Name : Shourov Kabiraj

ID : IT-17045

1.	a)	What is IP-V4? Describe each field of IP-V4 with diagram.	7
	b)	Mention some applications UDP. Explain UDP header with a proper diagram.	7
2.	a)	What is sub-netting? Write down the purpose of sub-netting.	4
	b)	What is NAT? Mention the working process of NAT.	5
	c)	Write the main protocols used in the application layer.	5
3.	a)	Explain multiplexing and de-multiplexing in transport layer.	7
	b)	Describe the header file of TCP segment format.	7
4.	a)	Write the difference between Static routing and Dynamic routing.	4
	b)	What is Socket address? briefly explain the End-to-End Communication.	5
	c)	Briefly explain the Timer management of TCP model.	5
5.	a)	What is Crash Recovery? Write about Error Control &and Flow Control.	4
	b)	What is congestion control? briefly explain the Bandwidth Management.	4
	c)	Why TCP is called connection-oriented reliable protocol? Describe the header fields of TCP segment format.	6
6.	a)	Briefly explain unicast routing protocol.	5
	b)	What is Tunneling Describe packet fragmentation of network layer.	5
	c)	Describe the working of address resolution protocol.	4
7.	a)	Describe Multicast Routing, Broadcast Routing and Anycast Routing.	7
	b)	Write the functions of Transport layer.	7
8.	a)	Describe internet control message protocol briefly.	5
	b)	Explain the Remote procedure call.	4
	c)	What is inter network briefly explain about connection oriented and connectionless services	5

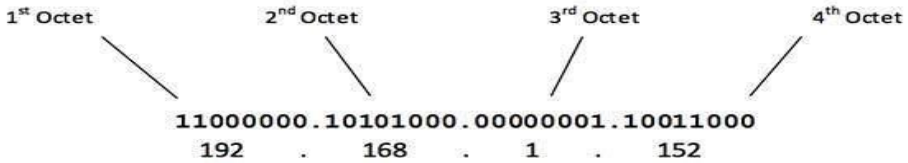
1. a) What is IP-V4? Describe each field of IP-V4 with diagram. 7

Ans:

IP-V4: Internet Protocol version 4 is the fourth version of the Internet Protocol. It is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks. IPv4 was the first version deployed for production in the ARPANET in 1983.

IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address −



The number of networks and the number of hosts per class can be derived by this formula −

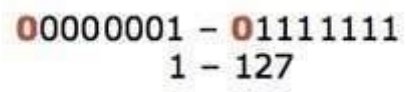
Number of networks = 2^network_bits

Number of Hosts/Network = 2^host_bits − 2

When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127,



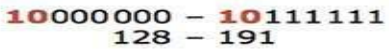
Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).

Class A IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10



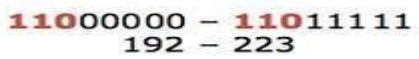
Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.

Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is –



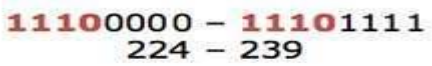
Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class C gives 2097152 (2^{21}) Network addresses and 254 (2^8-2) Host addresses.

Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of –



Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

b) Mention some applications UDP. Explain UDP header with a proper diagram. 7

Ans:

Following applications use UDP-

- Applications which require one response for one request use UDP. Example- DNS.
- Routing Protocols like RIP and OSPF use UDP because they have very small amount of data to be transmitted.
- Trivial File Transfer Protocol (TFTP) uses UDP to send very small sized files.
- Broadcasting and multicasting applications use UDP.
- Streaming applications like multimedia, video conferencing etc use UDP since they require speed over reliability.
- Real time applications like chatting and online games use UDP.
- Management protocols like SNMP (Simple Network Management Protocol) use UDP.

The following diagram represents the UDP Header Format-

UDP Header

1. Source Port-

1. Source Port is a 16 bit field.
2. It identifies the port of the sending application.

2. Destination Port-

1. Destination Port is a 16 bit field.
2. It identifies the port of the receiving application.

3. Length-

1. Length is a 16 bit field.
2. It identifies the combined length of UDP Header and Encapsulated data.

Length = Length of UDP Header + Length of encapsulated data

4. Checksum-

1. Checksum is a 16 bit field used for error control.
2. It is calculated on UDP Header, encapsulated data and IP pseudo header.
3. Checksum calculation is not mandatory in UDP.

