2020/Fall

1(a) Describe the demerits of computer network. Differentiate between client/server and peer-to-peer network models.

⇒

Computer network is defined as a set of interconnected autonomous systems that facilitate distributed processing of information. It results in better performance with high speed of processing. The demerits of computer networks are described below:-

(i) It lacks robustness:-

If a PC system's principle server separates, the whole framework would end up futile. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill.

(ii) It lacks independence:-

PC organizing includes a procedure that is worked utilizing PCs, so individuals will depend a greater amount of PC work, rather than applying an exertion for their jobs that needs to be done. Beside this, they will be subject to the primary document server, which implies that, in the event that it separates, the framework would end up futile, making clients inactive.

(iii) Virus and Malware:-

On the off chance that even

one PC on a system gets contaminated with an infection, there is a possibility for alternate frameworks to get tainted as well. Infections can spread on a system effectively. ~~In view of the between~~

(iv) Cost of network :-

The expense of executing the system including installation cost, cabling and equipment can be expensive.

(v) Requires time for administration

Client - Server Network :-

This model is broadly used network model. In this network, clients and serva are differentiated, specific server and clients are present. Here, centralized server is used to store the data as its management is centralized. Also, server responds the services which is requested by client. Eg:- web server.

Peer - to - Peer Network :

This model does not differentiate the clients and the servers. In this, each and every node is itself client and server. Here, every node can do both request and respond for the services. Eg:- skype, bittorrent.

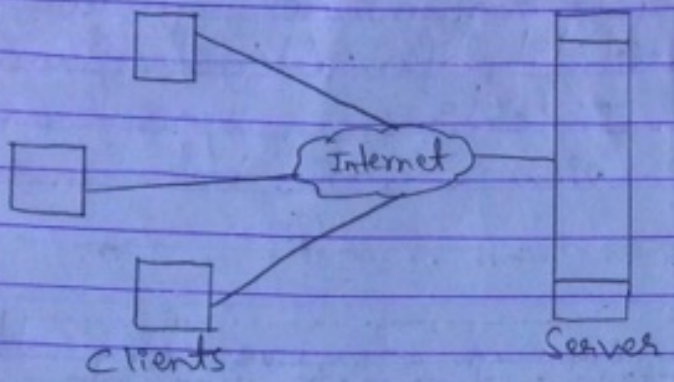

Fig:- Client-Server Network Model

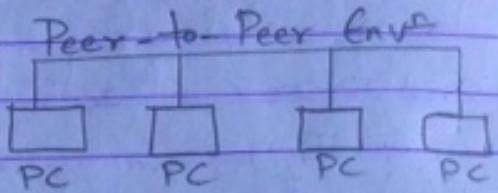

Fig:- Peer-to-Peer Network Model

Advantages of Peer-to-Peer Model	Advantages of client-Server Model
(i) Less expensive for implementation.	(i) Provides of better security
(ii) Doesn't require additional specialized network administration software.	(ii) Easier to administer when the network is large as administration is centralized.
(iii) Doesn't require a dedicated network administrator.	(iii) All date can be backed up on one central location.
Disadvantages	**Disadvantages**
(iv) Doesn't scale well to large network and administration becomes unmanageable.	(iv) Requires expensive, specialized network administrative and operational software.
(v) Less Secure	(v) Requires a professional administrator
(vi) All machine sharing the resources negatively impact the performance.	(vi) A single point of failure. User data is unavailable if the server is down.
(vii) Each user must be trained to perform administrative tasks.	(vii) Requires more expensive, more powerful hardware for the server machine.

1(b) How are interfaces, protocols and services of layered system related? Discuss the differences between OSI and TCP/IP models.

⇒

Interfaces are networking communication points for computer. Each interface is associated with a physical or virtual networking device. A layer's interface tells the processes above it how to access it. It specifies what the parameters are and at results to expect. It is not concerned about how the layer works inside.

A protocol is used for communication between entities in different systems. Protocol may be defined as a set of rules governing the exchange of data between two entities. It also may be conceived as a set of agreement between two communicating processes. The protocols used in a layer are for their own function. The layer can use many protocols it wants to, as long as it gets the job done. It can also exchange them without affecting software in higher layers.

A service is formally specified by a set of primitives (operations) available to a user or other entity to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity. A service is a set of operations that a layer provides to the layer above it.

A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.

The difference between OSI and TCP/IP models are

TCP/IP	OSI
(i) It is implementation of OSI model.	(i) It is reference model.
(ii) It is the model around which internet is developed.	(ii) It is a theoretical model.
(iii) It has only 4 layers.	(iii) It has 7 layers.
(iv) It is considered more reliable	(iv) It is considered a reference tool.
(v) It uses horizontal approach.	(v) It uses vertical approach.
(vi) It combines the session and presentation layer in app^{n} layer.	(vi) It has separate session and presentation layer.
(vii) Protocols were developed first and then the model was developed.	(vii) Here, model was developed before the development of protoco
(viii) It supports only connectionless communication in the network layer.	(viii) It supports connectionless and connection-oriented communica in the network layer.

(ix) It is protocol dependent standard.	(ix) It is protocol independent standard.
(x) Protocols are not strictly defined in this model.	(x) This model has strict boundaries for the protocols.

2(a) List the major function of internetworking device. Briefly explain the design issues of network layer.

⇒

Internetworking is combination of 2 words, inter and networking, which implies an association between totally different nodes or segments. This interconnection is often among or between public, private, commercial, industrial, or governmental networks. Internetworking is enforced in layer three (Network layer) of OSI model. The foremost notable example of internetworking is that the internet.

Some of the internetworking devices along with their functions are explained below:-

(i) Repeater:-

A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which

the signal can be transmitted over the same network. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength, but they do not amplify the signal. It is a 2 port device.

(ii) Hub :-

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. Also, they do not have the intelligence to find out best path for data packets which leads to inefficiencies and wastage.

(iii) Bridge :-

A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

(iv) Switch :-

A switch is a multiport bridge

with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forwards good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

(v) Routers :-

A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

(vi) Gateway :-

A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more

coraplex than switch or router.

(vii) Brouter:-

It is also known as bridging router device which combines features of both bridge and router. It can work either at a data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

Network layer is majorly focused on getting packets from the source to destination, routing error handling and congestion control. The network layer comes with some design issues which are described below:-

(1) Store and forward packet switching:-

The host sends the packet to the nearest router. This packet is stored there until it has fully arrived once the link is fully processed by verifying the checksum then it is forwarded to the next router till it reaches the destination. This mechanism is called "store and forwarde packet switching".

(2) Services provided to transport layer:-

Through the

network/transport layer interface, the network layer transfers its services to the transport layer. These services are described below. But before providing these services to the transfer layer, following goals must be kept in mind:-

- offering services must not depend on router technology.
- The transport layer needs to be protected from the type, number and topology of available router.
- The network addresses for the transport layer should use uniform numbering pattern also at LAN and WAN connections.

Based on connections, there are 2 types of services provided:-

(A) connectionless:- The routing and insertion of packets into subnet is done individually. No added setup is required.

(B) Connection-oriented:- subnet must offer reliable service and all the packets must be transmitted over a single route.

3) Implementation of connectionless service:-

Packet are termed as "datagrams" and corresponding subnet as "datagram subnets". When the message size that has to be transmitted is 4 times the size of packet, then the network layer divides into 4 packets and transmits each packet to router via a few protocol.

Each data packet has destination address and is routed independently irrespective of the packets.

(4) Implementation of connection-oriented service :-

To use a connection-oriented service, first we establish a connection, use it and then release it. In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender. It can be done in either two ways :-

- Circuit switched connection
- Virtual circuit switched connection

2(b) What are the metrices of network performance? Describe them in short.

⇒

Performance of a network pertains to the measure of service quality of a network as perceived by the user. There are different ways to measure the performance of a network, depending upon the nature and design of the network. The metrices of network performance are as follows:

- Bandwidth :-

Bandwidth is characterized as the measure of data or information that can be transmitted in a fixed measure of time. Bandwidth determines how rapidly the web server is able to upload

the requested information. In case of digital devices, bandwidth is measured in bits per second (bps) or bytes per second whereas in case of analog devices, bandwidth is measured in cycles per second, or Hertz (Hz). Also, more bandwidth does not mean more speed.

- **Throughput:-**

Throughput is the number of messages successfully transmitted per unit time. It is controlled by available bandwidth, the available signal-to-noise ratio and the hardware limitations. The maximum throughput of a network may be consequently higher than the actual throughput achieved in everyday consumption.

- **Latency:-**

In a network, during the process of data communication, latency (also known as delay) is defined as the total time taken for a complete message to arrive at the destination, starting with the time when the first bit of message is sent out from the source and ending with the time when the last bit of message is delivered at destination. In simpler terms, latency may be defined as the time required to successfully send a packet across a network. High latency leads to creation of bottlenecks in any network communication. It stops the data from taking full advantage of the network pipe and conclusively

decreases the bandwidth of the communicating network. Latency is also known as a ping rate and measured in milliseconds (ms).

- **Bandwidth-Delay Product :-**

Bandwidth and delay are two performance metrics of a link. The bandwidth-delay product defines the number of bits that can fill the link. What is significant in data communications is the product of two, the bandwidth-delay product.

- **Jitter :-**

Another performance issue related to delay is jitter. In technical terms, jitter is a "packet delay variance". It can simply mean that jitter is considered as a problem when different packets of data face different delays in a network and the data at the receiver application is time-sensitive, i.e. audio or video data. Jitter is measured in milliseconds (ms). It is defined as an interference in the normal order of sending data packets. Jitter is negative and causes network congestion and packet loss.

3(a) Explain how selective repeat works with figure.

⇒

Selective repeat mechanism is more efficient for noisy links, but the processing at the receiver is more complex. The selective repeat protocol uses two windows: a sender window and a receiver window and both windows have same size i.e. 2^{m-1}, where 'm' is the size of sequence number field in bits. Selective repeat protocol allows the receiver to accept and buffer the frames following a damaged or lost one. It attempts to retransmit only those packets that are actually lost (due to errors). For this, receiver must be able to accept packets out of order. Since receiver must release packets to higher layer in order, the receiver must be able to buffer some packets.

Selective Repeat Protocol (SRP) works better when the link is very unreliable. Because, in this case, retransmission tends to happen more frequently, selectively transmitting frames is more efficient than retransmitting all of them. SRP also requires full duplex link. Backward acknowledgements are also in progress. In SRP, window size should be less than or equal to half the sequence number to avoid packets being recognized incorrectly. Receiver stores correct packets until they can be delivered in order to higher layer.

