Hi This is Kapil :)

DOMS | Page No.
Date / /

# NETWORK Layer

Q1) Explain in detail the different classes of IPv4 addresses.

A1) IPv4 address is a 32 bit no. that uniquely identifies a given network interface on a system.
Address can be in 3 notations
- binary
- hexadecimal
- dotted decimal

Internetwork Protocol (IPv4) provides a best effort network layer service, and each endpoint is identified by a globally unique IP address. Network layer PDU's are known as packets or datagram's.

1. Classfull addressing

Classes are :-

A - 0 - 127.255.255.255 (n=8)
B - 128 - 191.255.255.255 (n=16)
C - 192 - 223.255.255.255 (n=24)
D - Multicast 224 - 239
E - Experimental 240 - 255.255.255.255

Problems :-
1. Class A, B address are wasted & no. of addresses in class C is very low.
2. Class D address are used for multicast ∴ available as a single block only.
3. Class E addresses are reserved.

2. Classless Addressing
- Helps to reduce wastage of blocks
- Uses Subsetting
- We give IP address & give no. of bits for mask along with it eg. 192.168.1.1/28

DOMS | Page No.
Date / /

Subnet mask is found by putting given no. of bits out of 32 as 1

- Subnetting - dividing a large block of addresses into several contiguous sublocks & assigning them to diff smaller networks.

Reduces network traffic & optimises network performance

In Classful

- No. of addresses in block $N = 2^{32-n}$
- to find first address we keep the n rightmost bits & set the (32-n) rightmost bits.
- To find last address n rightmost (32-n) leftmost

n = length of netid in bits

Classless Addressing

n = prefix length

$N = 2^{32-n}$

first address = (any address) AND (network mask)

Last address = (any address) OR [NOT (network mask)]

DOMS | Page No.
Date / /

Q2) Compare Virtual Circuits to Datagram Networks.

A2]

| | Virtual Circuits | Datagram Networks |
|---|---|---|
| 1. | Connection oriented service in which there is an implementation of resources like buffers, CPU bandwidth, etc. | • Connectionless service where no resources are required for transmission of data. |
| 2. | Less complex | • More complex. |
| 3. | Due to fixed path and assurance of fixed resources they are more reliable. | • Due to dynamic resource allocation & dynamic path they are less reliable |
| 4. | Same path is followed by all data packets | • Different path followed by all data packets |
| 5. | All packets use same header | • Different headers are used |
| 6. | All resources get reserved before the transmission path followed by first data packet is fixed & every other packet use same path | • Data packets are free to decide path thus path is not fixed. |
| 7. | ATM (Asynchronous Transfer Mode) used in telephone calls | • used by IP network used by Internet |

Q3] The address in block is given as 73.25.16.27. Find the no. of address in block, the first & last address.

Soln] Given IP address 73.25.16.27

73 is between 0 & 127 ∴ class of IP address = A

no. of bits in netid = 8 = n

$N = 2^{32-8} = 2^{24}$

first address - 73.0.0.0

last address - 73.255.255.255

Q4] Explain the concept of Subnetting & masking.

Subnetting - dividing a large block of addresses into several contiguous subblocks & assigning them to diffe small networks. Also called subnet routing / addressing

Benefits
- reduces network traffic
- optimises network performance
- simplified network management

Masking - a process that extracts the address of the physical network from an IP address is masking.
1. Boundary level masking two masking nos. are considered i.e 0 or 255
2. Non Boundary level masking - other values from 0 to 25

a) Address = 167.199.170.82/27

n = 27

∴ 27 1's & 5 0's

$N = 2^{32-n} = 2^5 = 32$

We use AND operation

Q4] Explain the concept of Subnetting & masking.

Subnetting - dividing a large block of addresses into several contiguous subblocks & assigning them to different small networks. Also called subnet routing / addressing

Benefits
- reduces network traffic
- optimises network performance
- simplified network management

Masking - a process that extracts the address of the physical network from an IP address is masking
1. Boundary level masking two masking nos. are considered i.e 0 or 255
2. Non Boundary level masking - other values from 0 to 255

Q) Address = 167.199.170.82/27

n = 27

∴ 27 1's & 5 0's

$N = 2^{32-n} = 2^5 = 32$

We use AND operation

Q7) IPV4 Datagram Header explain in detail.

