NAME: M Hamza Elahi

ID#: 14857

MODULE: Software Engineering

SEMESTER: 4

SECTION: B

SUBJECT: Computer Communication & Networks

INSTRUCTOR: MR. Mansour khan

---

1. Briefly describe the services provided by the data link layer

ANSWER:

The services provided by the data link layer as:

- **Framing & Link access:** Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link.
- **Reliable delivery:** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.
- **Flow control:** A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.
- **Error detection:** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.

- **Error correction:** Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.
- **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

2. 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:

Compare and Contrast:

1) byte-oriented and bit-oriented protocols:

Bit Oriented Protocol - In this any field can be an arbitrary number of bits long. So, if 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's as it is easy to process them. This will be loose packing of data compare to bit-oriented protocol.

2) 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 problem arises when 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 tex

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 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 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.

3) flow control and error control:

Flow Control is a technique so that transmitter and receiver with different speed characteristics can communicate with each other. Flow control ensures that a transmitting station, such as a server with higher processing capability, does not overwhelm a receiving station, such as a desktop system, with lesser processing capability. This is where there is an orderly flow of transmitted data between the source and the destination.

Error Control involves both error detection and error correction. It is necessary because errors are inevitable in data communication, in spite of the use of better equipment and reliable transmission media based on the current technology. In the preceding lesson we have already discussed how errors can be detected. In this lesson we shall discuss how error control is performed based on retransmission of the corrupted data. When an error is detected, the receiver can have the specified frame retransmitted by the sender. This process is commonly known as Automatic Repeat Request (ARQ). For example, Internet's Unreliable Delivery Model allows packets to be discarded if network resources are not available, and demands that ARQ protocols make provisions for retransmission.

4) HDLC and PPP:

Definition of HDLC

HDLC (High-level Data Link Control) is a WAN protocol intended to perform the encapsulation of the data in the data link layer. The encapsulation of the data means to change the format of the of the data. SDLC is the predecessor of the HDLC which stands for the **Synchronous Data Link Control protocol**. Both SDLC and HDLC protocol are developed by IBM and submitted to the ANSI and ISO for the acceptance as the international standards.

The HDLC protocol follows the bit-oriented concept and uses bit stuffing for achieving data transparency. Here bit-oriented approach signifies that the single bit is used to present the control information. The frame structure of HDLC contains the address, control, data, checksum and flag fields. The default encapsulation protocol in the Cisco devices is the HDLC. The Cisco proprietary HDLC only works when the devices in both of the ends of the link are of cisco. Standard HDLC can have different devices in the ends.

Frame format for the bit-oriented protocols

Frame format for HDLC protocol

- **Address field** – It is used to describe the terminal.
- **Control field** – The bits in the control field is intended for the sequence number and acknowledgements.
- **Data field** – This field is used to hold the information.
- **Checksum field** -In this field, the bits are reserved for the performing the cyclic redundancy code.

HDLC Commands and Requests

The HDLC uses a group of commands and responses for its working. There are three types of frames information, supervisory and unnumbered.

- **Information transfer format** (I-Frame) – It transports the numbered frames in a sequential manner, which contain the information field.
- **Supervisory format** (S-Frame) – The supervisory frames conduct the managerial functions such as acknowledgement, information transfer status, polling and error recovery. The commands and requests included in this are RECEIVE READY, RECEIVE NOT READY, REJECT, etcetera.
- **Unnumbered format** (U-Frame) – It basically extends the data link control functions. There several commands and requests fall under this category such as RESET, TEST, FRAME REJECT, REQUEST DISCONNECT, etcetera.

