Q. solve 20-21

6(c) What is the difference between a public IP and a private IP? Provide example of each. [3]

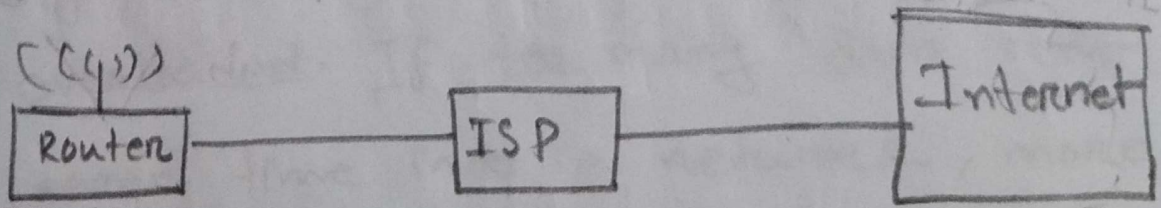
Note:

Public IP Address: Public IP address is the IP address that is used to communicate outside the network.

It is provided by ISP (Internet Service Provider)

Two types: (1) Dynamic and static IP Address
(Exmp: ISP) (Exmp: DNS)

Can we trace Public IP address? Ans: Yes, Public IP can be traced and easily find out someone geographical location.



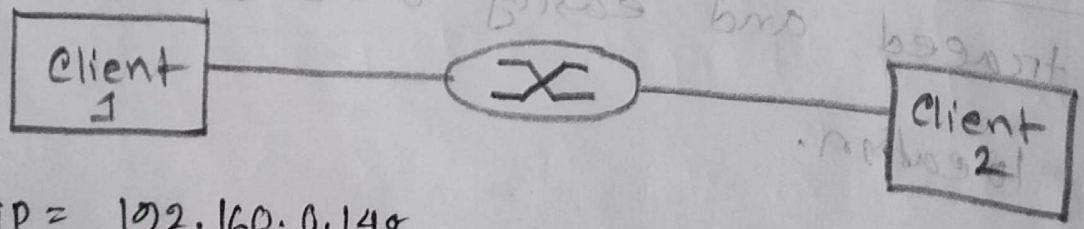
Public IP = 82.119.70.111

Private IP: The Private IP is a IP address that are used to communicate within a local area network (LAN). It allows device to send data privately.

It is assigned by router.

Can we trace private IP address?

⇒ Yes, we can trace but not like public IP. It is possible if two device are connected each other internally and one device into on the local network and other one the internet.



Private IP = 192.160.0.148

192.160.0.149

Q: Difference between Private and Public IP.

Aspect	Private IP	Public IP
Scope & Purpose	Works within a local Network (LAN)	Works globally over the Internet
Control & cost	controll by local admin and Free	Controll by ISP and not free.
NAT Requirement	Need NAT to access internet	No need NAT.
Check	write ipconfig in CMD	write "what is my IP" in browser.
Example	192.160.80.10	80.180.100.100

Q: 6(b)

What is congestion? Explain the slow algorithm used in TCP congestion control with a suitable Example. [4]

Ans: Congestion happens when the network gets overloaded. If too many data sent at a same time into a network, more than it can handle. ~~then the~~ This situation is known

congestion.

The slow start Algorithm helps TCP to avoid congestion by increasing sending rate gradually instead of sending too much data at once.

The process of slow start algorithm given below

step1: TCP begins data transfer with a tiny window (cwnd = 1 mss).

step2: Every time it gets Ack and gradually doubles the window (1 → 2 → 4 → 8...).

step3: If cwnd reaches ssthresh point TCP stops doubling.

step4: If any packet dropped, TCP understands that the network is overload and it goes back to slow start.

