SCHOLAR
Date
Page

15/7/24 CN

Network

smaller segment of large message → packet
packet → data, head
data → payload

Requirements of a traditional network:-
(i) Two or more entities
(ii) Commodity / information
(iii) System

IP → unique numerical identifier given to a device connected to the internet

Traditional Network is a system that carries commodity or information between two or more entities.

Computer Network is a system that carries information between two or more entities in the form ~~of two or more entities~~ electromagnetic waves or electrical signals.

Transport Network (Traditional Network) vs. Computer Network

Transport Network	Computer Network
→ Vehicle / Driver	→ Packet / Payload
→ Address	→ IP Addrss
→ Route to destination	→ Routing Algorithm
→ Intersection	→ Switch / Router
→ Traffic Jam	→ Network Congestion
→ Traffic signal	→ Flow Control
→ Accident ⇄ Injury / Death	→ Packet Collision ⇄ Packet Loss

Switch	vs.	Router
→ Preferable for intranet		→ Preferable for internet.

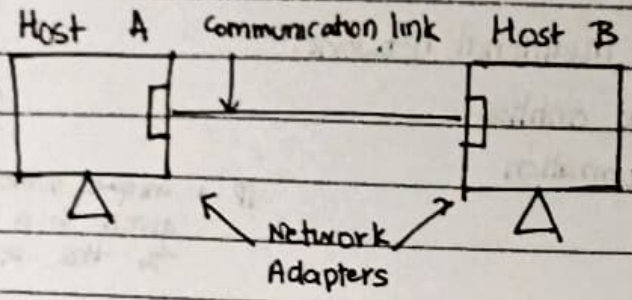
Switch	vs.	Hub
→ Operated on data link layer.		→ Operated on Physical layer.

Flow control → Regulates flow of packets

SCHOLAR

Date |
Page |

16/07 **Requirements for communication in a CN**



For communication in a network we require :-
Both Hardware and Software as follows :-

→ Hardware :-

(i) End device (Laptop, PC, phone)
(ii) Communication Link → Wireless
↳ Wired (Fiber optics, Coaxial cables, twisted pair)
(iii) Network Interface Control (NIC) card → Wired (Ethernet)
↳ Wireless (wifi)
(iv) Switches / Router

→ Software

(i) Applications

Goals of the Network :-

(i) Efficient (Minimum delay, Min^m cost, Min^m Packet loss)
(ii) Robust (Strong enough to handle failure & Error)
(iii) Scalable (Should accomodate n number of users)

SCHOLAR

Date |
Page |

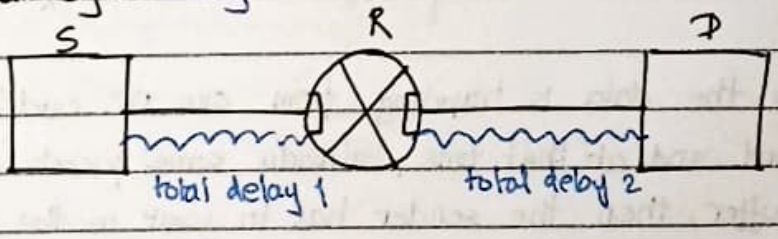
Means to achieve the goal

→ By efficiently designing the hardware & software, we can achieve the network goal.

Metrices to check whether the goal is achieved

(i) Throughput → Data rate / Bandwith

(ii) Latency → Delay



(a) 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 due to 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 this inspection. This delay is termed as Processing Delay.

SCHOLAR

(b) Queuing Delay.

→ Every NIC card is associated with a buffer.

→ Suppose the NIC card is having capability of 1 MBPS but is receiving 10 MB of data per unit time.

→ If it does not have the buffer, then first 1 MB of data will be sent and rest 9 MB of data will be lost in a unit time.

→ Suppose the data is traveling from one NIC card to another NIC card and at that time, already some packets are there in the buffer, then the sender has to wait in the queue for being processed. That introduces a delay in the network (waiting time in the queue) which is termed as Queueing Delay.

20/07 (c) Transmission Delay

→ The time taken to send the whole packet into the communication link is called as transmission delay.

→ Formula to find out transmission delay = $\frac{\text{Packet size}}{\text{Bandwith}}$

Unit → ms or s

(d) Propagation Delay

→ Time taken by any bit to traverse from one end to other end is called as propagation Delay.

→ Propagation Delay = $\frac{\text{Distance b/w two ends}}{\text{Speed of light in that medium}}$

In vacuum = 3×10^8 m/s

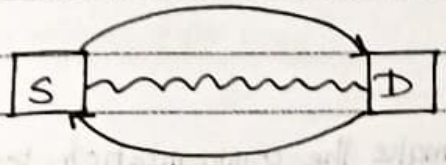
In fiber optic = 2.05×10^8 m/s

SCHOLAR

Date |
Page |

∴ Total Delay:- Processing Delay + Queuing Delay + Transmission Delay + Propagation Delay
↓
One way delay

Overall total delay = total delay 1 + total delay 2
delay from S to R
delay from R to D



The delay b/w S to D and D to S is known as Two Way Delay.
↓
RTT (Round Trip Time)

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

Ans. Speed = 2.4×10^8 m/s
Distance b/w two ends = 12000

Propagation Time = $\frac{12000 \times 1000}{2.4 \times 10^8} = 500 \times 10^3 \times 10^{-8}$ s

$= 5 \times 10^{-2}$ s

$= 50$ ms

SCHOLAR

Date |
Page |

1B = 8b

Q. If the message is 1 kB, bandwith is 1 MBPS. Calculate the transmission time in milisecond.

Ans. Transmission time = $\frac{1 \times 10^3}{1 \times 106}$

$= \frac{1}{1000} s$

$= 1 ms$

22/07 Functionalities required to make the communication possible in a CN:-

Postal System :-

① Hostel → Students

② Students → Letter (Generation of)

③ Letter → Information

④ Office Boy → Multiplexing / Demultiplexing

↓

Collects letters from multiple students and post it in the postbox

⑤ Postman — 5.1 Decides Path

5.2 Hop to Hop communication

⑥ Vehicle/Road - Physical Transmission

CN :-

① MyComputer → Application Programming

② Application program → Generate data (packets)

③ Packet → Information

④ Transport Software → Multiplexing / Demultiplexing

Collecting info from multiple applications & sending to receiver.

Delivering messages at the receiver end to the correct application layer

CN :-

① MyComputer → Application Programming

② Delivers letters to multiple students once the letters are received from postman

SCHOLAR

Date |
Page |

(5) – (5.1) Decides Path – Routing Algo
(5.2) Hop to Hop communication – Switch/Router

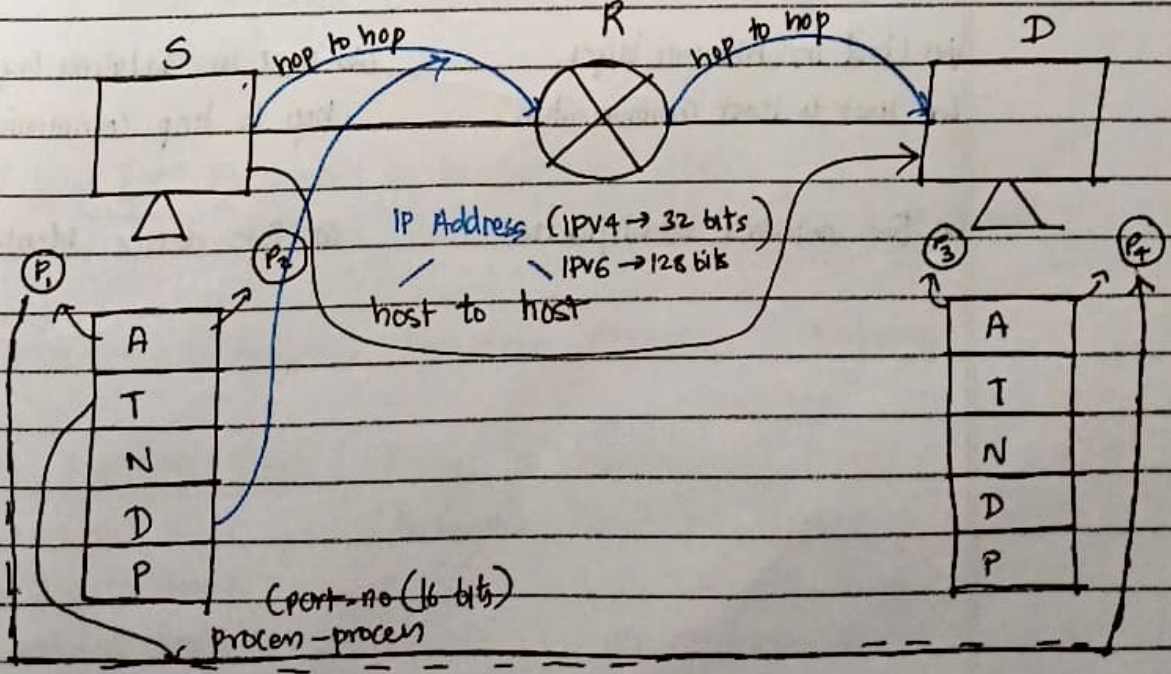
(6) Cables responsible for physical transmission of data in the form of electromagnetic waves

