Name : Shakhera Khanom

Course title: Computer Networks

ID: IT-18033

CT No :- 02

Question set

01.

a. Define Data-Link Layer. what are its sublayers? 4

b. List the functonality of Data-Link-Layer. 4

c. Data link layer is responsible for which mechanisms? Explain point to point flow control. 6

02.

a. what is MAC address? How does TCP deal with dead connections? 5

b. Compare and contrast byte-oriented and bit-oriented protocols. which category has been popular in the past? which category is popular now (explain the reason)? 6

c. Difference between Flow control and Error control. 3

03.

a. Define framing and the reason of for its need. 4

b. Explain the reason for moving from the stop and wait ARQ protocol to the Go-Back-N-ARQ protocol. 5

c. what are the key functions of error control technique? 3

d. what are the difference between error detection and error correction. 2

04.

a. Define Network Layer. What are the features of a network layer? 5

b. List the functionalities of network layer. 3

c. Why are different addressing needed in computer networks? 3

d. what is difference between Broadcast and multicast 3

05.

a. What is routing? What are the main routing protocols? 4

b. How can you manage a network using a routers? You need to connect two computers for file sharing. Is it possible to do this without using a hup or routers? 6

c. How does Multicast routing differ from Unicast routing? 4

06.

a. What does Internet Protocol Version 4 (IPv4) mean? Explain 5

b. What is the difference between IPv4 and IPv6? 3

c. Which fields of the IPv4 headers changes from routers to routers? 4

d. Why we migrate from IPv4 to IPv6? 2

07. a) Your company is given with IP address range of 192.168.160.0/27. The company has three dept: sales, customer services and IT. Each dept needs to have a separate subnet. Divide your IP address range so that each dept has a separate subnet with same number of IP addresses. What will be the network address and subnetmask of each subnet? Also write down the range of each subnet and the number of usable addresses that could be assigned to the users of each dept. 7

b.) A company got a C network (192.70.56.214) assigned and wants to divide the network into subnets works for 120 computers each.

i) How many of those subnets can be established?

ii) How many usable address does each subnet have

iii) which netmask do they have to used?

iv) which are the usable address per subnet? 7

08.

a. What is tunneling in internetworking? 3

b. What is data fragmentation? Explain how data fragmentation works? 4

c. Define IP (IPsec). What are the two protocols defined by IPsec? Briefly describe the services provided by IPsec. 4

d. What is the function of Internet Control Message Protocol ICMP? 3

Shakhera khanom
ID: IT-18033
Question and Answers

Ans. to the que no - 1(a)

Ques: Define Data Link Layer. what are its sublayers?

Answer:

Data link layer: Data link layer is second layer of OSI layered model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to ~~comm~~ communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be an same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

Data link layer has two sub-layers:

① Logical Link Control: It deals with protocols, flow-control, and error control

② Media Access Control: It deals with actual control of media.

Ans. to the ques. no- 1(b)

Q: List the functionalities of data link layer.

Answer: Data link layer does many tasks on behalf of upper layer. These are:

⇒ Framing: Data link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver's end, data link layer picks up signals from hardware and assembles them into frames.

⇒ Addressing: Data-link-layer provides layer-2 hardware addressing mechanism. Hardware

Address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

⇒ Synchronization: When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

⇒ Error Control: Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

⇒ Flow Control: Stations on same link may have different speed or capacity. Data-link-layer ensures flow control that enables both machine to exchange data on same speed.

⇒ Multi-Access: When host on the shared link tries to transfer the data, it has a high probability of collision. Data link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple systems.