2. a) What is sub-netting? Write down the purpose of sub-netting. 4

Ans:

Subnetting :Sub-netting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets). An IP address includes a network segment and a host segment.

five subnetting benefits you should consider:

1.Improve network performance and speed :A single broadcast packet sends out information that reaches every device connected to that network because each device has an entry point into the network. A large number of entry points, however, can negatively impact internetwork switching device performance, as well as your network's overall performance.

2. Reduce network congestion :Subnetting ensures that traffic destined for a device within a subnet stays in that subnet, which reduces congestion. Through strategic placement of subnets, you can help reduce your network's load and more efficiently route traffic.

3. Boost network security :What if a device in my network is comprised By splitting network into subnets, control the flow of traffic using ACLs, QoS, or route-maps, enabling you to identify threats, close points of entry, and target your responses more easily.

4. Control network growth :When you're planning and designing a network, size is something that needs to be taken into consideration. One of the key benefits of subnetting is that it enables you to control the growth of your network.

b) What is NAT? Mention the working process of NAT. 5

Ans:

NAT :Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

Working process of NAT :

- It is the private IP address of the private network.
- It is the registered public IP address allocated to the host of the private network when it is initiating communication with the outside network.
- It is the registered IP address allocated to the host on the Internet.
- It is the local IP address allocated to the host at the public domain.

- The address used by the internal network devices to communicate with each other internally is known as inside local address.
- The address which is used by devices on the internal network to communicate with the external network devices is known as an outside local address.
- The address used by the outside network devices to communicate with the devices on the private network is the inside global address.
- The address used by external devices to communicate with one another is outside global address.
- Whenever any organization built a networking system, the internet service provider will assign the pool of IP addresses to them. The assigned range of addresses includes registered and unique IP addresses which are known as inside global addresses.

c) Write the main protocols used in the application layer. 5

Ans:

Following are the main protocols used in the application layer:

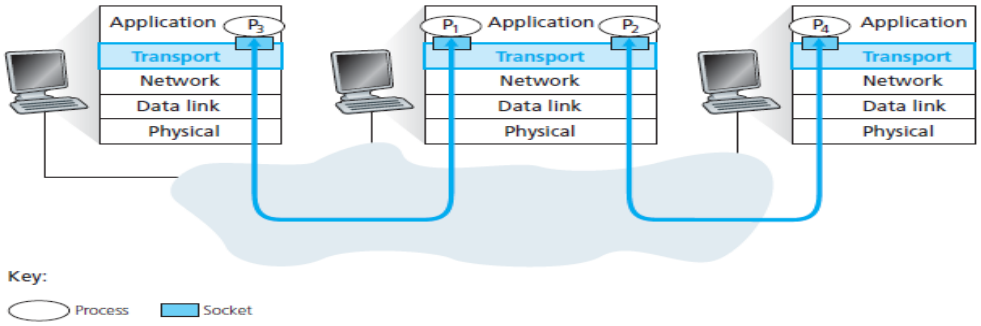
- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

3. a) Explain multiplexing and de-multiplexing in transport layer. 7

Ans:

Multiplexing and demultiplexing in transport layer means extending the host-to-host delivery service provided by the network layer to a process-to-process delivery service for applications running on the hosts. A multiplexing-demultiplexing service is needed for all computer networks. We know that a process can have one or more sockets, doors through which data passes from the network to the process and vice versa.

Thus as shown in the figure below, the transport layer in the receiving host does not actually deliver directly to a process, but instead to an intermediary socket. Because at any given time there can be more than one socket in the receiving host, each socket has a unique identifier. The format of the identifier depends on whether the socket is a UDP or a TCP socket.