Layered Architecture / Model

* & process to process communication

TCP/IP Stack (5 layer)	OSI model (7 layers)
(i) ⟶ (i), (ii), (iii) Clubbed together	
(i) Application layer → Generate message	(i) Application → Look & feel of message
(ii) Transport layer → multiplexing/demultiplexing *	(ii) Presentation
(iii) Network layer → Routing w/ Switches/Router	(iii) Session → Open, closing & managing session
(iv) Datalink layer → Hop to Hop communication	(iv) Transport
(v) Physical layer → Physical transmission in the form of electrical signals	(v) Network
Bit to Signal conversion: Encoding	(vi) Datalink
Signal to Bit conversion: Decoding	(vii) Physical

23/07



SCHOLAR

Date
Page

MAC → Media Access Control, Attached to NIC card

With reference to diagram:- 6 12 digit hexadecimal number

(i) Application layer → Message Generation (Processes run in this layer)
(ii) Transport layer → Process-Process Comm^n, multiplexing/Demultiplexing
(iii) Network layer → Host to Host Comm^n, Routing, IP Address facilitates
(iv) Datalink layer → We require MAC Address to perform hop to hop communication
(v) Physical layer → Encoding (bit to signal) & Decoding (signal to bit)

Internet Protocol IP Address	Media Access Control MAC Address
(i) Used in Network layer.	(i) Used in Datalink layer.
(ii) IPV4 → 32 bits IPV6 → 128 bits	(ii) Size is 12 digit hexadecimal number when attached to NIC card.
(iii) It is a dynamic logic address.	(iii) It is a permanent address. (physical address)
(iv) Used in Network layer for Host to Host communication.	(iv) Used in Datalink layer, to perform hop to hop communication.
(v) For network identification	(v) For device identification

SCHOLAR

Date |

Page |

Protocols of each layer

(1) Application layer → HTTP protocol, SMTP protocol (Simple mail Transfer Pro) DHCP ~~DNS~~ protocol, TELNET protocol

(2) Transport layer → TCP (Transmission Control Proto), UDP (User datagram Prot)
Connection oriented — more reliable
connection less

(3) Network layer → IP (Internet Protocol)

(4) Datalink layer → Ethernet (wired), wifi (802.11, wireless)

(5) ~~Phys~~ Physical layer

Baseband transmission is a data transmission technique in which one signal needs the whole bandwith of the channel to transfer the data.

Broadband transmission is a transmission technology in which many signals with different frequencies send data across a single channel at the same time.

(i) 10 Base T → Represents a baseband of 10MBPS
→ distance that can be traveled by that signal

(ii) OFDM → Orthogonal Frequency Division Multiplexing

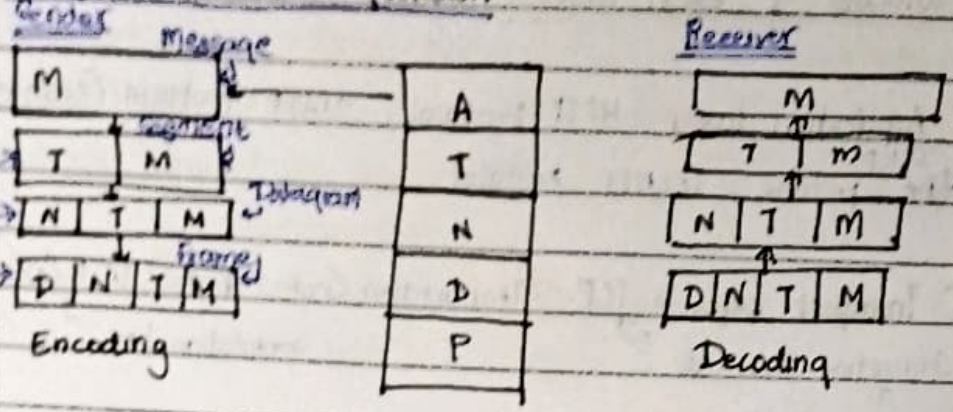
In TCP/IP Stack, Router is having 3 layers
(i) Network layer
(ii) Datalink layer
(iii) Physical layer

A Switch has 2 layers
(i) Datalink layer
(ii) Physical layer

SCHOLAR

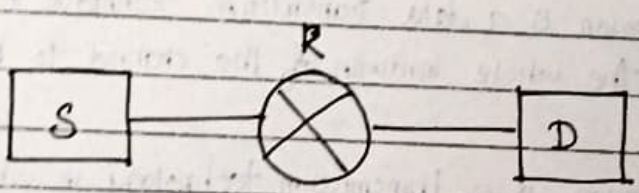
Date
Page

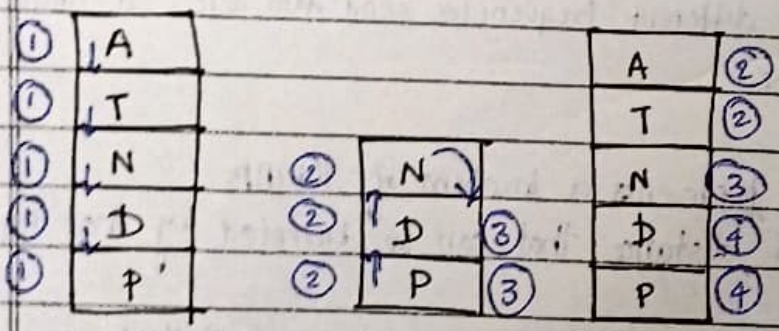
27/09 Encapsulation and Decapsulation



Adding the header on the sender side in their respective layers is known as Encapsulation.

Removing the header on the receiver side in their respective layers is known as decapsulation.

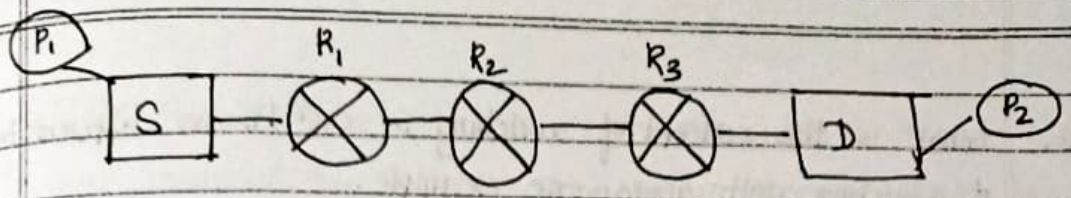




App. Layer – 2
T Layer – 2
N Layer – 3
D Layer – 4
P Layer – 4

SCHOLAR

Date:
Page:



A				A
T				T
N	N	N	N	N
D	D	D	D	D
P	P	P	P	P

Layers

A	–	2
T	–	2
N	–	5
D	–	8
P	–	8

Q. Differentiate b/w client server model and peer to peer model.

Ans

Client-Server Model	Peer to Peer model
(i) Clients and servers are differentiated Specific server and clients are present.	(i) Clients and servers are not differentiated.
(ii) Focuses on information sharing.	(ii) Focuses on connectivity.
(iii) Centralized server is used to store the data.	(iii) Each peer has its own data.
(iv) Server respond the services which is requested by client. Eg:- Email	(iv) Each & Every node can do both request & respond for services.

SCHOLAR

Q. What is the concept of switching in CN? Discuss different types of switching with appropriate example.

Ans. Switching is the process of transferring data packets from one device to another in a network or from one network to another using specific devices called switches.

There are three types of switching:-

(i) Message switching - Obsolete. Entire block/message is forwarded across the entire network thus making it inefficient.
Ex:- Email

(ii) Circuit Switching - A connection is established between the source and destination beforehand. This connection receives the complete bandwith of the network until data is transferred completely. Ex:- Analog Telephone Network.

(iii) Packet switching - Requires the data to be broken down into smaller components, data frames, or packets. These data frames are then transferred to their destinations according to available resources in the network at a particular time.
Ex:- ~~Analog telephone Network~~ Ethernet, Internet Protocol, UDP

Types of Network

(1) PAN : CN that connects computers / devices within the range of an individual person. (Personal Area Network)
Typically involves a computer, phone, tablet.