Ans. to the ques. no - 1(c)

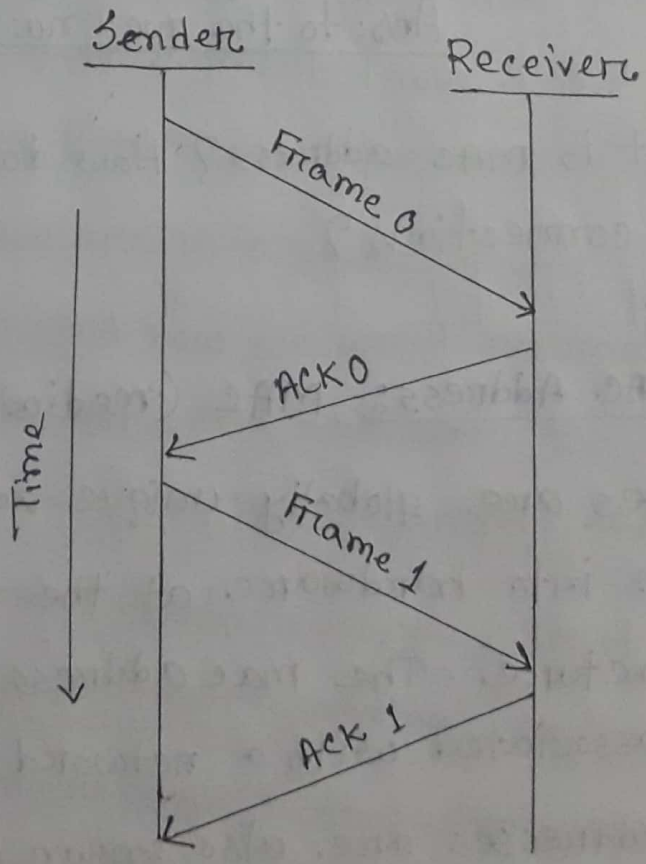
Q: Data link layer is responsible for which mechanisms? Explain point to point flow control.

Answer: Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer. Data-link layer is responsible for implementation of point-to-point flow and error control mechanism.

- **Flow Control:** When a data frame (Layer-2 data) is sent from one host to another over a sia single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/

software) of the sender or receiver differs? If sender is sending too fast receiver may be over-loaded, (swamped) and data may be lost. Two types of mechanisms can be deployed to control the flow.

• Stop and wait: This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received



• Sliding Window: In this flow control mechanism, both senders and receivers agree on the numbers of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

Ans: to the que: no: -2(a).

Q: What is MAC address? How does TCP deal with dead connections?

Answers:

MAC Address:- MAC (media Access Control) addresses are globally unique addressed that are written into hardware at the # time of manufacture. The mac address is a unique value associated with a network adapters. MAC addresses are also known as hardware addresses or physical addresses. The uniquely

an adapter on a LAN. MAC addresses are 12 digit hexadecimal numbers (48 bits in length) or 6 byte.

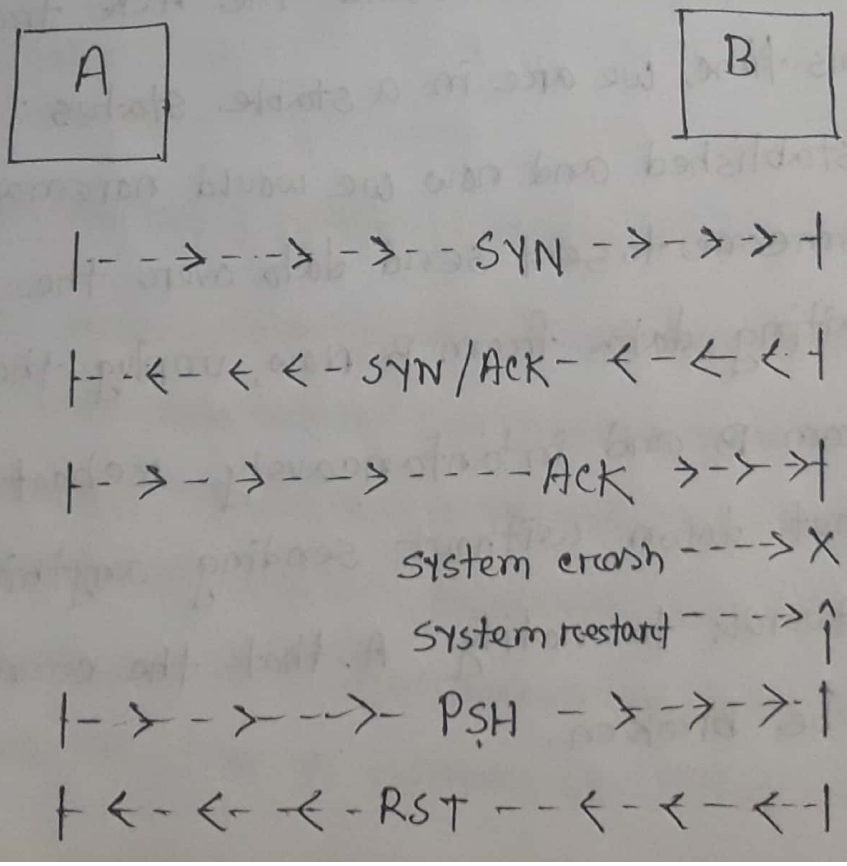
Tips to handle peer death in TCP connection:

After 3 way TCP handshake, TCP connection stays until normal 2-way termination protocol or abort due to error cases. Error cases can be network issue or peer death.

Think of a simple TCP connection between peer A and Peer B: there is the initial three way handshake, with one SYN segment from A to B, the SYN/ACK back from B to A, and the ACK from A to B. At this time, we are in a stable status: connection is established and now we would normally wait for someone to ~~sent~~ send data over the channel. Let A is waiting data from B. Now, unplug the power supply from B and instantaneously reboot B. It will shut down without sending anything over the network to notify A that the connection is going to be broken.

A. from its side, is ready to receive data, and has no idea that B has crashed. Now restore the power supply to B and wait for the system to restart. A and B are now back again, but while A knows about a connection still active with B, B has no idea.

The situation resolves itself when A tries to send data to B over the dead connection and B replies with an RST packet, causing A to finally to close the connection.



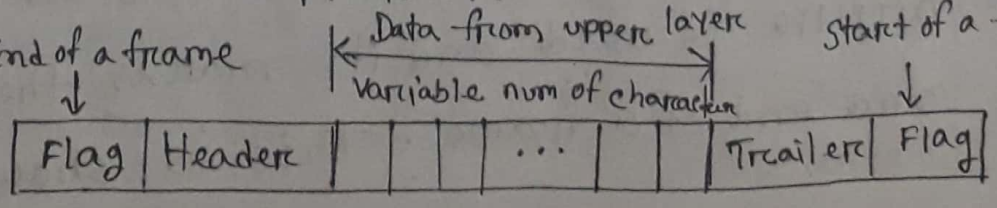
Ans. to the que. no - 2 (b)

Q: Compare and contrast byte-oriented and bit-oriented protocols. Which category has been popular in the past? Which category has been popular in now (explain the reason)?

Answer: In a character-oriented protocol, data to be carried are 8-bit characters (ASCII). The header carries the source and destination addresses and other control information, and the trailer carries error detection or error correction redundant bits, are also multiples of 8 bits.

To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame. The flag contains special characters and it indicates the start or end of a frame.

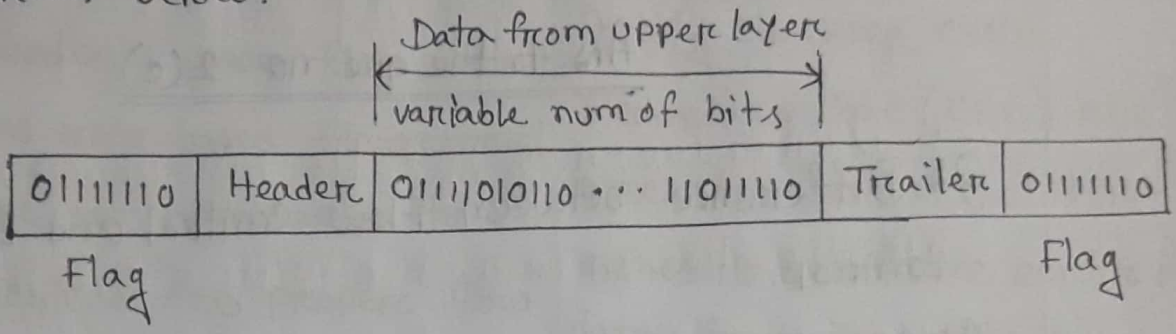
figure below shows the format of a frame in a character oriented protocol.