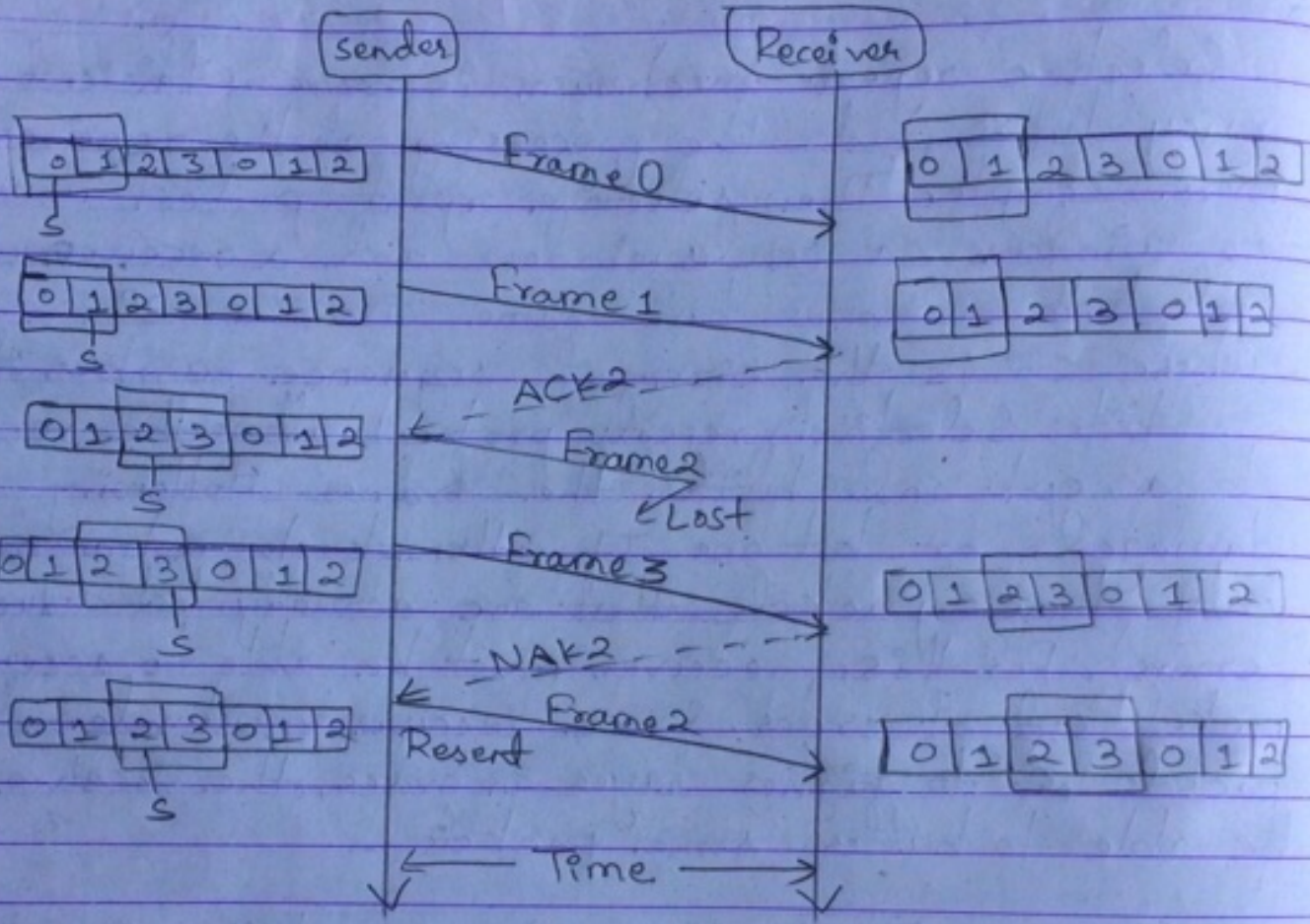

Fig:- The sender only retransmits frames, for which a NAK is received.

3(b) Describe framing by character count. How does byte stuffing overcome the disadvantages of character count algorithm?

⇒

The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

In a character-oriented protocol, data to be carried are 8-bit characters from a coding system such as ASCII. The header, which normally carries the source and destination addresses and other control information, and the trailer, which carries error detection or error correction redundant bits are also multiple 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 composed of protocol dependent special characters, signals the start or end of a frame. To fix this problem, a byte-stuffing strategy was added to character-count framing.

In byte stuffing, a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is ~~fulfilled~~ stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

Byte stuffing by the escape character allows the presence of the flag in the data section of the frame, but it creates another problem.

4(a) Why summarization is important? PU is planning to design new network for four different departments. Each department consists of 24 hosts with IP address 172.16.1.0/27. Explain the process how you will allocate the IP address, subnet mask for each of dept. using above IP address.

⇒

4(b) Explain IPv4 header protocol format and also differentiate between IPv4 and IPv6 features.

⇒

An IPv4 address is a 32-bit long address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the internet.

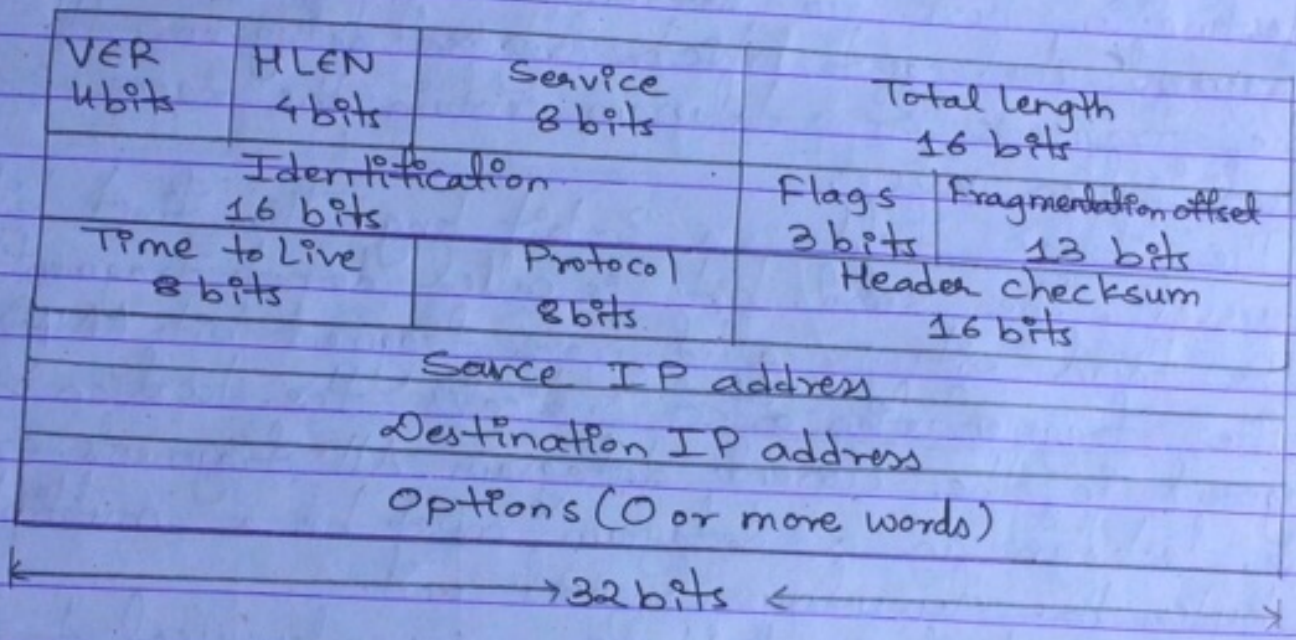

Fig:- IPv4 datagram format

An IP datagram consists of a header part and a text part. The header has a 20-byte fixed part and a variable length optimal part.

The version (VER) field keeps track of which version of the protocol the datagram belongs to.

Since the header length is not constant, a field in the header HLEN is provided to tell how long the header is, in 32-bit words. The minimum value is 5,

which applies when no options are present.

The service field allows the host to tell subnet what kind of service it wants.

The total length includes everything in the datagram - both header and data. The maximum length is 65,535 bytes.

The identification field is needed to allow the destination host to determine a newly arrived fragment belongs to which datagram. All the fragments of a datagram contain the same identification value.

The flags field is a 3-bit long. The first bit is reserved. The second bit is called do not fragment bit (DF). The third bit is called more fragment bit (MF).

The fragmentation offset indicates the location of the fragment in the current datagram. All fragments except the last that are in a datagram must be a multiple of 8 bytes, the elementary fragment unit.

The time to live field is a counter used to limit packet lifetimes. It counts time in seconds, allowing a maximum lifetime of 255 seconds. When it hits zero, the packet is discarded and a warning packet is sent back to the source host.

The protocol field tells which transport process has to be followed. For instance, TCP and UDP.

The header checksum verifies header only. These are useful for detecting errors generated by bad memory words inside a router. It is recomputed at each hop, because at least one field always changes.

The source ip address and destination ip address indicate the network number and host number.

The options field was designed in order to avoid allowing subsequent versions of the protocol to include information not present in the original design permitting experiments to try out new ideas. Also, it is variable length.

The difference between IPv4 and IPv6 features are:-

IPv4	IPv6
• Source & destination addresses are 32-bits.	• Source and destination addresses are 128 bits.
• IPv4 support small address space.	• Supports a very large address space sufficient for each and every people on earth.
• IPv4 header includes checksum.	• IPv6 doesn't include the checksum.
• Header includes options.	• All optional data is moved to IPv6 extension header.
• Broadcast address are used to send traffic to all nodes on a subnet.	• There is no IPv6 broadcast address. Instead a link local scope all-nodes multicast address is used.

5(a) Describe 4 way TCP handshaking with suitable diagram.

⇒

Any of the two parties involved in exchanging data (client or server) can close the connection, although it is usually initiated by the client. Most implementations today allow two options for connection termination: three-way handshaking and four-way handshaking with a half-close option.