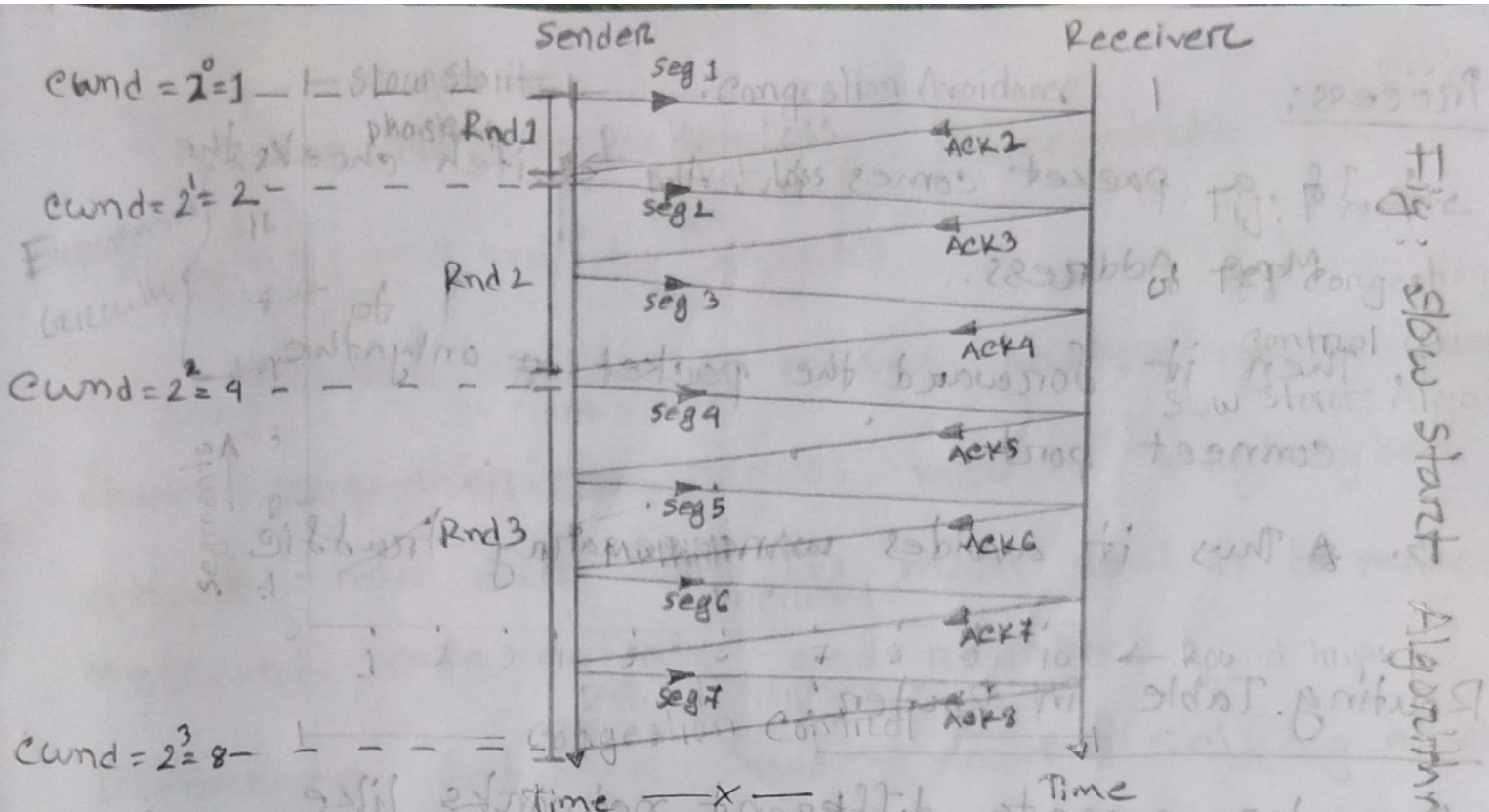


Fig: Slow start Algorithm

~~Note:~~

~~Congestion Control:~~

Q: 7(b) A switch ~~ca~~ uses a ~~ro~~ filtering table. and a router uses a routing table. Can you explain the difference? [3]

Filtering Table in switch:

A switch works inside a LAN. It uses a filtering table which ~~are~~ is basically a list of MAC addresses.

Process:

1. If a packet comes in, the switch check the Mac Address.
2. Then it forward the packet ~~to~~ only to the connect port.
3. Thus it avoides unneceesarry traffic.

Routing Table in Router:

A router connets different networks like LAN to WAN etc. It uses a routing table which contains routes based on IP Address.

Process:

1. When a packet comes, the router checks the destination IP.
2. Then it choose the best route/path to send this packet to next network.

Note

Flitering Table → Uses MAC Address to forward frames inside a LAN

Routing Table → Uses IP Addess to select best route between networks

Q: 7(c)

Define Network security. Differentiate between spoofing and sniffing attacks.

Ans: Network security means protecting a network from unauthorized access, misuse, ~~a syb~~ cyber attacks and data loss. Its main goal is to make network safe, private and reliable.

Difference between Spoofing and ~~&~~ Sniffing attack given below:

Aspects	Spoofing Attack	Sniffing Attack
Meaning	Attacker ~~pretends to~~ disguises themselves as trusted device by using fake identity.	Attacker secretly captures data traveling through a network.
How it work	Uses fake IP, MAC or email addesses.	Uses packet-sniffing tools.
Main Goal	To fool the victim and gain access.	To steal information.
Example	Fake IP address to ~~a~~enter a network	Using wireshark to ~~et~~ capture login passwords.

Note:

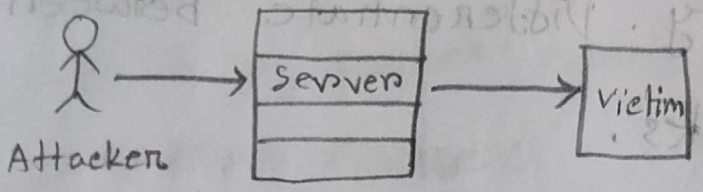
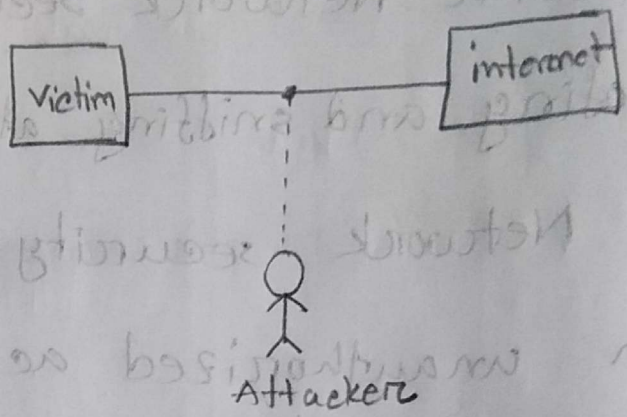


Fig: Spoofing Attack

Fig: Sniffing Attack



Q: 18-19

5 (b) What are the policies of congestion control in TCP? Explain any of them with necessary diagram.

