack} = 10ms$
$Pd = 20ms$
Bandwidth = 1Mbps

$U = \frac{8}{8+20+0.08+10} = \frac{8}{38.08} = 0.21$

Throughput = U x Bandwidth
$= 0.21 \times 1Mbps = 0.21Mbps$

The sequence number space = Send window size + receive window size

Q) Suppose we need to design a selective repeat protocol given bandwidth is 1Gbps, distance is 5000km, packet size is 50,000bits. propagation speed is 2×10^{8} m/s. Find out the maximum size of the send window, receive window and no. of bits in the sequence no.

Ans) Bandwidth = 1Gbps
distance = 5000km
packetsize = 50,000 bits
propagation speed = 2×10^{8}
U = 1

$U = \frac{N}{1+2a}$ TO get maximum send window size, U should be 100%

$U = 1$ $N = 1+2a$ $a = Pd/td$

$Pd = \frac{\text{distance}}{\text{speed of light}} = \frac{5000 \times 10^3}{2 \times 10^8} = 25\,ms = 0.025$

$td = \frac{\text{Packet size}}{\text{bandwidth}} = \frac{50{,}000 \text{ bits}}{1\,Gbps} = \frac{50 \times 10^3}{10 \times 10^9} = 0.05\,ms$

$a = \frac{0.025}{0.050} = 0.5$

$N = 1 + 2(500) = 1001$

Receive window size = 1002

Sequence no. space = Send window size + receive window size

$= 1001 + 1001 = 2002$

$2^{m-1} = 1001$

$m - 1 = \log 1001$

$m - 1 = 10$

$m = 11$

* 2^{32} = 4GB

Q// Let the bandwidth is 1MBps let the sequence number starts with 0. How long it'll take to go back to 0 sequence number again (wrap around time)

Ans) wrap around time = $\frac{2^{32} - 1}{1\,MBps}$ =

$= \frac{4 \times 10^3\,MBps - 1}{1\,MBps} = \frac{4 \times 10^3 - 1}{2^{20}}$ =

Q// Sender sends series of packet using 5 bits. If 0 is the seq. no. of the first bit what'll be the seq. no. of 100 packet

Ans) m = 5 bits

maximum value = $2^{m-1} = 2^{5-1} = 2^4 31$

for 100 packet = (100-1) mod 32 = 3

Q// UDP header in hexadecimal format: CB840000D001C001C

(a) What is the source port number? Ans) $(CB84)_{16}$, so the source port number is 52100 [first four hexadecimal]

(b) What is the destination port? Ans) Second four hexadecimal $(0000)_{16}$, which is 13.

(c) What is the total ~~decimal~~ length of the user datagram? Ans) Third four hexadecimal $(001C)_{16}$; the length of the whole UDP is 28 bytes

(d) What is the length of the data? Ans) length of the data = whole packet − length of the header = 28 − 8 = 20

(e) Is the packet directed from a client to a server or vice versa?

Ans) The port number is 13, so the packet is from the client to the server

(f) What is the client process? Ans) Client process is daytime

3/9/24

Pseudoheader for checksum calculation (UDP)

pseudoheader	32 bit source IP address	
	32 bit destination IP address	
	All 0s	8-bit protocol	16-bit UDP total length
header	Source port address 16 bits	Destination port address 16 bits
	UDP total length 16 bits	checksum 16 bits
	Data (16-bits)	

Q) If bandwidth is 1GBps. How many extra bits to be appended in the option field so, that the wrap around time will be equal to the life time of the segment.

Ans) In current network situation, the life time of the segment is 180 sec., it is also called MSL (Max. Segment Length)

Bandwidth = 1GBps

$\Rightarrow 180 = \frac{2^x}{1GBps} \quad \Rightarrow 180GBPS = 2^x$

$\Rightarrow 4GBps = 2^{32}$

$1GBps = \frac{2^{32}}{2^2} \quad = 2^{30} \times 180 \Rightarrow 2^{38} \times 2^8 = 2^{38}$

For $180GB = 180 \times 2^{30} = 38$ bits $[2^{38}]$

∴ approximately 38 bits

Original sequence number takes 32 bit. calculated sequence number 32.

hence 38 − 32 = 6 extra bits will be appended in the option.

Q) In TCP, how many sequence no.s are consumed by each of the following segments:

(a) SYN: It consumes one sequence number

(b) Ack: does not consume any seq. no.

(c) SYN+Ack: 1 seq. number

(d) Data: It consumes n seq. no. where n is the no. of bytes carried by the segment.

Q) Explain why in TCP a SYN, SYN+Ack and FIN segment each consume a seq. no. but an Ack segment carrying no data does not consume a seq. no.?

TCP flow control :- To achieve the flow control, TCP forces the receiver to adjust their window size although the size of the buffers for both parties is fixed, when the connection is established

:- Closing window means moves its left wall to the right

:- Opening window means moves its right wall to the right

:- Shrinking means moves its right wall to left.