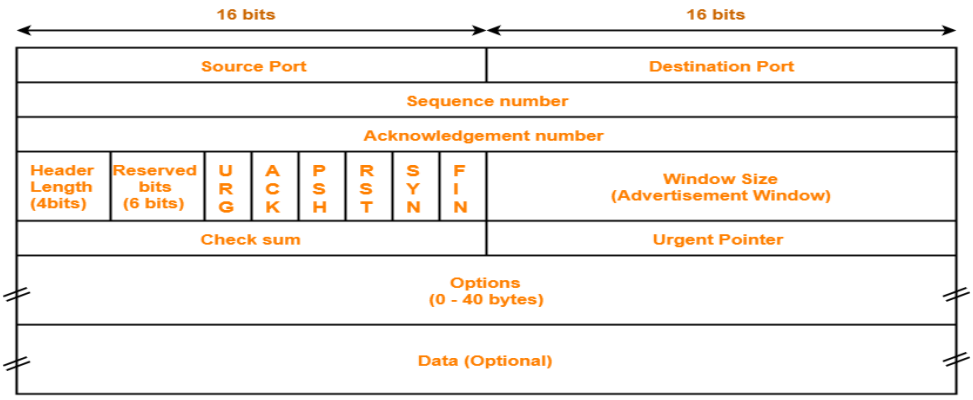
Now let's consider how a receiving host directs an incoming transport-layer segment to the appropriate socket. Each transport layer segment has a set of fields in the segment for this purpose. At the receiving end, the transport layer examines these fields to identify the receiving socket and then directs the segment to that socket. This job of delivering the data in a transport-layer segment to the correct socket is called demultiplexing . The job of gathering data chunks at the source host from different sockets, encapsulating each data chunk with header information to create segments, and passing the segments to the network layer is called multiplexing .

Note that the transport layer in the middle host (in the above figure) must demultiplex segments arriving from the network layer below to either process P_1 or P_2 above; this is done by directing the arriving segment's data to the corresponding process's socket. The transport layer in the middle host must also gather outgoing data from these sockets, form transport layer segments, and pass these segments down the network layer. Although we have introduced multiplexing and demultiplexing in the context of internet transport protocols, it's important to realize that they are concerns whenever a single protocol at one layer (at the transport layer or elsewhere) is used by multiple protocols at the next higher layer.
To illustrate the demultiplexing job, recall the household analogy in the previous session. Each of the kids is identified by his or her name. When Bill receives a batch of mail from the mail carrier, he performs a demultiplexing operation by observing to whom the letters are addressed and then hand delivering the mail to his brothers and sisters. Ann performs a multiplexing operation when she collects letters from her brothers and sisters and gives the collected mail to the mail person.

b) Describe the header file of TCP segment format. 7

Ans:

The following diagram represents the TCP header format-



TCP Header

Let us discuss each field of TCP header one by one.

1. Source Port-

- Source Port is a 16 bit field.
- It identifies the port of the sending application.

2. Destination Port-

- Destination Port is a 16 bit field.
- It identifies the port of the receiving application.

3. Sequence Number-

- Sequence number is a 32 bit field.
- TCP assigns a unique sequence number to each byte of data contained in the TCP segment.
- This field contains the sequence number of the first data byte.

4. Acknowledgement Number-

- Acknowledgment number is a 32 bit field.
- It contains sequence number of the data byte that receiver expects to receive next from the sender.
- It is always sequence number of the last received data byte incremented by 1.

5. Header Length-

- Header length is a 4 bit field.
- It contains the length of TCP header.
- It helps in knowing from where the actual data begins.

Examples:

- If header length field contains decimal value 5 (represented as 0101), then-

  Header length = 5 x 4 = 20 bytes

- If header length field contains decimal value 10 (represented as 1010), then-

  Header length = 10 x 4 = 40 bytes

- If header length field contains decimal value 15 (represented as 1111), then-

  Header length = 15 x 4 = 60 bytes

4. a) Write the difference between Static routing and Dynamic routing. 5

Ans:

Static routing	Dynamic routing
1. In static routing, user defined routes are used in routing table.	1. In dynamic routing, routes are updated as per the changes in network.
2. No complex algorithm used to figure out shortest path.	2. Dynamic routing employs complex algorithms to find the shortest routes.
3. Static routing provides higher security.	3. Dynamic routing is less secure.
4. Static routing is used in smaller networks	4. Dynamic routing is implemented in large networks
5. Static routing does not require any additional resources.	5. Dynamic routing requires additional resources like memory, bandwidth etc.
6. Static routing may not follow any specific protocol.	6. Dynamic routing follows protocols like BGP, RIP and EIGRP.
7. Static routing is a manual process.	7. Dynamic routing is an automatic process.