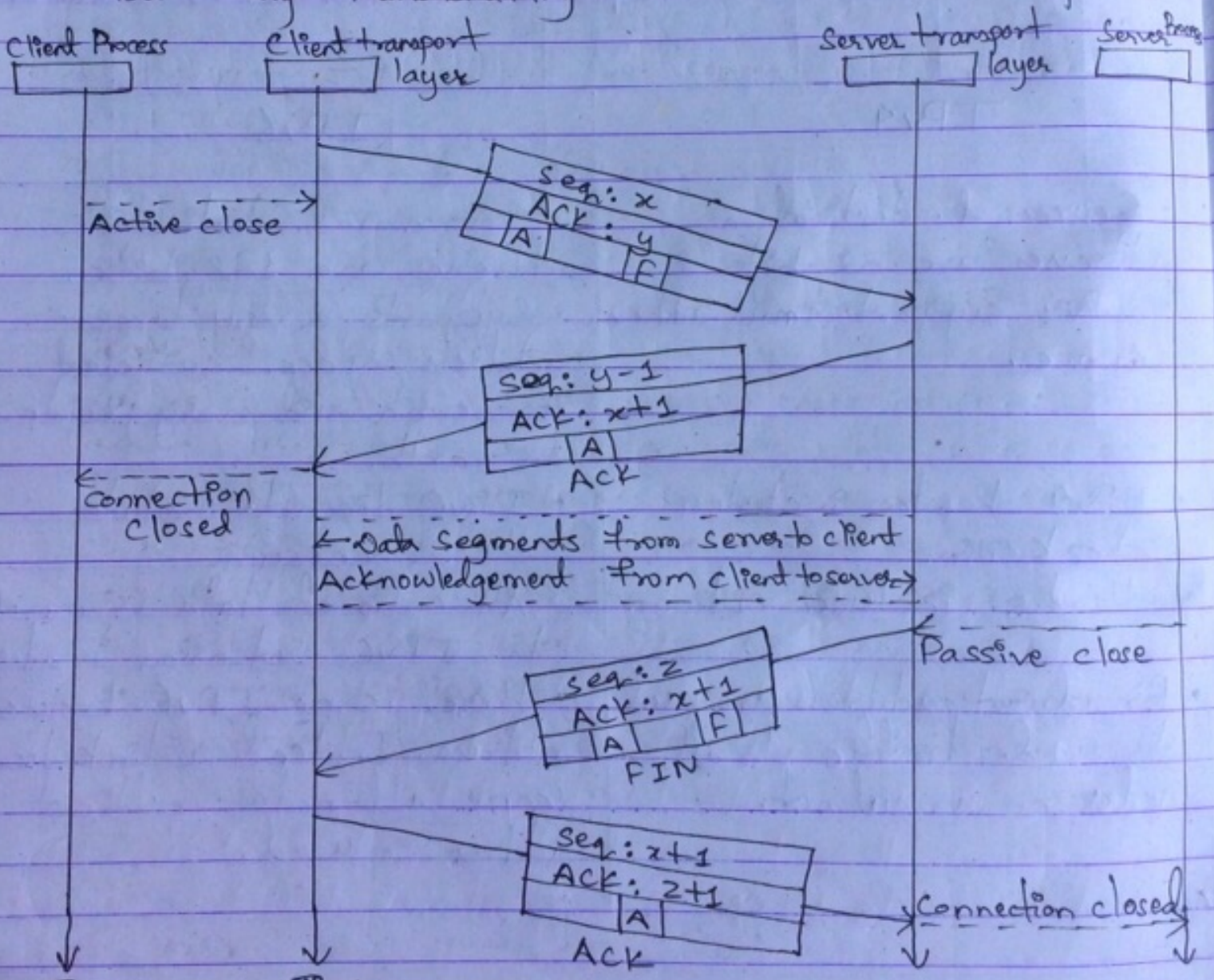

Fig:- Connection Termination using four way handshaking

5(b) Why congestion is prominent in Networks? Explain Explicit and Implicit control algorithm with a suitable example.

⇒

When too many packets are present in the subnet, performance degrades, this situation is called congestion. When the number of packets dumped into the subnet by the hosts within its carrying capacity, they all are delivered, but as traffic increases too far, the routers are no longer able to cope and they begin to lose packets. At very high traffic, performance collapses completely and almost no packets are delivered. Ideally the number of packets delivered is proportional to the number sent.

Implicit Control :-

In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network from other symptoms. For example, when a source sends several packets and there is no acknowledgement for a while, one assumption is that the network is congested. The delay in receiving an acknowledgement is interpreted as congestion in the network; the source should slow down.

Explicit Control :-

The node that experiences congestion

can explicitly send a signal to the source or destination. The explicit signaling method, however is different from the choke packet method. In the choke packet method, a separate packet is used for this purpose, in the explicit signaling method, the signal is included in the packets that carry data. It can occur in either the forward or the backward direction.

6(a) What is SMTP? Differentiate POP and IMAP protocols.

⇒

SMTP (Simple Mail Transfer Protocol) is an application layer protocol. The client who wants to send the email opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP ~~connection~~ process initiates a connection on that port (Port No. 25 for mail transfer. After successfully establishing the TCP connection, the client process sends the mail instantly.

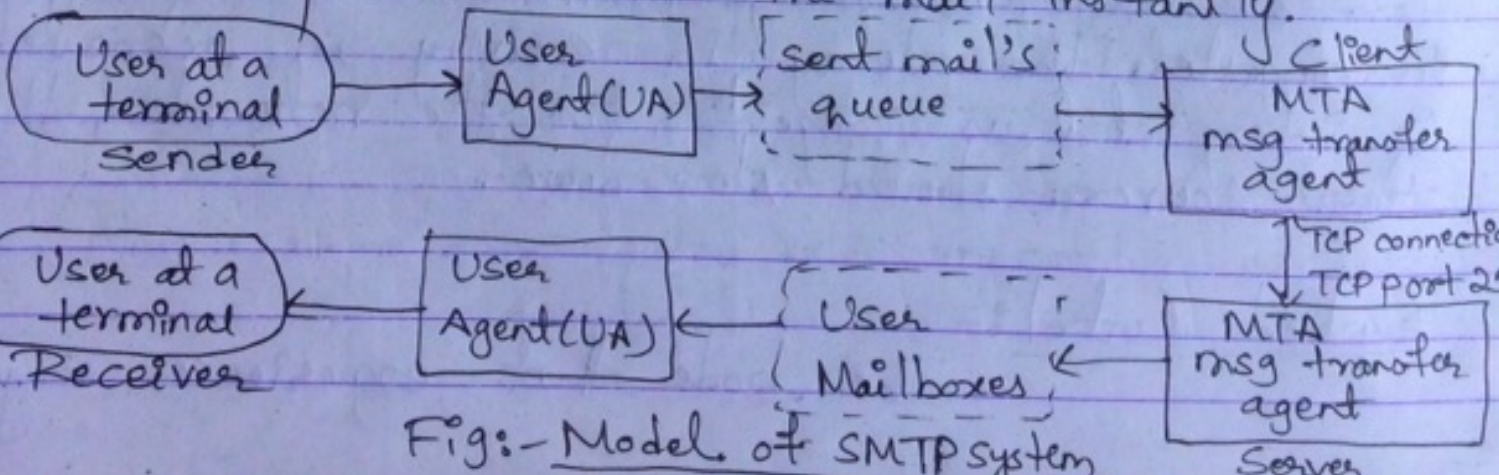

Fig:- Model of SMTP system

The difference between POP and IMAP protocols are:-

IMAP	POP
• IMAP is much more advanced and allows the user to see all the folders on the mail server.	• POP is a simple protocol that only allows downloading messages from inbox to local computer.
• The IMAP server listens on port 143 and the IMAP with SSL secure server listens on port 993.	• The POP server listens on port 110 and the POP with SSL secure server listens on port 995.
• Messages can be accessed across multiple devices.	• In POP, the mail can only be accessed from a single device at a time.
• The mail content can be read partially before downloading	• To read the mail, it has to be downloaded on the local system.
• The user can organize the emails directly on the mail server.	• The user cannot organize mails in the mailbox of mail server
• The user can create, delete or rename email on the mail server.	• The user cannot create, delete or rename email on the mail server.

• A user can search the content of mail for specific string before downloading.	• A user cannot search the content of mail before downloading to the local system.
• Message header can be viewed prior to downloading.	• All the messages are downloaded at once.

6(b) What do you mean by network security? Explain the operation of Data Encryption Standard Algorithm.

⇒

Networks are being used for banking, shopping, email, entertainment, etc. Because of this, there are arising more problems on network security. It is especially concerned with people trying to access remote services that they are not authorized to use and intended to gain some profit or harm some one. Also, making the network secure is more tedious than just keeping it free of programming errors. Normally, network security problems are of four types: secrecy, authentication, non-repudiation and integrity control. Secrecy has to do with keeping information out of hands of unauthorized users. Authentication deals with determining whom you are talking to before revealing sensitive information. Non-repudiation deals with signature that verifies the data has come from the correct user or source.

Data Encryption Standard (DES) Algorithm

- Block size → 64 bits
- No. of rounds → 16 round
- key size → 64 bits
- No. of sub keys → 16 sub-keys
- sub-key size → 48 bits
- Cipher text → 64 bits

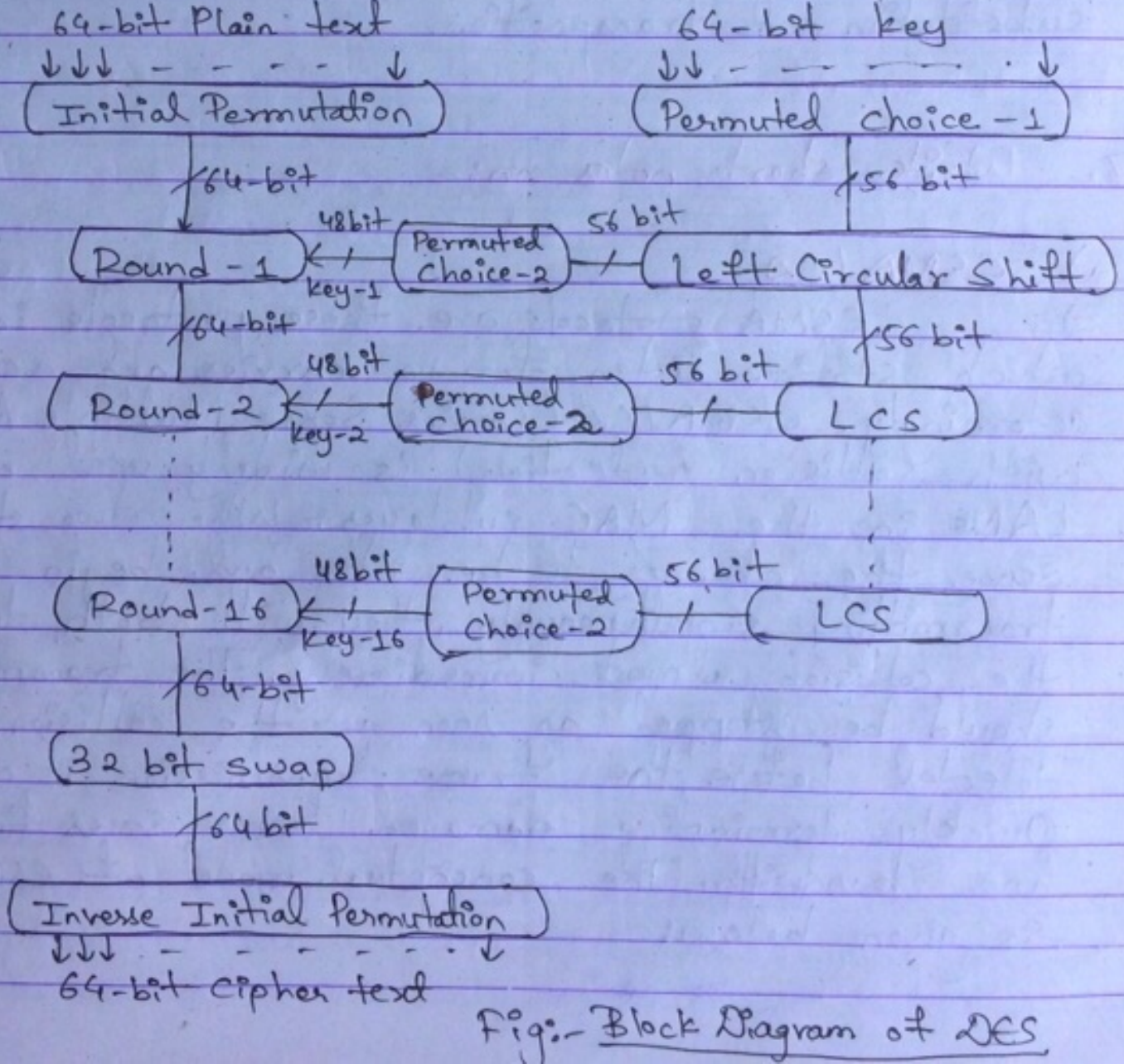

Fig:- Block Diagram of DES

DES is a block cipher and encrypts data in blocks of size of 64 bit each means 64 bits of plain text goes as the input to DES which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption. DES is based on the two fundamental attributes of cryptography: substitution and transposition. DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition.