A7) Datagram is a part of IPv4 header. It represents payload size & header. It is a 16 bit field. IPv4 is combination of both header & payload size and is in range of 20 bytes to 65535 bytes

- Header Size - 160 bits to 480 bits
  First 5 rows are mandatory.
- Payload - 0 bytes to 65535 bytes

IPV4 Datagram Header

| Version 4 | Header length | Type of Service | Total length 16 bits. |
|---|---|---|---|
| Identification (16 bits) | | 0 DF MF | Fragment offset |
| Time to live (8 bits) | Protocol (8 bits) | | (Header checksum) |
| Source IP | | | |
| Destination IP | | | |
| Option (0-40 bytes) | | | |
| Data | | | |

1. Version - 4 bits fixed to 0100 → decimal (4) for IPv4
2. HLEN - (Header length) 4 bits
3. Type of Service - 8 bit field used for quality of service
   - a) Precedance - means priority, immediate routine, etc
     lowest priority bits are discarded first
   - b) Delay - if needed delay = 1 else delay = 0
     used in video calling
   - c) Throughput

in all cases it need is high if a
else 0

DOMS | Page No.
Date / /

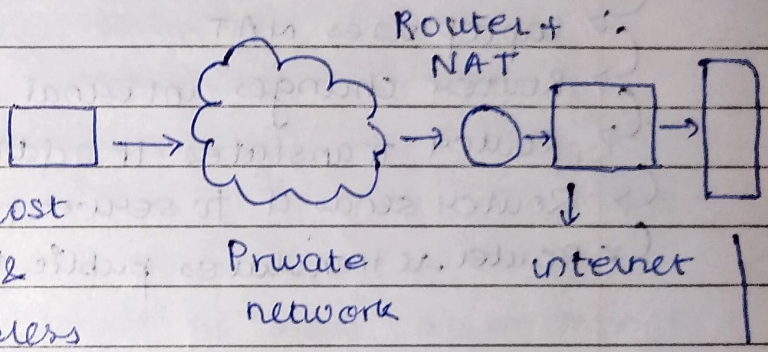
d) Reliability
e) Cost - low cost = 1 else = 0, helps to select shortest path towards destination
f) last bit - reserved for future purpose
4. total length - 16 bit field 20-65535 bytes
5. Identification - helpful for identifying fragments.
• when IP datagram fragmented each datagram is given a header no. - used in reassembly of fragments.

6. Flag bits — first bit is reserved bit
— second bit DF (Dont Fragment) ← 0, 1
when DF = 0 → fragment datagram
when DF = 1 → dont fragment
— MF (3rd bit) More Fragments.
MF = 0 → current fragment is last
MF = 1 → current fragment is NOT last

7. Fragment offset - 13 bit field. Tells position of a fragmented datagram
8. Time to live - 8 bits, indicates maximum no. of hopes
* if TTL = 0 datagram is discarded
9. Protocol - 8 bit no. that defines what protocol is used inside the IP packet
10. Header Checksum - 16 bit, checks for errors
11. Source IP address - 32 bit IP address of sender
12. Destination " " - " " " of recieiver
13. Option - makes or gives datagram option to be of a variable length.

Q8) Explain Network Address types and example.

A8) NAT allows multiple devices to alloco internet through a single public address. It is a process in which one or more local IP address is converted into one or more Gloabal IP address and vice versa.
Port nos are also translated. i.e masking of port no. of host with another port number.
Operates on router or a firewall




- a device on private net. sends a req to access internet.
- Router recieves the req & replaces the private IP address with it's own public address.
- Rounter sends req to access internet via public address
- When Response is recieved it translates back to host using a translation table to map public address to private address.

