Computer Networks - (MC-308)

Anish Sachdeva
DTU/2K16/MC/13

Assignment - II

Q1) State the disadvantages of classful addressing.

Ans 1) There are 3 main problems with classful addressing:-

i) Lack of internal address flexibility: Big organizations are assigned large, "monolithic" blocks of addresses that don't match well the structure of their underlying internal networks.

ii) Inefficient use of address space: The existence of only three block sizes (class A, B, C) leads to waste of limited IP space.

iii) Proliferation of Router Table entries: As the internet grows, more and more entries are required for routers to handle the routing of IP datagrams, which causes performance problems for routers. Attempting to reduce inefficient address space allocation leads to even more router table entries.

Addressing Inflexibility

Issue no. 1 results primarily from the fact that in the classful system, big companies get assigned a rather large class (class B) or truly enormous (class A) block of address, all of which is considered by the internet routers as a single network with one network ID. Now, imagine a medium to large sized company with 5000 computers and class B has been assigned to this organization. But would 5000 computers truly be hooked into the same network?

This inflexibility is one of the greatest disadvantages of the classful routing.

Q2) If one of the addresses of the block is 140.15.89.97/26 and the block is divided into 4 equal sub-blocks, calculate the range of the block and the range of the subblocks.

$(140.15.89.97)_{10} = (10001100.00001111.01011001.01100001)_2$

26 bits for the network IP address bits

32 - 26 = 6 bits for host IP address bits.

6 - 2 = 4 bits for host ID

2 bits ($2^2 = 4$) for subnet ID.

10001100.00001111.01011001.01100001

26 network ID bits | 2 subnet mask bits | apparent host

Network mask: (~~10001100~~ ~~00001111~~ ~~01011001~~ ~~01000000~~)$_2$

~~140.15~~

$= (11111111.11111111.11111111.11000000)_2$

$= (255.255.255.192)_{10}$

Network ID of the whole block =

140.15.89.97

AND 255.255.255.192

140.15.89.64

So, the network ID = $(140.15.89.64)_{10}$

$= (10001100.00001111.01011001.01000000)_2$

Network ID range =

(10001100.00001111.01011001.01000000, 10001100.00001111.01011001.01111111)

(140.15.89.64, 140.15.89.127)

Now, dividing the block into 4 sub-blocks and finding range of each subblock.

Block 0 (B_0)(00)

Range:

(10001100.00001111.01011001.0100 0000, 10001100.00001111.01011001.0100 1111)$_2$

(140.15.89.64, 140.15.89.79)

Block 1 (B_1)(01)

(10001100.00001111.01011001.0101 0000, 10001100.00001111.01011001.0101 1111)$_2$

(140.15.89.80, 140.15.89.95)$_{10}$

Block 2 (B_2 - 10)

(10001100.00001111.01011001.0110 0000, 10001100.00001111.01011001.0110 1111)$_2$

(140.15.89.96, 140.15.89.111)$_{10}$

Block 3 (B_3 - 11)

(10001100.00001111.01011001.0111 0000, 10001100.00001111.01011001.0111 1111)$_2$

(140.15.89.112, 140.15.89.127)$_{10}$

Q 3) Define Fragmentation offset

Ans 3) When a packet on a network exceeds the MTU value in size then in order to get the packet delivered to the destination, it is broken down into smaller chunks or fragmented packets are again reassembled from the original packets.

The source device must send some additional information in the IP header for the destination device to be able to reassemble the fragments of a packet to get the original packet.

Few of the fields in the IP header used for this purpose are:

Total length Field: After fragmenting, this field indicates the length of each fragment, not the length of the overall message. Normally the fragment size is selected to match the MTU value in bytes after subtracting the IP header size of 20 bytes or more.

Identification Number: All the fragments of a same packet have same identification number to allow the recieving device to identify all the fragments of a single packet.

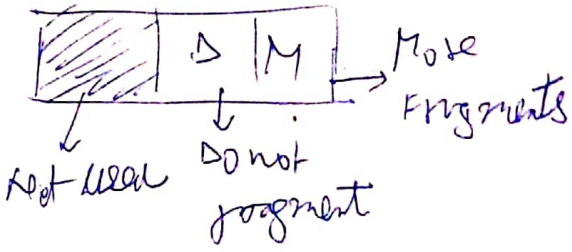
Flags: It is a 3-bit field which is used to identify the fragments

Bit 0: Reserved, must be zero

Bit 1: Don't fragment (DF)

Bit 2: More fragments (MF)

Flag Fields



The MF bit is set for all the fragments except the last one for which it is zero.