Drawbacks of character-oriented protocol: character oriented protocol framing was popular when only text was exchanged by the data link layers. The flag could be selected to be any character not used for text communication. But now we send other types of information such as graphs, audio, and vedio. Any pattern used for the flag could also be part of the information. If this happens, the receiver, when it encounters this pattern in the middle of the data, thinks it has reached of the end of the frame. This brawback is overcome by using a byte-stuffing strategy.

Bit-oriented protocol: In a bit-oriented protocol, the data section of a frame is a sequence of bits which is interpreted by the upper layer as text, audio, ~~vedio or~~ video, or graphics. To separate one frame from another, an 8-bit flag such as 01111110 is used and it marks the beginning and end of a frame. This is shown in the

diagram below:



Drawbacks: This flag can create the same type of problem as in the byte-oriented protocols. This is, if the flag pattern appears in the data, we needed to somehow inform the receiver that this is not the end of the frame. we do this by stuffing 1 single bit (instead of 1 byte) to prevent the pattern from looking like a flag. The strategy is called bit stuffing. In bit stuffing, if a 0 and five ~~consecutive~~ consecutive 1 bits are encountered, an extra 0 is added. This extra stuffed bit is eventually removed from the data by the receiver. Note that the extra bit is added after one 0 followed by five 1s regardless of the value of the next bit. This guarantees that the flag field sequence does not inadvertently appear in the frame.

Ans. to the que. no - 2(c)

Q: Difference between Flow control and Error control.

Answer:

Flow control: It is an important function of the Data Link Layer. It refers to a set of procedures that tells the sender how much data it can transmit before waiting for acknowledgement from the receiver.

Error Control: The error control function of data link layer detects the errors in transmitted frames and re-transmit all the erroneous frames.

Difference between Flow control and Error Control:

Flow Control	Error Control
Flow control is meant only for the transmission of data from sender to receiver.	Error control is meant for the transmission of error free data from sender to receiver.

Feedback-based flow control and rate-based flow control are the approaches to achieve the proper flow control.	Parity checking, cyclic Redundancy Code (CRC) and checksum are the approaches to detect the errors in data. Hamming code, Binary convolution codes, Reed-Solomon code, Low-Density Parity check codes are the approaches to correct the error in data.
Avoid overrunning of receivers buffer and prevents the data loss.	Detects and correct the errors occurred in the data
Example: Stop and wait Protocol and Sliding Window Protocol.	Example: Stop and wait ARQ and Sliding Window ARQ.

Ans. to the que. no- 3(a)

Q: Define framing and the reason for its need.

Answer: The stream of bits received from network layer is divided into smaller data units called frames. Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination. The physical layer provides bit synchronization to ensure that the senders and receivers use the same bit durations and timing. But, the data link layer must pack bits into frames, so that each frame is distinguishable from another.

What does framing do and why is it necessary?

1. Framing is the data link layer adds a sender address and a destination address. The destination address specifies where the packet should go; the sender address is used to send an acknowledgement back to the sender.

2. A whole message could be packed in one frame but that is not normally done, because a large frame can make flow and error control very inefficient.

3. When a message is carried in one very large frame, even a single bit error would required the retransmission of the whole message. When a message is divided into smaller frames, a single-bit error affects only that small frame and only the affected frame needs to be retransmitted.

Ans: to the que: no:- 3(b)

Q: Explain the reasons for moving from stop and wait ARQ to the Go-Back-N ARQ protocol?

Answer:

In Stop and wait ARQ, the sender needs to stop and wait for acknowledgement to each data frame that it has sent to the receiver. When the

sender sends a data frame to the receiver it starts timer. If the frame that the sender has ~~send~~ sent is damaged. The receiver will not get any frame received. so, it doesn't send any acknowledgement to that frame. By then, if the timer expires, the sender will resend that frame. In this protocol, sender has to get set the timer every time it send a frame. However in Go Back N ARQ, the sender ~~se~~ need not wait for ~~me~~ for the acknowledgement of the first frame it has sent. Sender can send multiple frames while waiting for acknowledgement. Several frames can be sent before we receive news about the previous frames. This is a over time. A task has begun before the previous ~~task~~ task has ended. Here the task is sending all the subsequent frames after sending the first frame before getting the acknowledgement

for the first frame. So eventually multiple frames are to be put in transition while waiting for acknowledgement. This is called pipelining, this improves the efficiency of the transmission.