Ans: TCP congestion control prevents network overload and manage data flow. It uses congestion window and some policies to adjust transmission rate. The congestion control policies in TCP are,

1. Slow start
2. Congestion Avoidance
3. Congestion Detection.

Slow Start Phase:

TCP stands sending data slowly and then increases quickly even exponentially but safely & until it reaches a limit. For this policy network doesn't get ~~love~~ overloaded suddenly.

Process:

1. Start with cwnd = 1 MSS
2. Every time received ACK and doubles cwnd.
3. Growth continues unit it reaches sshresh.
4. After that, TCP switch to congestion avoidance.

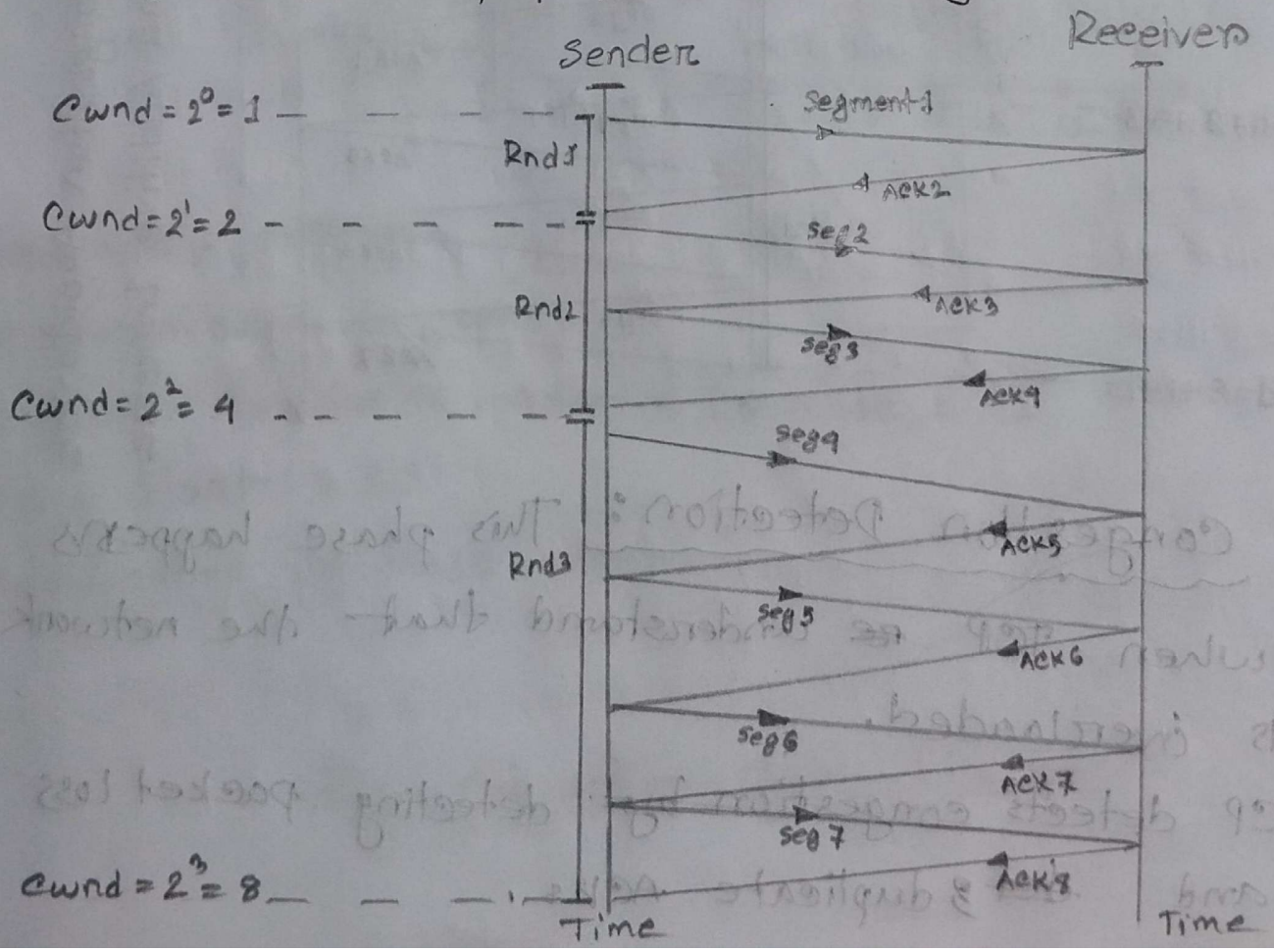


Fig: Slow Start Phase and Exponential Growth

Note:

2. Congestion Avoidance: When the congestion window reaches ssthresh, TCP stops ~~dud~~ the slow start phase means ~~stoping~~ stops doubling the rate.

It increases the cwnd slowly. by only 1 MSS per round trip (linear growth). This helps TCP to stay below the danger zone.