The DF bit is set to disable the fragmentation and in this case if packet size is greater than MTU value then it is dropped.

Fragmentation offset: This field helps the destination device to place the fragments in proper sequence to build the original. The fragmentation offset value for the first fragment is always 0. The field is 13 bits wide, so the offset can range from 0 → 8191. Fragments are specified in units of 8 bytes, which is why fragment length must be a multiple of 8.

Let us take an example to understand the calculation for fragmentation offset. Suppose we have a packet of 1700 bytes to be transmitted over an MTU of 1500 bytes.

First Fragment (F0):-

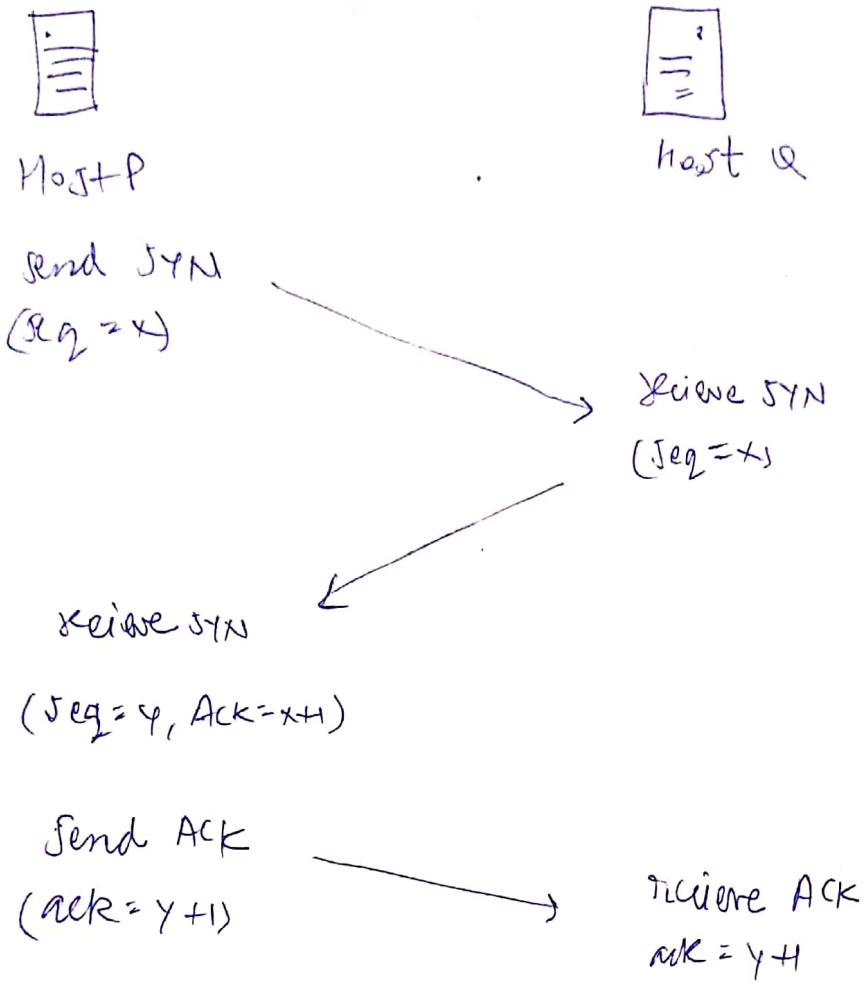
Fragment offset: 0
ID: 1
MF = 1
DF: 0
Total length: 1500 bytes
Data payload: 1500 - 20 bytes IP header = 1480

Second Fragment (F_1):

Fragment offset: 185
ID: 1
MF: 0
DF: 0
Total length: 240 bytes
Data payload: 240 bytes - 20 bytes of IP header

Q4) Explain 3 way handshaking technique:

Ans 4) The handshake technique is used in the TCP/IP protocol to affirm that a message/data packet has been successfully transmitted.



Step 1 (SYN): In this step the client wants to establish connection with server, so it sends a segment with SYN (Synchronize sequence number) which informs server that client is likely to start communicating and with what sequence number it starts its segment with.

Step 2 (SYN+ACK): Server responds to client request with SYN-ACK signal bits set. Acknowledgement (ACK) signifies the response of segment it recieved and SYN signifies with what sequence number it is likely to start the segment with.