Ans: to the que: no:- 3 (c)

Q: What are the key functions of error control technique?

Answer:

There are basically two types of errors, namely, (a) Damaged Frame
(b) Lost Frame

The key functions for error control techniques are as follows:

* Error detection
* Sending of positive acknowledgement (ACK) by the receiver for no error
* Sending of negative acknowledgement (NAK) by the receiver for error

* Setting of timers for lost frame
* Numbering of frames.

Ans: to the que: no- 3(d)

Q: What is the difference between error detection and error correction?

Answer:

Error detection:- Error detection involves checking whether any error has occurred or not. The number of error bits and the type of error does not matter.

Error correction:- Error correction involves ascertaining the exact number of bits that has been corrupted and the location of the corrupted bits.

Ans: to the ques: no:- 4(a)

Q: Define network layer. What are the features of a network layer?

Answer:

In the seven-layer OSI model of computer networking, the network layer is layer 3. The network layer is responsible for routing packets from source to destination within or outside a subnet. Two different subnet many have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols.

Features of network layer:

- Quality of service management
- load balancing and link management
- Security
- Interrelation of different protocols and subnets with different schema.
- Different logical network design over the physical network design.
- L3 VPN and tunnels can be used to provide end-to-end dedicated connectivity.

Ans: to the que. no:- 4 (b)

Q: List the functionalities of network layer.

Answer:

Devices which work on network layer mainly focus on routing. Routing may include various tasks aimed to achieve a single goal.

These can be:

Addressing devices and networks
Populating routing tables or static routes
Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets
Internetworking between two different subnets
Delivering packets to destination with best efforts
Provides connection oriented and connection less mechanism.

Ans: to the que: no:- 4 (c)

Q: why are different addressing needed in computer networks?

Answer:

IP addressing provides mechanism to

differentiate between hosts and network. Because IP addresses are assigned in hierarchical manner, a host always resides under a specific network. The host which needs to communicate outside its subnet, needs to know destination network address, where the packet/data is to be sent.

Hosts in different subnet need a mechanism to locate each other. This task can be done by DNS. DNS is a server which provides layer-3 address of remote host mapped with its domain name or FQDN. When a host acquires the Layer-3 Address (IP Address) of the remote host, it forwards all its packet to its gateway. A gateway is a router equipped with all the information which leads to route packets to the destination host.

Ans: to the ques: no:- 4 (d)

Q: What is difference between Broadcast and multicast ?

Answer:

Broad cast	Multi cast
The packet is transmitted to all the hosts connected to the network.	The packet is transmitted only to intended recipients in the network.
It has one sender and multiple receivers	It has one or more senders and multiple receivers
It sent data from one device to all the others devices in a network.	It sent data from one device to multiple devices
It works on star and bus topology.	It works on star, mesh, tree and bybrid topology.
It handwidth is wasted	It utilizes handwidth efficiently.
It has one-to-all mapping	It has one-to-many mapping
Example: Hub	Example: Switch

Ans: to the que: no: - 5 (a)

Q: What is routing? What are the main routing protocols?

Answer:

Network routing is the process of selecting a path across one or more networks. The principles of routing can apply to any type of network, from telephone networks to public transportation. In packet-switching networks, such as the internet, routing selects the paths for Internet Protocol (IP) packets to travel from their origin to their destination. These Internet routing decisions are made by specialized pieces of network hardware called routers.

Main routing protocols: In networking, a protocol is a standardized way of formatting

data so that any connected computers can understand the data. A routing protocol is a protocol used for identifying or announcing network paths.

The following protocols help data packets find their way across the Internet.

IP: The Internet Protocol (IP) specifies the origin and destination for each data packet. Routers inspect each packet's IP header to identify where to send them.

BGP: The Border Gateway Protocol (BGP) routing protocol is used to announce which networks connect to each other. BGP is a dynamic routing protocol.

The below protocols route packets within an AS:

OSPF: The open Shortest Path First (OSPF) protocol is commonly used by network routers to dynamically identify the fastest and shortest

available routers for sending packets to their destination.