(2) LAN : Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools and programs. Connected together by a switch, or a stack of switches using a private addressing scheme.
Eg:- Bluetooth

(3) MAN: Mentropolitan area Network covers a larger area than that covered by a LAN but smaller than a WAN. Connects two or more computers that are apart but reside in the same or different cities. Eg:- City wifi

(4) WAN: Wide Area Network that extends over a large geographical area, might be confined within the bounds of a state or country. High-speed and relatively expensive.
Eg:- Home wifi

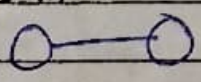
(5) Internet: Global network of linked computers, spans all over the world. Eg:- Email

29/07 Hybrid Architecture: It is the combination of client server architecture and peer to peer architecture. Eg:- Whatsapp

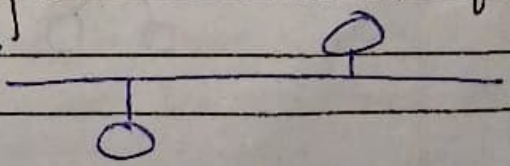
Network Topology

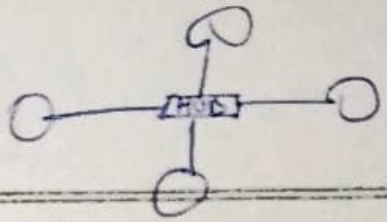
Q. What do you mean by Network Topology? Discuss the following:-
(i) Point to Point (ii) BusTopology (iii) Star Topology (iv) Ring Topology
(v) ~~mesh~~ Topology (vi) Tree Topology
Mesh

Ans. Network topology is the arrangement of the elements of a communication network.
(i) Point to point - Any network that connects two hosts in a dedicated fashion by cable. Unidirectional.

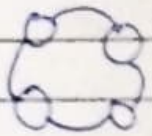


(ii) Bus Topology:- Nodes are directly connected to a common half-duplex link called a bus. Unidirectional.



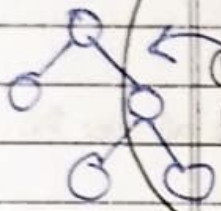


(iii) Star Topology: All Nodes are physically connected to a central node such as a router. Multidirectional.



(iv) Ring Topology: Nodes are connected in a circular manner.

(v) Mesh Topology: Nodes are connected in a decentralized manner. Each device connects multiple other devices.

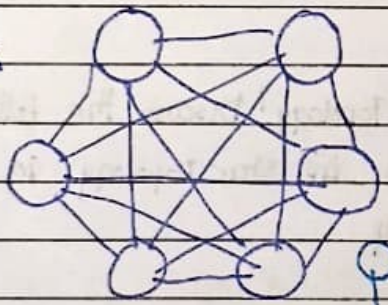


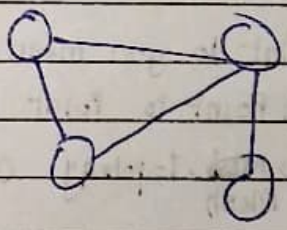
(vi) Tree Topology: A structure where nodes are connected hierarchically. Most commonly used.

Full Mesh & ↳ Partially Mesh Topology

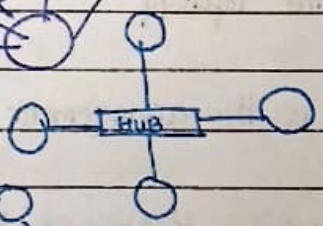
Each node is connected directly to all other nodes.

Only some nodes connect directly to one another.



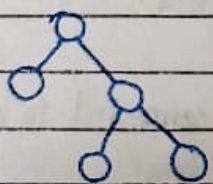


Star Topology:



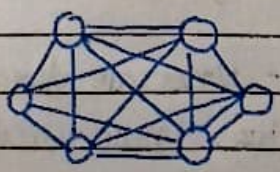
Ring " :

Tree " :

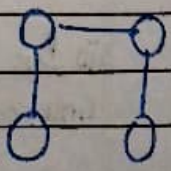


Mesh Topology

Full Mesh.



Partially Mesh



30/07/24

UNIT - 2

Application Layer

- Implements client server model, peer to peer model and hybrid model.

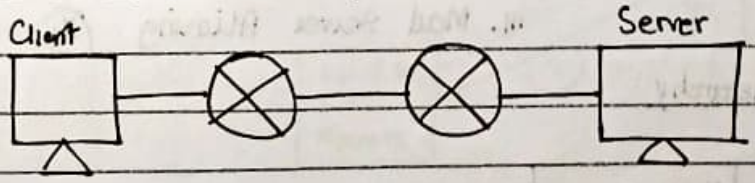
Socket is an API (Application Program Interface) that will be used for the communication b/w application layer and transport layer. So that communication will be possible in a computer network.

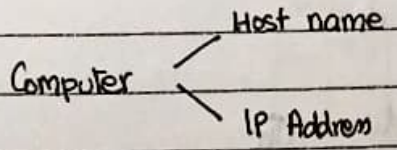
Protocol: It is representing the format and rules for exchanging messages in a computer network.

→ Basically, it represents what to send (i.e. format), when to send and how to act (rules)

Protocols of Application Layer

i) DNS (Domain Name System)





The services provided by DNS protocol:-

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

→ When the user wants to do a communication over the network, they prefer to use host name to identify a computer system in the network.

→ When the request is forwarded to the router, router does not understand host name. Routes only understands IP address to identify a machine in a network. Thus the DNS protocol is invoked to convert the domain name into IP address to continue communicating over the network & vice versa.

II. Host aliasing

Accounts for the most common typological errors from users, and these aliases redirect user to the original website also known as cannonical host name.

For ex:-

www.facebook.com ← cannonical host name

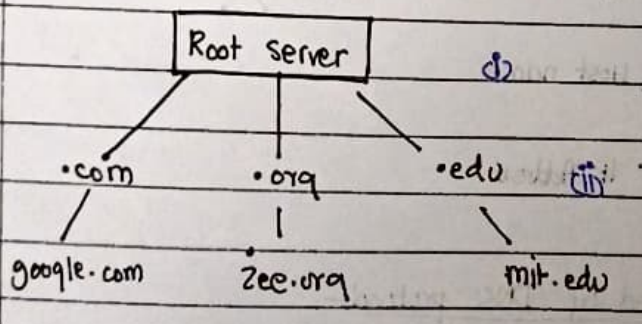
www.facebok.com ↑ redirects

→ A host with a complicated host name can have one or more alias (alternative names), as for the above example, the original host name is having two aliases. The original host name is called as cannonical host name.

→ DNS can be invoked by an application to obtain the cannonical host name for a supplied alias as well as to obtain IP address of the host.

III. Mail Server Aliasing

3/08/24 DNS Hierarchy



DNS servers are divided into 3 levels:-

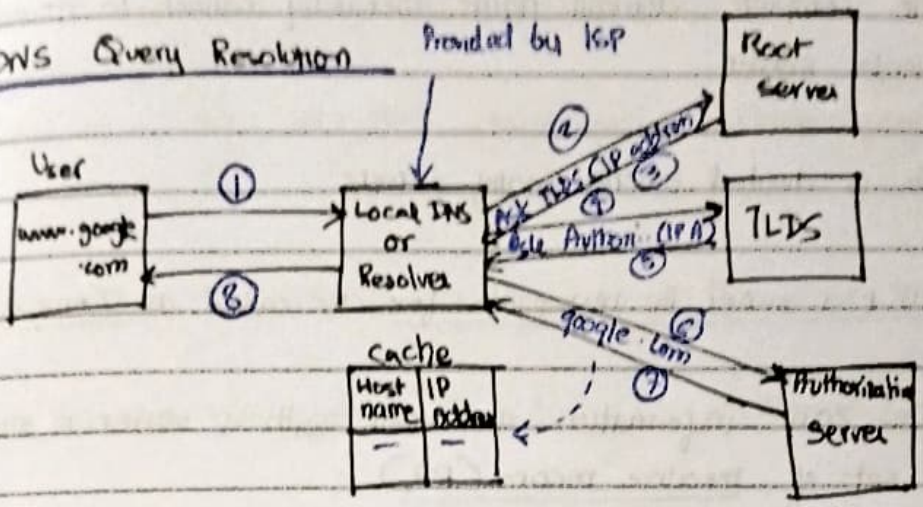
(i) Root DNS servers

(ii) Top level domain server (TLDs)

(iii) Authoritative server

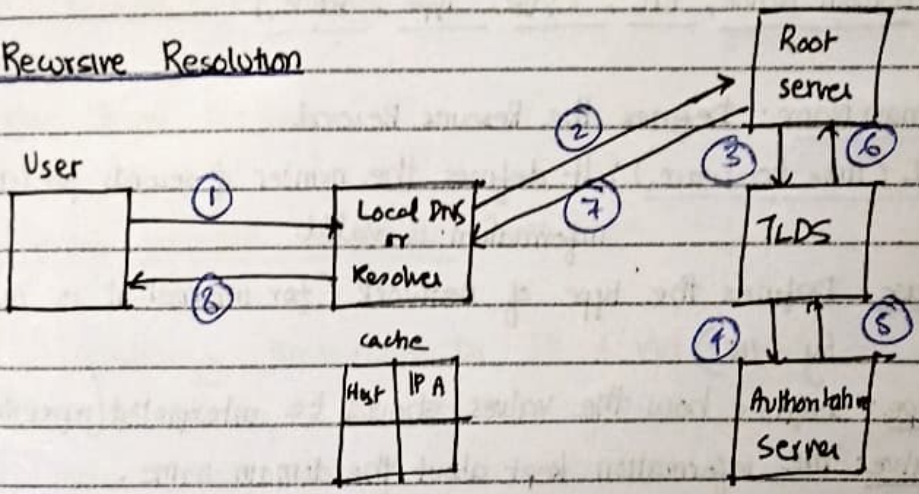
There exist 13 root DNS servers strategically placed around the world operated by 12 different organizations.