7. Write short notes on:-

a) CSMA/CD

⇒ CSMA protocols are those protocols in which stations listen for a carrier and act accordingly. CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is widely used on LANs in the MAC sublayer. When two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately. The transmission should be stopped as soon as the collision is detected before the frame transmission is completed. Quickly terminating damaged frames saves time and bandwidth. The conceptual model of CSMA/CD is given below:-

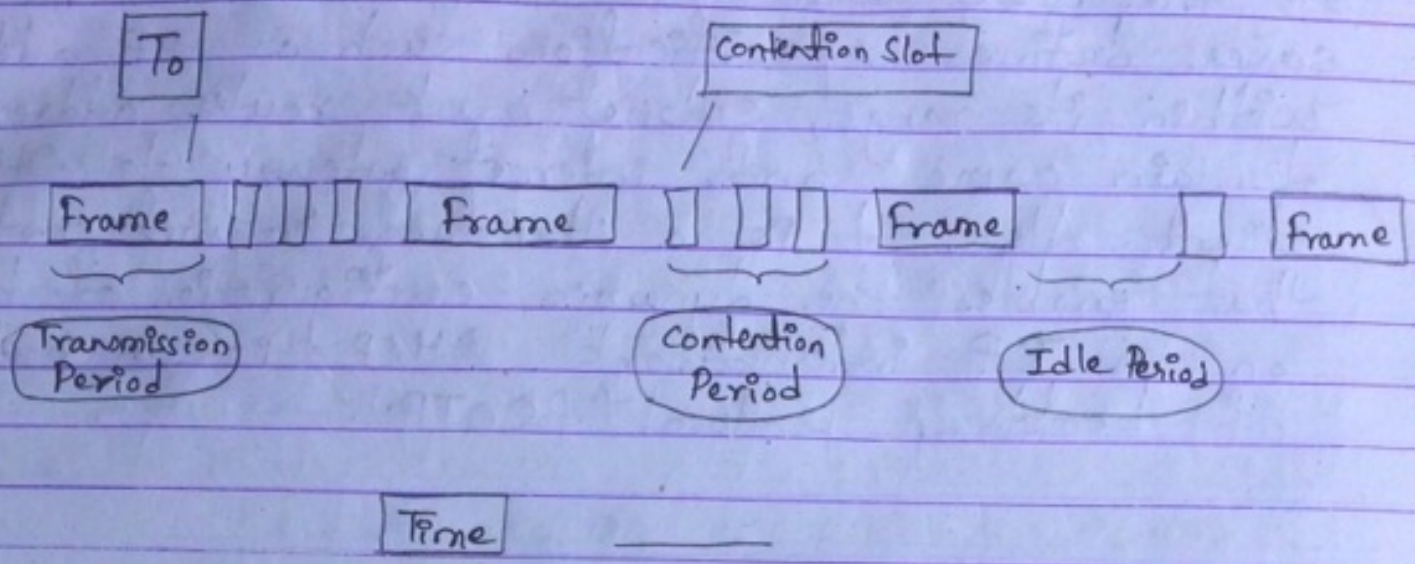

Fig:- Conceptual Model of CSMA/CD

(b) DHCP

⇒

DHCP (Dynamic Host Configuration Protocol) is one of the popular protocols in the networking environment. DHCP is responsible for assigning IP addresses to the various machines in the network. When a machine with a NIC card is booted up, it sends a DHCP request for obtaining an IP address. Then the DHCP server listens to it and grants the unique IP address to it so that the workstation/machine can communicate other machines in the network. DHCP server assigns an IP address either randomly or as per the MAC address

of the NIC card of the machine. DHCP saver defines specifications such as IP address within its range, subnet mask, router addres, domain name and internet gateway to DHCP client. Also, it is a standard internet protocol that enables the dynamic configuration of hosts on an IP internetwork. DHCP is an extension of bootstrap protocol (BOOTP).

(c) Firewall

⇒

Firewall refer to the mechanism of checking each and every network packet while entering and departing a fixed network (mostly LAN). The two basic components of firewall are packet filter and application gateway. Firewall defines any system or device that allows safe network traffic to pass while restricting or denying unsafe traffic. Firewalls are usually dedicated machines running at the gateway point between local network and the outside world and are used to control who has access to private corporate network from the outside. More generally, a firewall is any system that controls communication between two networks. For example, over the internet. There are three types of firewall.

- Network level firewall
- Circuit level firewall
- Application level firewall

2019 | Spring

1(a) Define Computer Network. Briefly explain the different types of network model.

⇒

Computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Computer network is also called a data network. Also, it is a series of points, or nodes interconnected by communication paths for the purpose of transmitting, receiving and exchanging data, voice and video traffic.

There are several classification for network model.

- Classification based on Scale (size)
  - (i) PAN (Personal Area Network)
  - (ii) LAN (Local Area Network)
  - (iii) CAN (Campus Area Network)
  - (iv) MAN (Metropolitan Area Network
  - (v) DAN (Desert Area Network)
  - (vi) CAN* (Country Area Network)
  - (vii) WAN (Wide Area Network)
  - (viii) GAN (Global Area Network)

- Classification based on Topology
  - (i) Bus Topology
  - (ii) Ring Topology
  - (iii) Mesh Topology

(iv) Star Topology
(v) Hierarchical Topology
(vi) Extended Star Topology

• Classification based on Architecture
(i) Peer-to-Peer Model
(ii) Client-Server Model

1(b) Why do you need layered architecture in network? Compare OSI model with TCP/IP model.

⇒

Some of the key design issues that occur in computer networking are present in several layers such as:-

(i) Every layer needs a mechanism for identifying senders and receivers. Since network normally has many computers, some of which have multiple processors means is needed for a process on one machine to specify with whom it wants to talk. As a consequence having multiple destinations, some form of addressing is needed in order to specify a specific destination.

(ii) Another set of design decision concerns the rules for data transfer, such as simplex, half duplex, full duplex.

(iii) Error control is an important issue because physical communication circuits are not perfect.

(iv) Not all communication channels preserve the order of messages sent on them. To deal with a possible loss of sequencing, the protocol must make explicit provision for the receiver to allow the pieces to be put back together properly.

(v) An issue that occurs at every level is how to keep a fast sender from swapping a slow receiver with data.

When there are multiple paths between source and destination, a route must be chosen sometimes this decision must be split over two or more layers.

2(a) Define transmission media. Explain different types of transmission media in detail.

⇒

A transmission media can be defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation in the air. The transmission medium is usually space, metallic cable, or fiber-optics cable.

The types of transmission media are:-

(A) Guided Transmission Media
  (i) Twisted - Pair Cable
  (ii) Coaxial Cable → Base-band C.C.
  (iii) Fiber - Optics Cable → Broadband C.C.
(B) Unguided Media
  (i) Free Space

2(b) What do you mean by framing? List the different framing technique and illustrate bit stuffing with examples.

⇒

The data link layer needs to pack bits into frames, so that each frame is distinguishable from another. The data link layer prepares a packet for transport across the local media by encapsulating it with a header and a trailer to create a frame. Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding address and a destination address.

The different framing techniques are:-

(i) Fixed - Size Framing
(ii) Variable - Size Framing
(iii) Character - Oriented Protocols
(iv) Bit - Oriented Protocols
(v) Flow Contro

Bit stuffing:-

In a bit-oriented protocol, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphics, audio, video and so on. However, in addition to headers we still need a delimiter to separate one frame from the other.

3(b) You are given IP address 150.152.0.0. and you need to subnet the given IP into five different Departments. Perform the subnetting and find the subnet mask, network Address, Broadcast address and usable host address in all subnet.

⇒

4(b) What is socket address and communication? Explain the services provided by transport layer.

⇒

Socket is termed as the concatenation of a port number and the network address (IP address) of host that supports the port service. Process-to-process delivery needs two identifiers, IP address and the port number, at each end to make a connection. The combination of an IP address and a port number is called a socket address. The client socket address defines the client process uniquely just as the server socket address defines the server process uniquely.

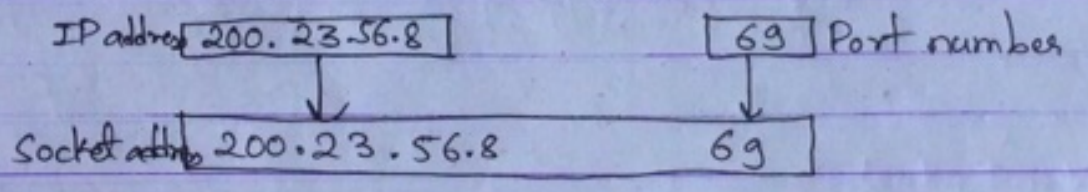

Fig:- Socket Address

Communication is achieved through commands and responses. Communication has three attributes: file type, data structure and transmission mode.

The transport layer is responsible for providing reliable transport services to the upper layer protocols. These services include the following:-

- Flow control to ensure that the transmitting device

does not send more data than the receiving device can handle.
- Packet sequencing for segmentation of data packets and remote reassembly.
- Error handling and acknowledgements to ensure that data is retransmitted when required.
- Multiplexing for combining data from several sources for transmission over one data path.
- Virtual circuits for establishing sessions between communicating stations.

5(a) What is congestion? Briefly explain different types of technique for traffic shaping.

⇒ Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity. Congestion in a network may occur if the load on the network (the number of packets sent to the network) is greater than the capacity of the network (the number of packets a network can handle).

Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network. The types of technique that can shape traffic are:-
- Leaky Bucket and
- Token Bucket

- **Leaky Bucket :-**

In networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate.