Definition of PPP

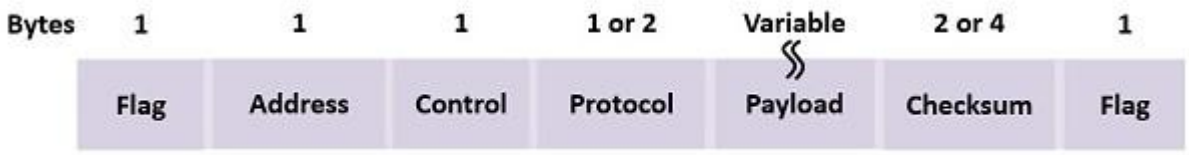
PPP (Point-to-Point Protocol) is also a WAN protocol, but there are several enhancements made in the PPP protocol after HDLC. Priorly, the PPP protocol is not proprietary, which means that it can be used with two different type of devices without committing changes over the format of the data. All of the links collaboratively treated as single, independent IP network which is having its own

frame format, hardware addressing method, and data link protocol. A point-to-point connection is obtained without assigning multiple IP addresses to the tangible wires, and it just needs the IP network number.

There are several features of PPP, which are discussed below.

- To clearly identify the start and end of the frame, the framing method is used on the asynchronous data. It is also beneficial in the detection of the errors.
- A **link control protocol** is used for enabling the network lines, testing them, terminate them when no longer used. This link control protocol is basically helpful in handling the synchronous and asynchronous circuits, and byte and bit-oriented encodings.
- It can select the **NCP (Network Control Protocol)** for each supported network layer.

Frame format for the PPP



Frame format for PPP protocol

The PPP frame contains two flag fields, a **protocol** filed to determine the type of packet residing in the **payload**, and a payload field which can variate. However, the rest of the fields are the same as the HDLC protocol.

5) Go-Back-N ARQ protocol and Selective-Repeat-ARQ protocol: Go Back And ARQ

- Go Back N ARQ is inefficient for the noisy link.
- Go Back N ARQ is less complicated than Selective Repeat ARQ.
- Go Back N ARQ Sender Windows Size is 2^(m)-1 and receiver window size is 1.
- Go-Back-N ARQ is a specific instance of the automatic repeat request (ARQ) protocol, in which the sending process continues to send the number of frames specified by a window size even without receiving an acknowledgment (ACK) packet from the receiver. It is a special case of the general sliding window protocol with the transmit window size of N and receive window size of 1.

Selective Repeat ARQ

- Selective repeat ARQ is efficient for noisy links.
- Selective Repeat ARQ is Complicated.
- In Sender and Receiver Window Size is 2^(m-1).

- Selective Repeat ARQ / Selective Reject ARQ is a specific instance of the AutomaticRepeat-Request (ARQ) protocol used for communications. It may be used as a protocol for the delivery and acknowledgment of message units, or it may be used as a protocol for the delivery of subdivided message sub-units.

6) circuit-switched network and a packet-switched network:

Definition of Circuit Switching

Circuit Switching establishes a physical path between the sender and receiver of the message before a message is delivered. When a connection is established between a sender and a receiver, the entire message travels through the established path from sender to the receiver. Once the message is delivered to the receiver, the source informs the network about the completion of transmission and all the switches released. Then the link and other connecting devices are used to set up another connection.
Circuit switching is always implemented at the **Physical Layer**. Circuit switching can be explained with an example of a telephone conversation. In a telephone conversation, once a connection is established, between a caller and the receiver, it remains connected, till the whole conversation is finished and both the caller and receiver hang up their phone.

The Circuit switching is not appropriate for data transmission because data is transmitted in spurts (stream) and the line remains idle for most of the times and hence, the bandwidth is wasted. Circuit Switching can be implemented using two technologies either **Space Division Switching** or **Time Division Switching**.

Definition of Packet Switching

Packet Switching is connectionless as it doesn't establish any physical connection before the transmission starts. In packet switching before the message is transmitted, it is divided into some manageable parts called packets. These packets are routed one by one from source to destination.

In packet switching, each packet may follow a different route to reach the destination. Packets arrived at the destination are out of order but, they are assembled in order before the destination forward it to the upper layer.