RIP: The routing Information Protocol (RIP) uses "hop count" to find the shortest path from one network to another, where "hop count" means number of routers a packet must pass through on the way.

Other interior routing protocols include EIGRP (the Enhanced Interior Gateway Routing Protocol, mainly for use with Cisco routers) and IS-IS (Intermediate System to Intermediate System).

Ans: to the que: no:- 5(b)

Q: How can you manage a network using a router? You need to connect two computers for file sharing. It is possible to do this without using a hup or router?

Answer:

Manage a network using a router: Routers have built in console that lets you configure different setting, like security and data logging. you can assign restrictions to computers, such as that resources it is allowed access, or what particular time of the day they can browse the internet. you can even put restrictions on what websites are not viewable accross the entire network.

yes. you can connect to computers with a special ethernet or et cross other cable. To

set up the basic wired home network, all you need is an inexpensive Ethernet crossover cable and the other requirement is that network cards also known as LAN or Ethernet cards should be installed on each of your computers.

An Ethernet crossover cable like a cable, make such that both machine are using the same work group. That means the data transmission of one cable is connected to the data received pin of the other cable and vice versa.

Ans: to the que: no:- 5 (c)

Q: How does multicast routing differ from Unicast routing?

Answer:

A unicast transmission sends ip

packets to a single recipient on a network. A Multicast transmission sends IP packets to a group of hosts on a network. If the streaming video is to be distributed to a single destination, then you would start a unicast stream by setting the destination IP address and port on the AVN equal to the destination's values. If you want to view the stream at multiple concurrent locations, then you would set the AVN's destination IP address to a vaid multicast IP address (224.0.0.0 - 239.255.255.255)

Note that while the multicast IP address range is from 224.0.0.0 - 239.255:255.255, the first octet (224.xxx.xxx.xxx) is generally reserved for administration. VSI recommends setting the first octet to 255 and the remaining three Octets to the AVN's IP address. For example, if

the AVN's IP address is 192.168.1.53, then set the destination IP address to 255.168.1.53 for multicast streaming.

Since multicasting is a relatively new technology. some legacy devices that are part of your network might not support multicasting

Before using the AVN encoders in multicast streaming mode, check the functional specifications of your network infrastructure to ensure that the multicast stream will not create major traffic on your network.

Ans: to the que: no:- 6 (a)

Q: What does Internet Protocol Version 4 (IPv4) mean? Explain

Answer:

Internet Protocol Version 4 (IPv4) is the fourth version of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides the logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices - including manual and automatic configurations - depending on the network type.

IPv4 is based on the best effort model. This model guarantees neither delivery nor avoidance of duplicate delivery; these addressing mechanism.

IPv4 is 32-bit addressing schema used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable. IPv4 provides hierarchical addressing schema which enables it to divide the network into subnetworks, each with well-defined number of hosts. IP addressing are divided into many categories:

- Class A - it uses first octet for network addresses and last octets for host addressing.
- Class B - it uses first two octets for network addresses and last two for host addressing.
- Class C - it uses first three octets for network addresses and last one for host addressing.
- Class D - it provides flat IP addressing schema in contrast to hierarchical

structure for above three.

• Class E - it used as expercimental. IPv4 also has well-defined address to be used as private address (not routable on internet), and public addresses (provided by ISPs and are routable on internet). Though IP is not reliable one: it provides 'Best Effort Delivery' mechanism.

Ans: to the que: no: 6 (b)

Q: What is the difference between IPv4 and IPv6 ?

Answer:

As we know that both IPv4 and IPv6 are the two major internet protocols which are used as the principal communications protocol in the Internet protocol suite for le relaying datagrams across network boundaries. Its routing function

enables internet working, and essentially establishes the Internet.

So on the basis of functionality and features we can ~~distri~~ distinguish between both IPv4 and IPv6 protocols.

Following are the important difference, between IPv4 and IPv6 protocols.

