Chapter 02: Application Layer

2). Describe how Web Caching can reduce the delay in receiving a requested object. Will Web caching reduce the delay for all objects requested by a user or for only some of the objects? Justify.

- Web Cache has its own disk storage & keeps copies of recently requested objects in this storage.
- When the user requests for an object, the User's HTTP requests are first directed to the web cache. If the requested object is present in the web cache then it sends the requested object to the client.
- If the requested object is not present in the web cache, then request message is sent to the origin server from the cache.
- In this way, the web caching ~~delays~~ reduces the delay in receiving the requested object.
- Here, we can see that Web Caching helps to ~~delay~~ reduce the delay for the requested objects that are present on its disk.
- However, for the objects that are not present in the cache, needs to be accessed from the server itself. So, here the delay is not reduced.

- So, Web caching does not reduce the delay for all the objects requested by a user.
- However, for the objects that are not present in cache, the copy of response is taken to the cache when the server sends the response to the request. So that, the next time if same request is requested then it can be fulfilled from cache itself.

3). List five non-proprietary Internet Applicat^n's and the application-layer protocols that they use.

They are as follows:-

a). The Web : HTTP

b). Remote login : Telnet

c). Network News : NNTP

d). e-mail : SMTP

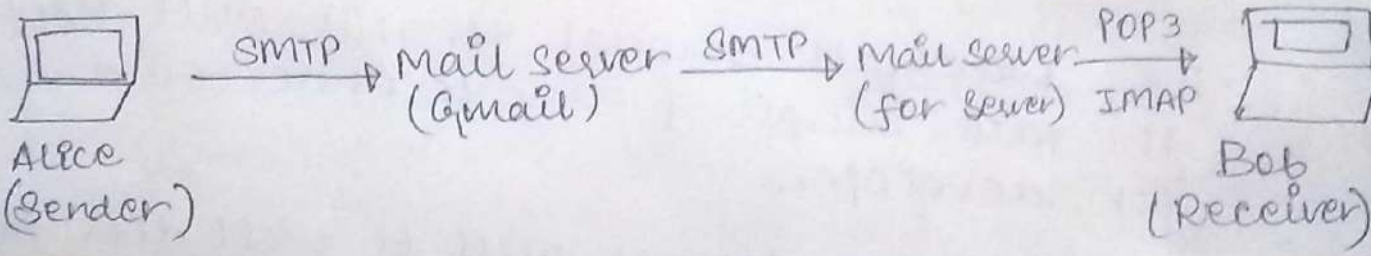
e). File-transfer : FTP

4). What is the difference between network architecture & application architecture?

- Network Architecture is the process of organizing the communication process into the layers.
- It can also be considered as the design of communication network.

- Application Architecture is the architecture which is designed by the application developer.
- This type of architecture usually dictates the complete or broad structure of an application.

5). Suppose Alice, with a Web-Based email account sends a msg to Bob, who accesses his mail from his mail server using POP3. Discuss how the message gets from Alice's host to Bob's host. Be sure to list the series of application-layer protocols that are used to move the message between the two hosts.



- Message is first sent from Alice's host to her mail server over HTTP/SMTP.
- ~~Alice~~ Then, Alice's mail server sends the message to Bob's mail server over SMTP.
- Bob then transfers the message from his mail server to his host over POP3.
- The main difference here b/w IMAP & POP3 is that IMAP has more features than POP3.
- IMAP : Internet mail access protocol.
- POP3 : Post office protocol.

6). From a user's perspective, what is the difference between download-and-delete mode and the download-and-keep mode in POP3?

- In the download-and-delete mode, client receives messages from a POP, then delete the messages.
- In the download-and-keep mode, client receives messages from a POP, and store messages, never deleted messages.

4). How does SMTP mark the end of a message body? How about HTTP? Can HTTP use the same method as SMTP to mark the end of a message body? Explain your answer.

