NAME: Momin Hussain

REG ID: 14672

COUSRE NAME: COMPUTER COMMUNICTAION AND NETWORKING

SECTION A

SESSIONAL ASSIGNMENT

DEPARTMENT OF BS SOFTWARE ENGINEERING

4TH SEMESTER

QUESTION : Briefly describe the services provided by the data link layer

ANSWER:

"The two main functions of the data link layer are data link control and media access control. Data link control deals with the design and procedures for communication between two adjacent nodes: node-to-node communication. Media access control deals with procedures for sharing the link."

QUESTION : Compare and Contrast

- byte-oriented and bit-oriented protocols
- byte-stuffing and bit-stuffing
- flow control and error control
- HDLC and PPP
- Go-Back-N ARQ protocol and Selective-Repeat-ARQ protocol
- circuit-switched network and a packet-switched network
- space-division and time-division switches

ANSWER:

byte-oriented and bit-oriented

protocols:

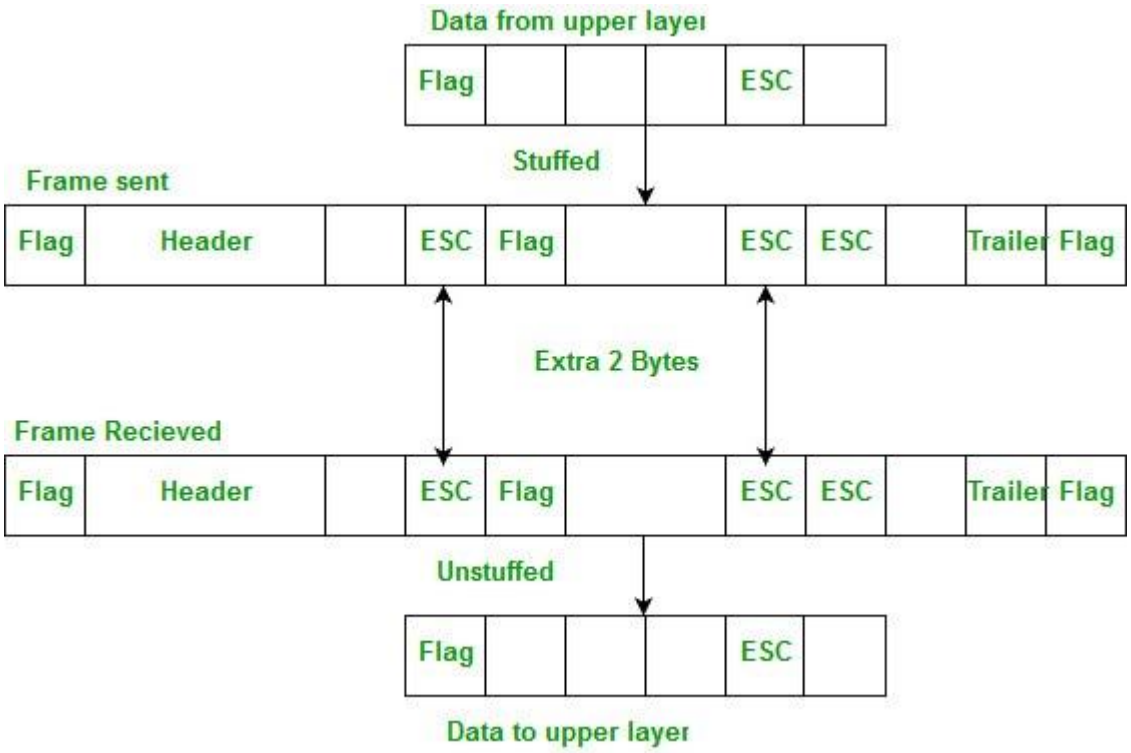
Bit Oriented Protocol - In this any field can be an arbitrary number of bits long. So if the field only needs 64 possible values, it can be only 6 bits long. They are typically used in hardware where bandwidth is an important consideration. This will allow tighter packing of data.

Byte Oriented Protocol - In this field up to 8 bits is allocated 1 byte. Fields up to 8-16 bits is given double byte. There are typically used in software as it is easy to process them. This will be loose packing of data compare to bit oriented protocol.

byte-stuffing and bit-stuffing:

Byte stuffing –
A byte (usually escape character(ESC)), which has a predefined bit pattern is added to the data section of the frame when there is a character with the same pattern as the flag. Whenever the receiver encounters the ESC character, it removes from the data section and treats the next character as data, not a flag.
But the problem arises when the text contains one or more escape characters followed by a flag. To solve this problem, the escape characters that are part of the text are marked by another escape character i.e., if the escape character is part of the text, an extra one is added to show that the second one is part of the text.