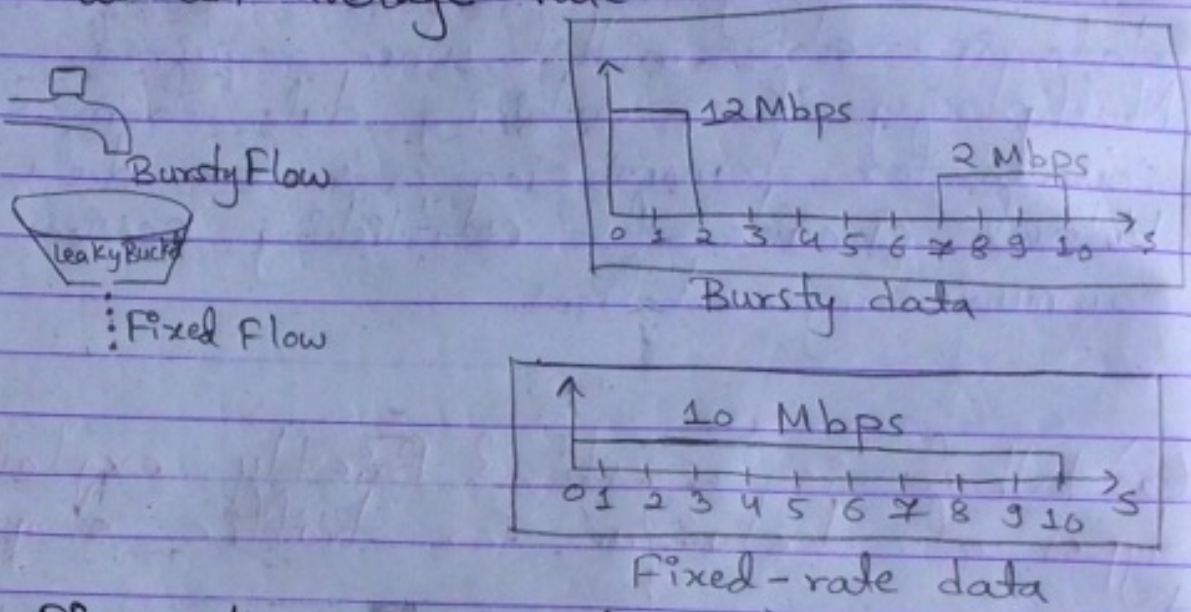

Fig:- Leaky Bucket

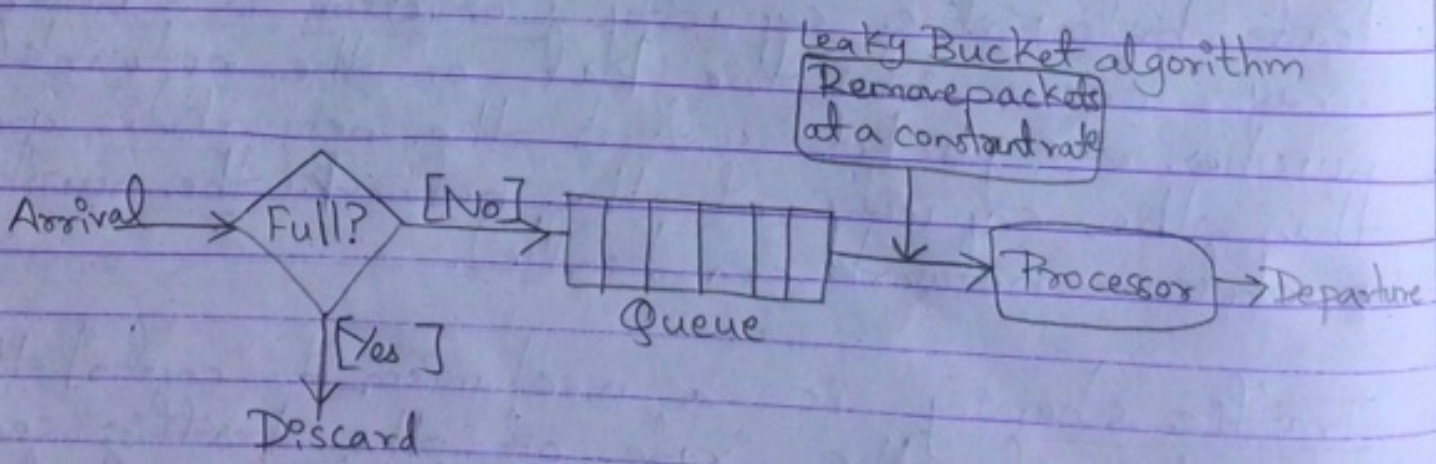

Fig:- Leaky Bucket implementation

• Token Bucket :-

The token bucket allows idle hosts to accumulate credit for the future in the form of tokens. For each tick of the clock, the system sends n tokens to the bucket. The system removes one token for every byte of data sent. Here, the host can send bursty data as long as the bucket is not empty.

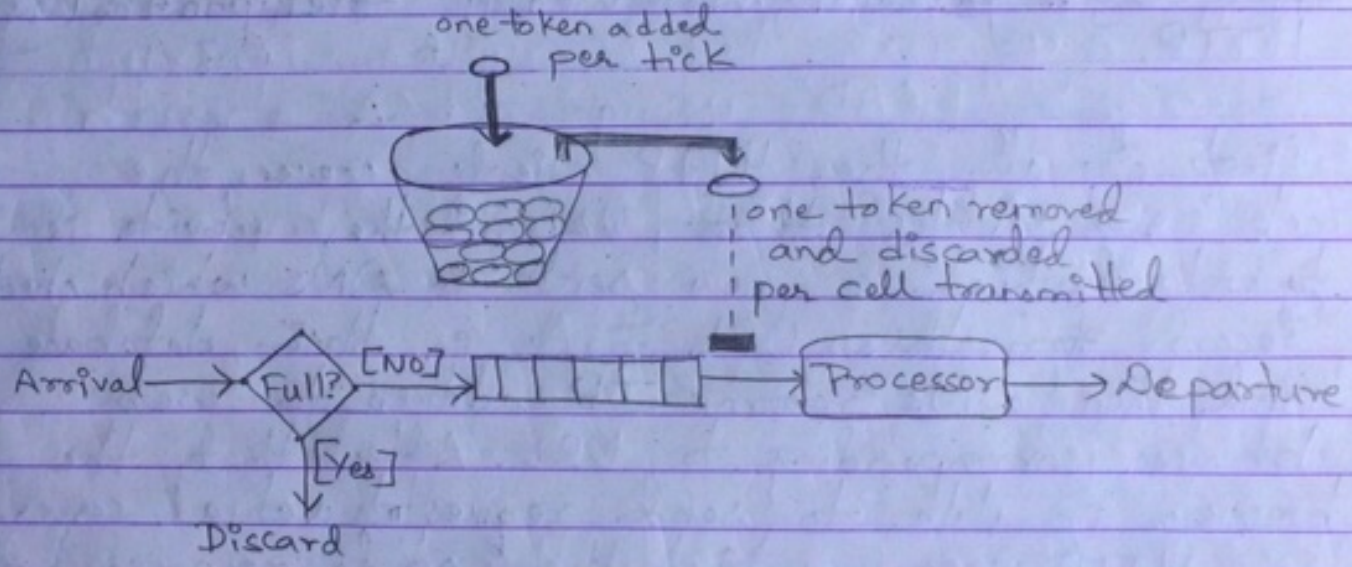

Fig:- Token Bucket

Q. No. 5(b) What is SSL? Explain how a request initiated by a HTTP client is served by a HTTP server.

⇒

Secure Socket Layer (SSL) is a protocol designed to provide security and compression services to data generated from the application layer. Typically, SSL can receive data from any app layer protocol, but usually the protocol is HTTP.

First of all, the HTTP client accesses the web server. After that, URL of the website is entered which is now sent to DNS which checks record for this URL first in their database and then DNS returns IP address to web browser corresponding to URL. After that, the browser is able to send request to actual server. i.e. HTTP server, which then sends response back to client. Then the connection is closed.

6(a) What is network security? How can firewalls enhance network security? Explain how firewalls can protect a system.

⇒ Network Security refers to the process of protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Firewall is a mechanism for preventing the attack on the network of the organization. For this, the system allows safe network traffic to pass while it restricts unsafe traffic.

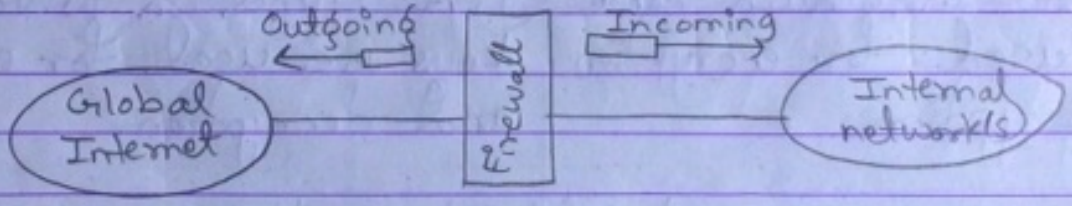

Fig:- Firewall

A firewall can be used as a packet filter. It can forward or block packets based on the information in the network layer and transport layer headers: source and destination IP addresses, source and destination port addresses and type of protocol (TCP or UDP). A packet-filter firewall helps to decide which packets must be discarded (not forwarded).

Also, we can install a proxy computer (sometimes called an appⁿ gate-way), which stands between the customer (user client) computer and the corporation computer. This is used for filtration at application layer. In this way, we can protect a system.

6(b) Compare symmetric key encryption method with asymmetric key encryption. Encrypt the message "READ" using RSA algorithm.

⇒

Symmetric key encryption	Asymmetric key encryption
(i) A cipher in which same key is used for encryption and decryption.	(i) A cipher in which two keys are used for encryption and decryption.
(ii) Here, the message is locked and unlocked with same key.	(ii) Here, the message is locked with public key and unlocked with private key.
(iii) The key is shared in this case.	(iii) The key is not shared in this case.
(iv) For example, DES, AES (Advanced Encryption Standard).	(iv) For example, Elgamal, RSA, DSA (Digital Signature Algorithm).

7(a) Integrated Services Digital Network

⇒

ISDN is a network that provides end-to-end digital connectivity to support a wide range of services including voice and data services. ISDN allows multiple digital channels to operate simultaneously through the same regular phone wiring used for analog lines, but ISDN transmits a digital signal rather than analog. Latency is much lower on an ISDN line than on an analog line. ISDN technology permits the use of digital data on the local loop, providing better access speeds for the remote users. ISDN standards define two main channel types, each with a different transmission rate:-

- The bearer channel or B channel
- Delta channel or D Channel.

7(b) UDP - connectionless

⇒

UDP is the connectionless transport protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without guaranteed delivery. It relies on higher-layer protocols to handle errors and retransmit data. UDP is faster than TCP. It adds only checksum and process-to

process addressing to IP and it is used for DNS and NFS. Also, it is used when socket is opened in datagram mode. It has no handshaking or flow control. It is a fire and forget type protocol. An appⁿ can use a UDP port number and another appⁿ can use the same port number for a TCP session from the same IP address. There is no error control; corrupted data is not retransmitted (even though UDP header has a checksum to detect errors and report these to the appⁿ).