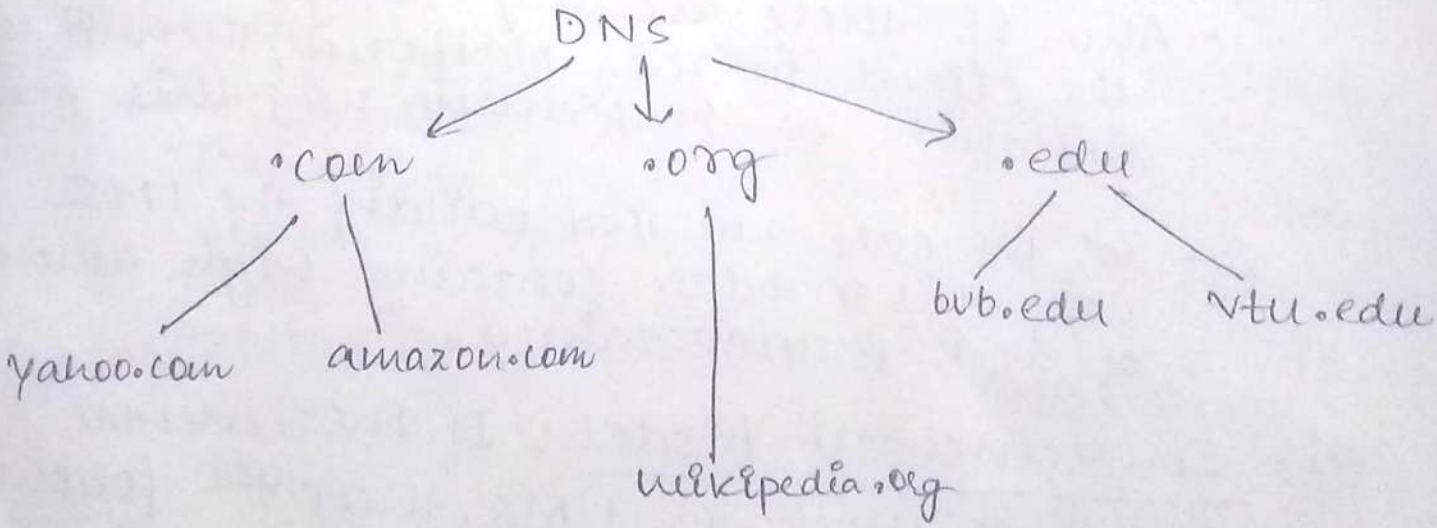
- SMTP uses a line containing only a period to mark the end of a message body.
- HTTP uses "Content-length header field" to indicate the length of a message body.
- NO, HTTP cannot use the method used by SMTP because HTTP message could be binary data, whereas in SMTP, the message body must be in a 7-bit ASCII format.

8). What information is used by a process running on one host to identify a process running on another host?

The IP address of the destination host and the port number of the destination socket is identified in such case.

9). What are the different categories of DNS present in real world?

- DNS stands for Domain Name Services.
- DNS is used for mapping of domain name-to IP address & vice-versa.
- Since, we have billions of servers across globe, remembering the IP address of each server is not possible.
- Hence, DNS are used as an appn that maps servers to IP address.



- DNS categories are:
  a). Recursive resolvers.
  b). root nameservers.
  c). TLD nameservers
  d). Authoritative nameservers

a). Recursive Resolver : It acts as a middleman b/w a client & DNS nameserver. After receiving a DNS query from a web client, a recursive resolver will either respond with cached data or send a request to a root nameserver.

b). DNS root nameserver : A root server accepts a recursive resolver's query which includes a domain name, & the root nameserver responds by directing the recursive resolver to a TLD nameserver, based on the extension of that domain (.com, .net, .org, etc).

c). TLD nameserver : ~~A T~~ It maintains information for all the domain names that share a common domain extension, such as .com, .net or whatever comes after the last dot in a ~~url~~ url.

d). Authoritative Nameserver : It is usually the resolver's last step in the journey for an IP address. The authoritative nameserver contains information specific to the domain name it serves (eg. google.com) & it can provide a recursive resolver with the IP address of that server found in the DNS record.

10). Explain the working of DNS system.

- The process of DNS resolution involves converting a hostname into a computer-friendly IP address.
- When a user wants to load a webpage, a translation must occur b/w what a user types into their browser and the machine friendly address necessary to ~~take~~ locate that webpage.
- There are 4 DNS servers ~~installed~~ involved in loading a webpage.

1). DNS recursor.
2). Root nameserver.
3). TLD nameserver.
4). Authoritative nameserver.

(write same explanation as previous question).

TRANSPORT LAYER (LP)

Ch-5

1). Explain the need of dataplane & control plane in network layer.

Sol$^{n^o}$:

* **DataPlane :-**

- In Routing, data plane refers to all the functions & processes that forward packets/ frames from one interface to another based on control plane logic.