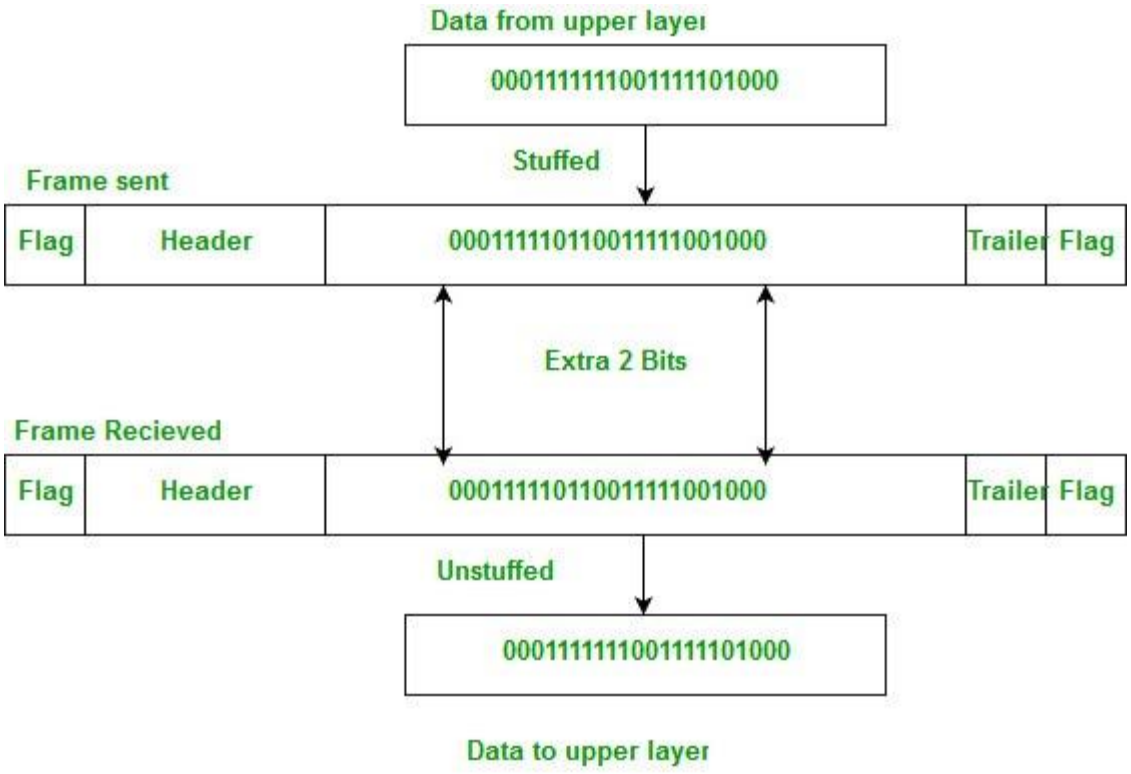
Example:



Note – Point-to-Point Protocol (PPP) is a byte-oriented protocol.

Bit stuffing –
Mostly flag is a special 8-bit pattern “01111110” used to define the beginning and the end of the frame.
Problem with the flag is the same as that was in case of byte stuffing. So, in this protocol what we do is, if we encounter 0 and five consecutive 1 bits, an extra 0 is added after these bits. This extra stuffed bit is removed from the data by the receiver.
The extra bit is added after one 0 followed by five 1 bits regardless of the value of the next bit. Also, as the sender side always knows which sequence is data and which is flag it will only add this extra bit in the data sequence, not in the flag sequence.

Example:



Note – High-Level Data Link Control(HDLC) is a bit-oriented protocol. **flow**

control and error control:

Flow control and Error control are the control mechanism at data link layer and transport layer. Whenever the sends the data to the receiver these two mechanisms helps in proper delivering of the reliable data to the receiver. The main difference between the flow control and error control is that the **flow control** observes the proper flow of the data from sender to receiver, on the other hand, the **error control** observes that the data delivered to the receiver is error free and reliable.
Key Differences Between Flow Control and Error Control

1. Flow control is to monitor the proper transmission of data from sender to receiver. On the other hand, Error Control monitors the error-free delivery of data from sender to receiver.
2. Flow control can be achieved by the Feedback-based flow control and rate-based flow control approach whereas, to detect the error the approaches used are Parity checking, Cyclic Redundancy Code (CRC) and checksum and to correct the error the approaches used are Hamming code, Binary Convolution codes, Reed-Solomon code, Low-Density Parity Check codes.
3. Flow control prevents the receivers buffer from overrunning and also prevents the loss of data. On the other hand, Error control detects and corrects error occurred in the data.