7(c) Virtual Private Networks

⇒

A VPN is a concept that describes how to create a private network over a public network infrastructure while maintaining confidentiality and security. VPNs use cryptographic tunneling protocols to provide sender authentication, message integrity, and confidentiality by protecting against packet sniffing. VPNs can be implemented at layer 2, 3 and 4 of the OSI model. The key to VPN technology is security. VPNs secure data by encapsulating the data, encrypting the data or both encapsulating data and then encrypting it.

Basically, a VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual"

connections routed through the Internet from the company's private network to the remote site or employee.

2019/Fall

1(a) Define converged networks. Discuss the merits and demerits of computer networks with a suitable example.

⇒

~~The network~~ A converged network is one where you connect multiple network media types to each other.

The merits of computer network are:-

(i) It enhances communication and availability of information.
(ii) It allows for more convenient resource sharing.
(iii) It makes file sharing easier.
(iv) It is highly flexible.
(v) It is an inexpensive system.

The demerits of computer networks are:-

(i) It lacks independence.
(ii) It poses security difficulties.
(iii) It lacks robustness.
(iv) It allows for more presence of computer viruses and malware.

1(b) What do you mean by routing device? Explain design issues of layers.

⇒

Routers are internetwork connectivity devices. An internetwork may consists of two or more

physical connected independent network. These networks can be of different type. For example, they can be ethernet and token ring network. Each network is logically separated and is assigned an address.

Solution for 2nd part: Same as 2019|Spring|1(b)

2(a) Explain twisted pair cable on basis of categories, connector used, performance, and application along with its suitable diagram.

⇒

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.

Fig:- Twisted-pair cable

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. There are two types of twisted-pair cable: unshielded twisted-pair (UTP) and shielded twisted-pair (STP).

Categories:-

The Electronic Industries Association (EIA)

has developed standards to classify UTP into seven categories. Categories are determined by cable quality, with 1 as the lowest and 7 as the highest. Each EIA category is suitable for specific uses.

Category	Specification	Data Rate (Mbps)	Use
1	UTP used in telephone	<0.1	Telephone
2	UTP originally used in T-lines	2	T-1 lines
3	Improved CAT2 used in LANs	10	LANs
4	Improved CAT3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension of category 5 that minimizes crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from same manufactures.	200	LANs
7	SSTP(shield of screen twisted-pair).	600	LANs

Categories of unshielded twisted-pair cables

Connector used :-

The most common UTP connector is RJ45 (RJ stands for registered jack). The RJ45 is

a keyed connector, meaning the connector can be inserted in only one way.

Performances:-

One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance. A twisted-pair cable can pass a wide range of frequencies. However, with increasing frequency, the attenuation, measured in decibels per kilometer (dB/km), sharply increases with frequencies above 100 kHz. Also, gauge is a measure of thickness of wire.

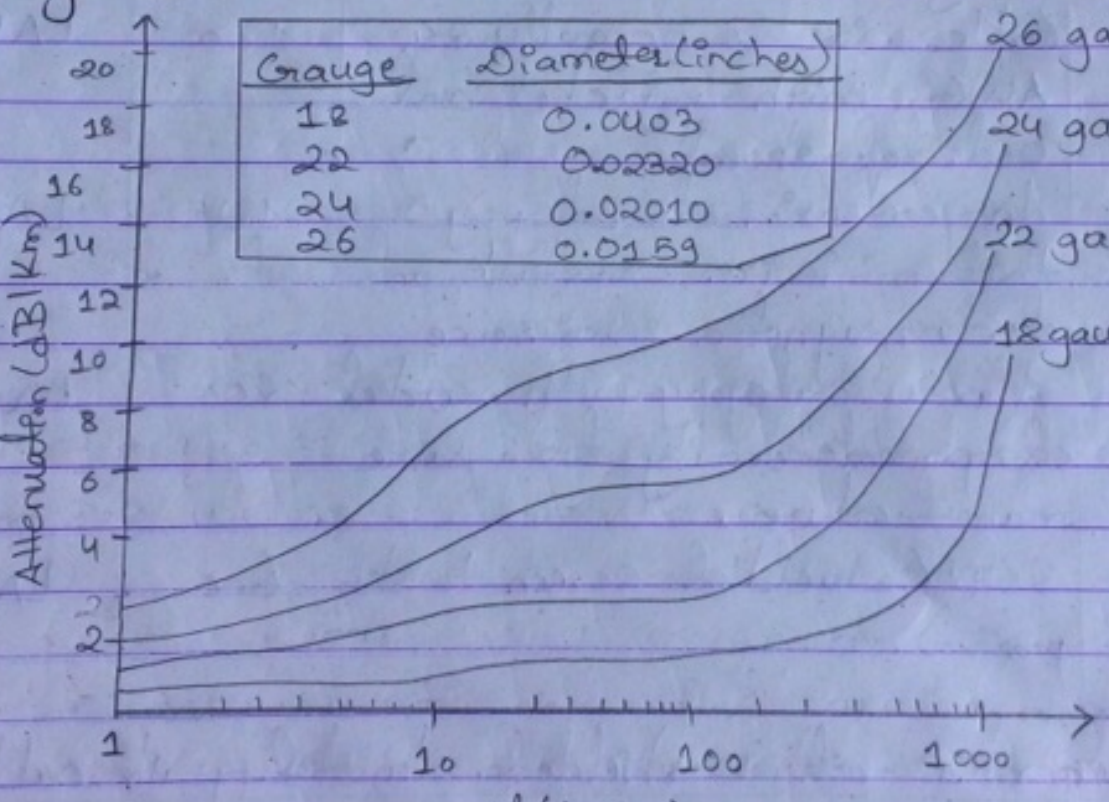

Fig:- UTP Performance

Application :-

Twisted-pair cables are used in telephone lines to provide voice and data channels. The DSL lines used by telephone companies provide high-data-rate connections also use high-bandwidth capability of UTP. Local area networks, such as 10Base-T, also use twisted-pair cables.

2(b) What are the functions of LLC and MAC sub-layer? Discuss different framing approaches used in data link layer.

⇒

LLC sub-layer :-

DSAP	SSAP	Control	Data

Fig:- LLC Frame Format

Logical link Control (LLC) is an interface to upper layer that is responsible for flow and error control. The LLC provides one single data link control protocol for all IEEE LANs. A single LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent. LLC defines a protocol data unit (PDU) that is somewhat similar to that of HDLC.

MAC sublayer :

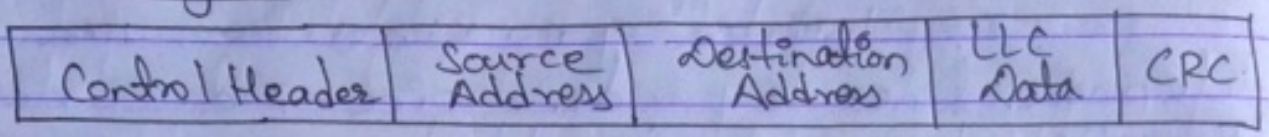

Fig:- General MAC frame format

The lower sublayer that is mostly responsible for multiple-access resolution is called media access control (MAC) layer. It defines specific access method for each LAN. Also, part of framing function is also handled by MAC layer. The MAC sublayer contains a number of distinct modules; each defines the access method and framing format specific to corresponding LAN protocol. It also frames data received from upper layer and passes them to physical layer.

3(a) What is error correction? Show how FEC technique will help to detect and correct the error with suitable example.

⇒

Error correction is the mechanism of knowing the exact number of bits that are corrupted and their location in the message so that they can be corrected.

Forward Error Correction (FEC) is the process in which the receiver tries to guess the message by using redundant bits. This is possible if the

number of errors is small. FEC automatically corrects certain errors at the receiver. Redundancy is achieved through various coding schemes. The sender adds redundant bits through a process that creates a relationship between the redundant bits and the actual data bits. The receiver checks the relationships between the two sets of bits to detect or correct the errors. The ratio of redundant bits to the data bits and the robustness of the process are important factors in any coding scheme.

3(b)

4(a) Differentiate between adaptive and non-adaptive routing. Explain about any intra-AS routing protocol.

⇒

Adaptive routing:-

When a router uses an adaptive routing algorithm to decide the next computer to which to transfer a packet of data, it examines the traffic conditions in order to determine a route which is as near optimal as possible. For example, it tries to pick a route which involves common lines which have light traffic.

Non-adaptive routing:-

When a router uses a non-adaptive routing algorithm, it consults a static table in order to determine to which computer it should send a packet of data. This is an contrast to an adaptive routing

algorithm, which bases its decisions on data which reflects current traffic conditions.

An autonomous system (AS) is a group of networks and routers under the authority of a single administration. Routing inside an autonomous system is referred to as intradomain - AS routing. Each AS can choose one or more intradomain routing protocols to handle routing inside the AS. There are two intradomain routing protocols: distance vector and link state.

Routing Information Protocol (RIP) is an implementation of the distance vector protocol. Open Shortest Path First (OSPF) is an implementation of the link state protocol.

In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in route (next-hop routing).

Link state routing has different philosophy from that of distance vector routing. Here, each node in the domain has the entire topology of the domain - the list of nodes and links, how they are connected including the type, cost (metric), and conditions of the links (up and down) - the node can use Dijkstra's algorithm to build a routing tab

4(b) Pokhara University has 3 sub division located at Pokhara as head office, Kathmandu as Examination office and Biratnagar as Contact office with 125, 60, and 29 host respectively. Now you as network administrator design the network with below details.

(i) All the LANs must implemented router as default Gateway.

(ii) Ensure that network is secure from inside and outside the network

(iii) Calculate Broadcast, Network, usable address along with subnet and wild card mask.

(iv) ISP provide IP address was 10.0.17.0/24

5(a) Differentiate between TCP and UDP with a suitable example.

⇒

Features	UDP	TCP
Acronym for	• User Datagram Protocol	• Transmission Control Protocol
Description	• Simple high speed low functionality "wrappes" that interface app^{n}s to network layer and does little else	• Full-featured protocol that allows app^{n}s to send data reliably without worrying about network layer issues
Protocol conn^n setup	• Connectionless; data is sent without setup	• Connection-oriented; conn^n must be established prior to transmission.
Data interface to app^n	• Message based ~~data~~ is sent in discrete packages by the app^n	• Stream-based; data is sent by app^n with no particular structure.
Reliability and acknowledgement	• Unreliable best-effort delivery without acknowledgements	• Reliable delivery of message, all data is acknowledged.
Retransmissions	• Not performed. App^n must detect lost data and retransmit if needed.	• Delivery of all data is managed, and lost data is retransmitted automatically.
Overhead	• Very low	• Low, but higher than UDP

Transmission Speed	• Very high	• High but not as high as UBDP
Data Quantity suitability	• Small to moderate amounts of data	• Small to very large amounts of data

6(a) Discuss the role of DHCP. Explain the operation of DNS in corporate networks.