- Routing table, forwarding table & the routing logic constitute the data plane function.

- Data plane packet goes through the router & incoming & outgoing of frames are done based on control plane logic.

- In short, we can say that it is responsible for moving packets from source to destination.

- It is responsible for forwarding actual IP packet.

* Control Plane :-

- It refers to all functions & processes that determine which path to use to send the packet or frame.
- It is responsible for populating the routing table, drawing network topology, etc.
- It is responsible for how packets should be forwarded.
- It performs its task independently.
- In general way, we can say in control plane it is learned what & how it can be done.

3). which fields of the IP header change from router to router? why the value is changing from router to router?

Sol^n Time-to-live (TTL) field of the IP header change from router to router.

- TTL is a limit that tells till how long the packet has to travel.
- It is a count which decreases by 1 by each passing router node. when it becomes 0, then the packet is burst off.
- This ensures that a packet is dropped once it reaches its pre defined hop-limit (end).
- This field changes its value from router to router to ensure that no packet lives infinitely in the network hence cause flooding.
- Every router checks this value against 0, & if it finds so, it drops the packet.

2). IPv4 protocol is an unreliable protocol, is it possible to make it as reliable for application layer? Justify your answer.

- IPv4 is an unreliable protocol because it does not guarantee the delivery of a datagram to its destination.
- It is the first layer that introduces the virtual network abstraction that is the basic principle of the Internet model.
- It does not provide any functionality for error recovering for datagrams that are either duplicated, lost or arrive to ~~the~~ remote host in another order than they are send.
- If no such errors occur in the physical layer, the IP protocol guarantees that the transmission is terminated successfully.

Drawback of Classful Addressing

7). Need for classless Addressing.

1). Large Blocks will result in address wastage :-
If an organization is assigned for a set of address in class A, then if it doesn't have enough addresses to be used then it might lead to address wastage.
Since, class A has 2^{24} hosts,
∴ There is a possibility that a set of addresses are wasted if we do class addressing.

2). Fewer blocks will result in insufficient address :-
Similarly, in this case if the organization has large no. of machines but is alloted with a set of address from class C, then the address will be insufficient.

3). less address left & more customers :-
If we do class addressing, then there is a possibility that the no. of address left is less than the requirement.
So, we go for classless addressing

Solutions to all these are :-
a). subnetting b). Masking
c). Supernetting

5c) Block 130.56.0.0/16

No. of subnets = 1024.

$2^{10} = 1024$

Block size = $2^{32-16} = 2^{16}$

Default is 16 bits for class B without subnetting
For subnetting we need extra 10 bits so
mask is /26

255.255.255.11000000

(a) → 255.255.255.192 // Subnet mask.

(b) No. of address in each subnet is nothing but no. of hosts

No. of hosts $= 2^h - 2$

$= 2^6 - 2 = 64 - 2 = 62$

(c) First & last in 1st subnet = 130.56.0.1

130.56.0.62

(d) First & last in last subnet = 130.56.255.193

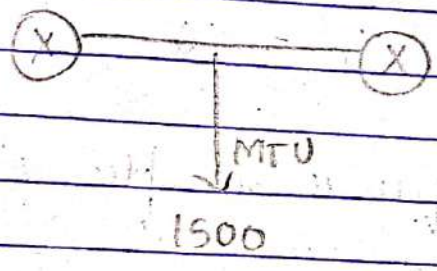
130.56.255.254

6a) No. of fragments = $\left\lceil \frac{\text{Datagram} - \text{header}}{\text{MTU} - \text{header}} \right\rceil$ ceil

Bytes Id # (same for all) fragno. flag frag offset (first byte / 8)

Various IP fields.