Step 3 (ACK): In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start the actual data transfer.

Topic: ..... Date: ..... Page No: .....

The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged.

The steps 2, 3 establish the connection parameter (sequence numbers) for ~~one~~ direction the other direction and its acknowledged. With these, a full-duplex communication is established.

Q 5) Define datagram address and socket and socket address.

Ans 5) : A datagram is a basic transfer unit associated with a packet-switched network. Datagrams are typically structured in header and payload sections. Datagrams provide a connectionless communication service across a packet-switched network. The delivery, arrival time and order of arrival of datagrams need not be guaranteed by the network.

Socket Address: In practice, socket usually refers to a socket in an Internet protocol (IP) network (where a socket may be called an internet socket), in particular for the Transmission Control Protocol (TCP), which is a protocol for one-to-one connections. In this context ~~TCP~~ sockets are assumed to be associated to specific socket addresses. Namely the IP address and the port number for the local node., and those is a corresponding socket address at the foreign node.

GOOD WRITE A Mark of Quality

Teacher Sign. .....

Q6) What are the functions of MAC?

Ans6) The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for the flow control and multiplexing for transmission medium. It controls the transmission of sending data packets via remotely shared channels. It sends data over the network interface card.

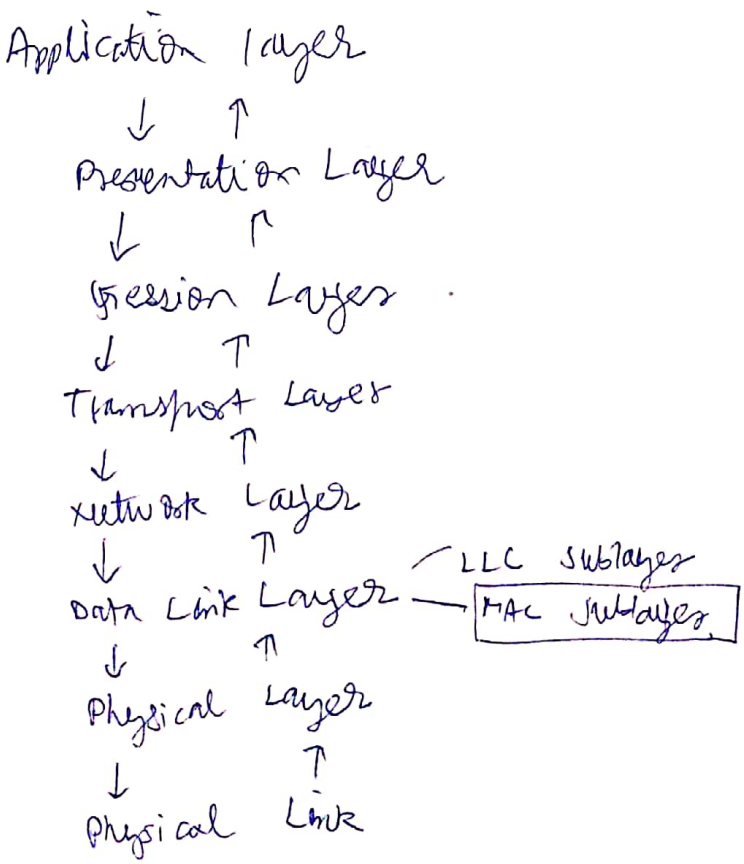
MAC layer in the OSI Model

The Open Systems interconnections (OSI) model is a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. The data link layer is the second lowest layer. It is divided into 2 sub-layers.

i) The logical link control (LLC) sublayer.

ii) The medium access control (MAC) sublayer

The following diagram depicts the position of MAC layer



Topic: ..... Date: ..... Page No: .....

Functions of MAC Layer:-

i) It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network

ii) It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.

iii) It resolves the addressing of source station as well as the destination station, or groups of destination stations.

iv) It performs multiple access resolution when more than one data frame is to be transmitted. It determines the channel access method for transmission.

Q7) Describe various transport layer features?

Ans 7)

i) Process-to-Process Delivery:-

While data link layer (DLL) requires the MAC address of source destination host to correctly deliver a frame and network layer requires the IP address for appropriate routing of packets, in a similar way transport layer requires a port numbers to correctly deliver the segments of data to the correct process amongst the multiple processes running on a particular host. A port number is a 16 bit address used to identify any client-server program uniquely.