DNS Query Resolution



Iterative Resolution

Recursive Resolution



Stale Cache : Becomes stale when it no longer matches the slower storage.

It is important to note that once the resolver (local dns) receives the IP Address, it will store it in its cache memory in case it receives another query for google.com, then it does not have to go through all those steps again. Instead it only takes 2 communications to resolve the query. (User → Local dns & Local dns → User ... user ⇄ DNS cache)

SCHOLAR

Date
Page

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 Zone.

→ The zone information associated with a server is implemented as a set of resource record (RR).

A Resource Record (RR) is a 5 tuple structure as below :-
[Domain Name, TTL, Class, Type, Value]

Domain Name: Defines the Resource Record
TTL (Time to Leave): It defines the number of seconds for which the information is valid.
Class: Defines the type of network (for internet it is represented by IN)
Type: Defines how the values should be interpreted (represents type of RR)
Value: The information kept about the domain name.

The most commonly used RRs are A, NS, CNAME, MX, PTR

$ dig ↵
↑ List out all 13 root servers

A → [www.google.com, 3600, IN, A, IPaddress]

Local DNS will also maintain A Resource Record as well as Authoritative Server and TLDS

$ dig www.google.com ↵

www.google.com 116 IN A 142.250.182.68

ECHOLAR

Date:
Page:

05/08/24 NS Record (Name Server)

It provides the authoritative server name

AUTHORITY SECTION:

google.com 53 IN SOA ns1.google.com. dns-admin.google.com. 6[illegible]4433 900 900 1800 60

SOA record value marks the beginning of the zone information.

NS Record - google.com 56 IN NS Authoritative Server Name

Canonical Name - google.com 54 IN CNAME Canonical Host Name

MX Record (Mail Exchange)

Mail Server Aliasing

(*) Services provided by DNS (cont.)

(i) Translating Host name to IP & vice versa
(ii) Host Aliasing
(iii) Mail Server Aliasing

→ If a person has an account with gmail then his mail id will be abc@gmail.com. which one is fauthally qualified domain name

simple mail transfer protocol

→ The host name of the gmail server ~~smtp smpt~~ smtp.gmail.com which is the fully qualified domain name.

→ DNS can be invoked by a mail application to obtain the canonical host name of the mail server for a supplied alias mail server as well as the IP address of the host.

SCHOLAR

Date
Page

(iv) Load Distribution

→ DNS is also used to perform load distribution among replicated servers.

→ Busy websites such as google.com are replicated over multiple servers and with each server running on a different end system and having a different IP Address

→ For replicated web servers, a set of IP Addresses is thus associated with 1 canonical host name.

→ DNS distributes the traffic among all replicated servers.

PTR Record → Stores Host name for given IP Address.

IP Address 20 IN PTR Host Name

ASSIGNMENT Q

Q1. Discuss different types of encoding schemes with appropriate example.
Q2. Differentiate b/w analogue signal & digital signal
Q3. Compare & Contrast simplex, half duplex and full duplex

SCHOLAR
Date:
Page:

6/08/24 DNS supports client server architecture

→ CS paradigm

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

→ But incase of transferring zone information from one server to another (> 512 Bytes) DNS operates over TCP.

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

2nd Application layer protocol: HTTP (Hyper Text Transfer Protocol)
→ Is the foundation of world wide web. & is used to load webpages using hypertext links

→ webpages are viewed using a program called browser.

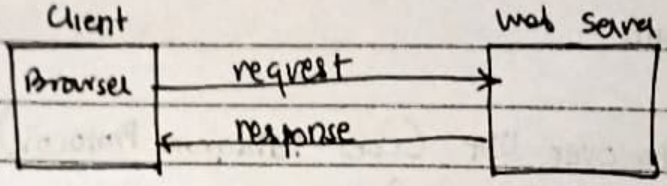
→ Every webpage contains Base Html and Base Html includes several reference objects like other Html file, Audio, Video, etc.

Each object is addressable by an URL (Uniform Resource Locator)
URL → http://kllt.ac.in/images/logo.gif
Protocol Host name path

→ HTTP 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 server to enable communication.

In this case, the client will be web browser & the server will be web-server.



Hence, HTTP supports client server paradigm.

→ HTTP uses the port number 80.

→ HTTPS achieves client server authentication, confidentiality, & integrity

→ HTTPS uses the port number 443.

There exists two popular versions of HTTP:-

(i) http 1.0 (ii) http 1.1

Non-persistent / persistent

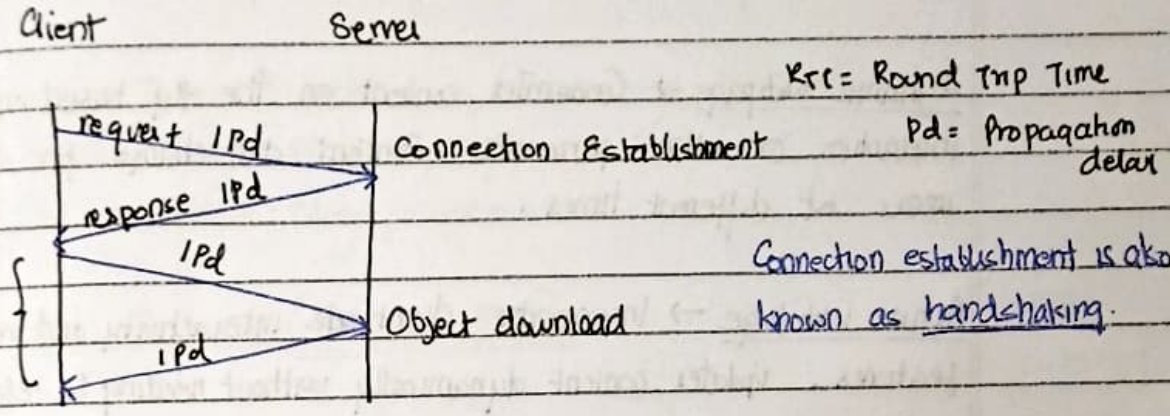
(i) Each object will use a new connection to be downloaded, Thus it is secure. Ex:- Bank Transaction

(ii) Same TCP connection will be used to download all objects. Thus it is faster but not secure. Ex:- E-commerce

→ HTTP operates over TCP in the transport layer if the amount of information exchanged b/w client and server is greater than 512 Bytes.

→ HTTP operates over UDP if the amount of information exchanged between client and server is less than 512 Bytes.

HTTP Response Time



→ To download one object we need 2 RTT.
→ If we want to access a webpage, by default 1 base HTML file will be downloaded along with other embedded object.

Q. Suppose we want to download a webpage embedded with 5 objects. What will be the overall response time to display the webpage fully using non-persistent and persistent connection

Ans. Response Time for non-persistent sequential connection

1 base HTML + 5 Embedded Obj
6 obj

RTT: Non-persistent sequential → 2 RTT + 5(2 RTT)
= 12 RTT

Response Time for non-persistent parallel connection:-
= 2RTT + 2RTT = 4RTT

Response Time for persistent sequential connection:- 2 RTT + 5 RTT = 7 RTT
Response Time for persistent parallel connection :- 2RTT + 1RTT = 3 RTT

SCHOLAR

Date.
Page.

Q. What are the different types of webpages?

Ans. Static webpage → Displays the same content to every user. Content is fixed and doesn't change unless the HTML file is manually updated.

Dynamic webpage → Generates content on the fly based on user interaction or other parameters. Content can change for different users at different times.

Active web page → Incorporates client-side interactivity and real time features. Updates content dynamically without needing to reload the entire page.