Bytes	ID	flag	frag offset
0-1479=[1480]	1	1	0
1480-2959	1	1	185
2960-4402	1	0	370



Theory

1) multiplexing & demultiplexing
2) ICMP ip4 , Congestion Control principles
3) Classfull addressing demerits
4) IP addressing . Differentiate classless & classfull
5) rdt FSM - rdt 1.0 rdt 2.0 rdt 3.0
6) Header formats - TCP, UDP, IP, ICMP
7) Pipelining - extra
8) 3 way handshake (timing diagram)
9) Compare virtual circuit network & datagram network
10) III dataplane & controlplane

1) * Simple & easy to implement
* Connection establishment time is reduced
* Data integrity or security not needed
* It is loss tolerable appl'n

3) 5-bit sequence no = $2^5 = 32$

0-31 (32)

0-31 (64)

0-31 (96)

97	98	99	100
0	1	2	3

4 is the sequence no after 100th

4) 0045 DF00 0058 FE20

Source Dest length checksum

(a) 69 = Source

(b) 56832 = Dest

(c) 88 = length

(d) Actual data = 80

(e) Server to client

(f) Trivial file transfer protocol

5) UDP protects boundaries of a msg not TCP
It doesn't fragment & reassemble like TCP

6) Not the case

7) | URG | ACK | PSH | RST | SYN | FIN |

→ UAPRSF (acro)

(i) all zeroes. The segment is part of data transmission without piggybacked acknowledgment

(ii) FIN set - FIN segment to request the termination of connection

(iii) ACK & FIN segment (iv) Request for resetting

(v) SYN segment (vi) SYN + ACK segment

9)

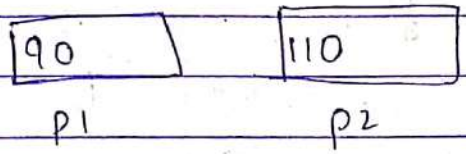
App: DNS (UDP) & HTTP (TCP)

DNS → to get the dest IP

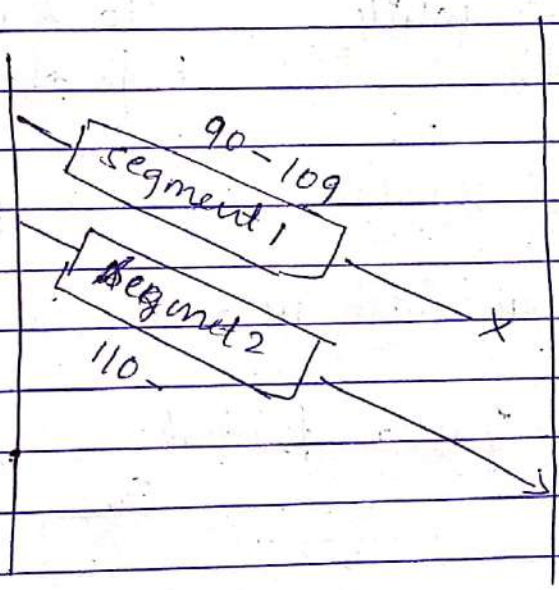
HTTP → to request data

10) rdt

11)



110 - 90 = 20 bytes



Ack = x, 90

12) Telnet port = 23 Client = Any random no above 1023

client A = 1467 client B = 1513

A → S	1467	23
B → S	1513	23
S → A	23	1467
S → B	23	1513

UNIT - 3

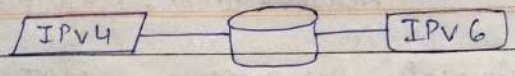
CHAPTER - 05

Network layer (IP) : Data Plane

1). Explain the process of NAT with diagram.

- By the help of NAT Protocol Translation Technique, the IPv4 and IPv6 networks can communi-cate with each other which do not understand the address of different IP version.

- Generally, an IP version doesn't understand the address of different IP version, for the solution of this problem we use NAT-PT device which remove the header of first (sender) IP version address & add the receiver IP version add so that the Receiver IP version add understant that request is sent by the same IP version & vice-versa.

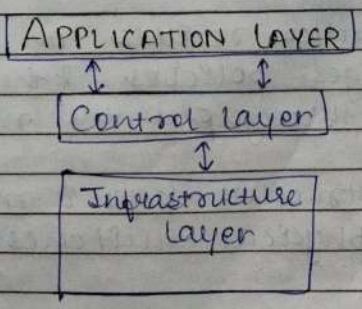


Host NAT Enabled Device

- In above diagram, an IPv4 add communicates with IPV6 add via a NAT-PT device to communicate easily.
- In this situation, IPv6 address understan that the request is sent by same IP version (IPV6) & it responds.
- In this method, based on the requirements, the header changes.

2). With neat diagram, explain SDN. (Software-Defined Networking)

- SDN is an architecture that aims to make networks agile and flexible.
- The goal of SDN is to improve network control by enabling service providers to respond quickly.
- A SDN architecture comprises of 03 layers:
  - (i) application layer
  - (ii) control layer
  - (iii) Infrastructure layer
- It allows programmatic management, control & optimization of network resources.