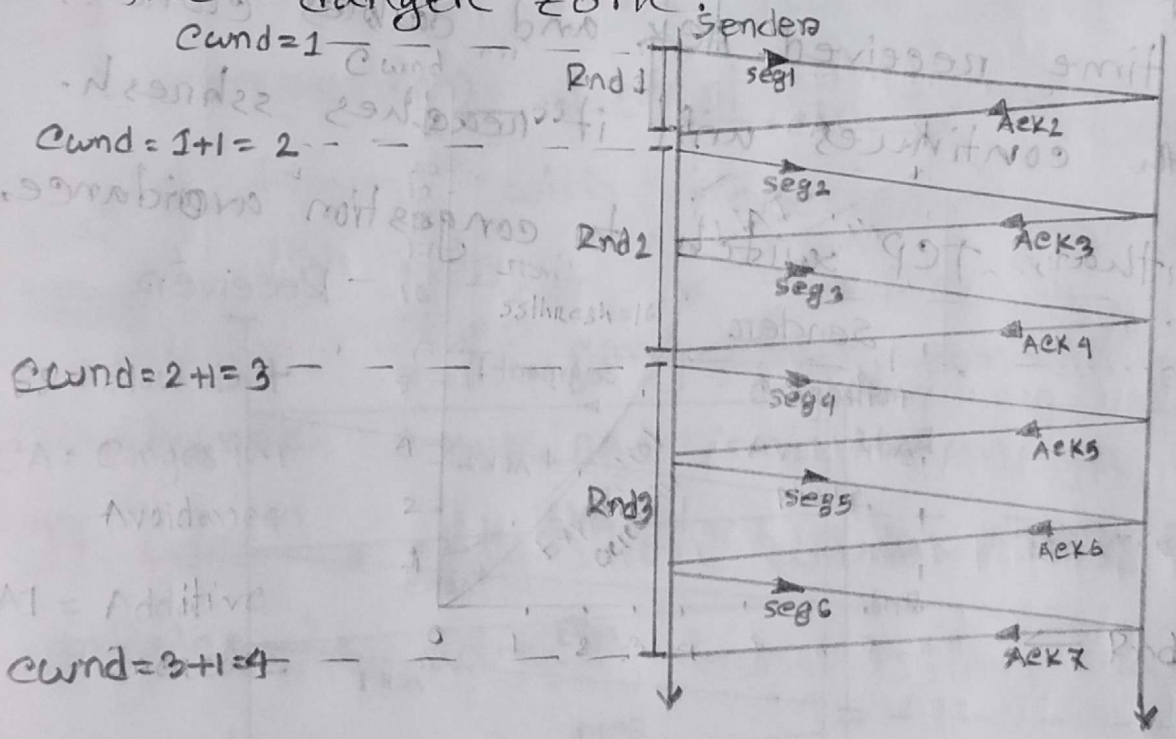


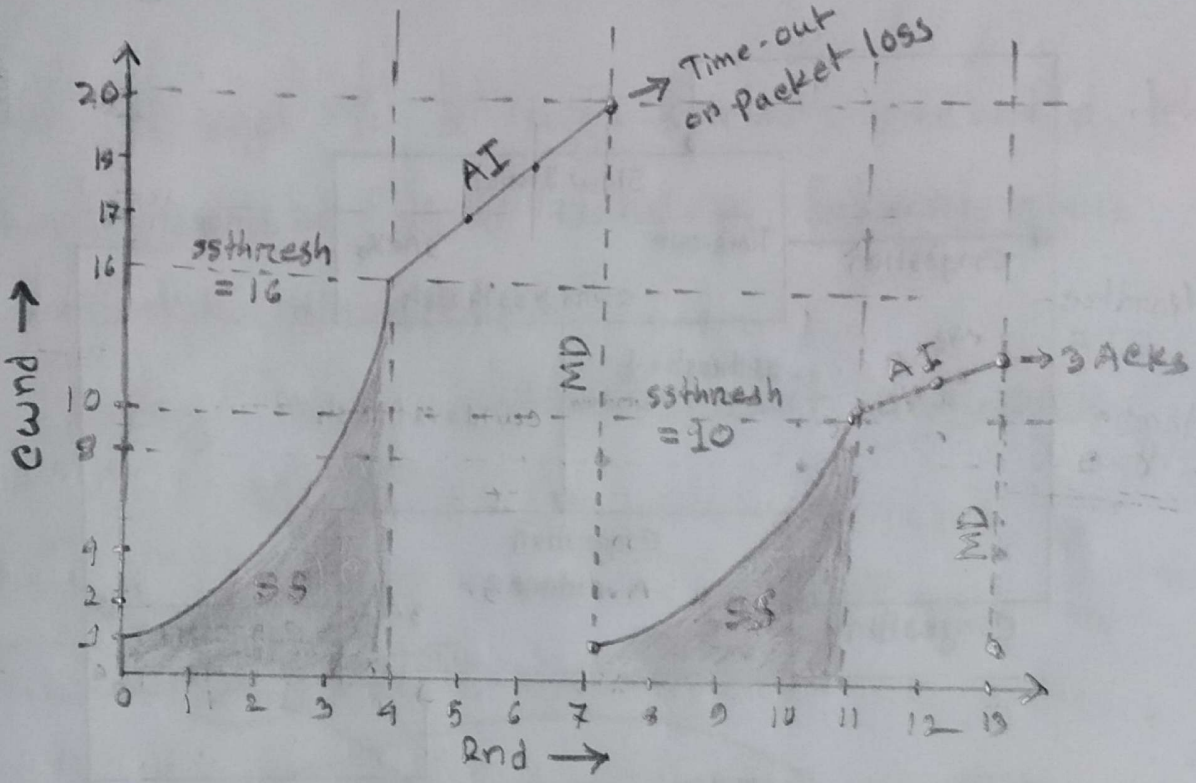
Fig: Congestion Avoidance and Additive Increase

3. Congestion Detection: This phase happens when TCP ~~as~~ understand that the network is overloaded.

TCP detects congestion by detecting packet loss and ~~det~~ 3 duplicate ACKs.

When TCP detect congestion it does such steps.