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

Ans. A computer or server that acts as an intermediary b/w the user and the internet is known as a proxy server.
The working principles are:-
(i) Request interception → captures and analyses incoming client requests
(ii) Address Translation → modifies source/destination addresses to hide client identity
(iii) Protocol Handling → interprets and processes various network protocols
(iv) Data Buffering → Temporarily stores data to manage traffic flow
(v) Caching Mechanism → stores frequently accessed content for faster retrieval.

SCHOLAR

Date:
Page:

10/08

Simple Mail Transfer Protocol (SMTP)

- SMTP uses TCP for reliable transmission of email messages
- It operates on port number 25
- The working principle of SMTP comprises of 3 phases:-
  - 1st Phase: Handshaking (Connection establishment)
  - 2nd Phase: Mail Transfer
  - 3rd Phase: Close Connection

Email Protocol (Electronic Mail)

Email architecture uses 3 major components:-

- User agent (UA)
- Mail Servers
- SMTP

User agent: It is a local program that composes, reads, replies and forward email messages

- It can either be text based or gui based
- Basically, UA can be either sender or reader.
  - sender → Mail Transfer Agent (MTA)
  - reader → Mail Access Agent (MAA)

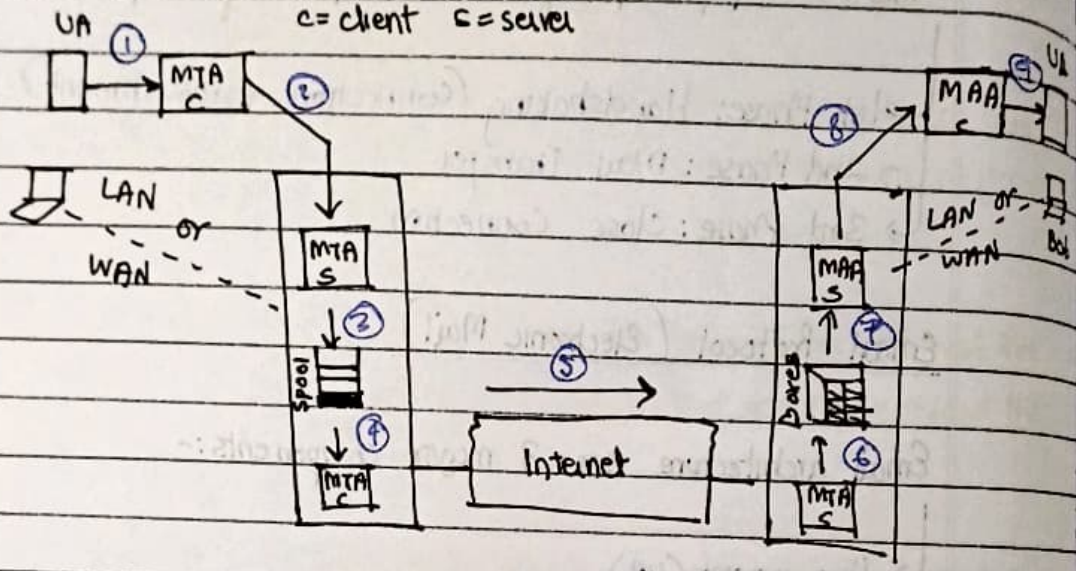
Mail Servers

- composed of mailbox (inbox)
  - contains incoming messages for users.

Message queue → used for outgoing messages

SMTP

→ Used for sending email messages b/w mail servers
→ Mail server is of two types :- Sending Mail server (Client)
Receiving Mail server (server)



Scenario : Alice sends message to Bob

① Alice uses UA to compose message & set the 'to' field value to bob@gmail.com

② Alice's UA sends message to her mail server ; sending mails is a push operation (SMTP or HTTP Protocol);
Microsoft Outlook ↳ Browser
Message placed in a message queue.

(SMTP mail transfer has 3 phases :- Connection Establishment, Mail Transfer & Connection Termination)

Mail server to mail server connection always use SMTP.

SCHOLAR
Date:
Page:

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 server places the message in Bob's mail box (inbox)
⑥ Bob invokes his user agent to read message; Receiving mail is a PULL operation (POP3, IMAP, HTTP)

POP3 → Post office Protocol 3
either or used to read Outlook or Thunderbird
Browser

Transport Layer (3rd Unit)

→ Process to process communication
→ Multiplexing & Demultiplexing
↳ Segment | Header | Payload |
8 bytes

Protocols used in Transport Layer

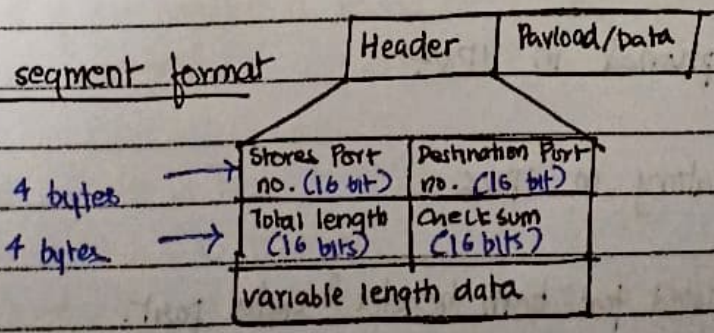
	UDP	TCP
	→ Connection less	→ Connection oriented
	→ Packet oriented	→ stream oriented/Byte oriented
	→ Faster	→ Slower
	→ Not reliable	→ reliable
	8 bytes	20-60 bytes

UDP (User Datagram Protocol)

Advantages of UDP
→ Faster communication
→ Less overhead per packet
→ UDP header size is of 8 bytes. Whereas TCP header size is 20-60 bytes.

12/08 Transport Layer

The UDP segment format



(i) If the sender wants to communicate with the receiver then destination port no. will be required.

(ii) If the receiver wants to communicate with the sender then source port no. will be reqd.

(iii) Hence, to support bi-directional communication - UDP segment is having source port no. (16 bits) & destination port no. (16 bits)

Total Length

→ Represents the length of the segment. The range of total length will be $0 - 2^{16}-1 \Rightarrow 0 - 65535$.

→ Similarly the range of source port no. & destination port no will be $0 - 2^{16}-1 \Rightarrow 0 - 65535$.

→ The length of payload can be calculated using the formula:-
= Total Length - Header size
= Total length - 8 bytes.

Check Sum

→ Is an error correction mechanism to check whether the received data is correct or corrupted.

→ Is optional in IPV4.

→ Mandatory in IPV6

→ Calculated for both header & data part.

→ For header part, to calculate check sum, first we need to set all

SCHOLAR

Date.
Page.

16 bits of checksum filled to 0.

→ After calculating check sum, update the check sum field with the calculated checksum.

Steps to calculate checksum

→ Divide the whole segment into 16 bit chunks

→ Let us consider 64 bit header & 64 bit payload, for a segment. Hence total = 128 bit is the segment size.

→ Divide this 128 bit into equal number of 16 bit chunks (8 chunks each of 16)

→ Add all 8 chunks using 1's compliment addition to yield final sum

→ Complement (set 0→1 , 1→0) the final sum to get the checksum of 16 bits.

→ At the receiver end, receiver will perform all the steps to find out final sum of the received data.

→ Then receiver will add the calculated final sum & received checksum.

→ If the result of the addition is having all 1 then, the data is correct else the data is corrupted.

Ex:- For simplicity, let us take 3 8 bit chunks

First chunk → 11 00 11 00 ..... 00 11 00 11

Second chunk → 10 10 10 10 ..... 01 01 01 01

Third chunk → 11 11 00 00 ..... 00 00 11 11

11 01 01 11

SCHOLAR

Date |
Page |

final sum = 11010111 (wrong)
+ 01011000

check sum = ~~00101000~~ 10100111

11111111 → all 1's (x)

= Data is correct.

13/08 Checksum

1st Chunk: 10100001
2nd Chunk: 01010110
3rd chunk: 11001100

11000011
1

final sum: 11000100

checksum: 00111011

Suppose the receiver receives the data as follows :-

10110001
01010110 = 11000100 final sum
11001100

~~11 0 11~~ = 00101011 check sum.

11010100
00111011

~~00011111~~

00011111 ← Corrupted.