HDLC and PPP:

The major difference between HDLC and PPP is that HDLC is the bit oriented protocol, while PPP is the character-oriented protocol. The HDLC and PPP are the crucial data link layer

protocols used in WAN (wide area network) where the HDLC can also be implemented with PPP for the efficient results.

HDLC describes the encapsulation technique employed on the data in the synchronous serial data link. On the other hand, the PPP protocol deals with the encapsulation of the data transported in the point-to-point links and it could be synchronous or asynchronous.

Go-Back-N ARQ protocol and Selective-Repeat-ARQ protocol:

Both Go-Back-N Protocol and Selective Repeat Protocol are the types of sliding window protocols.
The main difference between these two protocols is that after finding the suspect or damage in sent frames go-back-n protocol re-transmits all the frames whereas selective repeat protocol re-transmits only that frame which is damaged.

Now, we shall see the difference between them:

S.NO	GO-BACK-N PROTOCOL	SELECTIVE REPEAT PROTOCOL
1.	In Go-Back-N Protocol, if the sent frame are find suspected then all the frames are re-transmitted from the lost packet to the last packet transmitted.	In selective Repeat protocol, only those frames are re-transmitted which are found suspected.
2.	Sender window size of Go-Back-N Protocol is N.	Sender window size of selective Repeat protocol is also N.
3.	Receiver window size of Go-Back-N Protocol is 1.	Receiver window size of selective Repeat protocol is N.
4.	Go-Back-N Protocol is less complex.	Selective Repeat protocol is more complex.
5.	In Go-Back-N Protocol, neither sender nor at receiver need sorting.	In selective Repeat protocol, receiver side needs sorting to sort the frames.

circuit-switched network and a packet-switched network:

Circuit switching and packet switching are the two switching methods that are used to connect the multiple communicating devices with one another. Circuit Switching was particularly designed for voice communication and it was less suitable for data transmission. So, a better solution evolved for data transmission called Packet switching.

Key Differences Between Circuit Switching and Packet Switching

1. Circuit Switching is connection oriented that means a path is established between source and destination before the transmission occurs. On the other hand, Packet Switching is Connectionless that means a dynamic route is decided for each packet while transmission.
2. Circuit Switching was originally designed for voice communication whereas, Packet Switching was originally designed for data communication.
3. Circuit Switching is inflexible as once a path is established for transmission, it doesn't change while the duration of the session. On the other hand, Packet Switching is flexible as each packet may travel through a different route to reach its destination.

4. In packet switching, as each packet travels a different path hence, the packet are received out of order at the receiver side and later arranged in order. On the other hand, in circuit switching the entire message is received as it is as sent from a sender to receiver.
5. Space Division Switching or Time-Division Switching can be used to implement Circuit Switching whereas, Packet Switching can be implemented using two approaches Datagram Approach and Virtual Circuit Approach.
6. Circuit Switching is always implemented at physical layer whereas, Packet Switching is implemented on the network layer.

space-division and time-division switches:

"In a space-division switch, the path from one device to another is spatially separate from other paths. The inputs and the outputs are connected using a grid of electronic micro switches. In a time-division switch, the inputs are divided in time using TDM. A control unit sends the input to the correct output device."

QUESTION : Explain the protocols for noiseless and noisy channels.

ANSWER:

Noiseless Channel

An ideal channel in which no frames are lost, duplicated or corrupted is regarded as Noiseless Channel.