GOOD WRITE A Mark of Quality

Teacher Sign. .....

iii) End-to-end connection between Hosts

The transport layer is also responsible for creating the connection between hosts for which it mainly uses TCP and UDP. TCP is secure, connection-oriented protocol which uses a handshake protocol to establish a robust connection between the 2-end hosts.

iii) Multiplexing / Demultiplexing

Multiplexing allows simultaneous use of different applications over a network which is running on a host. The transport layer provides this mechanism which enables us to send packet streams from various applications. Similarly, demultiplexing is required at the receiver side to receive the data coming from various processes. Transport receives the segments of data from the network layer and delivers to appropriate process.

iv) Congestion Control

Congestion is a situation in which too many sources over a network attempt to send data and the routers buffers starts overflowing due to which loss of packets occur. As a result retransmission of packets from source increases the congestion further. Transport layer provides congestion control by using Open loop to prevent congestion and closed loop congestion control to alleviate and congestion.

v) Data Integrity & Error Check

Transport layer checks for errors in the messages coming from applications layer by using error detection codes, computing checksum. It checks whether received data is not corrupted and uses ACK and NACK services to inform sender if the data has arrived or not and also to check for integrity.

Topic: ..... Date: ..... Page No: .....

vii) **Flow Control:**

The transport layer provides a flow control mechanism between adjacent layers of the TCP/IP model. TCP also prevents data loss due to fast sender and slow receiver by imposing some flow control techniques. It uses the method of sliding window protocol.

Q8) If a network consists of 8 sub-networks, then identify the subnet address for given IP address:-

i) 182.270.37.102

$2^3 = 8$ subnets, hence $\log_2 8 = 3$ bits

$(10110110)_2 . (270.37.102)_{10}$

Class B, hence

182.270.37.102

182 . 270 — Network ID; 37.102 — Host ID

$(182.270.37.102)_{10} = (10110110.10000110.00100101.01100110)_2$

10110110.10000110 — Network ID; 00100101 — Subnet Mask

Mask = 255.255.224.0

	182.270.37.102	Subnet Address:-
AND	255.255.224.0	182.270.32.0
	182.270.32.0	

GOOD WRITE A Mark of Quality

Teacher Sign. .....

ii) 182. 270.118.155

$(182.270.118.155)_{10} = (10110110.10000111.01110110.10010111)_2$

(10110110.10000111 — Host network ID; 01110110 — subnet ID)

Mask = 11111111.11111111.11100000.00000000

Subnet address = $(10110110.10000111.01100000.00000000)_2$

$= (182.270.96.0)_{10}$

iii) $(182.270.189.23)_{10} = (10110110.10000110.10111101.00010111)_2$

Mask = 11111111.11111111.11100000.00000000

AND 10110110.10000110.10111101.00010111

10110110.10000110.10100000.00000000

$= (182.270.160.0)_{10}$ → subnet address

Q7) Write a short note on IGMP.