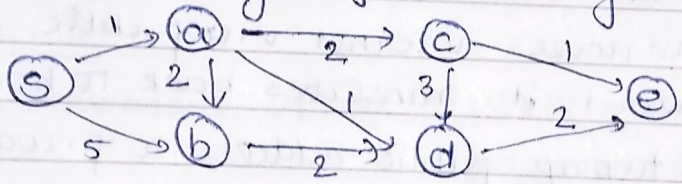
1. Static NAT - specific private IP address is always mapped to another public IP address
2. Dynamic NAT - a pool of public IP addresses are used to map a private IP address.
3. Port Address Translation - Single public IP address maps multiple private addresses using ports

Advantages:-
- conserves legally registered IP addresses.
- provides privacy
- elimnates address reaumbering

Disadvantages -
- path delays due to translation
- Online gaming doesn't function with NAT enabled
- Router tampers with port numbers.
- Complicates tunelling protocols IPsec.

Example :-
- Laptop connected to home address using NAT
- Network connects to a router
- Laptop uses NAT
- Router changes internal IP address from private to pub
- Router translates IP address
- Router sends it to server to access internet
- Router re translates public to private address.

Q9) Solve using Dijkstra's Algo.




Iteration 1

| s | a | b | c | d | e |
|---|---|---|---|---|---|
| - | s | s | - | - | - |
| ∞ | ~~1~~ | ~~5~~ | ∞ | b | b |

| s | a | b | c | d | e |
|---|---|---|---|---|---|
| - | s | A | A | A | - |
| - | 1 | 3 | 3 | 2 | ∞ |

| S | a | b | c | d | e |
|---|---|---|---|---|---|
| - | S | A | A | A | - |
| | 1 | 3 | 3 | 2 | ∞ |

no change since b → d will make total cost = 5 > 3.

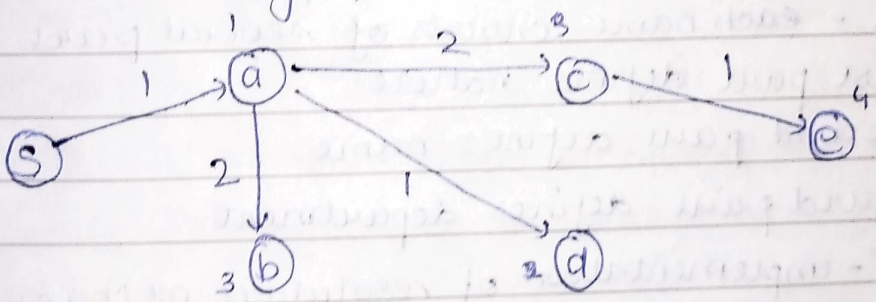
| S | a | b | c | d | e |
|---|---|---|---|---|---|
| | S | A | A | A | C |
| | 1 | 3 | 3 | 2 | 4 |

| S | a | b | c | d | e |
|---|---|---|---|---|---|
| | S | A | A | A | C |
| | 1 | 3 | 3 | 2 | 4 |

// Ans

P → E is total cost = 4 which is same so no change.

Now draw graph with only these edges.




traversed path is S, a - d, b, c, e

Q10) solve using Distance Vector Routing

DOMS | Page No.
Date / /

# APPLICATION LAYER

Q1) Explain DNS in detail.

A1) DNS is a host name to IP address translation service. It is a distributed database implemented in hierarchy of name servers. Helps to exchange message between clients and servers.

- A mapping is needed to change dns to IP address, so DNS converts domain name to IP address.

Domain → Generic .com, .edu, .mil etc.
Domain → Country .in, .us
Domain → inverse domain

- DNS record - stores all information related to Domain name
- Namespace - set of possible names, flat or hierarchical
  flat - sequence of characters w/o space structure
  hierarchical - each name consists of several parts
    ↳ first part defines nature
    ↳ second part defines name
    ↳ third part defines department
- Name Server - implementation of resolution mechanism
- Name address resolution

host ⟶ name server
host ⟵ name server

host requests DNS to resolve domain name & name server corresponds by returning IP address of that domain name.