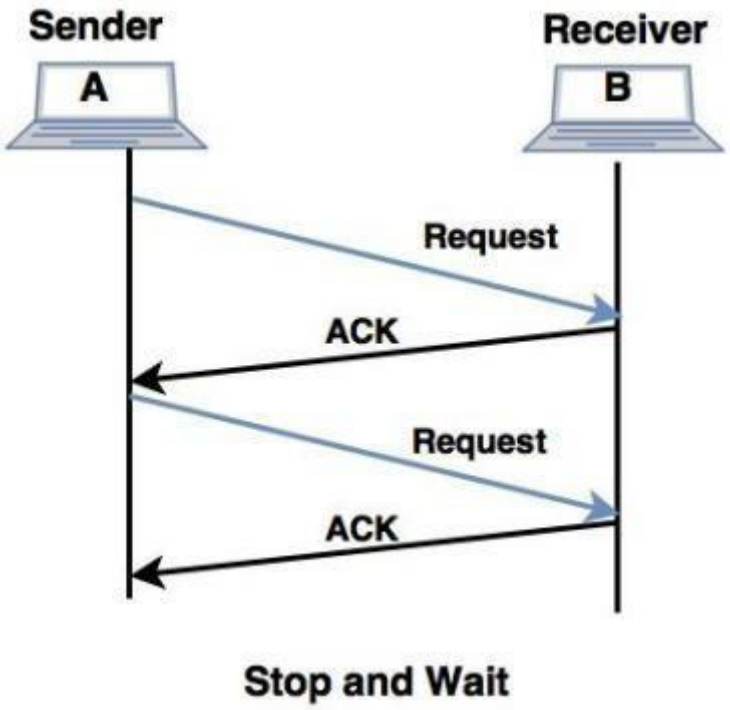
Simplest Protocol

- In simplest protocol, there is no flow control and error control mechanism. It is a unidirectional protocol in which data frames travel in only one direction (from sender to receiver).
- Also, the receiver can immediately handle any received frame with a processing time that is small enough to be negligible.
- The protocol consists of two distinct procedures :a sender and receiver. The sender runs in the data link layer of the source machine and the receiver runs in the data link layer of the destination machine. No sequence number or acknowledgements are used here.

Stop and Wait Protocol

- The simplest retransmission protocol is stop-and-wait.

- Transmitter (Station A) sends a frame over the communication line and then waits for a positive or negative acknowledgement from the receiver (station B).
- If no error occurs in the transmission, station B sends a positive acknowledgement (ACK) to station A.
- Now, the transmitter starts to send the next frame. If frame is received at station B with errors, then a negative acknowledgement(NAK) is sent to station A. In this case, station 'A' must retransmit the old packet in a new frame.
- There is also a possibility that the information frames or ACKs may get lost.
- Then, the sender is equipped with a timer. If no recognizable acknowledgement is received when the timer expires at the end of time out interval, the same frame is sent again.
- The sender which sends one frame and then waits for an acknowledgement before process is known as **stop and wait.**



Stop and Wait

Noisy Channels

Consider the normal situation of a communication channel that makes errors. Frames may be either damaged or lost completely.

1. Stop and Wait Automatic Repeat Request

- In a noisy communication channel, if a frame is damaged in transit, the receiver hardware will detect this when it computes the checksum.
- If a damaged frame is received, it will be discarded and transmitter will retransmit the same frame after receiving a proper acknowledgement.
- If the acknowledgement frame gets lost and data link layer on 'A' eventually times out. Not having received an ACK, it assumes that its data frame was lost or damaged and sends the frame containing packet 1 again. This duplicate frame also arrives at data link layer on 'B', thus part of file will be duplicated and protocol is said to be failed.
- A typical approach to solve this problem is the provision of a sequence number in the header of the message.
- The receiver can then check the sequence number determine if the message is a duplicate since only message is transmitted at any time.
- The sending and receiving station needs only 1-bit alternating sequence of '0' or '1' to maintain the relationship of the transmitted message and its ACK/ NAK.
- A modulo-2 numbering scheme is used where the frames are alternatively label with '0' or '1' and positive acknowledgements are of the form ACK 0 and ACK 1. **2. Sequence numbers**
- The protocol specifies that frames need to be numbered. This is done by using sequence number. A field is added to the data frame to hold the sequence number of that frame.
- The sequence numbers are based on modulo-2 arithmetic.
- Stop-and-wait ARQ is the simplest mechanism for error and flow control.

QUESTION : Explain Piggybacking in HDLC.

ANSWER:

used for piggybacking acknowledge. All of the HDLC protocols adhere to the convention that instead of sending the sequence number for the frame that has been received correctly, the acknowledgement contains the sequence number of the next frame that is expected (not received yet).

QUESTION: Explain blocking in a switched network.