7) space-division and time-division switches:

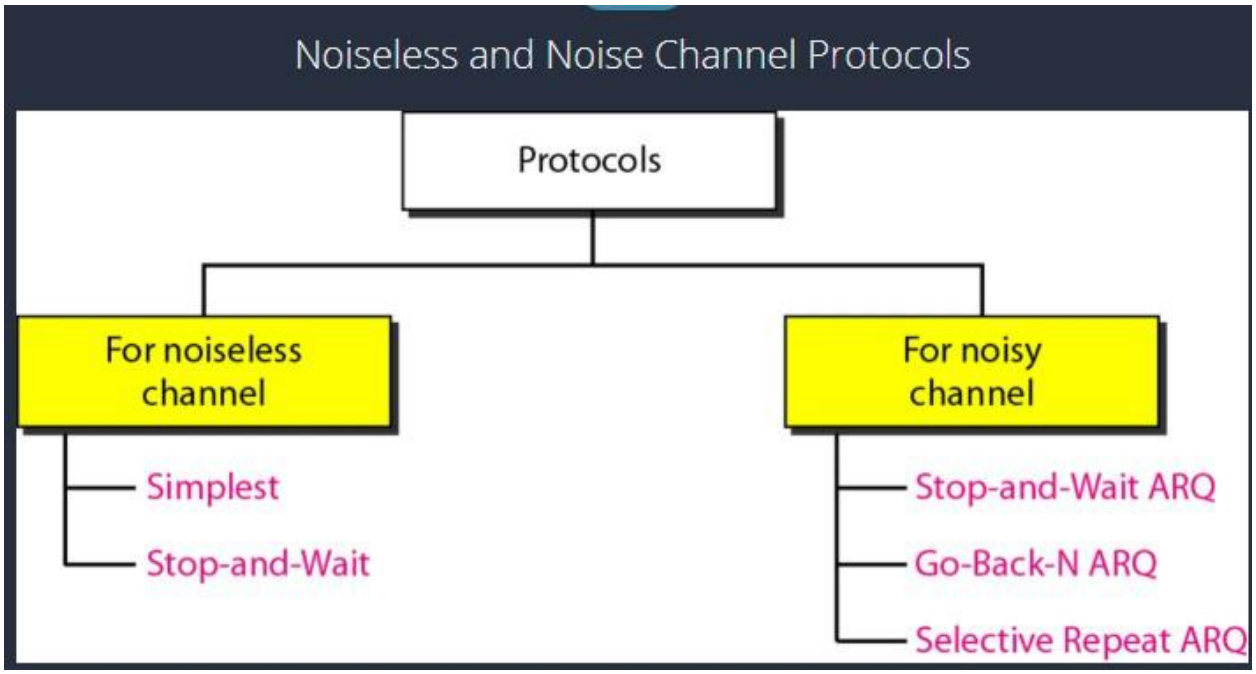
Time division switching takes the yields of a few time-division switches, and associates them as contributions as a space division switch. The impact of this matched course of action is that bundles can be swapped between various yield lines.

Space division switching is a component that depends on the through association of a lot of information lines specifically to a lot of yield lines.

The principle distinction between space division switching and time division switching is sharing of Crosspoint. cross points are not partaken in space division exchanging, while they can be partaken in time division switching but not for longer periods.

3. Explain the protocols for noiseless and noisy channels.

ANSWER:



Noisy Channels Protocol

- Stop-and-Wait Automatic Repeat Request. The Stop-and-Wait Automatic Repeat Request (Stop-andWait ARQ), adds a simple error control mechanism to the Stop-and-Wait Protocol. ...
- Go-Back-N Automatic Repeat Request. ...
- Selective Repeat Automatic Repeat Request.

Noiseless Channels: Let us first assume we have an ideal **channel** in which no frames are lost, duplicated, or corrupted. It has no flow or error control. It is a unidirectional **protocol** in which data frames are traveling in only one direction-from the sender to receiver.

4. Explain Piggybacking in HDLC.

ANSWER:

The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame. This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as **piggybacking**

Working Principle

Piggybacking data is a bit different from Sliding Protocol used in the OSI model. In the data frame itself, we incorporate one additional field for acknowledgment (called ACK).

Whenever party A wants to send data to party B, it will carry additional ACK information in the PUSH as well.