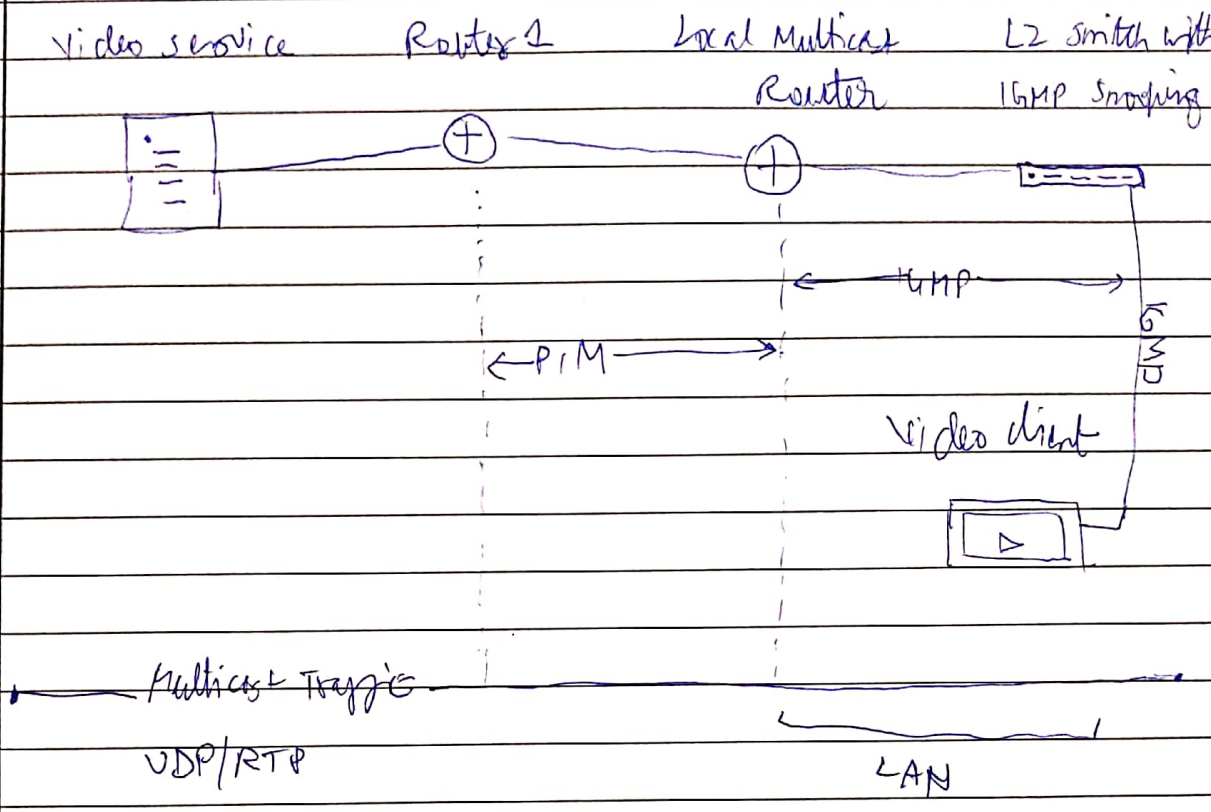
Ans) The internet group management protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPV4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast.

IGMP can be used for one-to-many networking applications such as online streaming video or online gaming, and allows more efficient use of resources when supporting these types of applications.

IGMP is used on IPV4 networks, multicast management on IPV6 networks is handled by multicast Listener discovery (MLD) which is part of ICMPV6 in contrast to IGMP's bare IP encapsulation

Topic: ..... Date: ..... Page No: .....

A network designed to deliver a multicast service using IGMP might use this basic architecture :-



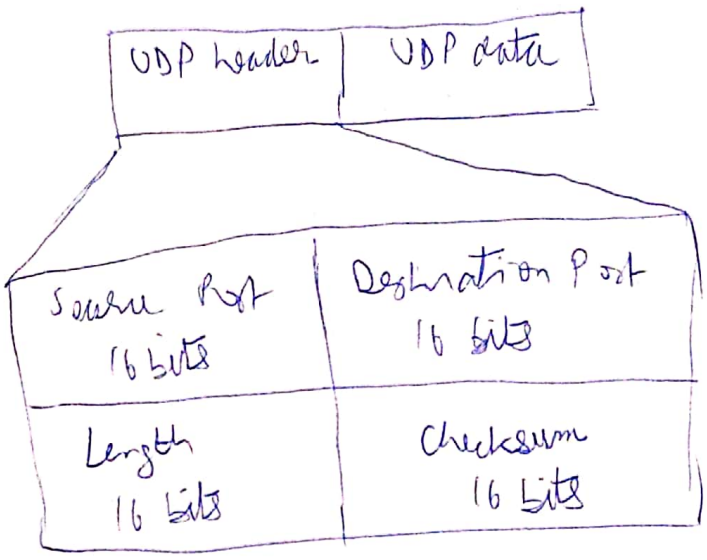
Q.9) Explain UDP header

Ans) The UDP header is a 8-bytes fixed header, while with TCP it may vary from 20 bytes - 60 bytes.

First 8 bytes contains all necessary header information and remaining part consists of data. UDP port number fields are each 16 bits long, therefore range for port numbers defined from 0 → 65535. Port 0 is Reserved. Port numbers help to distinguish different users requests or process

GOOD WRITE
A Mark of Quality

Teacher Sign. .....



1. Source Port : is 2 byte long field used to identify port number of source
2. Destination Port : It is 2 byte long field, used to identify the port of destination packet
3. Length : is the length of UDP including header and metadata. It is 16-bit field
4. Checksum : Checksum is 2 bytes long field. It is the 16-bit One's Complement of the One's complement sum of the UDP header. Pseudo header of information from the IP header and the data, padded with zero (0) octets at the end (if necessary) to make a multiple of 2 octets.