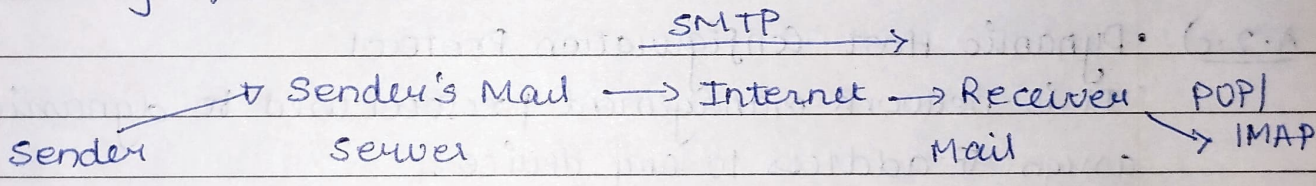
DOMS | Page No.
Date / /

Q2) Write a note on :- (5M) X3

a) SMTP protocol.

A-2a) • SMTP is Simple Mail transfer protocol.
It is an application layer protocol, and is used for sending emails efficiently and reliably. It is a push protocol.
• Uses TCP at Transport layer.
• Uses port no. 25
• Uses persistent TCP connections
• Connection Oriented protocol.
• Stateless protocol.
• Operates on listening mode

Working of SMTP :-




1. Client initiates TCP connection with SMTP server.
2. SMTP server listens for connection & initiates it on that port thereby esthablishing a connection.
3. Client informs SMTP you would like to send an email.
4. Client shares email to it's mail server.
5. Client's mail server uses DNS to get IP address of reciever email.
6. SMTP transfers mail from senders mail to recievers mail.

While sending email SMTP is used twice
1. Sender & sender's email server
2. Sender's mail server & reciever's Mail server.

DOMS | Page No.
Date / /

(b) Telnet

A.2b)
- Stands for terminal Network.
- It is a client server application that allows a user to log onto a remote machine and access application
- Uses NVT to encode characters on local system
- On server NVT decodes the characters
- Provides general, bi-directional 8 bit oriented communication facility
- Services offered on port 23

(c) DHCP

A.2.c)
- Dynamic Host Configuration Protocol
- It is network management protocol used to dynamically assign IP address to any device.
- Manages these configurations centrally
- Implemented on local network & large scale enterprise
- Default protocol used by routers
- Manages provision of all the nodes
- maintains unique IP address of the host using DHCP Server

Components of DHCP:-

1. DHCP Server - a networked device running DHCP service that holds IP addresses related configuration information
2. DHCP client - is the endpoint that receives configuration information from a DHCP Server
   can be any IOT device, laptop, computer
3. IP address pool - range of addresses available to DHCP client. IP addresses handed out sequentially low to high

DOMS | Page No.
Date / /

4. Subnet - partioned segment of IP networks. Used to keep networks manageable

5. Lease - length of time for which DHCP client holds the IP address.

6. DHCP relay - a host or router that listens for client messages being broadcast on that network. Server sends responses back to the relay agent that passes them along to client.

DOMS | Page No.
Date / /

# TRANSPORT Layer

Q1) Explain in detail services offered by Transport layer

- Transport layer is the 4th layer of the ISO/OSI model
- Provides communication services directly to application processes running on different host.

Services :-

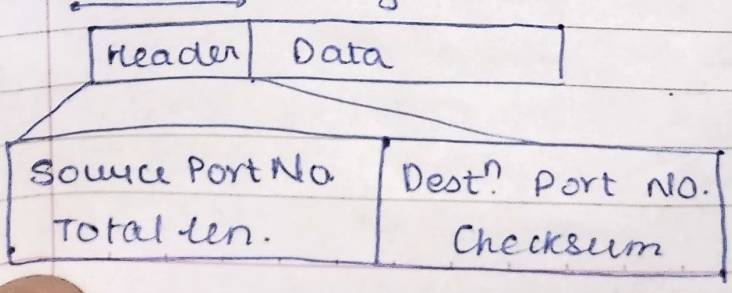
1. End to End delivery of entire message.
2. Addressing
3. Reliable delivery
   (i) Error control
   (ii) Sequence Control
   (iii) Loss Control
   (iv) Duplication Control
4. Flow control
5. Multiplexing / Demulti
   - upward
   - Downward.