For example, if A has received 5 bytes from B, which sequence number starts from 12340 (through 12344), A will place "ACK 12345" as well in the current PUSH packet to inform B it has received the bytes up to sequence number 12344 and expects to see 12345 next time. (ACK number is the next sequence number of the data to be PUSHed by the other party.) Three rules govern the piggybacking data transfer.

- If station A wants to send both data and an acknowledgment, it keeps both fields there.
- If station A wants to send just the acknowledgment, then a separate ACK frame is sent.
- If station A wants to send just the data, then the previous acknowledgment field is sent along with the data. Station B simply ignores this duplicate ACK frame upon receiving.

Advantages and Disadvantages

Advantages:

Improves the efficiency, better use of available channel bandwidth.

Disadvantages: The receiver can jam the service if it has nothing to send. This can be solved by enabling a counter (Receiver timeout) when a data frame is received. If the count ends and there is no data frame to send, the receiver will send an ACK control frame. The sender also adds a counter (Emitter timeout), if the counter ends without receiving confirmation, the sender assumes packet loss, and sends the frame again

5. Explain blocking in a switched network.

ANSWER:

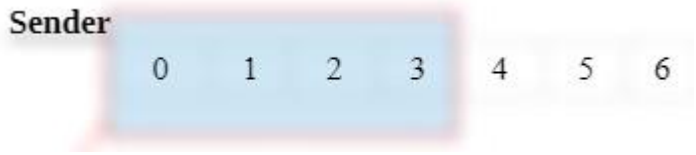
In multistage **switching**, **blocking** refers to times when one input cannot be connected to an output because there is no path available between them—all the possible intermediate

switches are occupied. One solution to **blocking** is to increase the number of intermediate **switches** based on the Clos criteria.

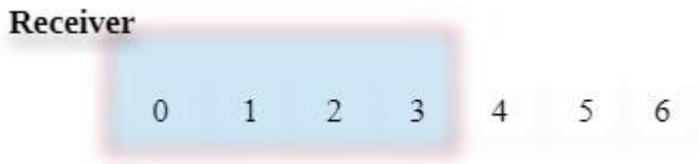
6. **Two neighboring nodes (A and B) use a sliding-window protocol with a 3-bit sequence number. As the ARQ mechanism, go-back-N is used with a window size of 4. Assuming A is transmitting and B is receiving, show the window positions for the following succession of events:**
   - **Before A sends any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

ANSWER a: Before A sends any frames



Window of PDU that may be transmitted = 4-bit window

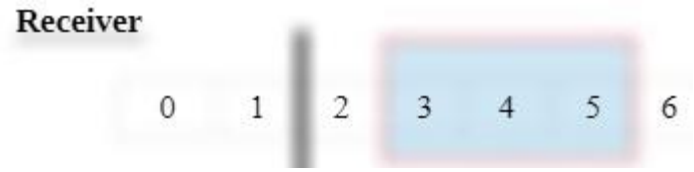


ANSWER b: After A sends frames 0, 1, 2 and receives acknowledgment from B for 0 and 1

Sender

A has shrunk its window as it has transmitted three PDUs but has received ack for 2 PDUs hence it is keeping copy of one PDU

Acknowledgment received for two bits



Receiver has received all data hence the window remains in 4-bit size

ANSWER c: After A sends frames 3, 4, and 5 and B acknowledges 4 and the ACK is received by A

Receiver

Acknowledgment received for two bits

7. List three techniques of digital-to-digital conversion.

ANSWER:

- **DIGITAL-TO-DIGITAL CONVERSION:**

three techniques of digital to digital conversion: line coding, block coding, and scrambling.

Line coding is always needed; block coding and scrambling may or may not be needed.

Line Coding

Line coding is the process of converting digital data to digital signals.

Line coding converts a sequence of bits to a digital signal.

At the sender, digital data are encoded into a digital signal; at the receiver, the digital data are recreated bydecoding the digital signal.

Signal Element Versus Data Element

In data communications, our goal is to send data elements. A data element is the smallest entity that can represent a piece of information: this is the bit.

In digital data communications, a signal element carries data elements.