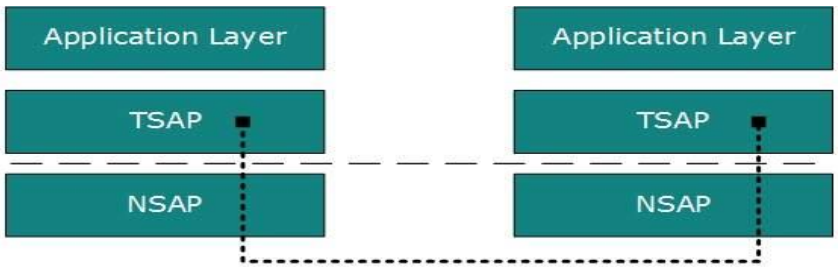
b) 4

What is Socket address? briefly explain the End-to-End Communication.

Ans**:**

Socket address : In the standard Internet protocols TCP and UDP, a socket address is the combination of an IP address and a port number, much like one end of a telephone connection is the combination of a phone number and a particular extension.

A process on one host identifies its peer host on remote network by means of TSAPs, also known as Port numbers. TSAPs are very well defined and a process which is trying to communicate with its peer knows this in advance.



For example, when a DHCP client wants to communicate with remote DHCP server, it always requests on port number 67. When a DNS client wants to communicate with remote DNS server, it always requests on port number 53 (UDP).

The two main Transport layer protocols are:

- **Transmission Control Protocol**

  It provides reliable communication between two hosts.

- **User Datagram Protocol**

  It provides unreliable communication between two hosts.

c) Briefly explain the Timer management of TCP model. 5

Ans:

Timer Management

TCP uses different types of timer to control and management various tasks:

Keep-alive timer:

- This timer is used to check the integrity and validity of a connection.
- When keep-alive time expires, the host sends a probe to check if the connection still exists.

Retransmission timer:

- This timer maintains stateful session of data sent.
- If the acknowledgement of sent data does not receive within the Retransmission time, the data segment is sent again.

Persist timer:

- TCP session can be paused by either host by sending Window Size 0.
- To resume the session a host needs to send Window Size with some larger value.
- If this segment never reaches the other end, both ends may wait for each other for infinite time.
- When the Persist timer expires, the host re-sends its window size to let the other end know.
- Persist Timer helps avoid deadlocks in communication.

Timed-Wait:

- After releasing a connection, either of the hosts waits for a Timed-Wait time to terminate the connection completely.
- This is in order to make sure that the other end has received the acknowledgement of its connection termination request.
- Timed-out can be a maximum of 240 seconds.

5. a) What is Crash Recovery? Write about Error Control &and Flow Control. 4

Ans**:**

TCP is very reliable protocol. It provides sequence number to each of byte sent in segment. It provides the feedback mechanism i.e. when a host receives a packet, it is bound to ACK that packet having the next sequence number expected (if it is not the last segment).

When a TCP Server crashes mid-way communication and re-starts its process it sends TPDU broadcast to all its hosts. The hosts can then send the last data segment which was never unacknowledged and carry onwards.

TCP uses port numbers to know what application process it needs to handover the data segment. Along with that, it uses sequence numbers to synchronize itself with the remote host. All data segments are sent and received with sequence numbers. The Sender knows which last data segment was received by the Receiver when it gets ACK. The Receiver knows about the last segment sent by the Sender by referring to the sequence number of recently received packet.

If the sequence number of a segment recently received does not match with the sequence number the receiver was expecting, then it is discarded and NACK is sent back. If two segments arrive with the same sequence number, the TCP timestamp value is compared to make a decision.

b) What is congestion control? briefly explain the Bandwidth Management. 4

Ans**:**

Congestion Control: When large amount of data is fed to system which is not capable of handling it, congestion occurs. TCP controls congestion by means of Window mechanism. TCP sets a window size telling the other end how much data segment to send. TCP may use three algorithms for congestion control:

- Additive increase, Multiplicative Decrease
- Slow Start
- Timeout React

TCP uses the concept of window size to accommodate the need of Bandwidth management. Window size tells the sender at the remote end, the number of data byte segments the receiver at this end can receive. TCP uses slow start phase by using window size 1 and increases the window size exponentially after each successful communication.

For example, the client uses windows size 2 and sends 2 bytes of data. When the acknowledgement of this segment received the windows size is doubled to 4 and next sent the segment sent will be 4 data bytes long. When the acknowledgement of 4-byte data segment is received, the client sets windows size to 8 and so on.