SCHOLAR

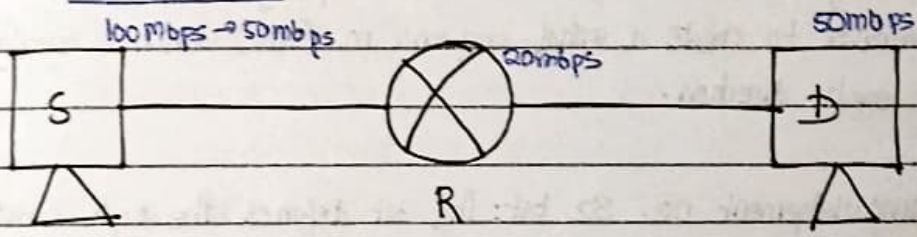
Date:
Page:

TCP

- Functionality: Process to process commn.
- Multiplexing, Demultiplexing
- Connection Oriented
- Stream / byte oriented
- Reliable

The reliability in TCP is achieved by

(i) Connection oriented architecture by achieving flow control, congestion control and error control

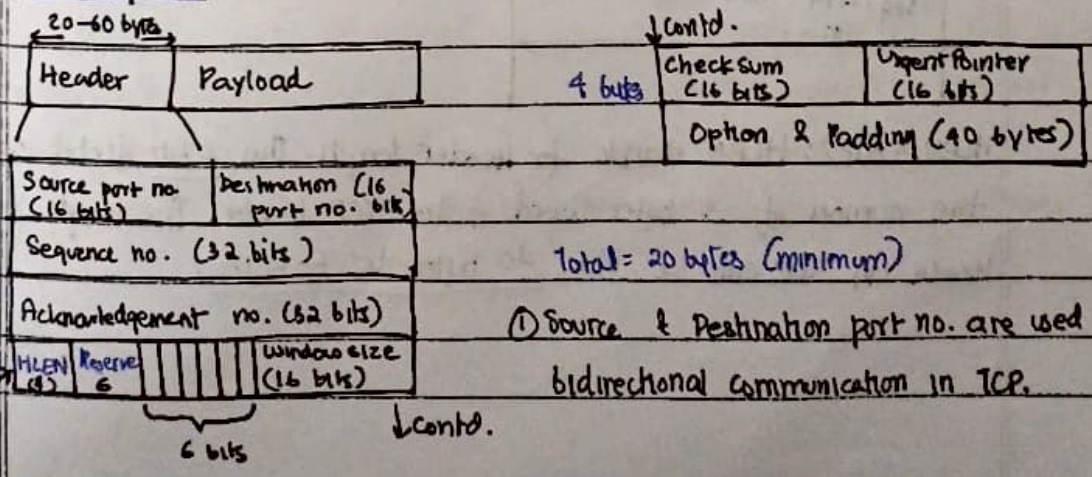


Flow control: Synchronizing the speed of sender & receiver

Congestion Control: Synchronizing the speed of the network

Error Control: Tells about how to handle packet loss, packet corruption & packet duplication

TCP Segment



Total = 20 bytes (minimum)

① Source & Destination port no. are used for bidirectional communication in TCP.

SCHOLAR

Date |
Page |

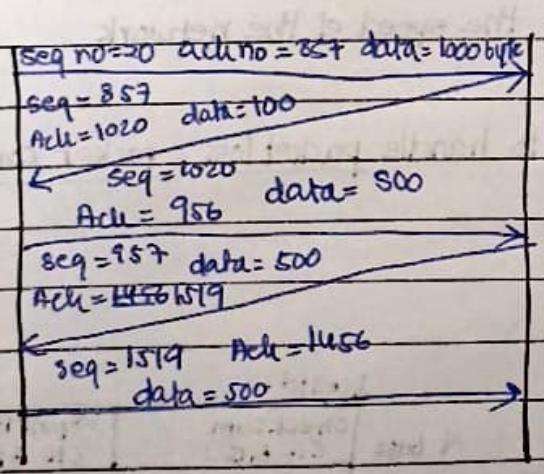
① Sequence number: This 32 bit field defines the number assigned to the first byte of data contained in the segment.

→ TCP is stream or byte oriented protocol, hence to ensure connection 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 a initial sequence no. (ISN) which is usually diff. in each direction.

Acknowledgement no. 32 bit: This bit defines 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 no.



HLEN (4 bits): HLEN stands for Header length. This 4 bit field indicates the number of 4 bytes word in the TCP header. The length of the heada in TCP can be btw 20 bytes to 60 bytes.

SCHOLAR

Date:
Page:

Therefore, the value of this field is always between 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. If the header length is 20 bytes then HLEN will store 5(2014). And if the header length is 60 bytes then HLEN will store 60 bytes.

Window Size (16 bits): It represents the receiver window size to achieve flow control. The maximum size of the window will be 0 to $2^{16}-1$ = 0 to 65535 bits.

checksum: Used for integrating checking and is mandatory for TCP header.

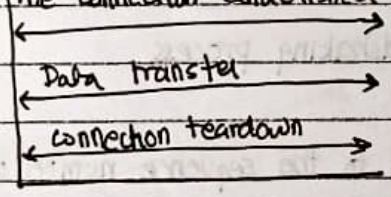
Flagbits:

URG	ACK	PSH	RST	SYN	FIN

The 3 flags (RST, SYN, FIN) flagbits are used for connection management.

connection management → connection establishment

Once, the connection established



FIN: Finish; connection teardown

SYN: synchronizing sequence no.

RST: Reset abnormal or forceful termination

PSH: PUSH (sending)

If PSH flag is 1 then it does not need to wait for the buffer (PSH will be 1 when we need to send the data). It is useful in sending the message immediately (no need to wait in the buffer until it is full).

URG: (Urgent Flag) Suppose the data was already sent and you need to call the abort then that case about information should go before sent data. That case about the urgent data and URG flag is sent to 1. Urgent pointer points to the last byte of urgent data.

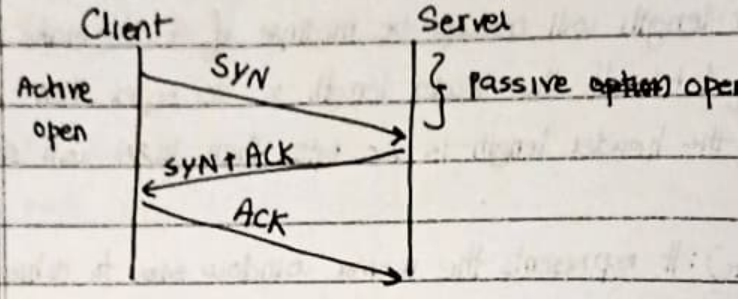
If the urgent flag is set to 1, then only the urgent pointer will be populated.

SCHOLAR

Date |
Page |

19/08

* Connection Establishment (3-way handshaking)



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

→ The client program issues a request for an active-open. A client that wants to connect to a open server tells its TCP that it needs to be connected to that particular server.

→ TCP can now start the 3-way handshaking process

SYN → One byte will be assigned to the sequence number of SYN so that client can know that whether the SYN has reached the server or not. (Byte oriented)

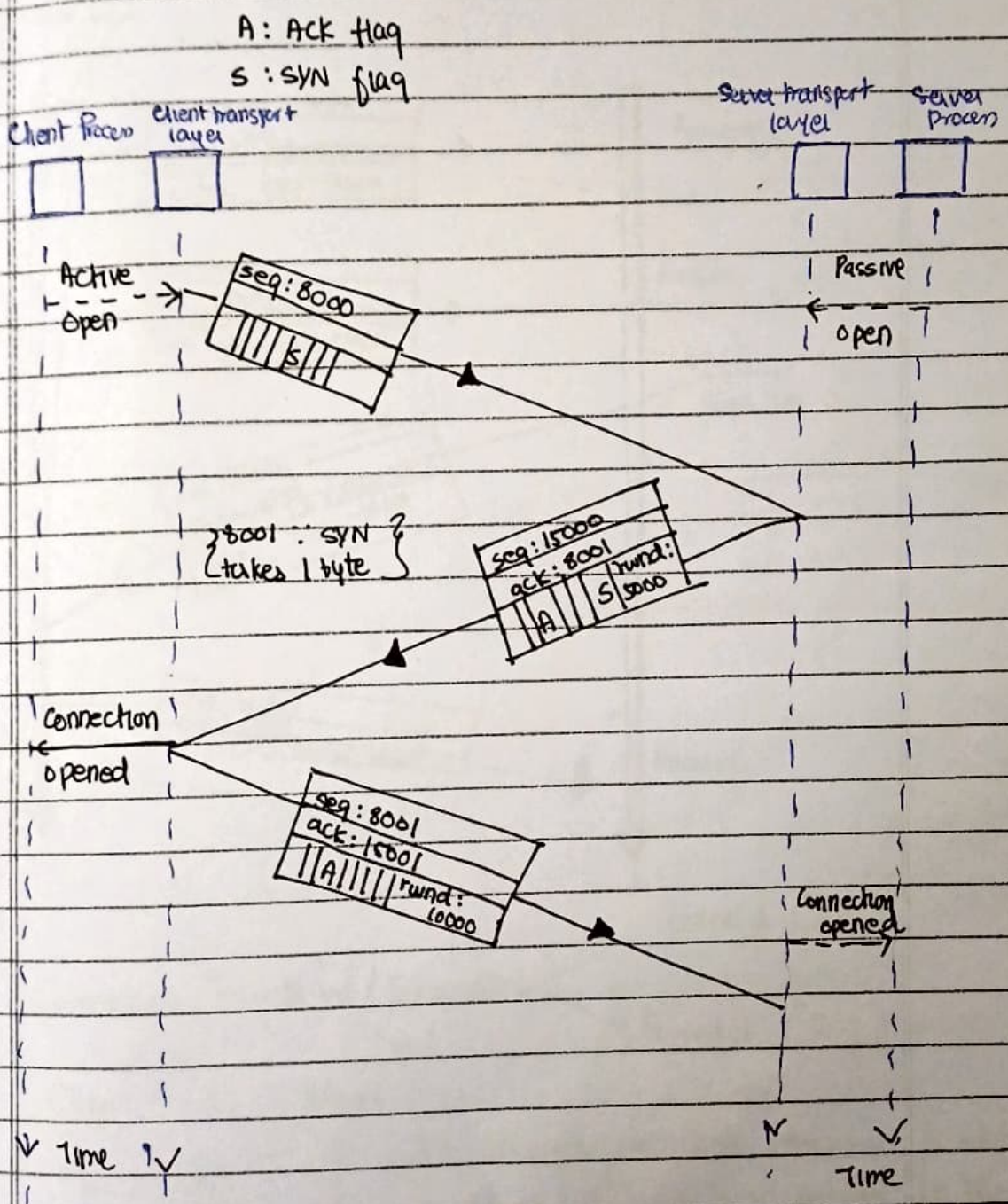
FIN → one byte (one sequence no.)