1. It cuts the congestion window (cwnd)
2. It sets a new ssthresh. (cwnd/2)
3. It ~~starts~~ restarts slow Start phase again.



Threshold = ssthresh

Congestion window = cwnd

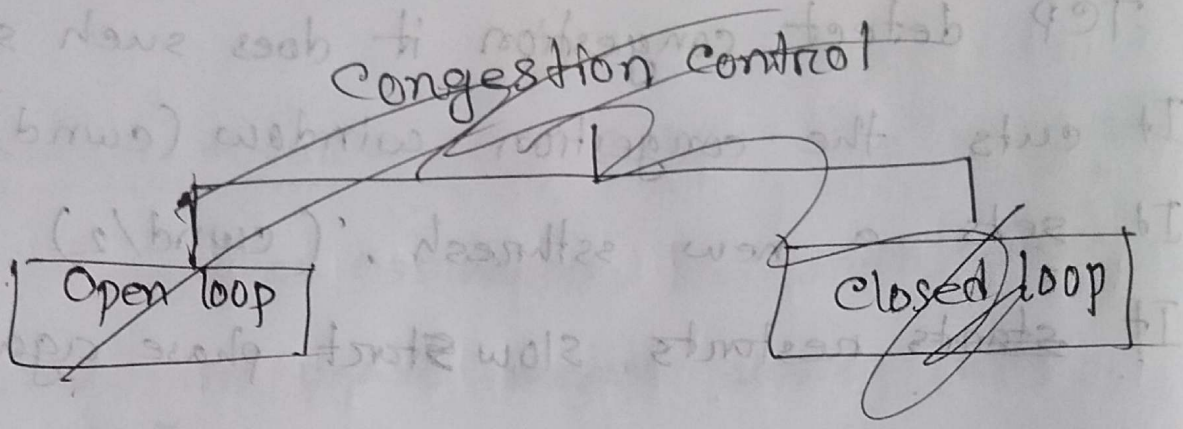
Congestion Avoidance, Additive Increase = AI

Slow Start = SS

Multiplicative Decrease = MD

Fig: Congestion Control in TCP

Note:



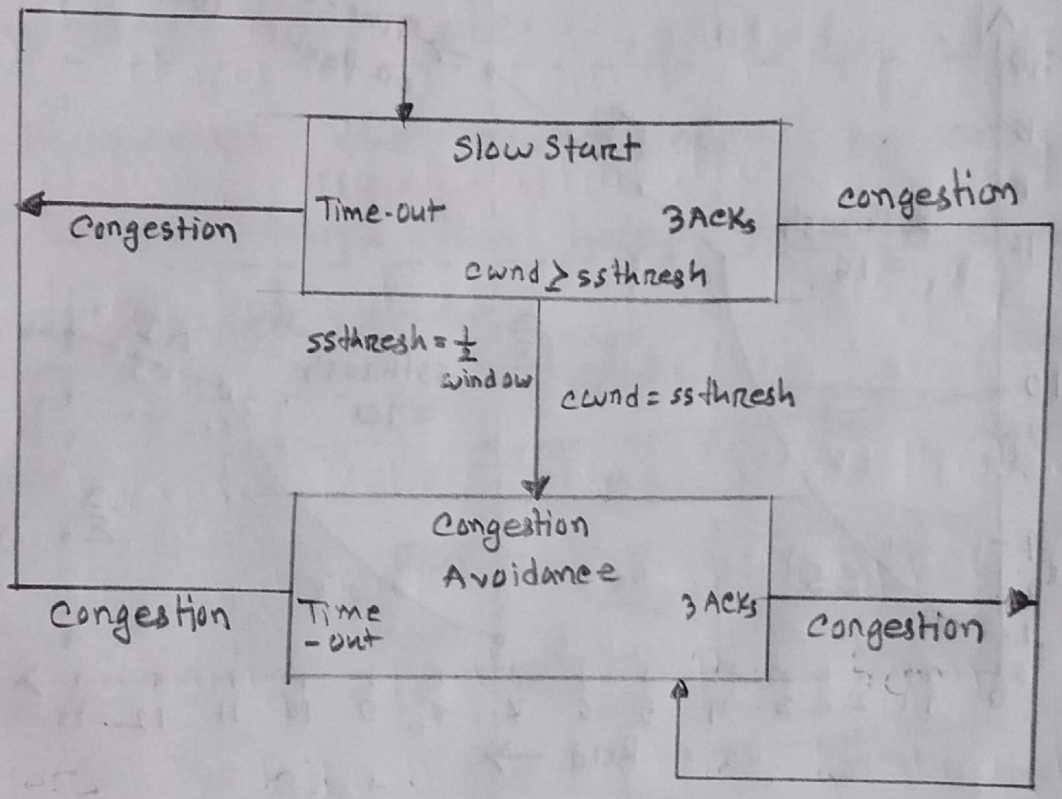


Fig: TCP congestion Policy Summary

Q: 19-20

6(a) What is Frame Relay? Why is Frame Relay a better solution for connecting LANs than T-1 lines? [3]

Ans: Frame Relays is a high-speed, packet switched WAN technology that sends data in frames over shared network circuits.

* Frame Relay is a virtual circuit network.