⇒

IP address are tough for human to remember and impossible to guess. Domain Name System (DNS) are usually used to translate a hostname or Domain name (Eg:- rec.edu.np) into an IP address (Eg:- 202.3f.9u.1f7). Domain name comprise a hierarchy so that names are unique, yet easy to remember. DNS makes it possible to refer to IP based systems (hosts) by human friendly names (domain names). The benefits of DNS are two folds. First, Domain Name can be logical and easily remembered. Second, should an IP address for a host change, the domain name can still resolve transparently to the users or application. DNS name resolution is critical Internet Service. Many network services require functional name service for correct operation.

7(a) Circuit switching and packet switching

⇒

Circuit switching :-

A dedicated path between the source node and the destination node is setup for the duration of communication session to transfer data. That path is a connected sequence of links between network nodes. On each physical link, a logical channel is dedicated to the connection. Communication via circuit switching involves three phases; circuit establishment, data transfer and circuit disconnect.

Packet switching :-

Messages are divided into subsets of equal length called packets. In packet switching approach, data are transmitted in short packets (few kilobytes). A long message is broken up into a series of packets. Every packet contains some control information in its header, which is required for routing and other purposes.

Main difference between packet switching and circuit switching is that the communication lines are not dedicated to passing messages from the source to destination.

7(b) Email Server protocol: SMTP

⇒

One of the most popular network services, email is supported by TCP/IP protocol SMTP. It provides system for sending message to other computers and provide a mail exchange between users. SMTP support sending of email only. It cannot pull messages from a remote server on demand. SMTP (Simple Mail Transfer Protocol) has a feature to initiate mail queue processing on a remote server so that the requesting system may receive any messages destined for it.

SMTP supports:

- sending a message to one or more recipients.
- sending message that includes texts, voice, video or graphics.
- sending message to users on the network outside the Internet.

2018 Spring

1(a) Define local Area Network. Discuss on any five applications of Computer Network.

⇒

LAN (Local Area Network) refers to a gn local network or a group of interconnected network that are under the same administrative control. In the early days of networking, LANs are defined as small networks that existed in a single physical location. While LANs can be a single network installed in a home or small office, the definition of LAN has evolved to include interconnected local networks consisting of many hundreds of hots, installed in multiple buildings and locations. LANs are designed to operate within a limited geographic area.

The five applications of CN are:-

- Exchange of information between different computers.
- Interconnected small computers in place of large computers.
- Communication tools
- Some applications and technologies are examples of distributed system. (Railway reservation system, distributed database, etc).

1(b) Why TCP/IP is called implementation model? Explain in brief about OSI model.

⇒

TCP/IP is called implementation model because it is the actual model used in todays' data communications. Also, the TCP/IP protocol suite became the dominant commercial architecture because it was used and tested extensively in the internet. TCP is a connection-oriented protocol that provide reliable full-duplex data transmission. TCP is a part of TCP/IP protocol stack. In a connection-oriented environment, a connection is established betwn both ends before the transfer of information can begin.

OSI model is a theoretical framework. Open Systems Interconnection (OSI) model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which ~~identifies~~ defines a part of the process of moving information across a network. An understanding of the fundamentals of the OSI model provides a solid basis for exploring data communications. In developing the model, the designers distilled the process of transmitting data to its most fundamental elements. They identified which networking functions had related uses ~~and~~ and collected those functions into discrete groups that became the layers. Each layer defines a

family of functions distinct from those of other layers. The designers created an architecture that is both comprehensive and flexible. The OSI model allows complete interoperability between otherwise incompatible systems.

2(b) What are the main functions of Data link layer? Discuss any two flow control mechanisms.

⇒ The main functions of data link layer are:-

- Framing:- The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- Physical addressing :- The data link layer adds a header to the frame that is distributed to different systems on the network. Also, receiver address is the address of the device for a system outside the sender's network.
- Flow control :- If the rate of data absorption by the receiver is less than the rate of data production in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- Error control :- The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames, recognize duplicate frames.
- Access control :- When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.

The two flow control mechanisms are:-

- **Stop & wait Protocol**

→ In this method, the sender sends a single frame to receiver and waits for an acknowledgement.

→ The next frame is sent by sender only when acknowledgement of previous frame is received.

→ This process of sending and waiting continues as long as the sender has data to send.

→ To end up the transmission sender transmits end of transmission (EOT) frame.

→ Its advantage is its accuracy and no chance of frame being lost.

→ Its disadvantage is that it is inefficient as it makes the transmission process slow.

- **Sliding Window Protocol**

→ In this method, multiple frames are sent by sender at a time before needing an acknowledgment.

→ Multiple frames sent by source are acknowledged by receiver using a single ACK frame.

→ Sliding window refers to an imaginary boxes that hold the frames on both sender and receiver side.

3(a) Discuss on CRC error detection and Hamming code.

∴

Cyclic Redundancy Check (CRC) is the most powerful and easy to implement technique. CRC is based on binary division. In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number. At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted. A remainder indicates that the data unit has been damaged in transit and therefore must be rejected. CRC is a very effective error detection technique.

The most common types of error-correcting codes used in RAM are based on the codes devised by R.W. Hamming. In the Hamming code, k parity bits are added to an n-bit data word, forming a new word of n+k bits. The bit positions are numbered in sequence from 1 to n+k. Those positions numbered with powers of two are reserved for parity bits. The remaining bits are data bits. The code can be used with words of any length.

3(b) What are the special IP addresses used in Classful addressing? A multi-national company is granted a site ip 172.16.0.15. Design an IP table with its subnets.

⇒

4(b) What do you understand by port addressing? Explain TCP header format.

⇒

In TCP/IP architecture, the label assigned to a process is called a port address. It is 16 bits in length. The physical addresses change from hop to hop, but the logical and port addresses usually remain the same. The port address identifies a process on a host. In TCP, the combination of IP and port addresses defines a connection.

TCP uses only a single type of protocol data unit, called a TCP segment.

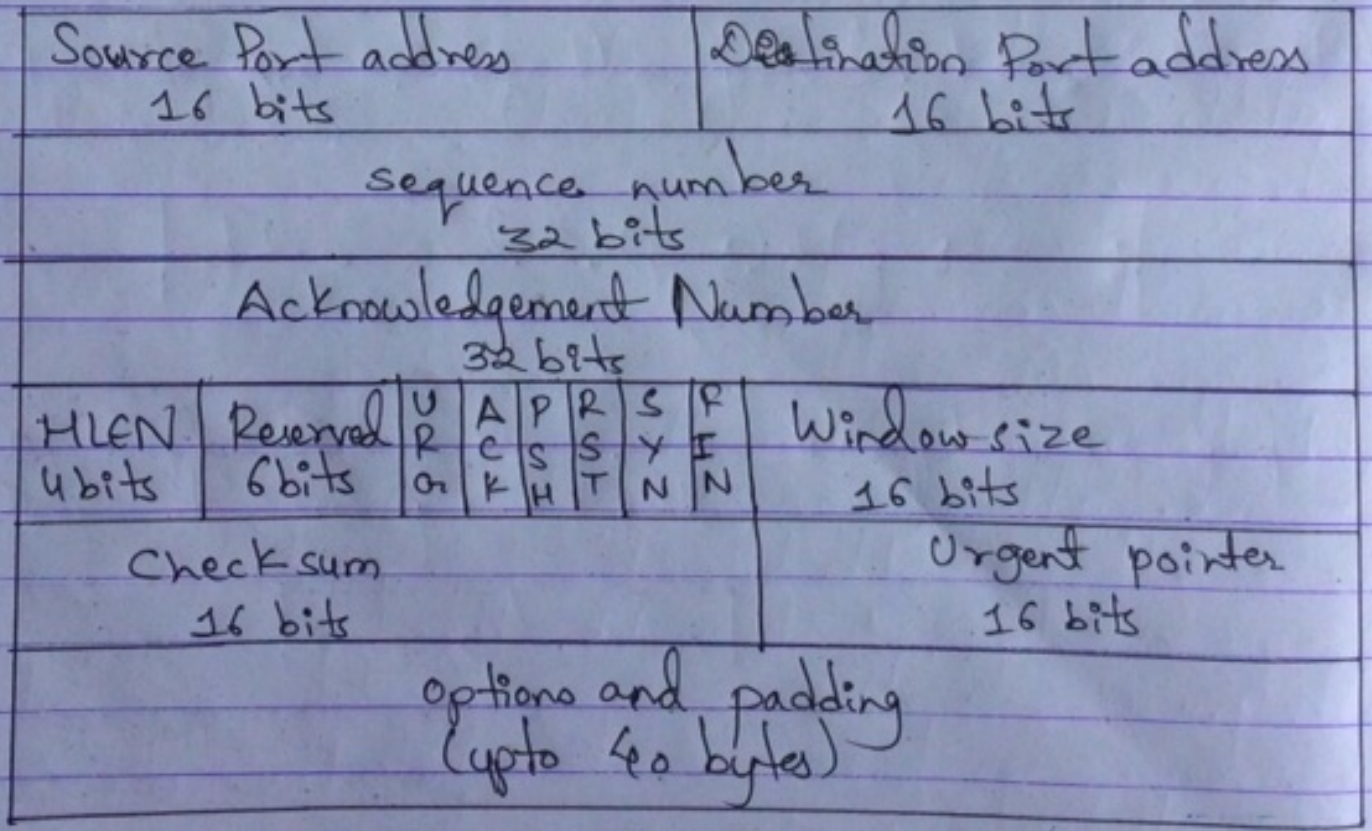

Fig:- TCP Header Format

The following are the fields in the TCP header segment:-

- Source port address
- Destination port address
- Sequence Number
- Acknowledgment number
- Header length (HLEN)
- Reserved
- Window size
- checksum
- Urgent poiter

6(a) What is cryptography? Write and explain the RSA algorithm.

⇒

Cryptography is the science of using mathematics to encrypt and decrypt data. It enables to store sensitive information or transmit it across in secured networks so that it cannot be read by anyone except the intended recipient.

RSA is asymmetric cryptography algorithm which means that it works on two different keys: public key and private key. RSA algorithm uses the following procedure to generate public and private key:-

(i) Select two large prime numbers p & q.
(ii) Multiply these numbers to find $n = p * q$,

where 'n' is called the modulus for encryption and decryption.

(iii) Choose a number 'e' less than 'n' such that 'n' is relatively prime to '(p-1)*(q-1)'. It means that 'e' and '(p-1)*(q-1)' have no common factor except 1.

(iv) If $n = p * q$ then, the public key is 'e'. A plain text message 'm' is encrypted using public key 'e'. To find the ciphertext from the plain text, use the formula

$$c = m^e \bmod n$$

(v) To determine the private key, 'd', following formula is used.

$$d * e \bmod \{(p-1)*(q-1)\} = 1$$

(vi) A ciphertext message is decrypted using private key 'd' using formula,

$$m = c^d \bmod n$$

7(b) Frame Relay

⇒

Frame Relay is a high performance WAN protocol that operates at the physical and Data link layers of the OSI reference model. X.25 has several disadvantages so Frame Relay was invented. It has following features:-

- It operates at a higher speed (1.544 Mbps and recently 44.376 Mbps). So, it can easily be used instead of a mesh of T-1 or T-3 lines.
- It operates in just the physical and data link layers. So, it can be easily used as a backbone network to provide services to protocols that already have a network layer protocol, such as the Internet.
- It allows bursty data.
- It allows a frame size of 9000 bytes, which can accomodate all LAN frame sizes.
- It is less expensive than other traditional WANs.
- It has error detection at data link layer only. There is no flow control or error control.