A signal element is the shortest unit (timewise) of a digital signal.

Data elements are being carried; signal elements are the carriers

8. **Distinguish between a signal element and a data 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.

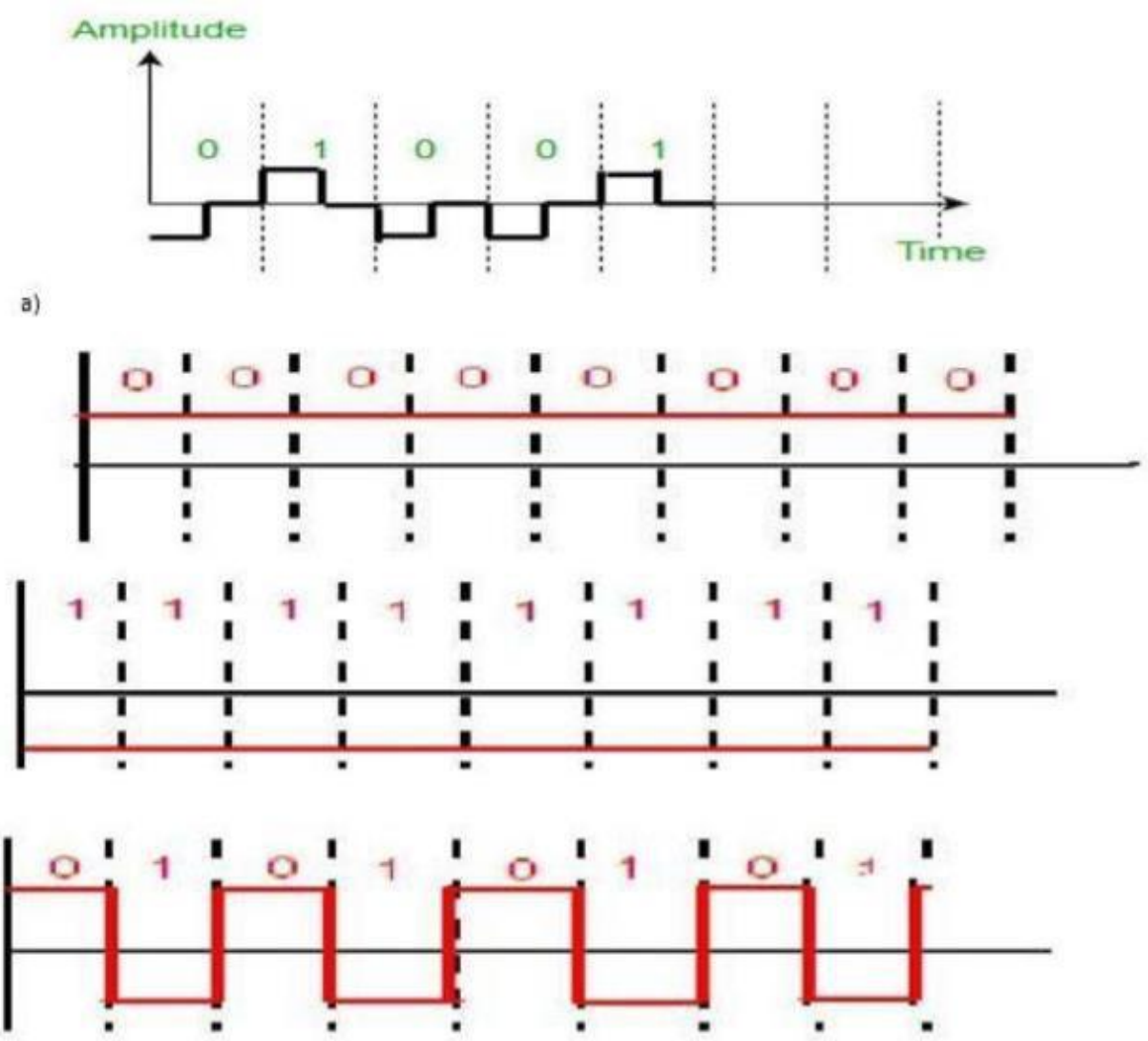
9. **Distinguish between data rate and signal rate.**

ANSWER:

Distinguish between data rate and signal rate. Data rate is also known as bit rate and it defines the # of data elements/bit sent is 1s. Signal rate is also known as the pulse rate and it is the # of single elements sent in 1s. Data rate unit is bps and Signa.