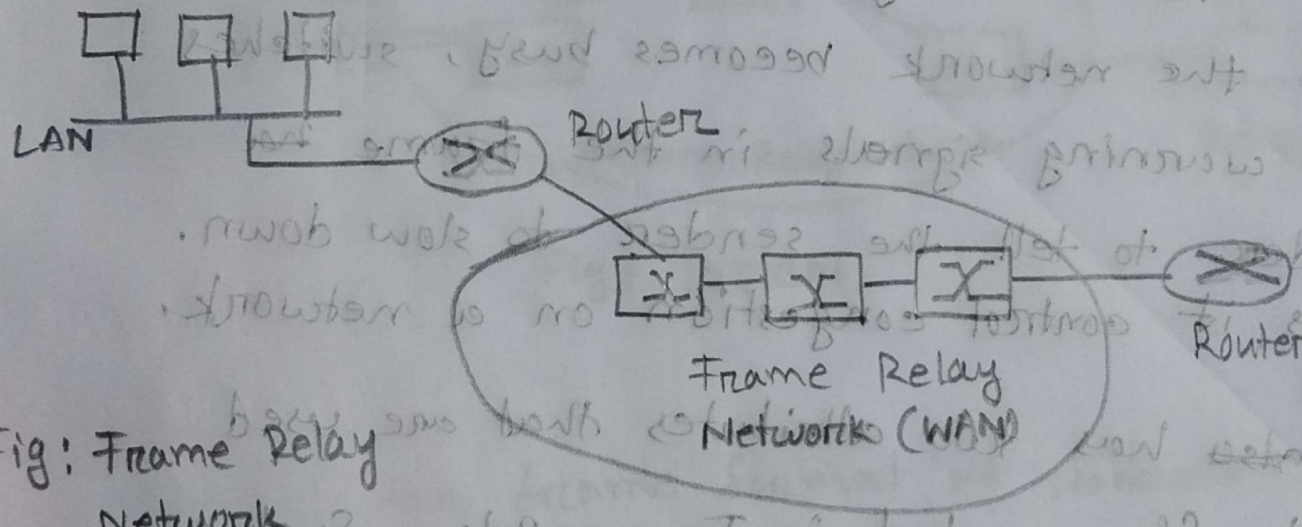


Fig: Frame Relay Network

Frame Relay is better than T-1 lines because it is cheaper, faster and flexible for connecting multiple LANs. It ~~share~~ uses a shared network instead of dedicated lines ~~of~~ for every location, reducing the cost. It also

allows extra bandwidth during heavy traffic and can be expanded easily. For those reason, Frame Relay is preferred over fixed speed T-1 lines.

6(d) 19-20 How does Frame Relay control congestion? What attributes are used for traffic control in Frame Relay? [3]

Ans:

Frame Relay uses a feedback mechanism. When the network becomes busy, switches send warning signals in the frame header to tell the sender to slow down. Thus it control congestion on a network.

It has two attributes that are used for traffic control in Frame Relay. Such as.

1. FECN (Forward Explicit Congestion Notification):

It warns the receiver that the path is congested.