If an acknowledgement is missed, i.e. data lost in transit network or it received NACK, then the window size is reduced to half and slow start phase starts again

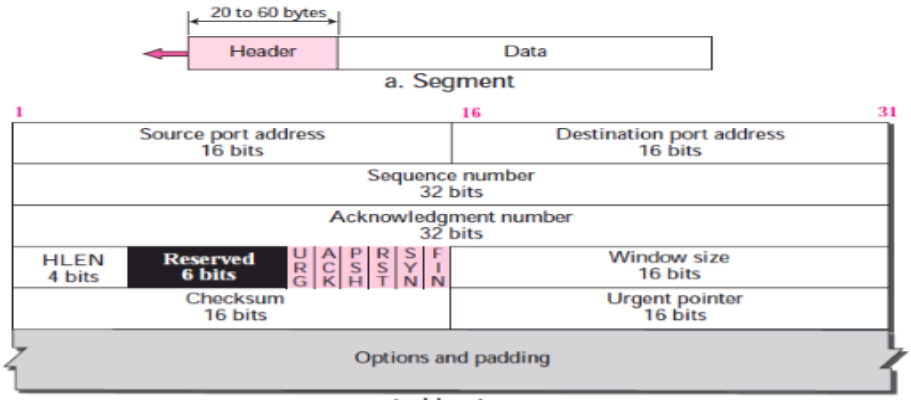
c) Why TCP is called connection-oriented reliable protocol? Describe the header fields of TCP segment format. 6

Ans:

Transmission Control Protocol is a connection-oriented protocol. For connection-oriented communications, each end point must be able to transmit so that it can communicate. Because they can keep track of a conversation, connection-oriented protocols are sometimes described as stateful. Transmission Control Protocol Applications that require the transport protocol to provide reliable data delivery use TCP because it verifies that data is delivered across the network accurately and in the proper sequence. TCP is a reliable, connection-oriented, byte-stream protocol.

The segment consists of a header of20 to 60 bytes, followed by data from the application program.

The header is 20 bytes.



i. Source port address: This is a 16-bit field that defines the port number of the application program in the host that is sending the segment. This serves the same purpose as the source port address in the UDP header.

ii. Destination port address: This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment. This serves the same purpose as the destination port address in the UDP header.

iii. Sequence number: This 32-bit field defines the number assigned to the first byte of data contained in this segment. TCP is a stream transport protocol. To ensure connectivity, each byte to be transmitted is numbered. The sequence number tells the destination which byte in this sequence is the first byte in the segment. During connection establishment each party uses a random number generator to create an initial sequence number (ISN), which is usually different in each direction.

6. a) Briefly explain unicast routing protocol. 5

Ans:

Unicast – Unicast means the transmission from a single sender to a single receiver. It is a point to point communication between sender and receiver. There are various unicast protocols such as TCP, HTTP, etc.

- TCP is the most commonly used unicast protocol. It is a connection oriented protocol that relay on acknowledgement from the receiver side.
- HTTP stands for Hyper Text Transfer Protocol. It is an object oriented protocol for communication.

There are three major protocols for unicast routing:

1. Distance Vector Routing
2. Link State Routing
3. Path-Vector Routing

Link State Routing

Link state routing is the second family of routing protocols. While distance vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using a shortest path computation.

Features of link state routing protocols –

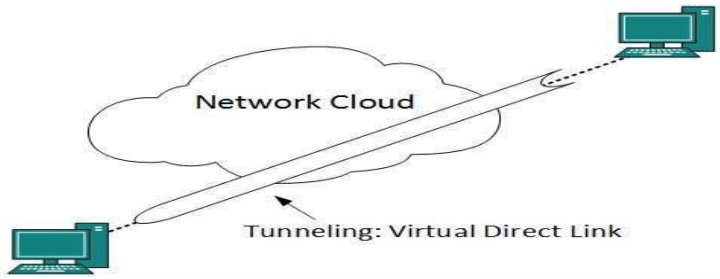
- **Link state packet –** A small packet that contains routing information.
- **Link state database –** A collection information gathered from link state packet.
- **Shortest path first algorithm (Dijkstra algorithm) –** A calculation performed on the database results into shortest path

Routing table – A list of known paths and interfaces

b) What is Tunneling Describe packet fragmentation of network layer. 5

Ans:

Tunneling is a mechanism by which two or more same networks communicate with each other, by passing intermediate networking complexities. Tunneling is configured at both ends.