Answer

In multistage switching, blocking refers to times when one input cannot be connected to an output because there is no path available between them—all the possible intermediate switches are occupied. One solution to blocking is to increase the number of intermediate switches based on the Clos criteria

---

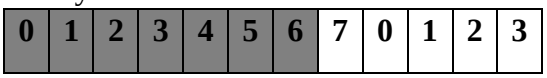
QUESTION : Two neighboring nodes (A and B) use a sliding-window protocol with a 3-bit sequence number. As the ARQ mechanism, go-back-N is used with a window size of 4. Assuming A is transmitting and B is receiving, show the window positions for the following succession of events:

- Before A sends any frames
- After A sends frames 0, 1, 2 and receives acknowledgment from B for 0 and 1
- After A sends frames 3, 4, and 5 and B acknowledges 4 and the ACK is

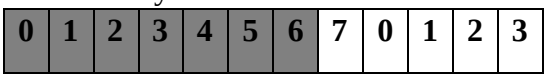
received by A ANSWER:

a. Before A sends any frames

System A - Initial



System B - Initial

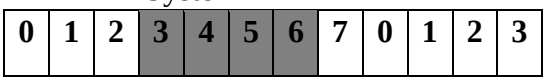


b.

System A sends 3 frames F0, F1, F2

No acknowledgments received

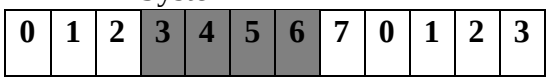
System A



System B receives 3 frames F0, F1, F2

No acknowledgments sent

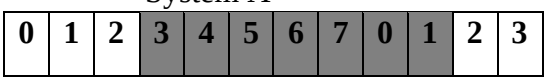
System B



c.

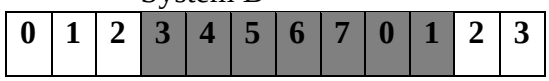
System A receives RR3 from B

System A



System B sends RR3

System B

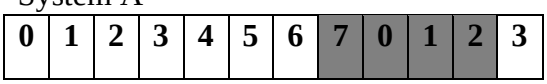


d.

System A sends F3, F4, F5, F6

System A receives RR4

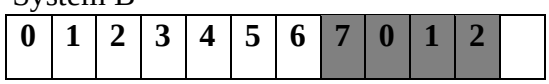
System A

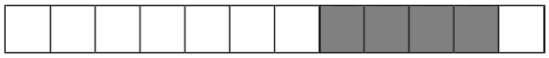


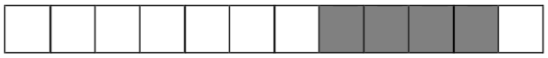
System B sends RR4

System B receives F4, F5, F6

System B







QUESTION: List three techniques of digital-to-digital conversion.

ANSWER:

The three different techniques are line coding , block coding , scrambling.

QUESTION: Distinguish between data element and signal element.

ANSWER:

A data element is the smallest entity that can represent a piece of information (a bit). A signal element is the shortest unit of a digital signal. Data elements are what we need to send; signal elements are what we can send. Data elements are being carried; signal elements are the carriers."

QUESTION: Distinguish between data rate and signal rate.

ANSWER:

Data rate – Number of **data** elements transmitted per second.

Signal rate – Number of **signal** elements transmitted per second

---

QUESTION : Draw the graph of the NRZ-L scheme using each of the following data streams, assuming that the last signa11evel has been positive. From the graphs, guess the bandwidth for this scheme using the average number of changes in the signal level. Compare your guess with the corresponding entry in Table 4.1.

a. 00000000
b. 11111111
c. 01010101
d. 00110011

ANSWER:

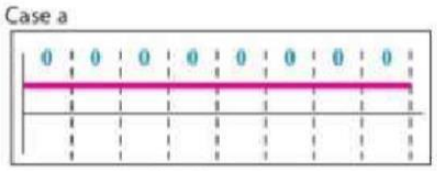
Average number of changes = (0 + 0 + 8 + 4)/4 = 3 for N = 8

Average Number of Changes = (0 + 0 + 8 + 4) / 4 = 3 for N = 8

B → (3 / 8) N

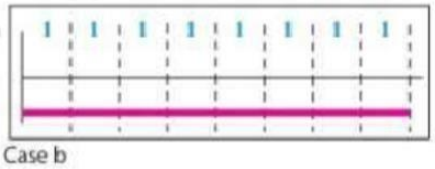
Solution: A

a.) 00000000



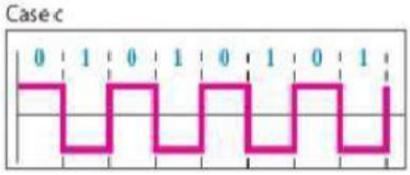
Solution: B

b.) 11111111

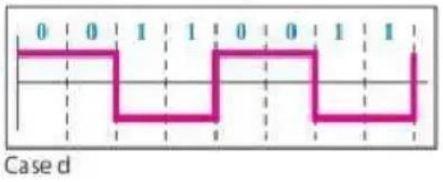


Solution: C

c.) 01010101



d.) 00110011



QUESTION : What is the number of bits in an IPv4 address? What is the number of bits in an IPv6 address?