10. **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:



11.What is the number of bits in an IPv4 address? What is the number of bits in an IPv6 address?

ANSWER:

Number of bits in an ipv4 address:

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. Addresses were assigned to users, and the number of unassigned addresses decreased.

The bits within the network portion of the address must be identical for all devices that reside in the same network. The bits within the host portion of the address must be unique to identify a specific host within a network. Regardless of whether the decimal numbers between two IPv4

addresses match up, if two hosts have the same bit-pattern in the specified network portion of the 32-bit stream, those two hosts will reside in the same network.

The number of bits in an IPv6 address:

An **IPv6 address** is 128 **bits** in length and consists of eight, 16-**bit** fields, with each field bounded by a colon. Each field must contain a hexadecimal **number**, in contrast to the dotted-decimal notation of **IPv4 addresses**.

IPv6 addresses are assigned to interfaces, rather than to nodes, in recognition that a node can have more than one interface. Moreover, you can assign more than one IPv6 address to an interface.

An IPv6 address is 128 bits in length and consists of eight, 16-bit fields, with each field bounded by a colon. Each field must contain a hexadecimal number, in contrast to the dotted-decimal notation of IPv4 addresses. In the next figure, the x's represent hexadecimal numbers.

12.What are the differences between class full addressing and classless addressing in IPv4?

ANSWER:

Class full addressing assigns an organization a Class A, Class B, or Class C block of addresses. Classless addressing assigns an organization a block of contiguous addresses based on its needs. All IP addresses have a network and host portion. In class full addressing, the network portion ends on one of the separating dots in the address (on an octet boundary). Classless addressing uses a variable number of bits for the network and host portions of the address. **Class full addressing** assigns an organization a Class A, Class B, or Class C block of addresses. ... In **class full addressing**, the network portion ends on one of the separating dots in the **address** (on an octet boundary). **Classless addressing** uses a variable number of bits for the network and host portions of the **address.** The **class full** IP **address** has a set and subnet mask.... A **classless** IP **address** does not have a set subnet mask. **The different** classes of IP addresses...can contain different numbers of networks.... The Class A can contain up to 128 networks.

13.List the classes in class full 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. In this case there is just one single email sender, and something recipient. Unicast transmission, in which a mail boat is actually routed from a individual origin to some specific getaway, continues to be the main kind of transmitting in LANs in addition to in the World-wide-web.

Many LANs (at the. Gary. Ethernet) as well as IP sites offer the unicast move setting, and a lot people understand the conventional unicast purposes (at the. Grams. Http, stop, ftp and also telnet) that utilize the actual TCP carry method.

A **class full network** is a network addressing architecture used in the Internet from 1981 until the introduction of Classless Inter- Domain Routing in 1993. The method divides the IP address space for Internet Protocol version 4 (IPv4) into five address classes based on the leading four address bits. Classes A, B, and C provide unicast addresses for networks of three different network sizes. Class D is for multicast networking and the class E address range is reserved for future or experimental purposes.

Since its discontinuation, remnants of class full network concepts have remained in practice only in limited scope in the default configuration parameters of some network software and hardware components, most notably in the default configuration of subnet masks.

14.What is a mask in IPv4 addressing? What is a default mask in IPv4 addressing?

ANSWER:

Mask in IPv4 addressing:

A subnet **mask** hides (or **masks**) the network part of a system's IP address and leaves only the host part as the machine identifier. It uses the same format as an **IPv4** address — four sections of one to three numbers, separated by dots.

Default mask in IPv4 addressing:

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). Subnetting is the process of dividing a Class A, B or C network into subnets, as we've seen in the preceding topics. In order to better understand how this “division of the whole” is accomplished, it's worth starting with a look at how the “whole” class A, B and C networks are represented in a Subnetting environment. This is also of value because there are situations where you may need to define an unsubnetted network using subnetting notation.