Q2) Explain the features of UDP & UDP header.

a)
- UDP stands for User Datagram Protocol. UDP is a simple protocol & provides non-sequenced transport functionalities
- UDP is a connectionless protocol.
- Used when security & reliability are not very imp
- end to end transport level protocol.
- User datagram - packet produced by UDP

b) UDP Header

→ 8 bytes



1. Source port no - 16 bit identifies which port sends packet
2. Destination port no - 16 bit " " " accepts packet
3. Length - specifies total length of UDP packet.
4. Checksum - 16 bit optional field
   ↳ Finds weather the information is accurate or not.
   if there is no checksum all 16 bits are zero, otherwise checksum is written by the application
5. Data - Encapsulated higher level that is sent

Q3] Consider UDP no. 06 32 00 0D 00 1C E2 17
Find source port no, destination port no. total length of UDP, length of data, Max. length of data in UDP frame

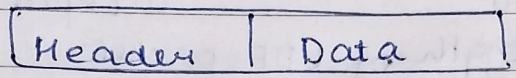
A3] Source port no = $(0632)_{16}$ = 1586.
Destination port no = $(000D)_{16}$ = 13
• Total length of UDP = $(001C)_{16}$
length of data = total length of UDP - length of header (8)
= 28 - 8
= 20 bytes
Minimum IP header is 20 bytes → max payload = 65515
To fit UDP frame of 8
$Data_{max}$ = 65515 - 8 = 65507 bytes // Ans.

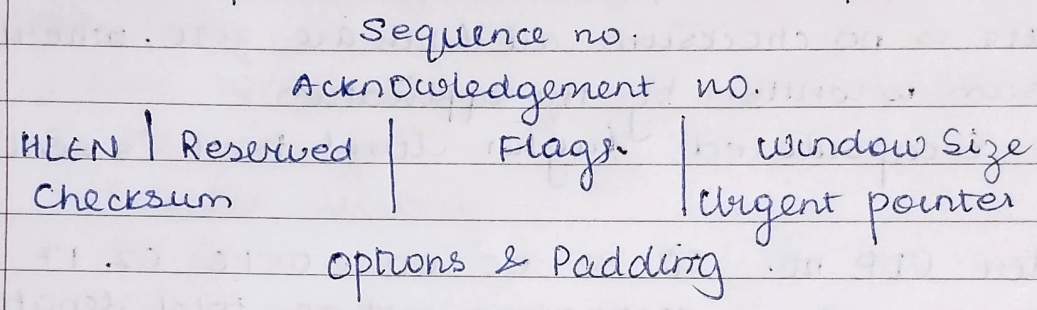
Q4]. Explain TCP header Segment in detail.

A4] TCP - Transmission Control Protocol is a transport layer protocol. Connection oriented protocol used with an IP protocol thus called TCP/IP.
Divides data into several packets, numbers them & transmits them to destination. On the reciever TCP reassembles packets & transmit them to application layer

DOMS | Page No.
Date / /

## TCP Header Format:




1. Source port add. - 16 bits - defines port which sends
2. Destination port add - 16 bits - " " receiver
3. Sequence no. - contains seq. no. of data bits in particular ses
4. Acknowledgement no. -
   When ACK flag is set then it contains the next seq. no of the data bit and acts as acknowledgement for the premously recieved data bit.
5. HLEN - Specifies size of header 20 - 60 bytes (5-15)
6. Reserved - 4 bit field reserved for future use.
   Default value is 0.

7. Flags -
   1. URG - urgent pointer, if set data is processed urgently
   2. ACK - if ACK = 0 data packet does not have an acknowledgement.
   3. PSH - if set request the recieved data to push data to recieving application w/o buffering
   4. RST - if set request to restart connection
   5. SYN - used to establish connection between hosts
   6. FIN - releases a connection, post which no data exchanges happen

8. Windowsize - 16 bit field, contains size of data receiver can accept, used for flow control.
9. Checksum - optional in UDP, mandat in TCP/IP
10. Urgent Pointer - points to urgent data if URG = 1
11. Options - provides additional options
if less than 32 bits needs padding

Q5)