Sessional Assignment

Computer Communications & Networking

Submission Date: 03th June, 2020

Submitted By: Aamir Saleem (12290)
Submitted To: Sir Mansoor Qadir

Class/Section: Software Engineering 8th Semester (Sec-A)

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

   Answer:

   1= It is responsible for encapsulation of the data packets from the network layer into frames.
   2= It is responsible for synchronization of frames.
   3= It is responsible for the error control function in its sublayer logical link control.
   4= It is responsible for Flow control in LAN Protocols such as ethernet.
   5= In its sublayer Medium Access Control it provides access control for all connections.
   6= It provides Physical Addressing via MAC addressing.
   7= It provides LAN switching, MAC filtering & shortest path bridging.
   8= It provides Quality of Service control.

2. **Compare and Contrast**

   - byte-oriented and bit-oriented protocols

     Answer: **Bit oriented** protocol can only be 6 bits long & can store 64 values. Used in bandwidth-oriented hardware.

     Byte oriented protocol can be 8bits long. Fields up to 8-16 bits is given double byte. It is used in softwares as it is easy to process.

   - byte-stuffing and bit-stuffing

     Answer: **Byte-stuffing** is a predefined bit pattern which is added to the data section of the frame where there is a character with the same pattern. For example, Point to point Protocol is a byte oriented protocol.

     Bit-stuffing is a special 8-bit pattern used to define the beginning & the end of a frame.

   - flow control and error control

     Answer: **Flow control** observes the proper flow of the data from sender to receiver.
     Whereas **Error Control** observes that the data delivered to the receiver is error free & reliable.

   - HDLC and PPP

     Answer: **HDLC** is a bit-oriented protocol while **PPP** is a character-oriented protocol.

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

     Answer: In **Go-back-N protocol** if the sent frame is suspected then all frames are re-transmitted from the lost packet. While in **Selective Repeat** only the suspected frames are retransmitted.

   - circuit-switched network and a packet-switched network

     Answer: **CSN** are connection-oriented networks, a dedicated route is established between the source & destination. Where **Packet Switched** networks are connectionless networks.

   - space-division and time-division switches

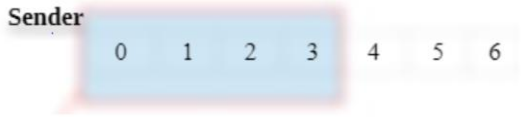
3. Explain the protocols for noiseless and noisy channels.
   Answer: For **noiseless channel** the 'Simplest', 'Stop & wait' protocols are used. In simplest the sender sends a sequence of frames without even thinking about the receiver.
   In **noisy channel** the stop & wait ARQ, Go-Back-N ARQ & Selective Repeat ARQ is used. In selective repeat protocol the size of the sender & receiver window must be one-half of 2m.

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
   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.

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: A before sending any frame



7. List three techniques of digital-to-digital conversion.
   Answer: The 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 by decoding the digital signal.
   Signal Element Versus Data Element
   In data communications, our goal is to send data elements. A

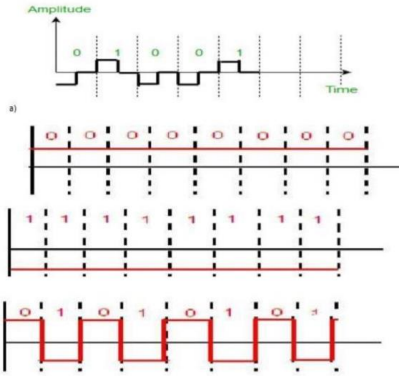
data element is the smallest entity that can represent a piece of information: this is the bit.
In digital data communications, a signal element carries data elements.
A signal element is the shortest unit (timewise) of a digital signal.
Data elements are being carried; signal elements are the carriers

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: **Data rate** is also known as bit rate and it defines the number of data elements/bit sent is 1s. **Signal rate** is also known as the pulse rate and it is the number of single elements sent in 1s. Data rate unit is bps and Signal.

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 IPv4addresses 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 classful 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.List the classes in classful addressing and define the application of each class (unicast, multicast, broadcast, or reserve).

13. 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 (27-2) and 16777214 hosts (224-2). 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.

14. 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

15. 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.

16. What is the address space in 16-bit addresses?

    Answer: One address address 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 216 different values. The signed range of integer values that can be stored in 16 bits is −32,768 (−1 × 215) through 32,767 (215 − 1); the unsigned range is 0 through 65,535 (216 − 1). Since 216 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.

17. 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 = 210. Since the logical address space consists of 8 = 23 pages, the logical addresses must be 10+3 = 13 bits. Similarly,

since there are 32 = 25 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.

18. Change the following IP addresses from dotted-decimal notation to binary notation.
    a. 129.14.6.8
    b. 208.34.54.12

    Answer:

    a) 10000101 00001001 11000101 10011001

    b) 10000101 00001001 11000101 10011001
19. Change the following IP addresses from binary notation to dotted-decimal notation.
    a. 01111111 11110000 01100111 01111101
    b. 10101111 11000000 11111000 00011101

    Answer:

    a) 127.240.103.125

    b) 175.192.248.298
20. 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