This might seem like a strange concept—if you aren't going to bother creating subnets, why do you need to consider how the old-fashioned classes are used under subnetting? The answer is that after subnetting became popular, most operating systems and networking hardware and software were designed under the assumption that subnetting would be used. Even if you decide not to subnet, you may need to express your unsubnetted network using a subnet mask.

In essence, a non-sub netted class A, B or C network can be considered the “default case” of the more general, custom sub netted network. Specifically, it is the case where we choose to divide the host ID so that zero bits are used for the subnet ID and all the bits are used for the host ID. I realize that this seems like a bit of a semantic game. However, this default case is the basis for the more practical subnetting.

15.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:

A mask is a 32-bit binary number that gives the first address in the block (the network address) when bitwise Handed 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.

The network address in a block of addresses is the first address quit defines the organization itself to the rest of the world Q4B. How can we find the network address if one of the addresses in the block is known? The mask can be handed with any address in the block to find the network address.

16.What is NAT? How can NAT help in address depletion?

ANSWER:

A **NAT** (Network **Address** Translation or Network **Address** Translator) is the virtualization of Internet Protocol (IP) **addresses**. **NAT helps** improve security and decrease the number of IP **addresses** an organization needs. **NAT** gateways sit between two networks, the inside network and the outside network. Theoretically, there are 2^32 IPv4 addresses, a little more than 4 billion IPv4 addresses. The number of IPv4 available addresses is actually less than the theoretical number, since some of the addresses in a network are reserved for broadcasting, multicasting or other special purposes, they cannot be assigned to hosts.

With the explosion of devices online, the available IPv4 addresses are just not enough. NAT was designed as a temporary solution to circumvent this problem and support IPv4 address reusability. NAT resulted in IPv4 addresses being divided into two broad categories: Public and Private. The range of private IPv4 addresses can be used by anyone and are unregistered, which means that they cannot be recognized outside the network in which they are assigned.

When a host with a private IP address wants to communicate with a server outside its private network, it uses the public IP address of the NAT to do so. This way the internal/private address is identified as the public address to the outside world because the server needs a unique and routable address, on the internet, to reply. A NAT device uses the PAT (Port Address Translation) method to remember the IP address and source port of the private host. It uses these records to translate the packets received and send them to the original host that requested that info.

17.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. **16-bit** integers, memory addresses, or other data units are those that are 16 bits (2 octets) wide. Also, 16-bit CPU and ALU architectures are those that are based on registers, address buses, or data buses of that size. 16-bit microcomputers are computers in which 16-bit microprocessors were the norm.

A 16-bit register can store 2^{16} different values. The signed range of integer values that can be stored in 16 bits is −32,768 (-1×2^{15}) through 32,767 ($2^{15} - 1$); the unsigned range is 0 through 65,535 ($2^{16} - 1$). Since 2^{16} is 65,536, a processor with 16-bit memory addresses can directly access 64 KB (65,536 bytes) of byte-addressable memory. If a system uses segmentation with 16-bit segment offsets, more can be accessed.

18.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, physical **addresses** are 5 + 10 = 15 **bits** long. In figuring, a location space characterizes a scope of discrete locations, every one of which may relate to a system have, fringe gadget, circle segment, a memory cell or other intelligent or physical element. 4096 bits are needed.

19.Change the following IP addresses from dotted-decimal notation to binary notation?

129.14.6.8 208.34.54.12 **ANSWER:**

a) 10000101 00001001 11000101 10011001

b) 10000101 00001001 11000101 10011001

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

01111111 11110000 01100111 01111101 10101111

11000000 11111000 00011101

ANSWER:

a) 127.240.103.125

b) 175.192.248.298

21. 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**: 182.44. 82.1 **Network address**: 182.44.

1. 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 block.
2. One host, first address: 182.44.82.1
   Network address: 182.44.82.0 Last address: 182.44.82.254 Limited address.