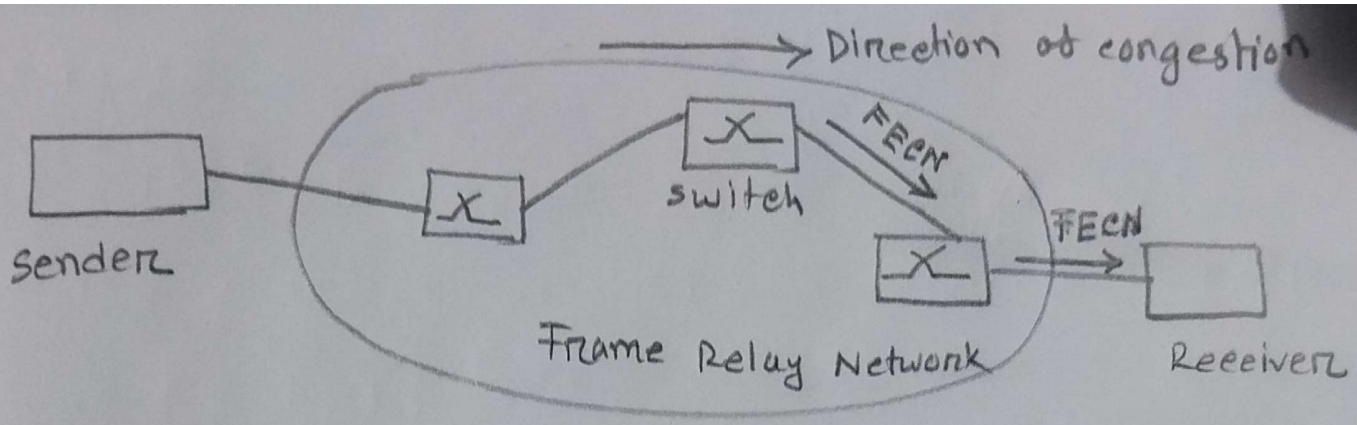


Fig: FECN

2. BECN (Backward Explicit Congestion Notification): It warns the sender that the path is congested.

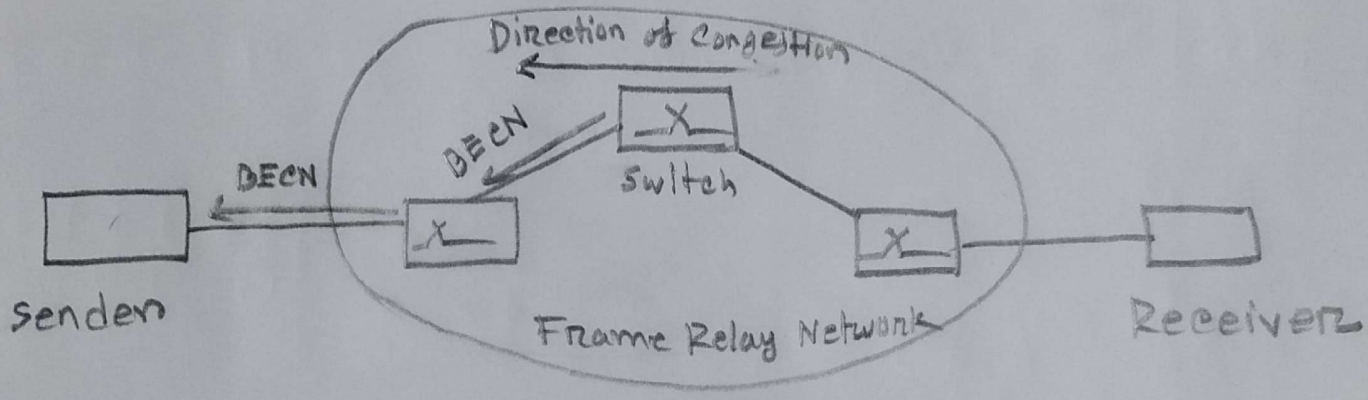


Fig: BECN

Q: 18-19

6(c) Depict the frame format of standard Ethernet. [3]

Ans: The ~~standard~~ frame format of standard ethernet is given below:

PREAMBLE	SFD	Destination Address	Source Address	Length	Data	CRC
7 bytes	1byte	6 bytes	6bytes	2bytes	46-1500 bytes	4 bytes

Details: The standard Ethernet frame contains the following fields:

1. PREAMBLE: It is a 7-byte section used for synchronization between sender and receiver.

2. SFD (Start Frame Delimiter): It is a 1 byte field that marks the exact starting of the frame

3. Destination MAC Address: This 6-byte field holds the address of receiver.

4. Source MAC Address: This 6-byte field holds the address of sender.

5. Length: A 2-byte field shows the length of data.

6. Data: This part carries the actual data and the capacity is 46-1500 bytes.

7. CRC: A 4 byte error-checking field used to detect corrupted bits using CRC method.

Q: 18-19

6 (b) Define physical, logical and ~~sok~~ socket address. [3]

Ans:

[1] Physical Address: A physical ~~Ad~~ address is the hardware address used at data link layer to indentify a device in the local network. It ~~devile~~ delivers data in the same network

Example: MAC Address → ~~A4:C8:02:02F:12:3D~~ 05:06:07:8A:9C:10

Note: You can write any 6 pairs of hexadecimal digit for MAC address.

[2] Logical Address: A logical address is the software assigned address used at the network layer to identify a ~~dr~~ deviee across the entire network.

Example: IP Address → 192.168.1.10

[3] Socket Address: A socket address is the combination of IP address and port address that uniquely ~~identify~~ identifies a specific endpoint for network communication ~~process on a device~~ between two process.

Example: ~~192.168~~ 192.168.1.10 : 80 → (IP + Port)

Note:

Port Address: The port address used at the transport layer of the TCP/IP model to identify the process running on a device.

Example: Port : 80 → HTTP (web browsing)
25 → Email (SMTP)
↳ simple mail transfer Protocol.

Specific Address: the specific address identifies the actual service ~~ma~~ name for the user.

Example: ~~www.mail.gmail.com~~ www.example.com

Q: 19-20

8(g) Write short note (any two): [4]

(i) Packet switching

(ii) circuit switching

(iii) HTTP

(iv) FDDI

(1.) Packet switching: Packet switching breaks data into the small packets and sends them independently through the ~~network. the~~ network.
Each packet may take a different path and they are reassemble at the destination.

Example: WhatsApp message is ~~em~~ sent as packet through the internet using the packet ~~swith~~ switching method.

(2.) Circuit switching: Circuit switching creates a dedicated path between sender and receiver before the transmission starts. The whole path stays reserved until the communication ends.

Example: Telephone calls use circuit switching.

(3.) HTTP (Hyper Text Transfer Protocol): HTTP is a application layer protocol used for transferring web pages between a browser and a web server. It works on a "request-response" model and usally uses port 80.

Example: When we open www.google.com, our browser uses HTTP to request the page.

(9.) FDDI (Fiber Distributed Data Interface):

FDDI is a high-speed network technology that uses optical fiber to create a fault-tolerant ring network. It offers speeds up to 100 Mbps.

Example: FDDI used as a backbone network in large organization.

Q: 19-20

6(e) Define subnetting and supernetting. How do their masks differ from default mask? [3]

Ans: Subnetting: Subnetting divides a large network into smaller sub-network. It used to manage IP address efficiently.

Supernetting: Supernetting merge multiple small networks into one large network. It is used by ~~IP~~ ISPs to reduce routing table size.

Difference from Default Mask:

* Subnet Mask: Uses more bits than the default mask.

Example: Default mask of class C → 255.255.255.0
Subnet mask → 255.255.255.192

* ~~Supnet~~ Supernet Mask: Uses fewer bits than the default mask.

Example: Combining class C networks uses mask 255.255.252.0.

Q: 18-19

8(b) How message authentication code (MAC) works? Does it provide confidentiality? Justify your answer. [4]

Ans: A Message Authentication Code (MAC) is short piece of information generated using

a secret key and the message.
When the sender sends the message, he also sends the MAC.