IPv4 protocol has address length of 32-bit represented in decimal format and it supports manual and DHCP configuration.	IPv6 has 128-bit address length represented in hexadecimal format and supports Auto-configuration and renumbering configuration.
In case of IPv4 4.29×10^9 addresses could get generated.	In case of IPv6 3.4×10^{38} which is much greater than as compared to that of in IPv4 case.
In case of IPv4 fragmentation in performed by both senders and Forwarding routers.	In case of IPv6 the fragmentation in performed only by senders routers.

IPv4 is being used as less secure protocol as its security section is dependent on application, it is proportional to the security that is provided or implemented at application level.	IPv6 has its in built security future named as IPSEC, which provide additional security feature along with the security provided or implemented at application level.
In IPv4 Encryption and Authentication facility not provided.	In IPv6 both Encryption and Authentication facility are available.
In IPv4 the request header is not fixed and may be between of 20-60 bytes size.	In IPv6 the request header is of fixed 40 bytes size, and could not be get varied.

Ans: to the que: no:- 6(c)

Q: which fields of the IPv4 headers changes from routers to routers?

Answers:

If no fragmentation occures at the routers, then the only field to change in the base headers is the time to live (TTL) field. If any of the multiple byte option are present then there will be changes in the option headers as well.

If fragmentation does occur, the total length field will change to reflect the total length of each datagram. The more fragment bit of the flag field and the fragmentation offset field may also change to reflect the fragmentation.

If options are present and fragmentation occures the headers length field of the base headers may also change to reflect wheathers are not the option was included in the fragments.

Ans: to the que: no:- 6(d)

Q: Why we migrate from IPv4 to IPv6?

Answer:

Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.

The Internet must accommodate real-time audio, and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided in the IPv4 design.

The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.

To overcome these deficiencies. IPv6 also known as IPng was proposed and is now a standard.

Ans: to the que: no:- 7(a)

Q: Your company is given with IP address range of 192.168.160.0/27. The company has three dept: sales, customers services and I.T. Each department need to have a separate subnet. Divide your IP address range so that each dept. has a separate subnet with same numbers of IP addresses. what will be the networks address and subnet mask of each subnet? Also write down the range of each subnet and number of usable address that could be assigned to the users of each department.

Answer:

Here,

Given IP = 192.168.160.0/27 (class c)

Subnet mask : 225.225.225.224

11111111 11111111 11111111 11100000

Here, /27 means first 27 bits are fixed. So that available address bit = (32-27)=5

Block size or Host $= 2^5 = 32$ [256 - 224 = 32]

number of subnet $= 2^3 = 8$

Usable address / valid Host $= 2^5 - 2$

$= 30$

1st subnet :- (sales)

Network address : 192.168.160.0

Range of usable address : 192.168.160.1 – 192.168.160.30

Broadcast address : 192.168.160.31

Subnet mask : 255.255.255.224

2nd subnet : (customer service)

Network address : 192.168.160.32

Range of usable address : 192.168.160.33 – 192.168.160.62

Broadcast address : 192.168.160.63

Subnet mask : 225.255.255.224

3rd subnet : (IT)

network address : 192.168.160.64

Range of usable address : 192.168.160.65 – 192.168.160.94

Broadcast address : 192.168.160.95

Subnet mask : 255.255.255.224

Here, company have only three department. So

remaining 5 subnet will be so on.

Ans: to the que: no:- 7(b)

Q: A company got a C network (192.70.56.214) assigned and wants to divide the networks into subnets works for 120 computers each.

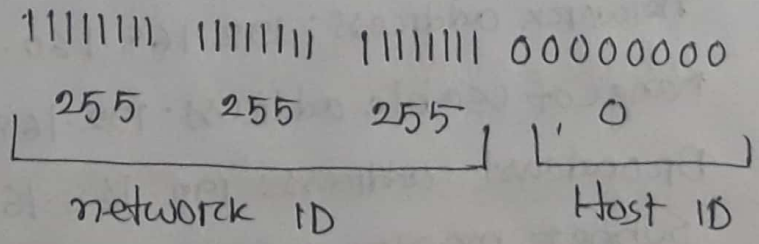
i) How many of those subnets can be established?
ii) How many usable address does each subnet have?
iii) which network do they have to used?
iv) which are the usable address per subnet?