ACK → 0 byte will be assigned to the sequence no. of the ACK has 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 Piggins Backing.

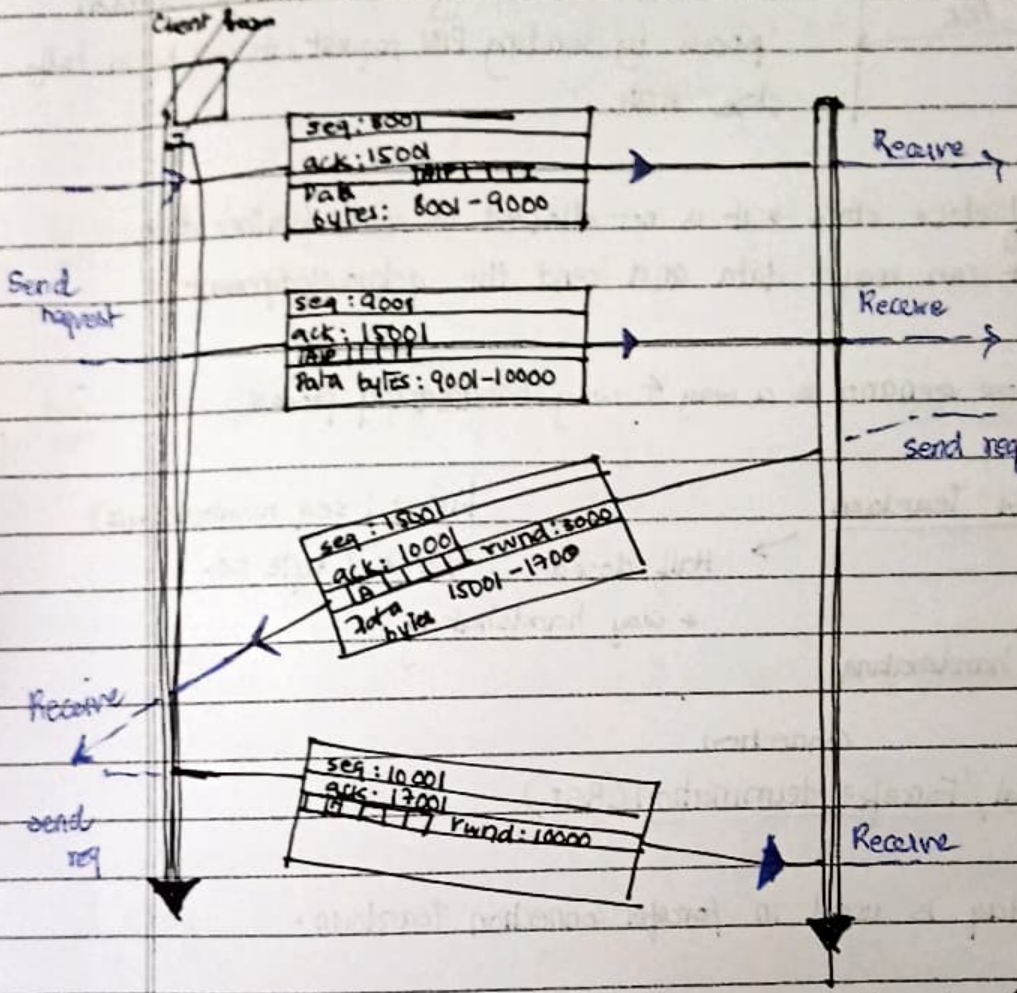
If the data is piggy-backed on ACK then ACK sequence no. will be dependent on the data.

for eg: Suppose the piggy bank data length is 100 byte then Ack sequence no. will be 100.

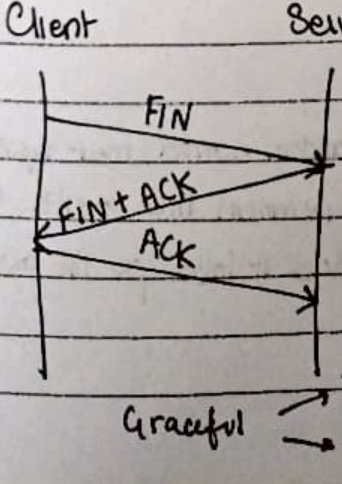


VRG	ACK	PSH	RST	SYN	FIN

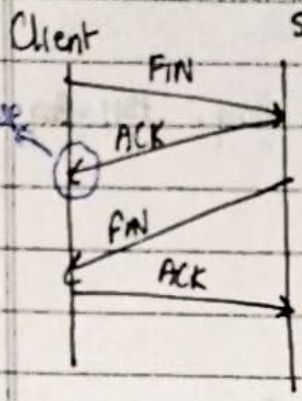
20/08 Data Transfer for that we require SYN flag, PSH flag, PSH flag and ACK flag.



Connection Teardown / Termination → Graceful (FIN)
→ Forceful (RST)



The Graceful connection Teardown is also known as 3 way handshaking. In the case where client & server finish their work at the same time.



This is known as 4 way Handshaking.
Half close scenario
↳ whoever is initiating the connection teardown process by sending FIN request, it will be in half close state.

→ In half close state → it is not allowed to send further data but it can receive data and send the acknowledgement.

→ Half close scenario is a ~~way~~ 4 way handshaking process

24/08

Graceful Teardown
- Normal 3 way handshaking
- Half closed 4 way handshaking

FIN → 1 seq number (1 byte)
SYN → 1 byte no.

Connection
Abnormal / Forceful termination (RST)

RST flag is used in forceful connection teardown.

Scenario for abnormal teardown :-
(i) TCP at one end may deny the connection request
(ii) may abort an existing connection
(iii) may terminate an ideal connection

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

SCHOLAR

Ans max value that seq no can take = $2^{32}-1$ (∵ seq no field is 32 bit long)
the counter will be implemented in every second: 64000x2
= 128000

$\therefore$ Time: $\frac{2^{32}-1}{128000}$ = ~~54s~~ 33561.43s
= 9h ~~20min~~ 32min

Q. TCP is sending data at 1MB/s. If the seq no. starts with 7000, how long does it take before the seq no goes back to 0.

Ans. max value = $2^{32}-1-7000$

If MB (bits) $\frac{2^{32}-1-7000}{10^6}$ = 4295

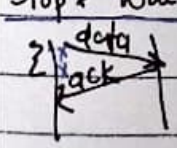
$\therefore$ Time: $\frac{2^{32}-1-7000}{8\times10^6}$ = 536.87s

TCP uses several protocols based on the types of environment i.e the channel can either be noiseless or noisy.

Channel
- Noiseless
  - ↳ Simple
  - ↳ Stop & Wait
- Noisy (Automatic Repeat Request)
  - ↳ Stop & wait ARQ
  - ↳ GBN Protocol
  - ↳ Selective Repeat Protocol

1. Simple Protocol
→ Assumed to be ideal (i.e. no error)
→ Not designed for flow or error control
→ Practically never true, ∴ Not used in practice.

Stop & Wait Protocol → simple protocol + flow control only
→ connection oriented, implements ~~both error &~~ flow control.