The receiver use the same ~~MAC key~~ shared secret key to generate a MAC at receiver side. Then compare both MACs.

→ If both MACs match → message is authentic.
→ If both MACs don't match → message is tempered.

Thus MAC provides message authentication.

No, MAC doesn't provide confidentiality. Because,
→ MAC checks whether the message was changed and whether it came from real sender.
→ It doesn't encrypt the message.
→ Anyone can read the message if they intercept it.

Confidentiality requires Encryption, not MAC.

Note:

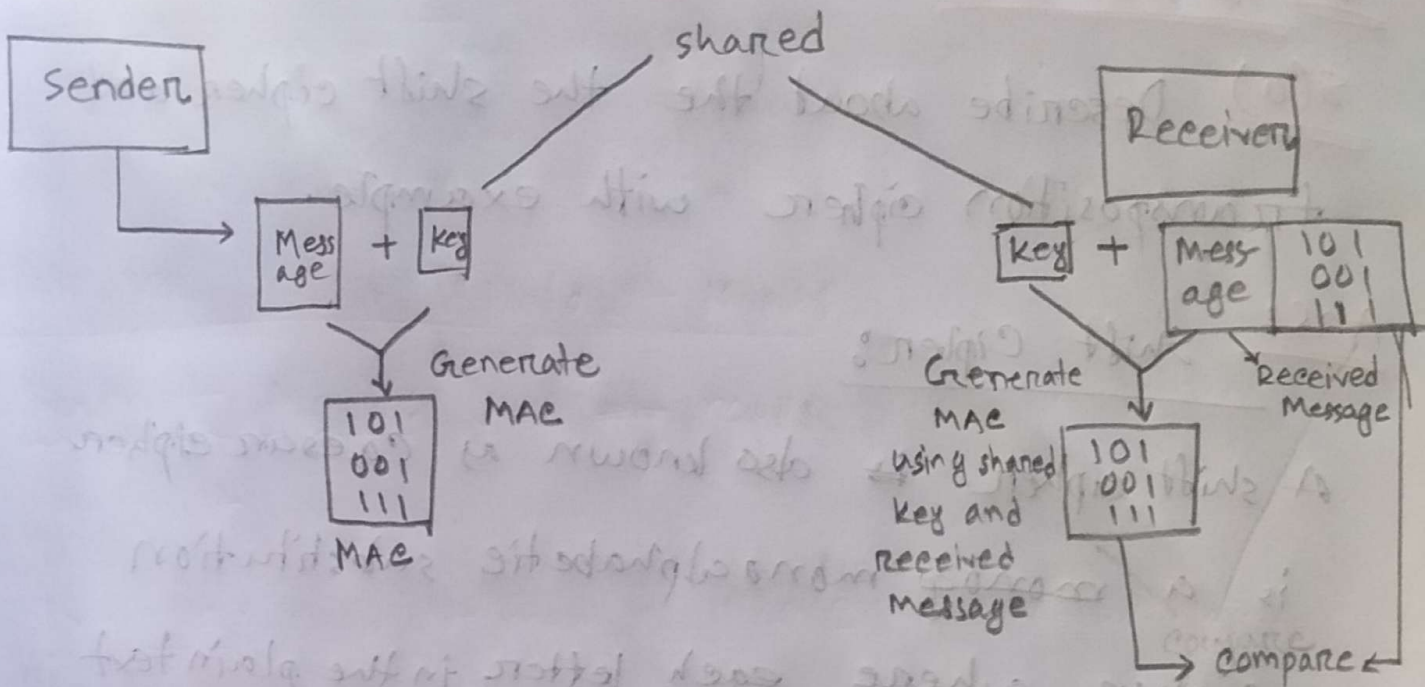


Fig: Working process of Message Authentication.

Q: 19-20

6(b) What are the difference between IPv4 and IPv6 addressing? [3]

Ans:

Aspects	IPv4 Addressing	IPV6 Addressing
Address size	32-bit	128-bit
Address format	Numeric, dotted decimal	Hexadecimal, colon-seperated
Example	192.168.10.1	2001:0db8::1
Address space	About 4.3 billion	Almost unlimited (3.4×10^{38})
Security	IPSec optional	IPSec mandatory
Header size	Large and complex	small and simple
Type of Addressing	unicast, broadcast, multicast	unicast, multicast, ~~broadcast~~ anycast.

Q: 19-20, 18-19

8(a) Describe about the the shift cipher and transposition cipher with example.

Ans:

Shift Cipher:

A shift cipher ~~is~~ also known as caesar cipher is a ~~monog~~ monoalphabetic substitution cipher where each letter in the plaintext is shifted by a fixed number (called key) of position in the alphabet.

→ ~~Eg~~ Encryption: Shift letters down by the key value.

→ Decryption: shift letters up by the key value

Example: key = 15

plaintext = HELLO

shift each letters positions by 15 and get: WTAAD.

Transposition cipher: (keyed)

A transposition cipher rearranges (permutes) the position of characters in a block. Block size ~~will be~~ given ~~in the question~~. = key length.

The key defines reordering ~~pat~~ pattern.

Example: key: 2 4 1 3 ∴ Block size = 4

Plaintext: Hello My Dear

Plaintext block: Hell OMYD earz [যদি block size 4 না হয় তাহলে কোথে একটা z add করে 4 বানাবে] (bogus characters)

Ciplertext: ElHl MDOY azer

ElHlMDOYazer → এভাবে বিনা space দিয়ে লিখতে হবে।