When the data enters from one end of Tunnel, it is tagged. This tagged data is then routed inside the intermediate or transit network to reach the other end of Tunnel. When data exists the tunnel its tag is removed and delivered to the other part of the network. Both ends seem as if they are directly connected and tagging makes data travel through transit network without any modifications.

Packet fragmentation: Most Ethernet segments have their maximum transmission unit (MTU) fixed to 1500 bytes. A data packet can have more or less packet length depending upon the application. Devices in the transit path also have their hardware and software capabilities which tell what amount of data that device can handle and what size of packet it can process. If the data packet size is less than or equal to the size of packet the transit network can handle, it is processed neutrally. If the packet is larger, it is broken into smaller pieces and then forwarded. This is called packet fragmentation. Each fragment contains the same destination and source address and routed through transit path easily. At the receiving end it is assembled again. If a packet with DF (don't fragment) bit set to 1 comes to a router which can not handle the packet because of its length, the packet is dropped. When a packet is received by a router has its MF (more fragments) bit set to 1, the router then knows that it is a fragmented packet and parts of the original packet is on the way. If packet is fragmented too small, the overhead is increases. If the packet is fragmented too large, intermediate router may not be able to process it and it might get dropped.

c) Describe the working of address resolution protocol. 4

Ans :

The working of address resolution protocol are given below:

1. At the network layer, when the source wants to communicate with the destination. Firstly, the source needs to find out the MAC address (Physical Address) of the destination. For this, the source will check the ARP cache and ARP table for the MAC address of the destination. If the MAC address of the destination is present in the ARP cache or ARP table, then the source uses that MAC address for the communication.

2. If the MAC address of the destination is not in the ARP cache or ARP table, then the Source generates an ARP Request message. The ARP Request message consists of the MAC address and the IP address of the source. It also contains the IP address and MAC address of the destination. The MAC address of the destination left null because the user has requested this.
3. The ARP Request message will be broadcasted to the local network by the source computer. All the devices in the LAN network receive the broadcast message. Now, each device compares its own IP address with the IP address of the destination. If the IP address of the device match with the IP address of the destination, then that device will send an ARP to reply message. If the IP address of the device does not match the IP address of the destination, then the device will automatically drop the packet.

7. a) Describe Multicast Routing, Broadcast Routing and Anycast Routing. 7

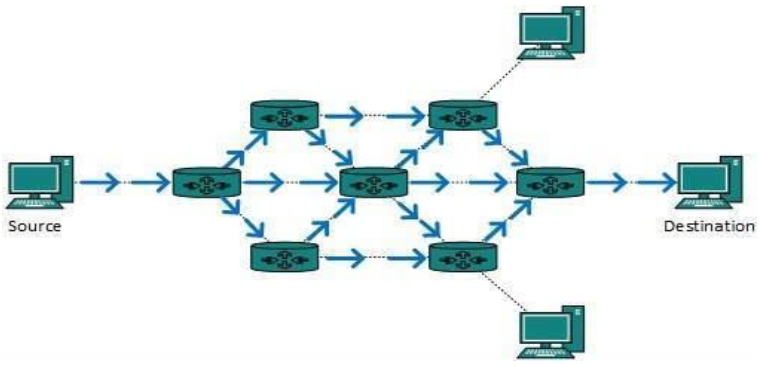
Ans :

Broadcast routing

By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

Broadcast routing can be done in two ways (algorithm):

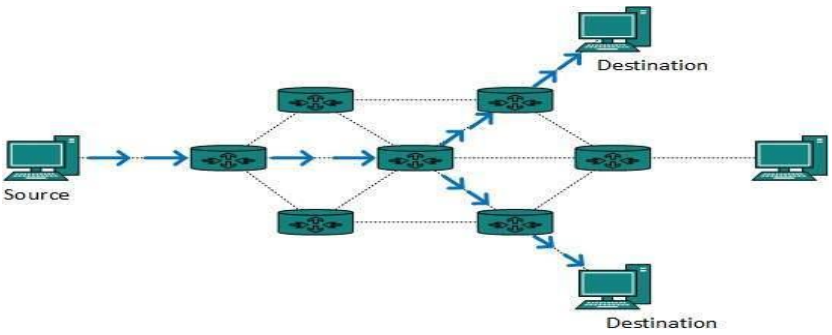
A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses. All packets are sent as unicast but because they are sent to all, it simulates as if router is broadcasting.This method consumes lots of bandwidth and router must destination address of each node.