ANSWER:

An IPv4 address is 32 bits long. An IPv6 address is **128** bits long. IPv4 uses 32-bit (four-byte) addresses, which limits the address space to 4294967296 (232) addresses.

QUESTION : What are the differences between classful addressing and classless addressing in IPv4?

ANSWER:

The **main difference** between classful and classless addressing is that classless addressing allows allocating IP addresses more efficiently than classful addressing.

Every device in a network has an IP address. The address helps to identify each device in the network and allows communicating with other devices in the network. An IP address consists of 32 bits. Every 8 bits is an octet, and they are separated by a dot. The address consists of two sections as network ID and host ID. The network ID represents the network while the host ID represents the host. There are two IP addressing types as classful and classless addressing.

QUESTION: List the classes in classful addressing and define the application of each class (unicast, multicast, broadcast, or reserve).

ANSWER:

"**Classes** A, B, and C are used for **unicast** communication. **Class** D is for **multicast** communication and **Class** E addresses are reserved for special purposes." "**Unicast** may be the saying used to go into detail connection when a bit of data is mailed derived from one of point to the other point.

QUESTION : What is a mask in IPv4 addressing? What is a default mask in IPv4 addressing?

ANSWER:

The **default** subnet **mask** for Class A IP address is 255.0. 0.0 which implies that Class A **addressing** can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).

Question : What is the network address in a block of addresses? How can we find the network address if one of the addresses in a block is given?

Answer:

The **network address** is the first **address**. The **network address** defines the **network** to the rest of the **Internet**. In classful **addressing**, the **network address** (the first **address** in the **block**) is the one that is assigned to the organization. Given the **network address** 17.0

A mask is a 32-bit binary number that gives the first **address** in the **block** (the **network address**) **when** bitwise ANDed with an **address** in the **block**. The **network address** is the beginning

address of each **block**. It can be found by applying the default mask to **any of the addresses** in the **block** (including itself).

Question : What is NAT? How can NAT help in address depletion? Answer:

NAT (Network Address Translation) is a mechanism in TCP / IP networks that allows to replace your local address with a white (public) address. NAT was developed to deal with the IP exhaustion problem and to prevent the appearance of the IP black market.

With network address translation, operators can assign private IPv4 and IPv6 addresses to clients, thereby reducing the use of global addresses. Carrier Grade NAT (CG-NAT) is responsible for the implementation of this functionality in the operator's network.

NAT allows the router to determine which services are behind the router and must be accessible from the Internet so that users can use these services from there. In simple terms, this mechanism allows all local network devices (computers, tablets, smartphones) to use a single IP address of the external interface for connection to the Internet.

Question : What is the address space in 16-bit addresses?
Answer:
One **address addresses** one byte. Using **16 bits**, you can write 65536 **addresses** (from 0 to 65535, that's 65536 different **addresses**), and **address** 65536 bytes.

QUESTION: An address space has a total of 1024 addresses. How many bits are needed to represent an address?
ANSWER:
Addressing within a 1024-word page requires 10 bits because $1024 = 2^{10}$. Since the logical address space consists of $8 = 2^3$ pages, the logical addresses must be 10+3 = 13 bits. Similarly, since there are $32 = 2^5$ physical pages, phyiscal addresses are 5 + 10 = 15 bits long.

QUESTION : Change the following IP addresses from binary notation to dotted-decimal notation.

a. 01111111 11110000 01100111 01111101
b. 10101111 11000000 11111000 00011101

ANSWER: a. 01111111 11110000 01100111 01111101 (127.240.103.125)
b. 10101111 11000000 11111000 00011101 (175.192.248.29)

QUESTION : In a block of addresses, we know the IP address of one host is 25.34.12.56/16. What are the first address (network address) and the last address (limited broadcast address) in this block?

ANSWER:

In a block of addresses, we know the IP address of the host is 25.34.12.56/16

One host, first address: 25.34.0.1

Network address: 25.34.0.0

Last address : 25.34.255.255

Limited address : 25.34.255.255

In the block.