Answer:

Given the IP = 192.70.56.214

which is a class C

So, the default masks of class C is /24



Now, we use that, Host = $2^8 = 256$

But we need only 120 address on host, but if we take 256 host address there are many address are waste.

If we ~~need~~ used 1 bit of the host as a net id then the Host $= 2^7 = 128$. It is related to 120.

∴ Here we use the ~~network~~ netmask for, /25

11111111 11111111 11111111 10000000

{ 255 255 255 } { 128 }

net. ID Host ID

(i) Number of subnet $= 2^1$.
$= 2$

(ii) number of usable address each subnet

$= 2^{32-25} = 2$

$= 2^7 - 2$

$= 126$

Block size $= 2^7 = 128$ [256 - 128 = 128]

(iii) Netmask to use is:

255.255.255.128

(iv) Usable address per subnet:.

Find network address :-

IP: 192.70.56.214	11000000	01000110	00111000	11010110
netmask 255.255.255.0	11111111	11111111	11111111	00000000
Logical AND operation :	11000000	01000110	00111000	00000000

Decimal value: 192. 70. 56. 0

For subnet 1:

network address: 192. 70. 56. 0

Usable Host Range: 192.70.56.1 – 192.70.56.126

Broadcast address : 192. 70. 56. 127

For subnet 2:

network address: 192. 70. 56. 128

Usable Host Range: 192.70.56.129 - 192.70.56.254

Broadcast address : 192. 70. 56. 255

Also we told that usable address: 192. 70. 56. 1 –

192. 70. 56. 254

Ans: to the que: no:- 8 (a)

Q: What is tunneling in internetworking?

Answer:

In computer networks, a tunneling protocol is a communications protocol that allows for the movement of data from one network to another. It involves allowing private network communications to be sent across a public network through a process called encapsulation.

Because tunneling involves repackaging the traffic data into a different form, perhaps with encryption as standard, it can hide the nature of the traffic that is run through a tunnel.

The tunneling protocol works by using the data portion of a packet to carry the packets that actually provide the service. Tunneling uses a layered protocol model such as those of the OSI or TCP/IP protocol suite, but usually violates the

layering when using the payload to carry a service not normally provided by the network. Typically, the delivery protocol operates at an equal or higher level in the layered model than the payload protocol.

Ans: to the que: no:- 8(b)

Q: What is data fragmentation? Explain how Data Fragmentation works?

Answer:

Fragmentation occurs when storage space is used inefficiently due to which storage capacity and performance is reduced.

Data fragmentation occurs when a large object is inserted into storage that has already suffered external fragmentation due to which the data object is broken up into many pieces that are not

close together.

When free storage becomes divided into many small pieces over time, its called External fragmentation.

Ans: to the que: no: 8 (c)

Q: Define IP (IP sec). What are the two protocols defined by IPsec? Briefly describe the services provided by IPsec.

Answer:

IPsec :- Internet Protocol security (IPsec) is the set of protocols that provides security for ~~the~~ Internet Protocol. It can use cryptography to provide security.

IP sec can be used for the setting up to ~~fei~~ virtual private networks (VPNs) in a secure manner. Also known as IP security.

The AH and ESP are two protocols that are defined

by IPsec. Transport mode Authentication Header (AH) provides integrity authentication services to IPsec capable devices.

Encapsulating security payload (ESP) protocol used for encrypted message.

Service by Provided by IPsec :-

i) Access control
ii) Comection less Integration
iii) Data origin authentication
iv) Rejection or replayed packets
v) Confidentially (encryption)
vi) Limited traffic flow confidentially

Ans: to the que: no:- 8 (d)

9: what is the function of Internet Control Message Protocol ICMP?

Answer: ICMP is a transport ~~tel~~ level protocol

Within TCP/IP which communicates information about network connectivity issues back to the source of the compromised transmission. It sends control message such as destination network unreachable, source route faild, and source quench. It uses a data packet structure with an 8-byte header and variable-size data section.

ICPM is used by a device, like a router, to communicate with the source of a data packet about transmission issues. For example, if a datagram is not delivered, ICMP might report this back to the host with details to help discern where the transmission went wrong. It's a protocol that believes in direct communication in the workplace.