This method is easy on router's CPU but may cause the problem of duplicate packets received from peer routers.

Multicast Routing

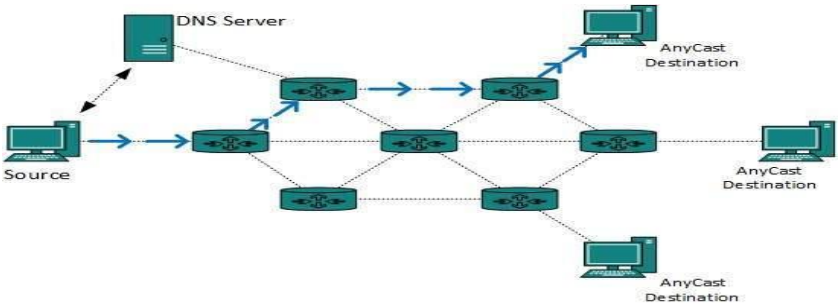
Multicast routing is special case of broadcast routing with significance difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets.



The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing works spanning tree protocol to avoid looping.

Anycast Routing

Anycast packet forwarding is a mechanism where multiple hosts can have same logical address. When a packet destined to this logical address is received, it is sent to the host which is nearest in routing topology.



Anycast routing is done with help of DNS server. Whenever an Anycast packet is received it is enquired with DNS to where to send it. DNS provides the IP address which is the nearest IP configured on it.

b) Write the functions of Transport layer. 7

Ans:

Specific functions of the transport layer are as follows:

1. Service-point addressing

- Computers often run many programs at the same time. Due to this, source-to-destination delivery means delivery from a specific job (currently running program) on one computer to a specific job (currently running program) on the other system not only one computer to the next.
- For this reason, the transport layer added a specific type of address to its header, it is referred to as a service point address or port address.
- By this address each packet reaches the correct computer and also the transport layer gets the complete message to the correct process on that computer.

2. Segmentation and Reassembly

- In segmentation, a message is divided into transmittable segments; each segment containing a sequence number. This number enables this layer to reassemble the message.
- Upon arriving at its destination system message is reassembled correctly, identify and replaces packets that were lost in transmission.

3. Connection Control

It can be either of two types:

i. Connectionless Transport Layer
ii. Connection Oriented Transport Layer

i) Connectionless Transport Layer

- This Transport Layer treats each packet as an individual and delivers it to the destination machine.
- In this type of transmission, the receiver does not send an acknowledgment to the sender about the receipt of a packet. This is a faster communication technique.

ii) Connection Oriented Transport Layer

- This Transport Layer creates a connection with the Transport Layer at the destination machine before transmitting the packets to the destination.
- To Create a connection following three steps are possible:
    - Connection establishment
    - Data transfer
    - Connection termination

When all the data are transmitted connection is terminated. Connectionless Service is less reliable than connection Oriented Service.

4. Multiplexing and Demultiplexing

- Multiple packets from diverse applications are transmitted across a network needs very dedicated control mechanisms, which are found in the transport layer.
- The transport layer accepts packets from different processes. These packets are differentiated by their port numbers and pass them to the network layer after adding proper headers.
- In Demultiplexing, at the receiver's side to obtain the data coming from various processes. It receives the segments of data from the network layer and delivers it to the appropriate process running on the receiver's machine.

5. Flow control

- The transport layer also responsible for the flow control mechanism between the adjacent layers of the TCP/IP model.
- It does not perform across a single link even it performs an end-to-end node.
- By imposing flow control techniques data loss can be prevented from the cause of the sender and slow receiver.

- For instance, it uses the method of sliding window protocol in this method receiver sends a window back to the sender to inform the size of the data is received.

6. Error Control

- Error Control is also performed end to end like the data link layer.
- In this layer to ensure that the entire message arrives at the receiving transport layer without any error(damage, loss or duplication). Error Correction is achieved through retransmission of the packet.
- The data has arrived or not and checks for the integrity of data, it uses the ACK and NACK services to inform the sender.

8. a) Describe internet control message protocol briefly. 5

Ans:

ICMP (Internet Control Message Protocol) is an error-reporting protocol network devices like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets. ICMP creates and sends messages to the source IP address indicating that a gateway to the Internet that a router, service or host cannot be reached for packet delivery. Any IP network device has the capability to send, receive or process ICMP messages. ICMP is not a transport protocol that sends data between systems. While ICMP is not used regularly in end-user applications, it is used by network administrators to troubleshoot Internet connections in diagnostic utilities including ping and traceroute.