- The application layer contains the typical network applications.
- The SDN programs within the application layer define the new approach of data communication b/w controllers & services that run over the network.
- The control layer represents the centralized SDN controller software that acts as the brain of the software-defined network.
- This controller resides on a server & manages policies & the flow of traffic throughout the network.
- The infrastructure layer is made up of the physical switches in the network.

Working of SDN:-

- SDN technology focuses on the separation of the network control plane from the data plane.
- where control plane makes decisions about how pkts should flow through the network, the data plane actually moves packets from place to place.

* Working of SDN:-

- A pkt arrives at a network switch & rules built into the switch's proprietary firmware tell the switch where to forward the packet.
- The switch (data plane device) queries the controller for guidance as needed and it provides the info about traffic it handles.

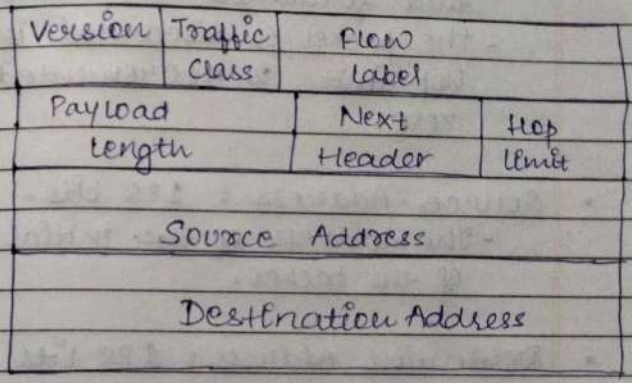
- The switch then sends every pkt going to the same destination along the same path & treats all the pkts the exact same way.

4). Differentiate between IPv4 and IPv6.

IPv4	IPv6
(i) Addresses are 32 bits (4 bytes) in length.	(i) Addresses are 128 bits (16 bytes) in length.
(ii) Address (A) resource records in DNS to map host names to IPv4 addresses.	(ii) Address (AAAA) resource records in DNS to map host names to IPv6 addresses.
(iii) Pointer (PTR) resource records in the INADDR.ARPA DNS domain to map IPv4 addresses to host names.	(iii) PTR resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
(iv) IPsec is optional & should be supported externally.	(iv) IPsec support is not optional.
(v) Header does not identify packet flow for QoS handling by routers.	(v) Header contains flow label field, which identifies pkt flow for QoS handling by router.
(vi) Both routers & the sending host fragment packets.	(vi) Routers do not support pkt fragmentation sending host fragments packets.
(vii) Header includes a checksum.	(vii) Header does not include a checksum.
(viii) Header includes options.	(viii) Optional data is supported as extension headers.
(ix) ARP uses broadcast ARP request to resolve IP to MAC/Hardware Address.	(ix) Multicast Neighbor Solicitation msgs resolve IP add to MAC adds.

(x) Internet Grp Mngmt Protocol (IGMP) manages membership in local subnet groups.	(xi) Multicast Listener Discovery (MLD) messages manages membership in local subnet groups.
(xi) Broadcast adds. are used to send traffic to all nodes on a subnet.	(xi) IPV6 uses a link-local scope all-nodes multicast address.
(xii) Configured either manually or through DHCP.	(xii) Does not require manual configuration or DHCP.
(xiii) Must support a 576-byte packet size (possibly fragmented)	(xiii) Must support a 1280-byte pkt size (without fragmentation)

3). Explain IPv6 Header with neat diagram.



- Version : 4 bit version number of Internet protocol = 6.
- Traffic class : 8-bit traffic class field.
- Flow-label : 20-bit field.
- Payload length : 16-bit unsigned integer, which is the rest of the packet that follows the IPV6 header, in octets.
- Next Header : 8-bit selector. Identifies the type of header that immediately follows the IPv6 header. Uses the same values as the IPv4 protocol field.

- Hop limit : 8-bit unsigned integer.
  - Decremented by one by each node that forwards the packet.
  - the packet is discarded if the hop limit is decremented to zero.

- Source-Address : 128 bits.
  - The address of the initial sender of the packet.

- Destination Address : 128 bits.
  - The address of the intended recipient of the packet.
  - The intended recipient is not necessarily the recipient if an optional routing header is present.