7(c) Proxy Server

⇒

Proxy Server is a computer that can act on the behalf of other computers to request content from the Internet or an intranet. Proxy Server is placed between a user's machine and the Internet. It can act as a firewall to provide protection and as a cache area to

speed up web page display. It is a firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it. ~~A soft~~ It is a software agent that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination. Proxy servers have two main purposes:-

- Improve performance
- Filter Requests.

2018/Fall

1(b) Discuss seven layer of OSI protocol stack. Also compare TCP/IP and OSI with a suitable example.

⇒

The layers of OSI protocol stack are:-

(i) Physical layer:-

It is the bottom layer of OSI reference model. It has four important characteristics-

- Mechanical:- Relates to physical properties of interface to a transmission medium.
- Electrical :- Relates to representation of bits and the data transmission rate of bits.
- Functional :- Specifies the functions performed by individual circuits of physical interface between a system and a transmission medium.
- Procedural :- Specifies the sequence of events by which bit streams are exchanged across the physical medium.

ii) Data link layer:-

The physical layer provides only a raw bit-stream service, the data link layer attempts to make the physical link reliable while providing the means to activate, maintain and deactivate the link. It consists of two sublayers:-

- LLC (logical link Control) layer
- MAC (Media Access Control) Layer

(iii) Network layer :-

The network layer is responsible for functions such as the following :-

- Logical addressing and routing of packets over the network.
- Establishing and releasing connections and paths between two nodes on a network.
- Transferring data, generating and confirming receipts and resetting connections.

The network layer also supplies connectionless and connection-oriented services to the transport layer above it.

(iv) Transport layer :-

This layer is responsible for providing reliable transport services to the upper-layer protocols. These services include the following :-

- Flow control to ensure that the transmitting device does not send more data than the receiving device can handle.
- Error handling and acknowledgments to ensure that data is retransmitted when required.
- Multiplexing for combining data from several sources for transmission over one data path.
- Virtual circuits for establishing sessions between communicating stations.

(v) Session layer :-

This layer enables sessions between computers on a network to be established and terminated. The session layer does not concern itself with issues such as the reliability and efficiency of data transfer between stations because these functions are provided by first four layers of OSI model.

(vi) Presentation layer :-

This layer is concerned with the syntax and semantics of the information exchanged between two systems. Specific responsibilities of this layer are :-

- Translation
- Encryption
- Compression

(vii) Application layer :-

In this layer, network-aware, user-controlled software is implemented. For example, email, file transfer utilities and terminal access. This layer represents the window between the user and the network. Examples of protocols that run at the application layer include File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), telnet and similar protocols that can be implemented as utilities the user can interface with.

3(b) Design an algorithm for CSMA/CD with a suitable example.

⇒

Carrier Sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

5(a) Why congestion occurs in the network? Explain the types of closed loop congestion control mechanism.

⇒

Congestion in a network may occur if the load on network (the number of packets sent to the network) is greater than the capacity of network (the number of packets a network can handle).

Closed loop congestion control mechanisms try to alleviate congestion after it happens. The mechanisms are:

(i) Back-pressure :-

The technique of backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. This may cause upstream node(s) to be congested, and they, in turn, reject data from their upstream node(s). And so on. Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source.

(ii) Choke Packet :-

A choke packet is a packet sent by a node to the source to inform it of congestion. Here, the warning is from the router, which has encountered congestion, to the source station directly. The intermediate nodes through which the packet has traveled are not warned. For example, ICMP.

(iii) Implicit Signaling:-

In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network from other symptoms. For example, when a source sends several packets and there is no acknowledgement for a while, one assumption is that the network is congested.

(iv) Explicit Signaling:-

The node that experiences congestion can explicitly send a signal to the source or destination. In this method, the signal is included in the packets that carry data. We can see this in Frame Relay congestion control which can occur in either the forward or backward direction.

5(b) Define DHCP. Explain the iterative and recursive DNS query for name resolution with suitable figure.

⇒

Iterative resolution:-

If the client does not ask for a recursive answer, the mapping can be done iteratively. If the server is an authority for the name, it sends the answer. If it is not, it returns (to the client) the IP address of the server that it thinks can resolve the query.

The client is responsible for repeating the query to this second server. If the newly addressed server can resolve the problem, it answers the query with IP address; otherwise, it returns the IP address of a new server to the client. Now the client must repeat the query to the third server. This process is called iterative resolution because the client repeats the same query to multiple servers.

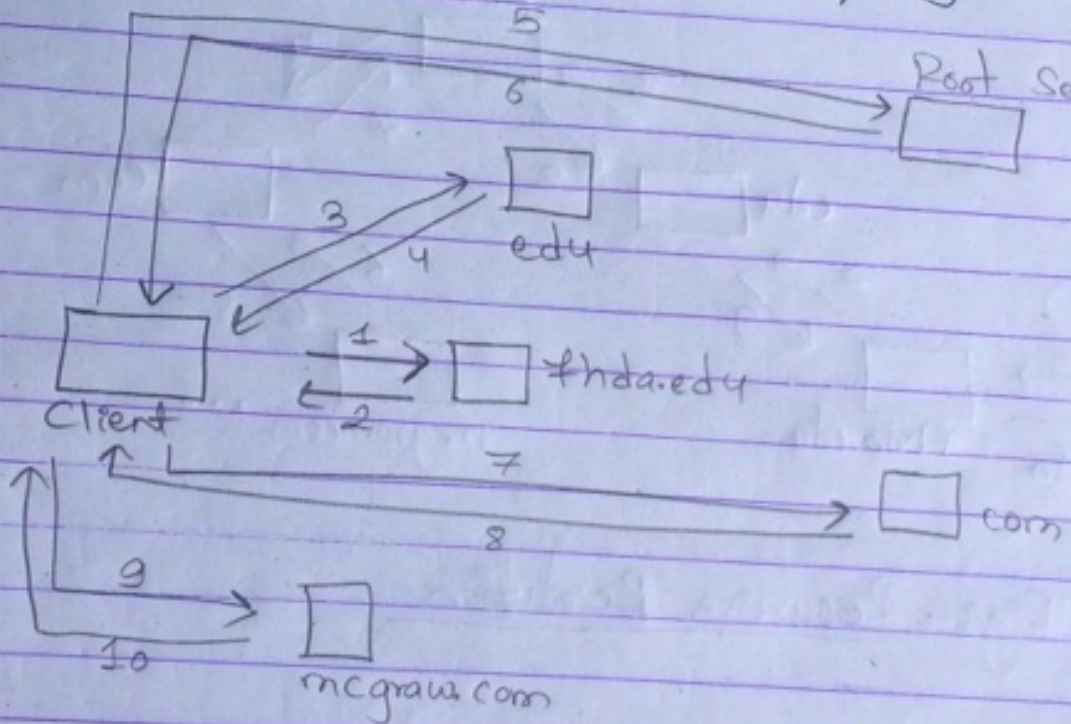

Fig:- Iterative resolution (the client queries four servers before it gets an answer from mcgraw.com server)

Recursive resolution :-

The client (Resolver) can ask for a recursive answer from a name server. This means that the resolver expects the server to supply the final answer. If the server is the authority for domain name

it checks its database and responds. If the server is not the authority, it sends the request to another server (the parent usually) and waits for response. If the parent is authority, it responds, otherwise, it sends the query to yet another server. When the query is finally resolved, the response travels back until it finally reaches the requesting client. This is called recursive resolution.

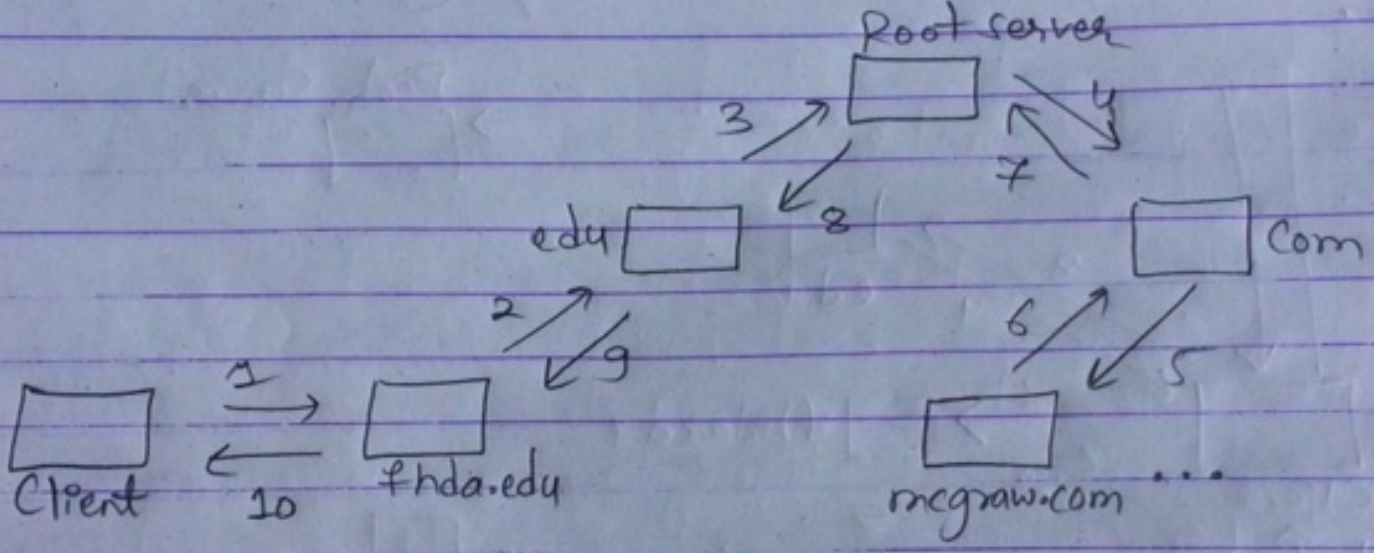

Fig:- Recursive Resolution

6(a) What is SNMP? Explain the advantages of using network management tools.

≠

Simple Network Management Protocol (SNMP) is an internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers and many more. It is used mostly in network management system to monitor network attached devices for conditions that warrant administrative attention. SNMP is a framework for managing devices in an internet using the TCP/IP protocol. It provides a set of fundamental operations for monitoring and maintaining an internet.

The advantages of using network management tools are:-

- It provides a set of fundamental operations for monitoring and maintaining an internet.
- It monitors and controls the network to ensure that it is as efficient as possible.
- It prevents users from monopolizing limited network resources.
- It prevents users from using the system inefficiently.
- It helps network managers to do short and long-term planning based on the demand for network use.