One of the main protocols of the Internet Protocol suite, ICMP is used by routers, intermediary devices or hosts to communicate error information or updates to other routers, intermediary devices or hosts. The widely used IPv4 (Internet Protocol version 4) and the newer IPv6 use similar versions of the ICMP protocol (ICMPv4 and ICMPv6, respectively).ICMP messages are transmitted as datagrams and consist of an IP header that encapsulates the ICMP data. ICMP packets are IP packets with ICMP in the IP data portion. ICMP messages also contain the entire IP header from the original message, so the end system knows which packet failedThe ICMP header appears after the IPv4 or IPv6 packet header and is identified as IP protocol number 1. The complex protocol contains three fields:

- The major type that identifies the ICMP message;
- The minor code that contains more information about the type field; and

- The checksum that helps detect errors introduced during transmission.

Following the three fields is the ICMP data and the original IP header to identify which packets actually failed.

b) Explain the Remote procedure call. 4

Ans:

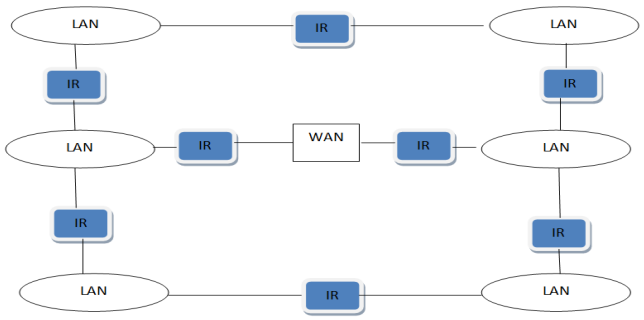
This is a mechanism where one process interacts with another by means of procedure calls. One process (client) calls the procedure lying on remote host. The process on remote host is said to be Server. Both processes are allocated stubs. This communication happens in the following way:

- The client process calls the client stub. It passes all the parameters pertaining to program local to it.
- All parameters are then packed (marshalled) and a system call is made to send them to other side of the network.
- Kernel sends the data over the network and the other end receives it.
- The remote host passes data to the server stub where it is unmarshalled.
- The parameters are passed to the procedure and the procedure is then executed.
- The result is sent back to the client in the same manner.

c) What is inter network briefly explain about connection oriented and connectionless services 5

Ans:

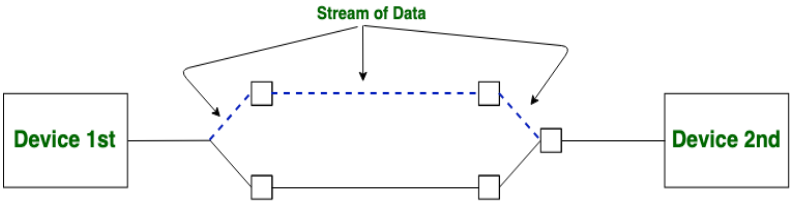
Inter Network or Internet is a combination of two or more networks. Inter network can be formed by joining two or more individual networks by means of various devices such as routers, gateways and bridges



INTERNETWORK

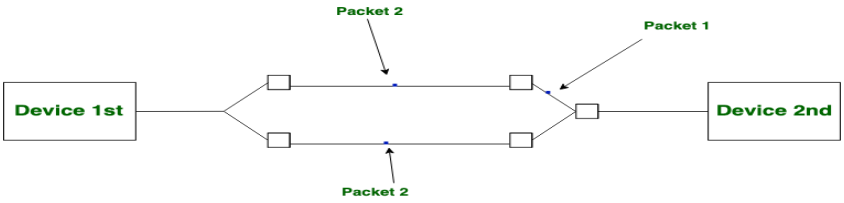
Both Connection-oriented service and Connection-less service are used for the connection establishment between two or more than two devices. These type of services are offered by network layer.

Connection-oriented service is related to the telephone system. It includes the connection establishment and connection termination. In connection-oriented service, Handshake method is used to establish the connection between sender and receiver.



CONNECTION-ORIENTED SERVICE

Connection-less service is related to the postal system. It does not include any connection establishment and connection termination. Connection-less Service does not give the guarantee of reliability. In this, Packets do not follow same path to reach destination.



CONNECTIONIESS SERVICE