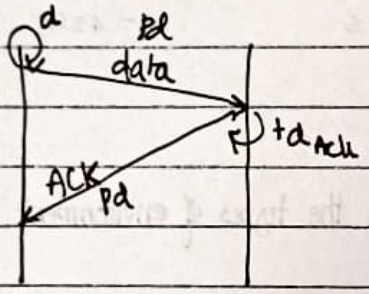
Imp: Stop & Wait Protocol is very ineffficient if our channel is is Thick (Large bandwith) & Long (Longer RTT)

RTT = 2 × PD (Propagation Delay)

Bandwith delay product = Bandwith × RTT

Channel utilization / Link utilization = $\frac{\text{packet size}}{\text{bandwith delay product}}$

Channel / Link utilization in Networking is represented using U.



Problems associated w/ stop & wait Protocol is poor link utilization

How to find link utilization (U).

Total end to end delay = $t_d + P_d + t_{d_{Ack}} + P_d$ (0 byte)

$= t_d + 2P_d$

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

$$= \frac{1}{1 + 2(P_d/t_d)}$$

In networking t_d/t_{pd} or $a = P_d/t_d$

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

Link util represented in the form of %.

Q. Let bandwith = 1Mb/ps . R_{TT} = 20ms . Packet size = 1000bits . Find % of channel / link util.

Ans. $P_d = \frac{20}{2} = 10ms = t_{pd}$

$t_d = 1000/10^6 = 1ms$

$a = \frac{P_d}{t_d} = 10$

$U = \frac{1}{21} = 4.7\%$

$B.D.P = 1000 \times 20$

$= 20000$ bits

$U = \frac{P.S}{B.D.P} = \frac{1000}{20000} = 5\%$

Q. Assume that in a stop & wait system, the bandwith of the line is 1 Mbps & 1 bit takes 20ms to make a round trip. What is the utilization % of the link if we have a protocol that can send upto 15 packets before stopping & worrying ab the ACK. Packet size = 1000 bits.

Ans. $B.D.P = 20000$ bits

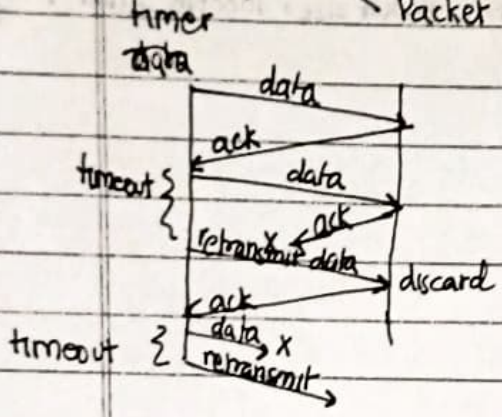
$U = \frac{15 \times 1000}{4\ 20000} = .75\%$

Noisy

27/08 Stop & Wait ARQ protocol

Simple Protocol + Flow Control + Error Control

Error Control — Packet Loss - using Timer
Packet corruption - using checksum
Packet duplication - using seq no. & ack no.



Go Back N-protocol

(i) The major problem associated w/ stop & wait protocol is poor link utilization.

(ii) How to improve efficiency: by introducing the concept of pipelining we can improve the channel utilization.

Pipelining is implemented using sliding window

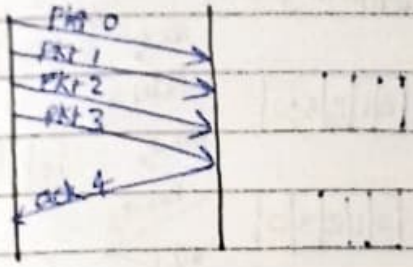
Go Back N ARQ protocol, which is a sliding window protocol uses send window size $2^m - 1$ where m is the no. of bits required to represent the sequence number. It uses the receive window size = 1.

If m = 3, Then send window size = $2^3 - 1 = 7$ & range of seq no = 0 to 7.

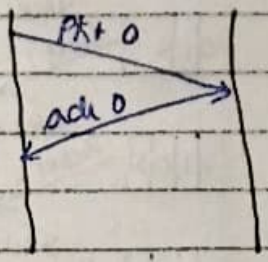
There exists 2 types of ACK:-

(i) Cumulative ACK (ii) selective ACK

Cumulative ACK ex:-



Selective Ack



GBN uses cumulative ack. imp Q: S.W.S is $2^m - 1$. why?

In GBN protocol, the send window size should be less than equal to $2^m - 1$. It should not be greater than $2^m - 1$. (ref Note 6, pg 4)

Selective Repeat Protocol

S.W size = R.W size = 2^{m-1}

Range of sequence no: 0 to 2^{m-1}

Selective Repeat Protocol uses selective Ack.

31/08 Sliding window Protocols

(1) Go-Back-N ARQ Protocol (uses cumulative Ack) → send window size = $2^m - 1$, R.W = 1

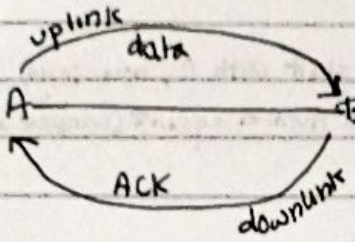
Range of seq no: $2^m - 1$

(2) Selective Repeat Protocol (uses selective Ack) → S.W ≤ 2^{m-1} = R.W.S

SCHOLAR

Date:
Page:

2/09/22



Bandwith → max capability of network.
Throughput → current capability of network. • U (Link Utilization × Bandwith) U x B.W

Q. Let the uplink for the data = 1 Mbps & downlink = 10 Mbps. Data size = 1000 bytes. ACK size = 100 bytes. Pd for the data = 20ms, Pd for ack = 10ms. What is the throughput achieved by this protocol?

Ans $U = \frac{td}{td + Pd + td_{ack} + Pd_{ACK}}$

$td_{data} = \frac{10^3 \times 8}{10^6}$ $\quad td_{ack} = \frac{100 \times 8}{10^7}$

$= 8ms$ $\quad = 0.08ms$

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

Throughput = U x B.W(data)
$= 0.21 \times 10^6$ mbps
$= 2.1 \times 10^5$ mbps

The sequence number space = S.W.S + receive W.S

Q. Suppose we need to design a selective repeat protocol given b.w = 1 Gbps distance = 5000km, packet size = 50,000 bit. Propagation speed = 2×10^8 m/s. Find out the maximum size of the send window, receive window & no. of bits in the sequence no.

5000 km / 2×10^8 ← pd = dist / sp. of light
50,000 / 1×10^9 ← td = packet size / b.w

Ans. To get maximum S.W.S, U should be 100%.
i.e, U = 1 Hence $1 = \frac{N}{1+2a}$ ⇒ $1 + 2a = N$

$a = \frac{25}{0.05} = 500$ (pd/td)

$N = 1 + 1000 = 1001$

Size of seq no = 1001 + 1001 = 2002

No of bits reqd: $2^m - 1 = 1001$ ⇒ $m - 1 = 10$

$m = 11$ ~~m = 10~~

$2^{32} = 4$ GB

Q. Let bw = 1mbps, Let seq no start with 0, how long will it take to go back to 0 sequence number again? (wraparound time)

Ans. Max value of seq no = $2^{32}-1$

$= \frac{2^{32}}{10^6} = 4096$ s

Q. sender sends series of packets using 5 bits, if 0 is the sequence no. of the first bit what will be the seq no of 100 packet.

Ans. max^m value of seq no will be = $2^5-1 = 31$

3/09/24 Pseudo header for UDP

32 bit source IP address		
32 bit destination IP address		
All 0s	8-bit protocol	16 bit UDP total length
Source port add 16 bits		Destination port address 16 bits
UDP total length 16 bits		Checksum 16 bits
Data (padding to make this data a multiple of 16 bits)		

Pseudo header

Q. If B·W = 1 GBps, how many extra bits to be appended in the option field so that the wraparound time will be equal to the lifetime of the segment.

In current network situation, the lifetime of the segment is 180 sec. (MSL)

MSL → maximum Segment length

Ans. 1 GB in 1s

180 GB in 180s

1GB → a^{30} bits

180GB → $180 \times a^{30}$ bits

$\therefore 2^x = 180 \times 2^{30}$ where x is the no. of the bits in GB

$x = 7.491$ ~~38~~ (approx)

~~$\div 8 \times 180 : 1440$~~

Original seq no takes 32 bit

Calc. seq number = 38 bit

Hence, 38 − 32 = 6 extra bits will be appended in the option field.

Q3-25) (from pdf)

a. SYN consumes one seq number

b. ACK does not consume any

c. SYN + ACK consumes one seq number

d. data seq → n seq num. where n is the no. of bytes carried by the data

TCP Flow Control

To achieve flow control, TCP forces the sender & receiver to adjust their window size although the size of the buffer for both parties is fixed when the connection is established.

(i) Closing window means moves its left wall to the right. Open window means moves its right wall to the right. Shrinking means moves its right wall to the left.